

Framework di intelligence digitale: Digital Forensics, OSINT e ADINT nel contesto GDPR Europeo 2024

La Digital Forensics rappresenta oggi il fondamento metodologico per comprendere l'evoluzione dell'intelligence digitale contemporanea. Questo articolo fa parte di una serie di approfondimenti dedicati all'Open Source Intelligence (OSINT) e all'Advertising Intelligence (ADINT), due approcci investigativi che stanno ridefinendo il panorama della sicurezza digitale e della raccolta informativa.

L'analisi esplora come la Digital Forensics fornisca il substrato scientifico necessario per implementare efficacemente sia le tecniche OSINT, basate su fonti pubblicamente accessibili, sia le metodologie ADINT, che sfruttano l'ecosistema pubblicitario digitale per scopi investigativi. Particolare attenzione viene dedicata al contesto normativo europeo, con focus su GDPR e AI Act, e all'integrazione dell'intelligenza artificiale nei processi forensi.

Digital Forensics e l'ecosistema della sorveglianza digitale

La Digital Forensics, nel panorama investigativo odierno, fornisce gli strumenti e le metodologie necessarie per l'identificazione, la raccolta, l'acquisizione, la conservazione delle prove in forma digitale[1], l'analisi e la presentazione delle prove digitali in modo scientificamente valido e legalmente ammissibile.

L'evoluzione della Digital Forensics

L'evoluzione della Digital Forensics riflette la trasformazione del panorama tecnologico e, come mostrato dallo studio condotto da Vasilaras et al. (2024), l'integrazione dell'IA ha portato ad un salto qualitativo nelle capacità investigative. Questa ricerca, basata su un'indagine condotta presso 48 istituti forensi e agenzie di "*law enforcement*", rivela che il 77% delle organizzazioni utilizza già capacità di AI nei loro software forensi, in particolar modo per la classificazione di immagini e video.

Questa evoluzione si manifesta in tre dimensioni principali:

1. Capacità tecniche: l'introduzione di algoritmi di Machine Learning ha potenziato notevolmente la capacità di analizzare grandi volumi di dati digitali. Come evidenzia Suryal (2024), i moderni strumenti forensi possono processare e categorizzare automaticamente enormi quantità di metadati, facilitando in questo modo l'identificazione di pattern e connessioni rilevanti per le indagini;
2. Metodologie operative: le procedure forensi si sono evolute per incorporare le nuove capacità tecnologiche mantenendo al contempo la necessaria rigidità scientifica. Questo ha portato allo sviluppo di protocolli standardizzati per l'acquisizione e l'analisi delle prove digitali;
3. Framework legali: il quadro normativo, in particolar modo nell'Unione Europea, si è adattato per affrontare le sfide poste dalle nuove tecnologie. Il GDPR e l'AI Act forniscono linee guida specifiche per il trattamento dei dati personali e l'utilizzo dell'AI nel contesto forense.

Framework OSINT e ADINT: metodologie operative per

l'acquisizione di prove digitali

La Digital Forensics fornisce il substrato metodologico per entrambe le tecniche investigative principali discusse in questa tesi. Per l'OSINT, fornisce gli strumenti necessari per l'acquisizione e l'analisi scientifica delle fonti aperte, mentre per l'ADINT supporta l'analisi dei dati pubblicitari e delle tracce digitali lasciate dagli utenti.

Vasilaras et al. (2024) identificano tre aspetti fondamentali in questa integrazione:

1. Trasparenza: i sistemi forensi devono essere trasparenti nel loro funzionamento, permettendo di comprendere come vengono generate le prove digitali. Questo è particolarmente importante negli Stati membri dell'UE, dove l'AI Act richiede che i sistemi automatizzati siano spiegabili;
2. Interpretabilità: i risultati delle analisi forensi devono essere interpretabili non solo dagli esperti tecnici ma anche dagli operatori del diritto. Questo requisito assume particolare rilevanza quando si utilizzano tecniche avanzate di IA;
3. Robustezza: le metodologie forensi devono essere sufficientemente robuste da resistere al controllo giuridico e scientifico. La loro affidabilità deve essere dimostrabile in modo oggettivo.

La standardizzazione delle procedure

Un aspetto critico emerso dalla ricerca di Vasilaras et al. (ibidem) è l'assenza di procedure standardizzate per l'utilizzo dell'IA nelle investigazioni forensi digitali. Questo rappresenta una sfida particolare nel contesto europeo, dove il quadro normativo richiede un alto livello di trasparenza e *accountability*.

Per rispondere a questa sfida, gli autori suggeriscono un *framework* di governance strutturato, che integra diversi

elementi chiave per garantire la conformità normativa e l'affidabilità delle analisi forensi. Uno degli aspetti centrali del *framework* è l'adozione di protocolli standardizzati per l'acquisizione delle prove digitali, assicurando che la raccolta e la conservazione delle informazioni seguano criteri uniformi, tali da preservarne l'integrità e l'ammissibilità in contesti giudiziari.

Inoltre, viene enfatizzata l'importanza di procedure di validazione rigorose per gli algoritmi di intelligenza artificiale utilizzati nelle indagini, al fine di garantire trasparenza, spiegabilità e assenza di bias nei processi decisionali automatizzati. Un ulteriore pilastro del *framework* è rappresentato dai meccanismi di audit, progettati per monitorare e verificare costantemente la conformità ai requisiti normativi, riducendo il rischio di violazioni e garantendo una maggiore accountability nelle pratiche di digital forensics. Infine, il *framework* prevede l'implementazione di linee guida dettagliate per la documentazione delle analisi forensi, assicurando la tracciabilità e la riproducibilità delle indagini, elementi essenziali per la validazione delle prove e la credibilità del lavoro investigativo.

Le sfide future

La Digital Forensics si trova ad affrontare una serie di sfide complesse e in continua evoluzione, che risultano particolarmente rilevanti nel contesto dell'OSINT (Open Source Intelligence) e dell'ADINT (Advertising Intelligence). L'analisi forense digitale, che si occupa della raccolta, conservazione e interpretazione di prove digitali, deve adattarsi a un panorama tecnologico in rapido cambiamento, garantendo al contempo il rispetto delle normative sulla privacy e l'affidabilità delle informazioni raccolte.

Tra le principali sfide che emergono, la prima riguarda l'evoluzione tecnologica e il rapido sviluppo delle tecnologie

digitali, che impongono un aggiornamento costante delle metodologie e degli strumenti utilizzati nella Digital Forensics. L'adozione di reti decentralizzate, il crescente utilizzo di sistemi di crittografia avanzati e la diffusione di dispositivi IoT rendono sempre più complesso l'accesso e l'analisi delle informazioni. Inoltre, le nuove piattaforme basate su blockchain e tecniche di anonimizzazione pongono ostacoli significativi alla tracciabilità delle attività online, richiedendo lo sviluppo di strumenti più elaborati.

Un altro aspetto cruciale è il bilanciamento tra efficacia investigativa e protezione della privacy. L'attuale quadro normativo, con regolamenti stringenti come il GDPR, impone restrizioni sulla raccolta e sull'uso dei dati personali, limitando l'accesso a determinate fonti di informazione. Un esempio di questo conflitto riguarda l'analisi OSINT dove, pur basandosi su dati pubblicamente accessibili, il loro utilizzo può comunque sollevare questioni etiche e legali, specialmente quando si tratta di profilazione avanzata o di attacchi che permettono l'estrapolazione di informazioni sensibili da dati apparentemente innocui.

Un ulteriore sfida riguarda la standardizzazione delle procedure e delle metodologie forensi, visto che la grande varietà di tecnologie, formati di dati e piattaforme digitali rende difficile la creazione di un protocollo unico e universalmente accettato per la raccolta e l'analisi delle prove digitali. I software e le tecniche di analisi utilizzati nelle indagini variano notevolmente a seconda della giurisdizione e dell'ambito operativo, generando problemi di interoperabilità tra diversi sistemi. La mancanza di standard uniformi può influenzare l'affidabilità delle indagini e la capacità di condividere informazioni tra diverse agenzie investigative.

Infine, l'ammissibilità legale delle prove digitali rappresenta un ostacolo sempre più complesso. Difatti, per essere utilizzabili in tribunale le prove digitali devono

soddisfare rigorosi requisiti di autenticità, integrità e tracciabilità. Ogni fase della raccolta e dell'analisi deve essere documentata per garantire la catena di custodia, evitando contestazioni sulla validità delle prove. Inoltre, l'uso crescente di intelligenza artificiale e machine learning nelle indagini forensi introduce nuove sfide legate alla trasparenza degli algoritmi e alla spiegabilità dei risultati. La giurisprudenza sta ancora cercando di adattarsi a queste innovazioni, con differenze significative tra le normative adottate nei vari paesi.

Oltre a queste quattro sfide principali, emergono ulteriori problematiche legate alla sovrabbondanza di dati disponibili per l'analisi forense e al rischio di manipolazione delle informazioni digitali. L'aumento delle tecniche di *deepfake* e di alterazione forense dei dati rende più difficile distinguere tra contenuti autentici e manipolati, aumentando la necessità di strumenti di verifica avanzati.

Per affrontare queste sfide, è fondamentale investire in formazione specialistica, sviluppo di strumenti forensi avanzati e creazione di normative più flessibili ma efficaci, che consentano agli investigatori digitali di operare in modo efficiente senza compromettere i diritti fondamentali dei cittadini. Il futuro della Digital Forensics dipenderà dalla capacità di adattarsi a un ecosistema digitale in continua trasformazione, mantenendo un equilibrio tra innovazione tecnologica e tutela della giustizia.

OSINT: generalità ed evoluzione

L'Open Source Intelligence (OSINT) rappresenta uno dei pilastri fondamentali dell'intelligence digitale contemporanea. Da strumento tradizionalmente utilizzato in ambito militare e governativo, l'OSINT si è evoluto fino a diventare un metodo sofisticato per la raccolta e analisi di informazioni da fonti pubblicamente accessibili, con

particolare rilevanza nel contesto dei social media e delle piattaforme digitali.

Fonte: Bederov, I. (2024) "How to track a person using open data?"

Evoluzione storica e definizione

L'OSINT ha origini che precedono l'era digitale, essendo stata inizialmente sviluppata come metodologia per l'analisi di fonti informative pubbliche durante la Seconda Guerra Mondiale. Con l'avvento di Internet e dei social media, ha subito un cambiamento profondo, ampliando le sue metodologie e potenzialità. Suryal (2024) evidenzia come la crescente disponibilità di dati digitali abbia introdotto una rivoluzione nell'OSINT, migliorando l'accesso a fonti di dati e tecniche di analisi.

Hayes e Cappa (2018) sottolineano l'importanza dell'OSINT per migliorare la sicurezza aziendale e nazionale, dimostrando come questa metodologia permetta di identificare vulnerabilità tecniche e umane nelle infrastrutture critiche e nel personale chiave. Inoltre, Yadav et al. (2023) illustrano il ruolo crescente dell'intelligenza artificiale e del machine learning nell'OSINT, che permette un'analisi più approfondita dei dati e l'implementazione di modelli autonomi per la gestione delle minacce.

Nel contesto contemporaneo, l'OSINT si distingue per la sua dipendenza da fonti pubblicamente accessibili, una caratteristica che comporta significative implicazioni legali ed etiche, particolarmente nel contesto europeo regolato dal GDPR.

Metodologie e strumenti

L'OSINT moderna utilizza una varietà di strumenti per la raccolta e l'analisi dei dati. Suryal (2024) identifica sei categorie principali di metadati utili per le investigazioni

OSINT:

1. *EXIF data*: informazioni tecniche e contestuali sulle immagini;
2. *Geotags*: per tracciare dimensioni geografiche delle informazioni;
3. *Timestamps*: per ricostruire eventi temporali;
4. *User metadata*: dettagli sui comportamenti degli utenti;
5. *File properties*: dati tecnici sui file digitali;
6. *Social graph data*: relazioni tra utenti e contenuti.

Hayes e Cappa (2023) integrano questa visione analizzando il modo in cui strumenti come “Maltego” e “FOCA” possano mappare connessioni e individuare metadati nascosti, migliorando l'efficacia delle analisi. Parallelamente, Yadav et al. (2018) descrivono l'uso di algoritmi di deep learning per rilevare schemi nei dati, migliorando la capacità predittiva delle applicazioni OSINT, soprattutto nel campo della sicurezza informatica.

Il ruolo dei social media

I social media hanno trasformato l'OSINT in una risorsa chiave per investigazioni e analisi di rischio. Le piattaforme social forniscono un ricco tessuto informativo che, se analizzato correttamente, può rivelare dettagli significativi su individui, organizzazioni ed eventi. Come evidenziato da Suryal (2024), l'analisi delle fonti aperte deve bilanciare efficacia investigativa e rispetto della privacy. Nella ricerca svolta da Hayes e Cappa (2018), si dimostra che le reti sociali rappresentano sia un'opportunità per il monitoraggio di minacce sia un rischio, visto che offrono dati che possono essere sfruttati per l'ingegneria sociale.

Sfide tecniche e metodologiche

Le sfide principali dell'OSINT comprendono la gestione dei dati, la verifica delle informazioni e l'integrazione di fonti eterogenee. Per affrontarle sono emersi strumenti avanzati

spesso supportati da tecnologie di IA, in grado di migliorare sia la velocità sia la precisione delle analisi. Nella ricerca svolta da Hayes e Cappa (2018) si illustra, ad esempio, come la classificazione del rischio dei dipendenti possa orientare le risorse aziendali verso una maggiore sicurezza.

Prospettive future

Il futuro dell'OSINT sarà sempre più influenzato dall'evoluzione tecnologica e dalla regolamentazione normativa. L'integrazione con l'intelligenza artificiale e il machine learning offre un potenziale significativo per la personalizzazione delle analisi e l'automazione dei processi, come dimostrato da Yadav et al. (2023). Tuttavia, è importante affrontare le varie questioni etiche e normative, soprattutto nel contesto europeo, dove la protezione dei dati rappresenta una priorità fondamentale.

ADINT: generalità ed evoluzione

L'Advertising Intelligence (ADINT) rappresenta una delle innovazioni più significative e potenzialmente dirompenti nel panorama dell'intelligence digitale contemporanea. Come dimostrato da Vines, Roesner e Kohno (2017) nella loro ricerca, l'infrastruttura pubblicitaria digitale può essere utilizzata per mettere in atto forme sofisticate di sorveglianza con risorse relativamente limitate.

Il funzionamento dell'ADINT

L'ADINT sfrutta in modo innovativo l'ecosistema pubblicitario esistente. Gli autori della ricerca hanno dimostrato come, con un budget di soli mille dollari, sia possibile:

1. Tracciare la posizione degli individui con una precisione di 8 metri attraverso il targeting pubblicitario cosiddetto "iperlocale". Questo termine viene usato per riferirsi ad una forma molto precisa di

pubblicità basata sulla localizzazione, che permette agli inserzionisti di targetizzare gli utenti in aree geografiche molto ristrette. In particolar modo, il *targeting* iperlocale consente di indirizzare le pubblicità agli utenti basandosi sulle loro coordinate GPS esatte con un livello di granularità molto fine (fino a circa 4-11 metri di risoluzione) e di definire aree target circolari con raggi minimi di 1 metro intorno a coordinate GPS specifiche. In questo modo è in grado di mostrare annunci solo agli utenti all'interno di quelle precise aree geografiche;

2. Inferire informazioni sensibili sull'utilizzo di determinate applicazioni, incluse app per dating, religiose o mediche (dunque i cosiddetti "dati ad alto rischio", cioè quei dati che, se pubblicati e scoperti da un attore malevolo, porterebbero potenzialmente a danni importanti a quella determinata persona, come ad esempio frodi e il furto d'identità);
3. Monitorare gli spostamenti quotidiani tra casa e lavoro;
4. Determinare il numero di dispositivi presenti in una determinata località;
5. Identificare le connessioni sociali tra utenti basandosi sui pattern di co-localizzazione (ciò può essere usato per monitorare raduni o eventi).

Questo funzionamento si basa su un meccanismo relativamente semplice ma molto efficace: l'acquisto mirato di spazi pubblicitari per i dispositivi mobili permette di verificare se un particolare utente visualizza l'annuncio in una specifica posizione o mentre utilizza determinate applicazioni.

L'ecosistema pubblicitario dei dispositivi mobili (Mobile Advertising) nel contesto europeo

La ricerca mostra come diverse piattaforme pubblicitarie per i dispositivi mobili forniscano agli inserzionisti informazioni molto dettagliate. Un caso particolare è "MoPub", che

condivide sia l'identificatore del dispositivo (GAID o hash dell'Android ID) che la localizzazione precisa, permettendo potenzialmente la ricostruzione dei percorsi degli utenti.

Nell'Unione Europea questa pratica solleva rilevanti questioni di conformità al GDPR, toccando diversi principi fondamentali della protezione dei dati personali. Uno degli aspetti più critici riguarda il requisito del consenso informato, indispensabile per il trattamento dei dati di localizzazione, che deve essere esplicito, libero e revocabile in qualsiasi momento.

Parallelamente, il trattamento di tali informazioni deve basarsi su una base giuridica legittima, che giustifichi la raccolta e l'analisi dei dati personali, garantendo il rispetto delle normative vigenti. Un ulteriore elemento essenziale è rappresentato dall'obbligo di trasparenza, che impone ai soggetti responsabili del trattamento di chiarire in modo dettagliato le finalità per cui i dati vengono raccolti e utilizzati, evitando ambiguità o usi impropri.

Infine, si applica il principio di minimizzazione dei dati, che richiede di limitare la raccolta esclusivamente alle informazioni strettamente necessarie per gli scopi dichiarati, evitando un accumulo eccessivo o non giustificato di dati sensibili. Questi aspetti rendono il trattamento dei dati di localizzazione una questione complessa, che richiede un equilibrio tra necessità operative e rispetto della privacy individuale.

Implicazioni privacy e vulnerabilità

L'Advertising Intelligence solleva preoccupazioni significative per quanto riguarda la privacy degli utenti. Come dimostrato da Goldfarb e Que (2023) nella loro ricerca, il valore crescente dei dati digitali ha creato forti incentivi economici per lo sviluppo di tecniche sempre più sofisticate di tracciamento e profilazione.

Contromisure e mitigazioni

La ricerca propone diverse strategie per mitigare i rischi associati all'Advertising Intelligence (ADINT) e garantire una maggiore tutela degli utenti. Una delle soluzioni proposte consiste nell'introduzione di limitazioni tecniche, che impongano restrizioni sulla precisione dei dati di localizzazione condivisi con gli inserzionisti, riducendo così il rischio di tracciamento invasivo e di profilazione dettagliata. Un altro approccio riguarda l'inasprimento dei controlli normativi, con una regolamentazione più rigorosa sull'utilizzo dei dati pubblicitari per scopi di sorveglianza, impedendo che informazioni destinate a fini commerciali vengano sfruttate per attività di monitoraggio non autorizzate.

A questo si affianca la necessità di una maggiore trasparenza, che garantisca agli utenti una chiara comprensione di come i loro dati vengano raccolti, trattati e utilizzati nel sistema pubblicitario, dando loro la possibilità di esercitare un controllo più efficace sulle proprie informazioni personali. Per concludere, un ulteriore aspetto cruciale è l'implementazione del principio di *privacy by design*, che prevede lo sviluppo di sistemi pubblicitari in cui la protezione della privacy sia integrata fin dalle fasi iniziali della progettazione. Questo implica l'adozione di meccanismi che minimizzino la raccolta dei dati, limitino la conservazione delle informazioni personali e offrano agli utenti strumenti per gestire in modo semplice e consapevole il proprio livello di esposizione ai meccanismi di tracciamento pubblicitario.

Prospettive future

Il futuro dell'Advertising Intelligence sarà probabilmente caratterizzato da uno scontro continuo tra le crescenti capacità tecniche e le esigenze di protezione della privacy. Inoltre, l'integrazione dell'IA potrebbe rendere ancora più

elaborate le capacità di inferenza e tracciamento.

Nel contesto europeo, con l'AI Act ci saranno ulteriori requisiti per i sistemi automatizzati utilizzati nella pubblicità, potenzialmente limitando alcune delle capacità dell'ADINT. Tuttavia, come evidenziano Vines et al. (2017), la natura essenzialmente aperta dell'ecosistema pubblicitario rende piuttosto difficile prevenire del tutto queste tipologie di sorveglianza.

Differenze e similitudini tra i due approcci

L'analisi comparativa tra OSINT e ADINT rivela un quadro complesso di convergenze e divergenze metodologiche che merita un'attenta considerazione. Questa comparazione risulta particolarmente significativa nel contesto europeo, dove il quadro normativo impone vincoli specifici ad entrambe le metodologie.

Fondamenti metodologici

La principale differenza tra OSINT e ADINT riguarda le rispettive metodologie. L'OSINT si basa sull'analisi sistematica di fonti pubblicamente accessibili, seguendo una tradizione consolidata di intelligence. Come evidenzia Surya (2024), questa metodologia si è evoluta per incorporare le nuove fonti di dati digitali, mantenendo però il suo focus sulla raccolta e analisi di informazioni pubblicamente disponibili.

L'ADINT, al contrario, rappresenta un approccio innovativo che, come dimostrato da Vines et al. (2017), sfrutta in modo creativo l'infrastruttura pubblicitaria digitale per i dispositivi mobili esistente per ottenere informazioni che normalmente non sarebbero accessibili attraverso fonti aperte. Questa differenza fondamentale ha importanti implicazioni sia

tecniche che etiche.

Acquisizione delle informazioni

Le modalità di acquisizione delle informazioni differiscono significativamente tra i due approcci. L'OSINT si basa su fonti pubblicamente accessibili, usa strumenti appositamente creati per l'aggregazione dei dati, e le competenze richieste variano da ciò che si desidera fare. Ad esempio, per fare una ricerca su dove è maggiormente diffuso un determinato argomento su X (ex Twitter) basteranno competenze minime, mentre per combinare i dati delle immagini satellitari presenti su Google Maps e quelle presenti su X per analizzare un determinato conflitto si avrà bisogno di competenze avanzate.

Per quanto riguarda l'ADINT, essa sfrutta in maniera attiva l'infrastruttura pubblicitaria digitale, e richiede un certo investimento economico (anche se, come dimostrato in precedenza, sono sufficienti risorse economiche limitate). L'Advertising Intelligence opera attraverso l'acquisto di spazi pubblicitari per i dispositivi mobili, e dunque sfrutta gli strumenti standard del c.d. *"digital advertising"*.

Implicazioni legali nel contesto europeo

Nel contesto normativo europeo, sia l'Open Source Intelligence (OSINT) che l'Advertising Intelligence (ADINT) devono operare nel rispetto del Regolamento Generale sulla Protezione dei Dati (GDPR) e dell'AI Act, affrontando tuttavia sfide specifiche legate alla natura stessa dei dati trattati e alle modalità di raccolta e analisi delle informazioni.

L'OSINT, essendo basato sulla raccolta e l'analisi di dati provenienti da fonti pubbliche, si trova a dover gestire questioni legali complesse legate alla legittimità dell'aggregazione delle informazioni disponibili online. Nonostante molte delle fonti siano pubbliche per definizione, la loro raccolta e aggregazione su larga scala potrebbe

entrare in conflitto con i principi di minimizzazione dei dati e finalità del trattamento previsti dal GDPR. Un'altra problematica riguarda i limiti del riutilizzo delle informazioni, poiché i dati originariamente resi pubblici per uno scopo specifico non possono sempre essere riutilizzati liberamente per finalità investigative o di profilazione.

Un ulteriore requisito fondamentale per l'OSINT è la documentazione della provenienza dei dati, che garantisce non solamente la trasparenza del processo di raccolta, ma è fondamentale per dimostrare la validità e l'affidabilità delle informazioni, soprattutto in contesti giudiziari o investigativi.

L'ADINT, invece, essendo direttamente coinvolto nella raccolta di dati a fini commerciali e pubblicitari, deve affrontare restrizioni ancora più stringenti. Il consenso informato degli utenti è un requisito essenziale, e secondo il GDPR deve essere esplicito, libero e revocabile in qualsiasi momento. La sfida principale per le aziende che utilizzano ADINT è quindi quella di garantire trasparenza nelle finalità del trattamento, evitando pratiche opache o ambigue nella gestione dei dati.

Questo implica la necessità di informare chiaramente gli utenti su come i loro dati verranno utilizzati, evitando formulazioni vaghe o generiche. Inoltre, il principio della minimizzazione dei dati raccolti impone alle aziende di raccogliere solo le informazioni strettamente necessarie per lo scopo dichiarato, evitando di accumulare grandi volumi di dati senza una giustificazione adeguata. Infine, la limitazione delle finalità richiede che i dati acquisiti per una determinata attività non possano essere riutilizzati per scopi diversi senza un nuovo consenso, rendendo più complesso l'uso secondario delle informazioni all'interno delle strategie di marketing e pubblicità.

In sintesi, sia per l'OSINT che per l'ADINT l'ambiente

normativo è sempre più complesso, dato che la necessità di accesso ai dati si scontra con le rigorose tutele imposte per la protezione della privacy. Per entrambe le metodologie l'adozione di strategie conformi ai principi di *accountability*, trasparenza e protezione dei dati diventerà cruciale per operare in modo efficace senza incorrere in violazioni regolamentari.

Capacità investigative e integrazione futura di OSINT e ADINT

Le capacità investigative di OSINT e ADINT rappresentano approcci complementari ma distinti per quanto riguarda la raccolta di informazioni. L'OSINT dimostra particolare efficacia nell'analisi delle reti sociali, nella ricostruzione di eventi pubblici, nella verifica delle informazioni dichiarate e nell'identificazione di pattern e tendenze sociali più ampie. Per contro, l'ADINT eccelle nel tracciamento preciso delle localizzazioni, nell'inferenza di comportamenti privati, nell'analisi dei pattern di movimento e nella valutazione dei comportamenti di gruppo.

Per quanto riguarda l'integrazione dell'IA, Vasilaras et al. (2024) evidenziano come ciascun approccio affronti sfide specifiche. L'Open Source Intelligence richiede algoritmi sofisticati capaci di processare e analizzare grandi volumi di dati mantenendo accuratezza contestuale e trasparenza analitica. L'Advertising Intelligence, d'altra parte, si concentra sullo sviluppo di algoritmi predittivi per il targeting, affrontando al contempo le sfide della c.d. "*privacy preserving computation*" (cioè un sistema in cui l'output non contiene dati identificabili oltre a ciò che è stato dato dall'utente nell'input) e della spiegabilità delle decisioni.

L'evoluzione futura di entrambi gli approcci è condizionata da fattori distinti ma interconnessi, visto che la traiettoria di sviluppo dell'OSINT è influenzata dalla crescente disponibilità di dati pubblici e dall'evoluzione delle piattaforme social, mentre il futuro dell'ADINT è legato ai cambiamenti nell'ecosistema pubblicitario e ai progressi nelle tecnologie di *targeting*. Entrambi devono adattarsi a un panorama normativo in evoluzione, particolarmente all'interno del robusto quadro sulla privacy dell'Unione Europea.

Dal punto di vista etico, entrambi gli approcci condividono preoccupazioni comuni riguardo al bilanciamento tra efficacia investigativa e protezione della privacy, nonché al potenziale impatto sui diritti fondamentali. Tuttavia, differiscono significativamente nel loro contesto operativo: l'OSINT lavora con informazioni pubblicate volontariamente, mentre l'ADINT opera spesso attraverso meccanismi che gli utenti potrebbero non comprendere pienamente e con autorizzazioni che l'utente potrebbe concedere senza volerlo.

L'integrazione potenziale tra OSINT e ADINT, come suggerito dallo studio svolto da Goldfarb e Que (2023), offre prospettive promettenti per capacità investigative avanzate, ma richiede particolare attenzione agli aspetti etici e legali, specialmente nel contesto europeo. La sfida principale consiste nello sviluppare *framework* di integrazione che rispettino i principi del GDPR, mantengano la trasparenza delle procedure e garantiscano sia l'interpretabilità dei risultati che la tutela dei diritti fondamentali degli individui.

Questa visione di integrazione deve necessariamente considerare le specificità del contesto europeo, dove la protezione dei diritti fondamentali assume un ruolo pivotale nella regolamentazione delle tecnologie investigative, distinguendosi significativamente dall'approccio normativo statunitense più orientato al mercato.

L'analisi presentata ha evidenziato come Digital Forensics, OSINT e ADINT rappresentino tre pilastri interconnessi dell'intelligence digitale contemporanea, ciascuno con specificità metodologiche e sfide normative distintive nel contesto europeo. L'integrazione dell'intelligenza artificiale ha amplificato le capacità investigative di tutti e tre gli approcci, richiedendo tuttavia framework di governance più sofisticati per garantire conformità al GDPR e all'AI Act.

Nel prossimo articolo approfondiremo gli aspetti tecnici della raccolta e analisi dati per l'approccio OSINT e ADINT, esplorando strumenti, metodologie operative e implementazioni pratiche per professionisti del settore.

Per un ulteriore approfondimento invitiamo a scaricare il white paper di **Sergiu Deaconu, "Open Source Intelligence e Advertising Intelligence: applicazioni e impatti in ambito industriale, civile e dell'intelligence europea"**. Il documento offre un'analisi approfondita su come OSINT e ADINT stiano trasformando il settore dell'intelligence digitale.

Fonti:

[1] Come definito dalla norma ISO 27037 del 2017 (febbraio) corretta il 10 maggio 2022 a pagina 2.

Profilo Autore



Professionista con formazione multidisciplinare in economia, diritto e tecnologia, che unisce solide competenze accademiche a esperienza pratica nello sviluppo software. Attualmente opera come programmatore iOS e sviluppatore software, specializzandosi in Swift, C# e Python per lo sviluppo di applicazioni web e mobile e la progettazione di architetture software avanzate.

Ha conseguito una Laurea magistrale in 'European Economy and Business Law' presso l'Università degli Studi di Roma "Tor Vergata", focalizzandosi su economia digitale e diritto

europeo, e ha completato un Master in 'Informatica giuridica, nuove tecnologie e diritto dell'informatica' presso l'Università "La Sapienza" di Roma. La sua ricerca post-lauream si è concentrata sulle implicazioni di Big Data, IoT e Intelligenza Artificiale in settori strategici quali agricoltura, industria e smart cities, nonché sull'analisi delle tecniche OSINT e ADINT in relazione a privacy e sicurezza nazionale.

Certificato in Project Design & Management a livello europeo e con competenze linguistiche avanzate in inglese (IELTS 7.5), combina capacità analitiche e di leadership con una profonda comprensione dell'intersezione tra tecnologia, diritto ed economia nell'era digitale.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/framework-intelligence/>