FIGHTING CYBERCRIME WITH OSINT (FICO)

VALUTAZIONE DELLA PROTEZIONE DEI DATI NELLA RICERCA UTILIZZANDO LA METODOLOGIA OSINT

Avv. Filippo Bianchini

Perugia, 20 giugno 2023

A.D. 1308
unipg
UNIVERSITÀ DEGLI STUDI
DI PERUGIA

LICENZA D'USO

- Questo materiale è rilasciato sotto licenza:

Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo 3.0 Italia (CC BY-NC-SA 3.0 IT)

- Alcune immagini della presentazione sono citazioni o "fair use" di opere protette da copyright dei legittimi proprietari.

- Tutti i marchi citati appartengono ai legittimi proprietari.

_>WHOIAM

- Avvocato cassazionista, iscritto al Foro di Perugia
- DPO certificato UNI 11697:2017 – Lead Auditor 27001:2012 - CIPP/E
- Membro supplente Autorità Garante per la protezione dei dati personali di San Marino
- Membro del Comitato Direttivo di ASSO DPO
- Membro del Cybersecurity National Lab (nodo UniPG)
- Docente al Master universitario in "Data protection, Cybersecurity e Digital forensics" dell'Università per gli Studi di Perugia

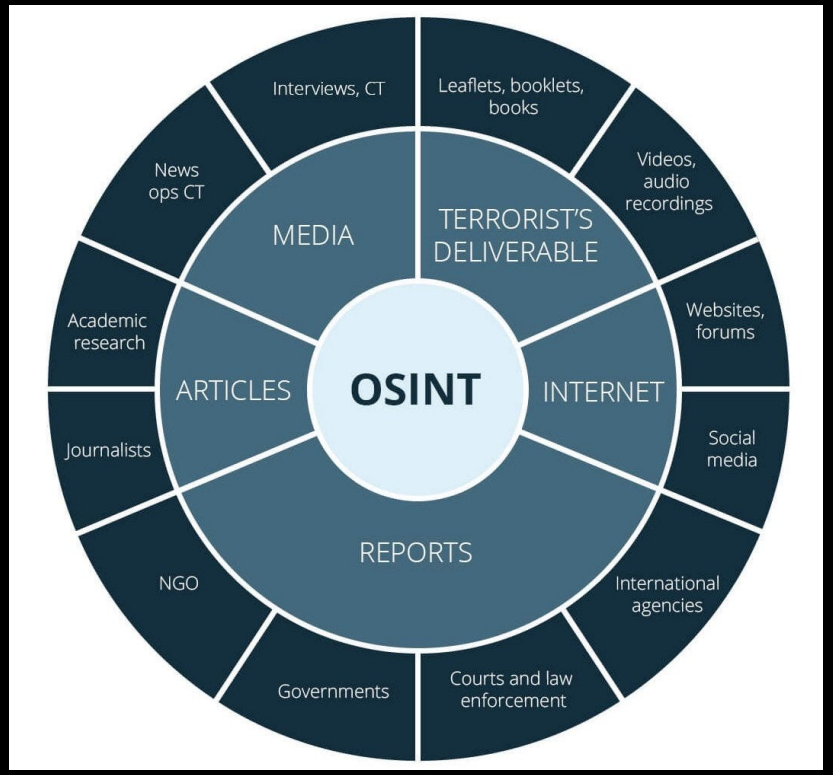
INTRODUZIONE

- **Scopo**: *awareness raising* sugli obblighi relativi alla protezione dei dati personali con specifico riferimento al trattamento dei dati raccolti ed utilizzati nell'ambito del progetto di ricerca scientifica *FIghting Cybercrime with OSINT* - **FICO**.
- L'Open Source Intelligence (OSINT) si riferisce alla **raccolta di informazioni da fonti aperte o pubblicamente disponibili**. La metodologia OSINT si concentra sull'identificazione, la raccolta, la filtrazione, l'analisi e la distribuzione di queste informazioni in modo sicuro ed efficace.
- L'OSINT pone delle sfide per la protezione dei dati personali e l'applicazione della disciplina relativa alla proprietà intellettuale. Una strategia per affrontare queste sfide consiste nell'adattare la progettazione degli strumenti OSINT per **incorporare, *by design* e *by default*, i requisiti normativi**.

COS'È OSINT?

- Tipi e fonti di OSINT:

1. **Internet**
2. **Media**
3. **Public Data**
4. **Academic**
5. **Geospatial**
6. **Business**
7. **IoT → Internet of Human Beings**



METODOLOGIA OSINT

1. **Definizione del problema e identificazione delle necessità informative**: Comprensione di quale sia il problema o la domanda di ricerca, e cosa si spera di ottenere dall'intelligence.
2. **Raccolta di informazioni**: Identificazione e accesso alle fonti aperte per raccogliere le informazioni necessarie. Questo può includere la ricerca su Internet, l'accesso a database pubblici, l'esame dei social media, e altro ancora.
3. **Elaborazione e analisi delle informazioni**: Questo può includere l'analisi dei dati, la valutazione della credibilità e della rilevanza delle informazioni, e l'identificazione di schemi o tendenze. Gli strumenti utilizzati in questa fase possono includere software di analisi dei dati, strumenti di visualizzazione dei dati, e software di analisi del testo.
4. **Produzione e distribuzione dell'intelligence**: Condivisione con coloro che ne hanno bisogno. Questo può includere la creazione di rapporti, la presentazione di briefings, o la condivisione di dati attraverso piattaforme di intelligence.
5. **Valutazione e feedback**: Questa fase finale coinvolge la valutazione della qualità e dell'efficacia dell'intelligence prodotta, e la raccolta di feedback per migliorare i processi futuri. Questo può coinvolgere l'uso di strumenti di valutazione, sondaggi, e sessioni di feedback.

IMPORTANZA DELLA PROTEZIONE DEI DATI

- La protezione dei dati nella ricerca è fondamentale per il rispetto dei diritti individuali alla privacy, per garantire la conformità con le leggi sulla protezione dei dati e per mantenere l'integrità e la validità della ricerca.
- La protezione dei dati inadeguata può avere una serie di conseguenze gravi:

1. **Sanzioni legali**: Le violazioni delle leggi sulla protezione dei dati possono portare a sanzioni legali significative, compresi pesanti ammende e potenziali azioni legali.
2. **Danno alla reputazione**: Una violazione della protezione dei dati può danneggiare seriamente la reputazione di un'organizzazione o di un individuo. Questo può avere un impatto sulla fiducia del pubblico e sulla capacità di condurre ricerche future.
3. **Perdita di dati**: La protezione dei dati inadeguata può portare alla perdita di dati importanti, che possono essere costosi o impossibili da recuperare.
4. **Rischi per la sicurezza**: Se i dati sensibili non sono adeguatamente protetti, possono cadere nelle mani sbagliate, mettendo a rischio la sicurezza delle persone a cui si riferiscono i dati.
5. **Invalidazione della ricerca**: Se i dati non sono gestiti correttamente, i risultati della ricerca possono essere messi in discussione, invalidando potenzialmente l'intera ricerca.

LEGGI E REGOLAMENTI

- Le normative hanno un impatto significativo su come l'OSINT può essere utilizzato nella ricerca:

1. **Raccolta di dati**: Anche se l'OSINT si basa su informazioni pubblicamente disponibili, ciò non significa che tutte le informazioni pubbliche possono essere raccolte senza restrizioni. Ad esempio, il GDPR richiede che la raccolta di dati personali sia limitata allo scopo specifico per cui i dati sono stati raccolti.
2. **Elaborazione dei dati**: Il GDPR e il CCPA stabiliscono regole su come i dati personali possono essere elaborati. Questo include il diritto degli individui di sapere come i loro dati vengono utilizzati e di opporsi a tale uso in certe circostanze.
3. **Conservazione dei dati**: I dati personali non possono essere conservati più a lungo del necessario per lo scopo per cui sono stati raccolti. Questo ha un impatto su come i dati OSINT possono essere archiviati e conservati.
4. **Diritti degli individui**: Il GDPR e il CCPA conferiscono agli individui diritti significativi in relazione ai loro dati personali. Questi diritti devono essere rispettati quando si utilizza l'OSINT nella ricerca.

CONSIDERAZIONI ETICHE

- L'utilizzo della metodologia OSINT nella ricerca comporta una serie di considerazioni etiche importanti:

1. **Rispetto per la privacy**: Anche se l'OSINT si basa su informazioni pubblicamente disponibili, ciò non significa che non vi siano considerazioni sulla privacy. Gli individui potrebbero non essere a conoscenza del fatto che le informazioni che hanno condiviso pubblicamente possono essere raccolte e analizzate.
2. **Consapevolezza del contesto**: Le informazioni raccolte tramite OSINT possono essere estratte dal loro contesto originale, il che può portare a interpretazioni errate. È importante essere consapevoli di questo e fare del proprio meglio per comprendere il contesto in cui le informazioni sono state originalmente condivise.
3. **Responsabilità**: Questo significa evitare di causare danno agli individui o alle organizzazioni a cui si riferiscono le informazioni.
4. **Rispetto per le leggi e le normative**: Come discusso in precedenza, esistono numerose leggi e normative che regolano l'uso dei dati personali. È importante che i ricercatori rispettino queste leggi quando utilizzano l'OSINT.
5. **Trasparenza**: È importante essere trasparenti su come si raccolgono e si utilizzano le informazioni. Questo può includere l'informazione dei partecipanti alla ricerca su come i loro dati saranno utilizzati.

VALUTAZIONE DELLA PROTEZIONE DEI DATI

- Valutare il livello di protezione dei dati nella ricerca utilizzando OSINT richiede un'attenta considerazione di diverse aree chiave. Alcuni possibili indicatori di una buona protezione dei dati:

1. **Conformità normativa**: Il primo indicatore è la conformità con le leggi e i regolamenti sulla protezione dei dati pertinenti, come il GDPR o il CCPA. Questo può includere la revisione delle politiche e delle procedure di gestione dei dati per assicurarsi che siano in linea con le normative vigenti.

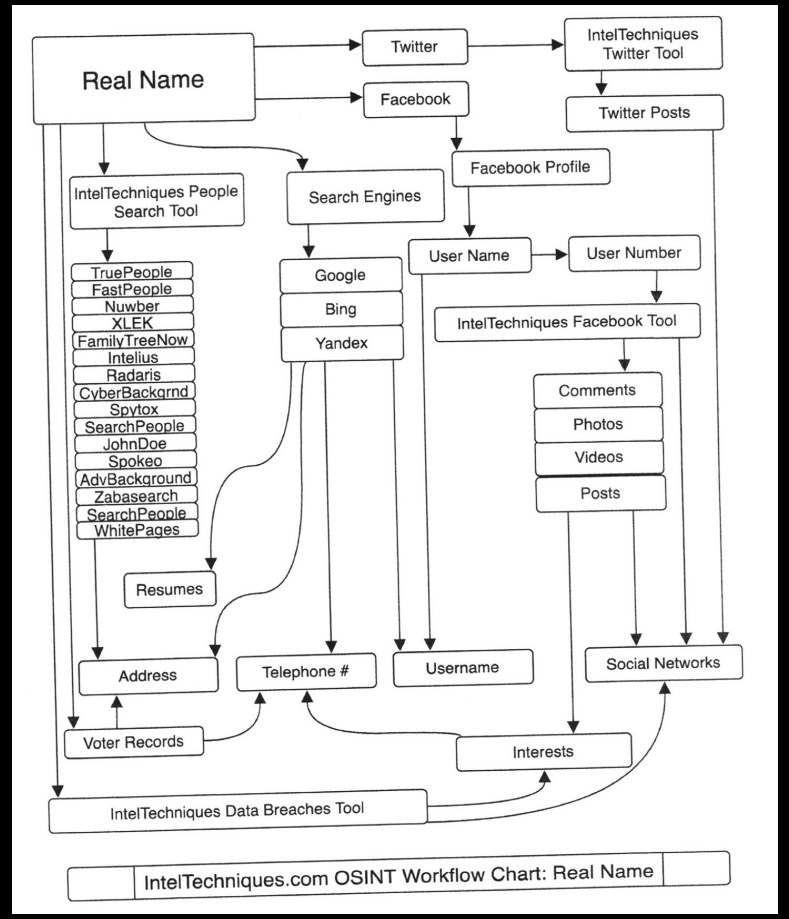
2. **Minimizzazione dei dati**: Un altro indicatore è l'aderenza al principio di minimizzazione dei dati. Questo significa che dovresti raccogliere solo i dati che sono strettamente necessari per la tua ricerca.

3. **Sicurezza**: Le misure di sicurezza dei dati in atto possono servire come un altro indicatore. Questo può includere l'uso di crittografia, la protezione contro l'accesso non autorizzato e le procedure per rispondere alle violazioni dei dati.

4. **Consenso**: Per la ricerca che coinvolge dati personali, le procedure di consenso possono servire come un indicatore della protezione dei dati. Questo può includere la verifica che il consenso sia stato ottenuto in modo appropriato e che i partecipanti siano stati pienamente informati su come i loro dati saranno utilizzati.

5. P**rocessi di revisione etica**: I processi di revisione etica possono fornire un indicatore della protezione dei dati. Questo può includere la revisione da parte di un comitato di etica della ricerca o di una simile entità per assicurarsi che la ricerca rispetti i principi etici, inclusa la protezione dei dati.

- La protezione dei dati non è un obiettivo statico ma un processo continuo.

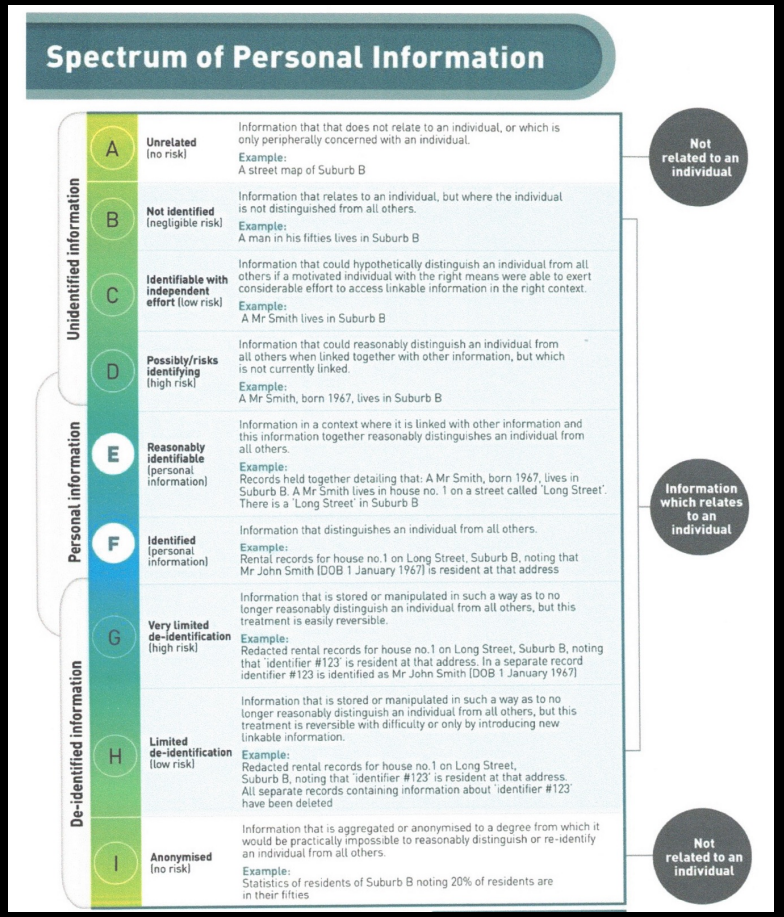


L'immagine è tratta da *OSINT Techniques: Resources for Uncovering Online Information* di Michael Bazzell

MIGLIORI PRATICHE PER LA PROTEZIONE DEI DATI IN OSINT

- Quando si utilizza la metodologia OSINT nella ricerca, è fondamentale proteggere i dati in ogni fase del processo. Ecco alcune raccomandazioni su come farlo:

1. **Raccolta di dati consapevole**: Ciò significa raccogliere solo i dati necessari per la tua ricerca e rispettare i diritti di privacy degli individui.
2. **Gestione sicura dei dati**: Questo può includere l'uso di crittografia per proteggere i dati durante il trasporto e lo stoccaggio, l'uso di password forti, la limitazione dell'accesso ai dati solo a coloro che ne hanno bisogno e la protezione fisica dei dispositivi su cui i dati sono conservati.
3. **Anonimizzazione dei dati**: Se possibile, i dati dovrebbero essere anonimizzati per proteggere l'identità degli individui.
4. **Formazione e sensibilizzazione**: È importante che tutti coloro che lavorano con i dati siano adeguatamente formati sulle migliori pratiche per la protezione dei dati.
5. **Revisione e aggiornamento delle politiche**: Le politiche di gestione dei dati dovrebbero essere regolarmente riviste e aggiornate per assicurarsi che siano adeguate.



LINEE GUIDA PER IL TRATTAMENTO DEI DATI PERSONALI

- **Base giuridica** (liceità) del trattamento dei dati
  - *Il trattamento dei dati personali nell'ambito delle attività di ricerca del progetto FICO è lecito se ed in quanto necessario per lo svolgimento dell'attività di ricerca, così come individuata nel progetto.*
- **Principi e modalità** di trattamento: quali dati bisogna trattare e come bisogna trattarli?
  - *I dati raccolti ed utilizzati per le finalità di ricerca del progetto FICO possono essere trattati solo ed esclusivamente per le attività di ricerca del progetto.*
  - *Il ricercatore che intenda trattare dati personali a fini di ricerca scientifica, non deve verificare e dimostrare che tale finalità è compatibile con quella iniziale (tale compatibilità è presunta dalla legge). Inoltre, nel caso di trattamento per scopi di ricerca scientifica, è prevista una deroga al generale divieto di trattare categorie particolari di dati personali*
  - A) **Misure di sicurezza**:
    - A.1) Tecniche di pseudonimizzazione (per dati comuni) e anonimizzazione (per categorie particolari)
    - A.2) Altre misure di sicurezza: capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
  - B) **Conservazione** dei dati (*i dati raccolti possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente per i medesimi fini di ricerca scientifica*) e **comunicazione** dei dati a partner di ricerca
  - C) Altri adempimenti: **registro** dei trattamenti, **informazioni** da fornire (avviso nel sito), **DPIA**

https://fico.dmi.unipg.it/res/wp4/FICO_linee%20guida%20trattamento%20dati%20personali%20nell'ambito%20della%20ricerca_%20WP4_21%20aprile%202023.pdf

UN CASO SPECIALE: MATERIALE CSAM

1. Non raccoglierlo ← ⚠ artt. 600-*ter* ss. c.p.
2. Notifica al supervisore
3. Riporta l'incidente all'autorità
4. Riporta l'incidente a chi si occupa di persone scomparse
5. Riporta l'incedente alla piattaforma coinvolta
6. Documenta l'incidente
7. Se necessario, chiedi supporto psicologico

CONCLUSIONI

- La protezione dei dati è di fondamentale importanza quando si utilizza la metodologia OSINT nella ricerca. Nonostante l'OSINT riguardi informazioni aperte e pubblicamente disponibili, non dobbiamo dimenticare che tali informazioni possono essere personali e «sensibili», e il loro uso improprio può avere conseguenze significative.
- Quando utilizziamo OSINT nella ricerca, dobbiamo fare tutto il possibile per proteggere i dati che raccogliamo, elaboriamo e conserviamo. Questo include l'adozione di misure di sicurezza dei dati, l'anonimizzazione dei dati quando possibile, la formazione continua e la consapevolezza delle questioni relative alla protezione dei dati, e il rispetto delle leggi e dei regolamenti sulla protezione dei dati.
- Dietro i dati ci sono **persone**, e queste persone hanno il diritto di avere i loro dati protetti. Come ricercatori, esiste il dovere di rispettare questo diritto e di fare tutto il possibile per proteggere i dati che vengono utilizzati.

https://www.assodpo.it

Q&A
Grazie per l'attenzione!

«[…] se non v'è dispiaciuta affatto, vogliatene bene a chi l'ha scritta, e anche un pochino a chi l'ha raccomodata. Ma se in vece fossimo riusciti ad annoiarvi, credete che non s'è fatto apposta.»

Avv. FILIPPO BIANCHINI

Via Bontempi, 1

06122 PERUGIA

Tel: (+39) 075 5723243 – (+39) 349 2864103

E-mail: info@bianchini.legal

LinkedIn: studiolegale

Twitter: @legale