OSINT e ADINT: impatti economici e sociali

OSINT e ADINT rappresentano oggi due delle metodologie più influenti nell'ecosistema dell'intelligence digitale moderna, rivoluzionando il modo in cui vengono raccolte, elaborate e utilizzate le informazioni per scopi di sicurezza, commerciali e di governance.

Quest'ultimo approfondimento si concentra sui meccanismi economici, tecnici e normativi che governano l'utilizzo di queste tecnologie, evidenziando come con investimenti relativamente contenuti sia possibile implementare sistemi di sorveglianza sofisticati capaci di tracciare individui, analizzare comportamenti e inferire informazioni sensibili.

La dimensione economica della privacy e della sorveglianza

L'analisi economica di OSINT e ADINT rivela una complessa interazione tra costi, benefici e dinamiche di mercato. Vines et al. (2017) forniscono un'analisi dettagliata dei costi operativi dell'ADINT, dimostrando come con un investimento di 1000 dollari sia possibile implementare sistemi sofisticati di tracciamento. Il loro studio analizza approfonditamente la struttura dei costi, evidenziando come i costi di implementazione iniziale, quelli operativi continui e quelli relativi all'analisi dei dati si combinino in modo complesso. Particolarmente significativa è la loro scoperta che i costi marginali di tracciamento diminuiscono significativamente all'aumentare del numero di obiettivi, suggerendo importanti economie di scala nelle operazioni di sorveglianza.

Montes et al. (2019) approfondiscono queste implicazioni economiche analizzando le dinamiche di mercato

dell’informazione personale. Il loro modello matematico dimostra come il valore di mercato dei dati personali sia influenzato dalla granularità dell’informazione disponibile, dalla facilità di accesso ai dati attraverso piattaforme pubblicitarie e dall’esistenza di mercati secondari per l’informazione raccolta.

Gli autori dimostrano come queste dinamiche creino un c.d. “effetto moltiplicatore”, dove il valore iniziale dei dati può essere amplificato attraverso analisi successive e combinazioni con altri dataset, portando a implicazioni significative per la privacy degli individui. Questo avviene attraverso mercati secondari che ricombinano dati provenienti da diverse fonti, creando un ecosistema di sorveglianza e analisi sempre più invasivo. Tuttavia, questo effetto amplifica anche i rischi per la privacy, poiché la combinazione di dati apparentemente innocui può portare a una re-identificazione dei soggetti e a nuove forme di profilazione comportamentale.

Un altro elemento chiave è il fenomeno del “*digital privacy paradox*“, descritto da Dirk Bergemann et al. (2022). Questo paradosso si verifica quando gli utenti, nonostante dichiarino di dare un grande valore alla loro privacy, sono disposti a cedere i propri dati per benefici economici o servizi di valore apparentemente marginale, come sconti o accesso a contenuti personalizzati. Questo comportamento, guidato da incentivi economici e dalla mancanza di consapevolezza, alimenta mercati dei dati in cui il prezzo delle informazioni personali è spesso molto inferiore al loro reale valore economico e sociale.

In parallelo, Daron Acemoglu et al. (2022) sottolineano che i mercati dei dati tendono a generare una condivisione eccessiva a causa delle esternalità informative. Quando un individuo condivide i propri dati, produce effetti involontari sui dati altrui, riducendo il valore della privacy degli altri. Questa dinamica porta a una situazione di mercato inefficiente, in

cui il prezzo dei dati è artificialmente basso e le piattaforme acquisiscono una quantità di informazioni superiore a quella socialmente desiderabile.

Meccanismi di raccolta e analisi dei dati

Il framework di privacy differenziale proposto da Dwork et al. (2006) fornisce una base matematica rigorosa per la comprensione dei meccanismi di protezione della privacy. Gli autori introducono il concetto di "budget di privacy" (ε), che quantifica il compromesso tra utilità dei dati e protezione della privacy. Il loro *framework* matematico dimostra come la perdita di privacy sia cumulativa attraverso *query* multiple e come esista un limite fondamentale alla quantità di informazione che può essere estratta mantenendo garanzie di privacy. Questo aspetto risulta particolarmente rilevante nel contesto dell'OSINT e dell'ADINT, dove le interrogazioni multiple dei sistemi pubblicitari possono portare a una progressiva erosione della privacy.

Abowd e Schmutte (2015) applicano questi concetti al contesto pratico della divulgazione statistica, dimostrando come il framework possa essere utilizzato per quantificare il rischio di re-identificazione e ottimizzare il compromesso tra accuratezza e privacy. La loro analisi risulta fondamentale per comprendere come i sistemi di sorveglianza basati su dati pubblicitari possano essere progettati per bilanciare efficacia operativa e protezione della privacy.

Impatti sulla sicurezza e sulla privacy

Acquisti et al. (2016) forniscono un'analisi approfondita delle esternalità generate dai sistemi di sorveglianza digitale. Gli autori evidenziano come gli effetti della

sorveglianza si propaghino ben oltre gli obiettivi iniziali, creando esternalità dirette attraverso la perdita di privacy per individui non target e la discriminazione basata su associazioni. Particolarmente significativi sono gli effetti indiretti, che includono modifiche comportamentali dovute alla consapevolezza della sorveglianza e impatti sulla libertà di espressione. A livello sistemico, gli autori identificano problematiche legate alla concentrazione del potere informativo e alle asimmetrie informative nei mercati.

Il ruolo dell'ADINT nella sorveglianza moderna

Vines et al. (2017) forniscono un'analisi tecnica dettagliata delle metodologie di tracciamento attraverso l'ADINT. La loro ricerca dimostra come sia possibile utilizzare le piattaforme pubblicitarie per ottenere una localizzazione geografica estremamente precisa, fino a 8 metri di accuratezza, permettendo il tracciamento dei movimenti nel tempo e l'identificazione di pattern ricorrenti. Il sistema può anche essere utilizzato per il monitoraggio delle applicazioni installate e dei loro tempi di utilizzo, consentendo una profilazione comportamentale approfondita. Particolarmente significativa è la capacità di questi sistemi di operare in modo continuo nel tempo, permettendo l'inferenza di relazioni sociali e la deduzione di interessi sensibili attraverso l'analisi dei pattern di utilizzo.

Le piattaforme pubblicitarie non solo raccolgono dati personali, ma li usano anche per influenzare decisioni individuali e collettive. Ad esempio, le tecnologie di "*Algorithmic Cognitive Warfare*", sviluppate in particolare in Cina, sfruttano algoritmi avanzati per identificare e influenzare bersagli specifici. Questi sistemi sono in grado di creare "ritratti cognitivi" che analizzano lo stato psicologico e i comportamenti degli utenti, utilizzando queste

informazioni per diffondere contenuti mirati e influenzare opinioni e decisioni (Lange, 2024).

Implicazioni per la policy e la regolamentazione

Goldfarb e Que (2023) propongono un *framework* completo per la regolamentazione che integra considerazioni tecniche, economiche e sociali. A livello tecnico, gli autori enfatizzano l'importanza di standard minimi di protezione e meccanismi di trasparenza algoritmica, dal punto di vista economico invece il *framework* considera gli incentivi per la protezione della privacy e le strutture di mercato necessarie per garantire una competizione efficiente, mentre la dimensione sociale viene affrontata attraverso la protezione dei diritti fondamentali e *l'accountability* democratica. Gli autori sottolineano come questi diversi aspetti debbano essere considerati simultaneamente per creare un sistema di regolamentazione efficace e sostenibile.

Confronto con i paesi autoritari

La raccolta massiva di dati personali da parte di aziende private e governi per scopi commerciali, di sicurezza o di governance può erodere la fiducia pubblica e creare un senso di sorveglianza costante. Questo fenomeno, noto come "effetto chilling", porta gli individui a limitare le proprie interazioni online e a modificare i propri comportamenti per timore di essere monitorati e per paura di conseguenze legali, sociali o economiche. Questo può avvenire quando ci sono leggi, regolamenti o azioni di sorveglianza che creano un senso di insicurezza o timore di repressione.

Un caso interessante è rappresentato dal c.d. "*Algorithmic Cognitive Warfare*", introdotto in precedenza in questo capitolo al paragrafo 4. Questa strategia, utilizzata in

maniera considerevole dalle agenzie di intelligence della Repubblica Popolare Cinese, sfrutta algoritmi avanzati per creare “ritratti cognitivi” dettagliati degli individui, mappando lo stato psicologico, i comportamenti e le reti sociali di ciascun utente. Gli algoritmi vengono progettati non solo per identificare i *target*, ma anche per influenzare le loro percezioni attraverso contenuti mirati e adattati in tempo reale alle loro condizioni psicologiche e comportamentali (Lange, 2024). Questo viene ottenuto attraverso varie tecniche (ibidem):

- Raccolta e analisi di dati psicometrici: grazie ai dati raccolti da applicazioni e piattaforme digitali, è possibile costruire un quadro dettagliato delle emozioni, delle convinzioni e delle vulnerabilità di un individuo;
- Targeting comportamentale predittivo: utilizzando modelli di machine learning, i sistemi ADINT sono in grado di anticipare i comportamenti futuri e agire in modo proattivo per influenzare le scelte dei target;
- Amplificazione dei contenuti: gli algoritmi manipolano la visibilità di determinati contenuti per rafforzare determinate narrazioni o polarizzare gruppi sociali attraverso il fenomeno delle “bolle informative” e dei c.d. “*eco-chamber*“[1].



Fonte: Lange (2024)

Esaminando le tecnologie di sorveglianza, emerge un netto contrasto tra l’approccio occidentale alla privacy e quello adottato dai regimi autoritari. Un caso emblematico è rappresentato dal sistema di videosorveglianza di massa iraniano, sviluppato con tecnologia cinese di “Tiandy Technologies”, che utilizza telecamere intelligenti e sistemi di riconoscimento facciale per identificare e sanzionare automaticamente le donne che non rispettano l’obbligo del velo[2]. Questo sistema si basa su una vasta rete di

telecamere di sorveglianza ed è stato significativamente potenziato nel 2022 in risposta alle proteste per Mahsa Amini, rappresentando un esempio concreto di come le tecnologie OSINT e ADINT possano essere utilizzate per il controllo sociale (Feldstein, 2019).

Il caso iraniano si inserisce in un più ampio fenomeno che Polyakova e Meserole (2019) definiscono "*digital authoritarian spillover*", dove le tecnologie di sorveglianza vengono condivise tra regimi autoritari, con la Cina che emerge come principale esportatore. Come analizzato da Zuboff (2019) queste tecnologie, originariamente sviluppate per scopi commerciali in Occidente, vengono adattate per il controllo sociale in contesti autoritari.

La situazione è particolarmente preoccupante considerando il quadro normativo internazionale. Difatti, mentre l'Unione Europea ha implementato il Regolamento 2021/821 per controllare l'esportazione di tecnologie dual-use e il GDPR per proteggere i dati personali, i regimi autoritari possono aggirare queste restrizioni attraverso collaborazioni tecnologiche dirette (Deibert, 2020). Come evidenziato da Polyakova e Meserole (2019), questo ha creato un "mercato parallelo" di tecnologie di sorveglianza tra stati autoritari.

Sfide future OSINT e ADINT: bilanciamento privacy e sicurezza nazionale

L'analisi della letteratura evidenzia la natura multidimensionale degli impatti di OSINT e ADINT, sottolineando la necessità di un approccio bilanciato che consideri simultaneamente aspetti economici, tecnici e sociali. La sfida per il futuro sarà sviluppare *framework* regolatori che possano adattarsi all'evoluzione tecnologica mantenendo protezioni efficaci per i diritti fondamentali e

solamente con una comprensione approfondita delle diverse dimensioni del fenomeno sarà possibile sviluppare risposte normative adeguate alle sfide poste da queste tecnologie.

Conclusioni

La rapida evoluzione tecnologica e la crescente digitalizzazione della società moderna hanno trasformato enormemente le modalità usate per raccogliere, elaborare e utilizzare i dati personali.

Questa tesi si è focalizzata principalmente sull'analisi approfondita delle tecniche OSINT (Open Source Intelligence) e ADINT (Advertising Intelligence), esaminando come queste metodologie di raccolta informazioni possano impattare significativamente sulla privacy degli individui. L'analisi ha evidenziato come gli strumenti pubblicitari e i dati pubblicamente disponibili possano essere utilizzati per condurre attività di sorveglianza mirata, spesso con investimenti economici relativamente contenuti.

La sezione riguardante l'ADINT ha rivelato come le piattaforme pubblicitarie possano essere sfruttate per tracciare gli individui e ricavare informazioni sensibili sul loro comportamento e le loro preferenze. La possibilità di utilizzare il *targeting* pubblicitario per questi scopi solleva importanti questioni etiche e di privacy, in particolar modo considerando che queste tecniche sono accessibili ad un'ampia gamma di attori, non solo alle grandi organizzazioni o alle agenzie governative.

L'analisi delle tecniche OSINT ha mostrato come l'aggregazione di informazioni provenienti da fonti pubbliche possa creare profili dettagliati degli individui, evidenziando la necessità di riconsiderare il concetto di privacy nell'era digitale. La facilità con cui queste informazioni possono essere raccolte e correlate rappresenta una sfida notevole per la protezione della privacy individuale.

La tesi ha anche esaminato le possibili contromisure tecniche e normative per proteggere gli individui da queste forme di sorveglianza. Le tecnologie c.d. "*privacy-preserving*", come la privacy differenziale e le tecniche di anonimizzazione, possono offrire alcune protezioni ma devono essere bilanciate con la necessità di mantenere l'utilità dei dati per scopi legittimi. Particolare attenzione è stata dedicata all'analisi delle soluzioni che possono mitigare i rischi collegati all'Advertising Intelligence, come il controllo più rigoroso sul targeting pubblicitario e la limitazione della granularità dei dati disponibili per gli inserzionisti.

Questa tesi ha inoltre esplorato il complesso equilibrio tra la protezione della privacy e l'utilità dei dati, analizzando sia gli aspetti tecnici che quelli regolatori, con particolare attenzione al contesto europeo. L'analisi ha rivelato come questo equilibrio sia non solo una sfida tecnica ma anche una questione di fondamentale importanza sociale ed economica.

Si è evidenziato come il compromesso tra privacy e utilità dei dati sia inevitabile ma gestibile attraverso approcci formali come la privacy differenziale e come questi metodi avanzati offrano garanzie rigorose sulla protezione della privacy, permettendo allo stesso tempo di estrarre valore dai dati. Tuttavia, la loro implementazione pratica richiede una attenta calibrazione dei parametri e una profonda comprensione dei trade-off coinvolti. Si è dimostrato inoltre come diverse tecniche possano essere impiegate per raggiungere diversi livelli di protezione della privacy, ciascuna con i propri vantaggi e limitazioni.

Il contesto normativo europeo, caratterizzato dal GDPR, ha stabilito uno standard globale per la protezione dei dati personali, distinguendosi significativamente dall'approccio più frammentato adottato negli Stati Uniti. La legislazione europea pone particolare enfasi sui diritti individuali, sul consenso informato e sulla trasparenza nel trattamento dei dati, influenzando profondamente il modo in cui le

organizzazioni devono gestire i dati personali. Questa differenza normativa ha importanti implicazioni per lo sviluppo e l'adozione di tecnologie *privacy-preserving*, creando un framework più rigido ma anche più chiaro per le organizzazioni che operano in Europa.

Un aspetto cruciale emerso dall'analisi riguarda l'economia della privacy, che ha mostrato come le organizzazioni debbano bilanciare i costi dell'implementazione di misure di protezione della privacy con i benefici derivanti dall'utilizzo dei dati. Allo stesso tempo, gli individui devono valutare il valore della loro privacy rispetto ai servizi e ai benefici che possono ottenere condividendo i loro dati. Questo equilibrio economico influenza significativamente l'adozione e l'evoluzione delle tecnologie *privacy-preserving*.

La presente tesi ha esaminato non solo gli aspetti tecnici ma anche le profonde differenze nell'utilizzo di metodi come OSINT e ADINT tra democrazie occidentali e regimi autoritari. Si è evidenziato come nell'Unione Europea l'utilizzo di queste tecniche di intelligence sia regolamentato da un quadro normativo che cerca di bilanciare le esigenze di sicurezza nazionale con la protezione dei diritti fondamentali dei cittadini, e il confronto con il sistema cinese ha rivelato differenze sostanziali nell'approccio alla sorveglianza digitale.

Mentre le agenzie di intelligence europee operano sotto vincoli legali e costituzionali stringenti, il sistema cinese integra tecniche come l'OSINT e l'ADINT in un più ampio apparato di controllo sociale, dove queste tecniche vengono utilizzate sistematicamente per il monitoraggio della popolazione. Questa differenza fondamentale riflette visioni contrastanti sul rapporto tra Stato e cittadino e sul valore della privacy individuale.

Le agenzie di intelligence europee hanno sviluppato *framework* operativi che cercano di massimizzare l'efficacia delle

attività di intelligence nel rispetto dei diritti fondamentali. Questo approccio si manifesta attraverso procedure di autorizzazione e supervisione, limiti temporali alla raccolta dati e la necessità di giustificare specificamente ogni attività di sorveglianza. In contrasto, i regimi autoritari utilizzano queste tecnologie come strumenti di controllo sociale pervasivo, senza significative limitazioni legali o etiche.

La tesi ha anche evidenziato come il settore privato europeo sia soggetto a regolamentazioni più stringenti nell'uso di OSINT e ADINT rispetto ad altri contesti internazionali. Il GDPR impone limiti significativi sulla raccolta e l'uso dei dati personali, influenzando direttamente come queste tecniche possono essere impiegate per scopi commerciali. Questa *compliance* normativa ha portato allo sviluppo di approcci più sofisticati e rispettosi della privacy nel contesto europeo.

Inoltre, la cooperazione internazionale e lo sviluppo di standard comuni saranno fondamentali per affrontare queste sfide in un mondo sempre più interconnesso, e l'esperienza europea nel regolamentare la privacy dei dati può fornire importanti lezioni per altre giurisdizioni, contribuendo a stabilire un framework globale per la protezione dei dati personali.

Per quanto riguarda l'usabilità e l'accessibilità delle soluzioni *privacy-preserving*, la complessità tecnica di queste soluzioni non deve tradursi in barriere all'adozione da parte di utenti non tecnici, e dunque sarà cruciale sviluppare interfacce intuitive e meccanismi di comunicazione efficaci dei rischi per la privacy per permettere l'adozione diffusa di queste tecnologie. La formazione e l'educazione sulla privacy dei dati rappresentano un ulteriore aspetto fondamentale per il futuro, e di conseguenza è necessario aumentare la consapevolezza sia tra gli individui che tra le organizzazioni riguardo l'importanza della protezione dei dati personali e alle metodologie disponibili per garantirla.

In conclusione, mentre le sfide tecniche e normative nella protezione della privacy dei dati rimangono significative, gli sviluppi recenti forniscono ragioni di ottimismo. L'evoluzione delle tecnologie *privacy-preserving*, unitamente al rafforzamento del quadro normativo, specialmente in Europa, sta creando un ambiente più favorevole alla protezione dei dati personali. La continua ricerca e sviluppo in questo campo, combinata con una maggiore consapevolezza dell'importanza della privacy dei dati, suggerisce che emergeranno soluzioni sempre più efficaci per proteggere la privacy degli individui mantenendo al contempo l'utilità dei dati per la società.

L'analisi approfondita delle metodologie OSINT e ADINT rivela un panorama complesso in cui tecnologia, economia e diritti fondamentali si intersecano creando nuove sfide per la società digitale contemporanea. Questo studio ha evidenziato come le tecniche di Open Source Intelligence e Advertising Intelligence possano essere implementate con investimenti contenuti, raggiungendo livelli di precisione nella sorveglianza e profilazione comportamentale precedentemente impensabili.

Per approfondire questi temi cruciali per il futuro della privacy digitale e della sicurezza nazionale, scarica gratuitamente il white paper di **Sergiu Deaconu "Open Source Intelligence e Advertising Intelligence: applicazioni e impatti in ambito industriale, civile e dell'intelligence europea".**

Fonti:

[1] Si tratta di un ambiente in cui le persone, spesso in forum online e vari social media, sono esposte principalmente a opinioni e informazioni che confermano e rafforzano le loro convinzioni preesistenti, creando un circolo vizioso in cui continueranno ad ascoltare le stesse opinioni e saranno sempre più restii a discutere con persone che hanno opinioni

divergenti dalle loro.

[2] Iran resorts to security cameras, ostracism to deter unveiled women. Reuters. com.

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/adint/