PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Linee guida sulle questioni etiche e legali della protezione dei dati nella ricerca e nell'innovazione delle TIC

SOCIAL NETWORK

Quest'opera è rilasciata con licenza Creative Commons Attribuzione-Non commerciale-Non opere derivate 4.0 Internazionale.

Questo progetto è stato finanziato dal programma di ricerca e innovazione Horizon 2020 dell'Unione Europea con l'accordo di sovvenzione n. 788039. Il presente documento riflette esclusivamente il punto di vista degli autori e l'Agenzia non può essere ritenuta responsabile per l'uso che può essere fatto delle informazioni in esso contenute.

Social network per scopi di ricerca: requisiti etici e legali relativi alla protezione dei dati

Jose Antonio Castillo Parrilla e Iñigo de Miguel Beriain (UPV/EHU)

Le versioni preliminari di questo documento sono state riviste da Dr Denise Amram, ricercatrice affiliata al LIDER Lab - Istituto DIRPOLIS, Scuola Superiore Sant'Anna (Italia) e assistente della cattedra *di diritto privato comparato alla Scuola Superiore Sant'Anna e il Prof. Giovanni Comandé, Dirpolis, Scuola Superiore Sant'Anna, Pisa, Italia.*

Questa parte degli Orientamenti è stata convalidata da Iñaki Pariente, ex direttore dell'Agenzia Basca di Protezione dei Dati

I social media possono essere descritti come piattaforme online che consentono lo sviluppo di reti e comunità di utenti, tra i quali vengono condivise informazioni e contenuti. Altre funzioni dei social network sono la personalizzazione, l'analisi e la pubblicazione (principalmente attraverso servizi di targeting), che consentono sia iniziative freelance che offerte di servizi più ampie. I social media consentono agli individui di creare account personali per interagire con altri utenti e sviluppare e ampliare le connessioni e le reti. Gli utenti condividono dati con gli amministratori della rete e con altri utenti per scopi totalmente diversi. Il contenuto condiviso dalle persone può essere creato da loro stessi (contenuto generato dall'utente) o meno. [1]

D'altra parte, è importante ricordare che la finalità principale dei dati inseriti in una rete sociale è quella di consentire alle persone di interagire, di relazionarsi. Infatti, un utente stabilisce due tipi di relazioni: una relazione verticale con la società che possiede la rete, e una relazione orizzontale con altre persone con cui vuole interagire. Questa relazione può essere generale (profili aperti) o particolare (profili con accesso limitato). A seconda del tipo di interazione in gioco, lo status giuridico del trattamento dei dati sarà, probabilmente, diverso.

In generale, i social network sono ideali per le **pratiche di estrazione massiva di dati**. Infatti, esistono strumenti software disponibili in grado di raccogliere automaticamente i dati degli utenti web dagli spazi pubblici online. Inoltre, la maggior parte dei social network abilita le Application Programming Interfaces, o API [2], che semplificano lo sviluppo e l'innovazione del software e rendono possibile alle applicazioni lo scambio di dati e funzionalità in modo semplice e sicuro. Queste circostanze rendono i social network particolarmente interessanti per alcuni tipi di ricerca, ma creano anche sfide impegnative in termini di protezione dei dati.

[1] Linee guida CEPD 8/2020 sul targeting degli utenti di social media, pag. 3.

[2] Vedi, sulle API: Oscar Borgogno & Giuseppe Colangelo, Data Sharing and Interoperability Through APIs: Insights from European Regulatory Strategy, Stanford-Vienna European Union Law Working Paper No. 38, http://ttlf.stanford.edu; Russell, N. Cameron and Schaub, Florian and McDonald, Allison and Sierra-Pambley, William, APIs and Your Privacy (5 febbraio 2019). Disponibile su SSRN: https://ssrn.com/abstract=3328825 o http://dx.doi.org/10.2139/ssrn.3328825

Questa parte degli Orientamenti intende essere di ausilio ai ricercatori o agli **innovatori delle TIC che utilizzano dati personali ottenuti dai social network.** Vale la pena menzionare che non ci occuperemo qui dell'uso dei social network per raccogliere dati (come, ad esempio, utilizzando i sondaggi di Google per ottenere dati su una determinata serie di domande da persone reali). Ciò è dovuto a una semplice ragione: in questi casi, i dati stessi non provengono da un social network ma attraverso un social network. Infatti, i social network agiscono solo come uno strumento di raccolta di quei dati. Pertanto, questi dati non sono così diversi da qualsiasi altro dato raccolto in modo più tradizionale (come un sondaggio su carta) e, quindi, non meritano particolare attenzione qui.

Se gli sviluppatori delle TIC che consultano i presenti Orientamenti intendono utilizzare strumenti di intelligenza artificiale per elaborare i dati ottenuti da queste reti, dovrebbero consultare la parte degli Orientamenti dedicata all'intelligenza artificiale (IA). Se ne stanno pianificando l'uso per scopi legati alla biometria, all'Internet degli oggetti o alla localizzazione geospaziale, dovrebbero consultare le sezioni di questi Orientamenti a essi dedicate. Al fine di evitare inutili ripetizioni, lasciamo tali questioni fuori da questa analisi.

DISCLAIMER

Questa parte degli Orientamenti è stata scritta in un momento in cui il Regolamento in materia di ePrivacy non era stato approvato. È possibile che, al momento dell'uso di questo strumento, il Regolamento sia in vigore. In tal caso, sarà necessario prendere in considerazione i possibili cambiamenti che questo può aver prodotto nel quadro normativo. Fino a quando il Regolamento in materia di ePrivacy non entrerà in vigore, esisterà una situazione frammentata. Infatti, le autorità di controllo affrontano ora una situazione in cui coesiste interazione tra la Direttiva sull'ePrivacy e l'RGPD, e pone questioni relative alle competenze, ai compiti e ai poteri delle autorità di protezione dei dati in quei casi che implicano l'applicazione sia dell'RGPD che delle leggi nazionali di attuazione della Direttiva ePrivacy.

1 Introduzione ai social network e alle questioni in materia di protezione dei dati

Alcuni consigli preliminari: È assolutamente necessario tener presente **che il fatto che gran parte dei dati contenuti in un social network siano facilmente apprendibili non ne legittima il trattamento.** Questo è un aspetto cruciale quando si tratta del trattamento di dati ottenuti dalle reti sociali: I ricercatori e gli innovatori delle TIC devono assicurarsi attentamente di avere una base giuridica che consenta loro l'accesso a e la conservazione di questi dati. Una volta ottenuto l'accesso, dovranno assicurarsi che la stessa e/o altre basi di legittimità li autorizzino a un ulteriore trattamento di questi dati. In generale, questo significa che devono avere una conoscenza approfondita delle Politiche dello sviluppatore imposte dalle reti sociali (vedere la sezione 3 (liceità) di questo documento per ulteriori letture in merito).

Inoltre, la trasparenza implica che i soggetti interessati dalla prevista ricerca dovrebbero essere informati, ad un certo punto, della ricerca che si sta svolgendo, del tipo di dati

personali che i titolari del trattamento stanno raccogliendo e di come saranno usati. Alcuni servizi chiariscono che ciò deve essere fatto prima di iniziare la raccolta. In assenza di una politica specifica e quando i ricercatori/innovatori conducono una ricerca osservazionale, che la necessità di ottenere il previo consenso potrebbe danneggiare, dovrebbero informare i soggetti interessati il prima possibile. I ricercatori/innovatori delle TIC dovrebbero sempre rimuovere dalla loro raccolta i soggetti che non prestano il loro consenso all'inclusione.

1.1 Concetti principali

La natura imprecisa dei dati raccolti dai social network, insieme alle norme legali sulla protezione dei dati personali, suggerisce ai gestori di reti sociali, e a coloro che utilizzano i dati raccolti da queste reti per scopi di ricerca, che, più che la categoria della rete sociale, dovrebbero prendere in considerazione **sia il tipo di dati oggetto di trattamento che i seguenti criteri principali:**

- la finalità per cui stanno usando i dati;

- la normativa applicabile, e in particolare i conflitti normativi che possono derivare dalla loro attività e le finalità originarie della raccolta di dati personali nelle reti sociali.

Una rete sociale è un **servizio della società dell'informazione.** Il concetto di servizio della società dell'informazione è menzionato nell'Articolo 2 lettera a) e nei Considerando 17 e 18 della Direttiva CE 2000/31, così come nell'Articolo 4 (25) RGPD. Essi rinviano tutti all'articolo 1, paragrafo 1, lettera b) della Direttiva UE 2015/1535. Un servizio della società dell'informazione è qualsiasi servizio normalmente fornito dietro retribuzione, a distanza, con mezzi elettronici e a richiesta individuale di un destinatario di servizi.

Gli operatori di una rete sociale hanno il doppio status di fornitore di servizi sociali e di titolare del trattamento dei dati, secondo la loro politica in materia di privacy, che li considera come tali.[3] Come fornitori di servizi sociali, sono soggetti a responsabilità ai sensi degli Articoli da 12 a 15 della Direttiva 2000/31/CE. Come titolari del trattamento dei dati, sono responsabili sia di garantire che i dati siano trattati in conformità con l'Articolo 5 RGPD, sia di comprovarlo (art. 5, paragrafo 2 RGPD). Chi utilizza il social network per finalità che esulano da quelle di un semplice utente (ad esempio, uso dei social network per la ricerca) **deve essere considerato anche come titolare del trattamento, e ne risponderà di conseguenza. Tuttavia, è anche vero che, in caso di controllo congiunto,** i titolari del trattamento possono essere coinvolti in diverse fasi del trattamento dei dati personali e in

[3] Al fine di chiarire i rispettivi ruoli e responsabilità dei fornitori di social media e dei targeter, è importante tenere conto degli Orientamenti del CEPD (Linee guida 8/2020 sul targeting degli utenti di social media Versione 2.0 Adottato il 13 aprile 2021, disponibile all'indirizzo: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf, pag. 11) e della relativa giurisprudenza della CGUE. Le sentenze in Wirtschaftsakademie (C-210/16), Jehovah's Witnesses (C-25/17) e Fashion ID (C-40/17) sono, qui, particolarmente rilevanti.

misura diversa. In tale scenario, il livello di responsabilità di ciascuno di essi deve essere valutato in relazione a tutte le circostanze pertinenti del caso specifico. [4]

1.2 Sfide

L'uso dei dati raccolti dai social network solleva, di per sé, alcune **sfide** relative al trattamento dei dati, che devono essere prese in considerazione. Queste sfide possono essere ancora più singolari quando la finalità del trattamento è legata alla ricerca. Le principali questioni coinvolte nell'uso dei dati raccolti attraverso i social network per finalità di ricerca sono le seguenti:

- I social network favoriscono ed esaltano il costante riutilizzo dei dati, il che comporta rischi legati a
    - l'applicazione di principi come la limitazione della finalità (Art. 5, paragrafo 1, lettera b)), la limitazione del periodo di conservazione (Art. 5, oaragrafo 1, lettera e)), l'integrità e la riservatezza (Art. 5, paragrafo 1, lettera e)); ecc.
    - o lo status giuridico dei profili personali e altri dati derivati, in particolare se rimangono dati personali e se sono anche opere di proprietà intellettuale (PI) (la questione se i dati personali inferiti siano dati personali o solo PI dei loro produttori).
- La scelta e l'uso corretto di una base giuridica per la raccolta di dati dalle reti sociali, che richiede un'adeguata comprensione e l'adempimento dei requisiti delle loro politiche dello sviluppatore
- La scelta di una base giuridica per il riutilizzo dei dati ottenuti attraverso le reti sociali e l'uso adeguato di questi dati secondo la base selezionata:
    - Il consenso (e la possibilità di ottenere un "consenso altruistico", soprattutto alla luce della proposta di legge sulla governance dei dati).
    - Interesse legittimo
    - Interesse pubblico
    - Eccezione della ricerca
- L'identificazione dei rischi derivanti dalla ricerca con i dati dei social media, tra cui spiccano i seguenti:
    - danno alla vita privata dell'individuo attraverso l'analisi di massa di dati personali o non personali (privacy di gruppo), ad esempio a causa dell'identificazione (o re-identificazione) degli interessati mediante profili personali (questo chiaramente comporta un rischio estremamente elevato a causa dell'intenzione di promuovere l'analisi di massa di dati che potrebbe portare alla profilazione);

[4] Cfr.: 4 Sentenza in Wirtschaftsakademie, C-210/16, paragrafo 43; Sentenza in Testimoni di Geova, C-25/17, paragrafo 66 e Sentenza in Fashion ID, C-40/17, paragrafo 70.

- o danni all'onore, alla privacy o all'immagine di individui o gruppi, per esempio, pubblicando dati grezzi senza passare attraverso un corretto processo di aggregazione o pseudonimizzazione.

- La natura espansiva dei dati personali, che rende consigliabile assumere per default che si stiano trattando dati personali, anche se a prima vista potrebbe non sembrare così. [5]

- Anche se in molte occasioni, e sempre di più, la ricerca attraverso le reti sociali nasce come ricerca, è frequente anche che i profili delle reti sociali del ricercatore non abbiano questo scopo iniziale e lo acquisiscano solo dopo qualche tempo.

- Il presupposto comune che i dati resi pubblici attraverso i social media possano essere utilizzati liberamente. **Ciò è chiaramente falso, salvo che i dati non siano effettivamente pubblicati in profili totalmente pubblici ("resi manifestamente pubblici dall'interessato") e deve essere accuratamente evitato.**

- Infine, l'opacità degli algoritmi di trattamento dei dati può avere un impatto negativo sugli utenti e scoraggiare la ricerca (cfr. la sezione "Esposizione generale" nella parte IA dei presenti Orientamenti)

1.3 Tipi di dati che possono essere raccolti attraverso i social network

I social network possono fornire ai ricercatori tre diversi tipi di dati: dati forniti, dati osservati e dati inferiti/derivati (o una loro combinazione). Questi tipi di dati potrebbero essere definiti in questo modo[6]:

- I "dati forniti" si riferiscono alle informazioni fornite attivamente dalla persona interessata al fornitore di social media e/o al titolare del trattamento. Ad esempio: gli utenti dei social media potrebbero indicare la loro età nella descrizione del loro profilo. Nei presenti Orientamenti non affronteremo il trattamento di tali dati, poiché non sono diversi da altri dati raccolti da un fornitore di servizi.
- I "Dati osservati" si riferiscono ai dati forniti dal soggetto interessato in virtù dell'utilizzo di un servizio o di un dispositivo. Essi includono:

[5] Il progetto Historic Graves è un progetto di patrimonio di base incentrato sulla comunità. I gruppi della comunità locale vengono addestrati per un'indagine sul campo ad alta tecnologia a basso costo dei cimiteri storici, e per la registrazione delle loro storie orali. Elaborano un registro online multimediale delle tombe storiche nelle loro aree e si uniscono per formare una risorsa nazionale. Poiché si tratta di un progetto che raccoglie dati dai cimiteri, si potrebbe pensare che si tratta di dati dei defunti e quindi l'RGPD non si applica (Considerando 27). Tuttavia, i dati sui cimiteri e sulle tombe sono forniti dai parenti dei defunti, che, ovviamente, non sono deceduti, e fornendo i dati dei loro parenti defunti stanno anche fornendo i propri dati personali.

[6] Linee guida 8/2020 sul targeting degli utenti di social media Versione 2.0 Adottata il 13 aprile 2021, disponibile all'indirizzo: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf

- dati di un determinato utente di social media potrebbero essere raccolti sulla base della sua attività sulla stessa piattaforma di social media (ad esempio, i contenuti che l'utente ha condiviso, consultato o apprezzato);
- dati relativi all'uso dei dispositivi dove viene eseguita l'applicazione del social media (ad esempio, coordinate GPS, numero di telefono cellulare);
- dati ottenuti da un terzo sviluppatore di applicazioni utilizzando interfacce di programmazione delle applicazioni (API) o kit di sviluppo del software (SDK) offerti dai fornitori di social media;
- dati raccolti attraverso siti web di terzi che hanno incorporato social plugin o pixel;
- dati raccolti tramite terzi (ad esempio, soggetti con cui l'interessato ha interagito, acquistato un prodotto, sottoscritto tessere fedeltà); oppure
- dati raccolti attraverso servizi offerti da aziende di proprietà o gestite dal fornitore di social media.

- I "dati inferiti" e i "dati derivati" sono quelli creati dal titolare del trattamento dei dati sulla base dei dati forniti dall'interessato o osservati dal titolare del trattamento. Essi potrebbero essere inferiti tramite calcoli deterministici o dedotti in modo probabilistico. Ad esempio, un fornitore di social media potrebbe dedurre che un individuo è probabilmente interessato a una certa attività o prodotto sulla base del suo comportamento di navigazione web e/o delle connessioni di rete.

Il modo di ottenere i dati non è rilevante né per qualificarli come dati personali o non personali né per decidere se appartengono a categorie particolari di dati ai sensi dell'Art. 9 RGPD. Tuttavia, **può avere conseguenze importanti sotto altri aspetti.** Ad esempio, nel determinare se gli interessati potevano prevedere o meno un particolare trattamento, o nel determinare i limiti del loro diritto di portabilità o le informazioni da fornire loro. Si deve tenere presente che nel caso di dati osservati, inferiti o derivati, gli utenti, di solito, non sono consapevoli della raccolta o creazione di quei dati.

Riquadro 1: Inferenza dei dati. Esempi

Esempio 1

"La società X ha sviluppato un'applicazione che, analizzando i dati grezzi dei segnali dell'elettrocardiogramma generati da sensori commerciali comunemente disponibili per i consumatori, è in grado di rilevare modelli di dipendenza dalla droga. Il motore dell'applicazione può estrarre dai dati grezzi dell'ECG caratteristiche specifiche che, secondo precedenti risultati investigativi, sono legate al consumo di droghe. Il prodotto, compatibile con la maggior parte dei sensori sul mercato, potrebbe essere utilizzato come applicazione autonoma o tramite un'interfaccia web che richiede il caricamento dei dati. Per elaborare i dati a tale scopo, è necessario ottenere il consenso dell'utente per quella finalità. Il rispetto di questo requisito del consenso può essere soddisfatto negli stessi casi e nel momento in cui si ottiene il consenso dell'interessato ai sensi dell'Articolo 7, lettera a)."

Fonte: Parere 8/2014 del Gruppo di lavoro dell'Art. 29 in materia dei recenti sviluppi dell'Internet degli oggetti (16 set 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

Esempio 2+

I dati Fitbit potrebbero essere rilevanti per potenziali datori di lavoro, che potrebbero fare inferenze su "l'impulsività e l'incapacità di ritardare la gratificazione - entrambe deducibili dalle abitudini di esercizio di una persona - correlate con l'abuso di alcol e droga, disturbi alimentari , fumo di sigaretta, maggiore debito della carta di credito, e minor solvibilità. La mancanza di sonno, di cui il Fitbit tiene traccia, è stata collegata a uno scarso benessere psicologico, problemi di salute, scarse prestazioni cognitive ed emozioni negative come rabbia, depressione, tristezza e paura".

Fonte: Peppet, Scott R 'Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent' (2014) 93 Tex. L. Rev. 85.

Bisogna considerare che l'inferenza di dati sanitari è un trattamento particolarmente sensibile poiché questi dati (non importa se inferiti o meno) sono dati di categorie particolari

1.4 Categorie di dati raccolti attraverso i social media

In linea di principio, è perfettamente possibile raccogliere **diversi tipi di dati attraverso i social media. Infatti, possono essere dati personali e non personali.** La comprensione dei dati come non personali è di grande importanza a livello giuridico e, ovviamente, per la preparazione dei presenti Orientamenti, nella misura in cui l'RGPD non sarebbe applicabile, ma il Regolamento UE 2018/1807 sì. In pratica, questa suddivisione tra questi due tipi di dati si sta attenuando a causa del crescente uso della tecnologia di analisi dei dati, che consente una maggiore capacità di trattamento dei dati e l'estrapolazione di risultati

(privacy di gruppo). Questa situazione offusca il confine tra dati personali e non personali nella misura in cui, ad esempio, i profili stanno diventando sempre più accurati anche se non collegati a nessun individuo specifico e non sono, quindi, dati personali.

Il limite per considerare i dati come personali risiede nella loro capacità di identificare direttamente o indirettamente una persona e, in particolare, se i costi e il tempo necessari per tale identificazione non sono eccessivi[7]. Tuttavia, questo tipo di classificazione non è così facile da applicare nella pratica. Per cominciare, alcuni dati che sembrano anonimi a prima vista potrebbero essere de-anonimizzati[8] (cfr. la sotto-sezione "Identificazione, pseudonimizzazione e anonimizzazione" nella sezione "Concetti principali" della Parte generale dei presenti Orientamenti). Inoltre, i dati personali come concetto giuridico godono di una sorta di natura espansiva nella misura in cui l'iper-produzione di dati e la capacità di trattarli e analizzarli è in costante crescita, riducendo, così, i costi e il tempo necessari per identificare una persona da qualsiasi set di dati (personali o non personali)[9].

Tenendo conto di tutto questo, si deve concludere che, **nel caso dei social network, il trattamento dei dati personali è, generalmente, la regola.** Ciò è particolarmente vero se consideriamo che in questo contesto è comune che gli utenti si registrino con una serie di dati personali. È del tutto possibile che (1) molti di questi dati non siano strettamente necessari per il login e, quindi, non si rispetti il principio di minimizzazione dei dati (Art. 5, paragrafo 1, lettera c) RGPD) o che (2) i dati siano utilizzati per finalità che vanno oltre il semplice login, violando, in tal caso, il principio di limitazione della finalità (Art. 5, paragrafo 1, lettera b) RGPD). Infine, la profilazione personale può raggiungere un alto livello di precisione indipendentemente dal tipo di dati utilizzati per la produzione di tali profili. **Ciò impone di prendere in considerazione le seguenti precauzioni:**

- I titolari del trattamento **dovrebbero presumere per default che stanno trattando dati personali** e agire di conseguenza.

- È consigliabile evitare questa presunzione solo se i dati da utilizzare e i dati inferiti dal titolare del trattamento sono totalmente non personali (ad esempio, i dati meteorologici). In questi casi, i titolari del trattamento devono documentarlo nei registri del trattamento.

- Se i dati da trattare si riferiscono a persone decedute o a persone giuridiche, devono essere adottate precauzioni volte ad evitare che questi dati siano collegati a persone fisiche (ad esempio, parenti di persone decedute o persone fisiche collegate a persone giuridiche).

- Se i dati da trattare si riferiscono a persone decedute, devono essere prese in considerazione anche le norme nazionali sul trattamento dei dati, poiché i dati di persone decedute non sono dati personali secondo l'RGPD.

---

[7] Cfr. Cons. 26 RGPD: "Per stabilire l'identificabilità di una persona, è opportuno considerare tutti i mezzi di cui ci si può ragionevolmente avvalere".

[8] Cfr. Cons. 26 RGPD: "I dati personali che sono stati sottoposti a pseudonimizzazione, che potrebbero essere attribuiti a una persona fisica mediante l'uso di informazioni aggiuntive dovrebbero essere considerati come informazioni su una persona fisica identificabile"

[9] Cfr.: in generale, G. Comandé (Editore) Encyclopedia of Data Science and Law Edwards Eldgar, 2021; di prossima pubblicazione; G. Comandé - G. Malgieri, *"Sensitive-by-distance: quasi-health data in the algorithmic era" (2017)*, in *Information & Communications Technology Law*, Vol. 26, Iss. 3, p. 229-249; G. Comandé - G. Schneider, *"Regulatory Challenges of Data Mining Practices: The Case of the Never-ending Lifecycles of 'Health Data'" (2018),* in *European Journal of Health Law*, Volume 25, Issue 3, pp. 284 - 307.

- Dovrebbe essere definito un livello di granularità nella profilazione, allo scopo di garantire adeguatamente la privacy degli individui che possono potenzialmente essere collegati a tale profilazione.

- Dovrebbero essere sviluppati dei protocolli volti a prevenire o ridurre la possibilità di reidentificazione degli utenti i cui dati siano stati trattati per la profilazione. Essi devono includere un compromesso giuridicamente vincolante di non cercare tale reidentificazione nonché l'adozione di misure volte a evitare la reidentificazione involontaria.

Oltre alla distinzione iniziale tra dati personali e non personali, bisogna considerare, all'interno dei dati personali, **se si tratta di categorie particolari di dati personali**. Questa distinzione è importante nella misura in cui le condizioni di trattamento dei dati variano a seconda che si tratti o meno di categorie particolari di dati (Articolo 9 RGPD).

Infine, bisognerebbe riflettere sui **dati derivati o inferiti**. C'è stata qualche controversia sul se i dati derivati, e in particolare i profili personali, debbano essere considerati o meno come proprietà intellettuale. A prescindere da ciò, va ricordato che secondo l'Articolo 4(1) RGPD **tali dati sono dati personali nella misura in cui si riferiscono a una persona identificata o identificabile.** Va aggiunto che è possibile trarre conclusioni relative a ciò che l'Articolo 9 dell'RGPD considera categorie particolari di dati da dati personali ordinari o anche da dati non personali combinati con altri dati personali (privacy di gruppo) [10]. Nella misura in cui queste inferenze si riferiscono a una persona identificata o identificabile, dovrebbero essere trattate come categorie particolari di dati, indipendentemente dalla loro comprensione (o meno) come oggetto di proprietà intellettuale.

2 Passi preliminari: le questioni cruciali da considerare

In questa sezione, forniamo alcuni consigli generali su come affrontare un progetto di ricerca nelle **prime fasi del suo ciclo di produzione,** ovvero quando non è ancora poco più di un'idea che non è ancora stata implementata. È importante tenerli in considerazione se si vuole assicurare l'implementazione di politiche di protezione dei dati fin dalla progettazione (cfr. la sezione "Protezione dei dati fin dalla progettazione e per impostazione predefinita" nella parte Concetti dei presenti Orientamenti).

I consigli essenziali sono:

1. Assicurarsi che il proprio progetto sia compatibile con il quadro di protezione dei dati
2. Attuare un programma di formazione su questioni etiche e legali per gli sviluppatori delle TIC e altre parti interessate
3. Definire i ruoli giocati da tutti gli agenti coinvolti nel trattamento
4. Promuovere l'impegno degli utenti finali

[10] Cfr. in generale Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) *Group Privacy: new challenges of data technologies*, Dordrecht, Springer.

2.1 Assicurarsi che il proprio progetto sia compatibile con i valori fondamentali dell'UE

Prima di considerare l'uso dei dati raccolti dai social network per il progetto, lo sviluppatore dovrebbe avere chiaro in mente il suo obiettivo primario. Potrebbe accadere, ad esempio, che quest'uso non sia compatibile con gli standard etici e legali dell'UE inclusi nella Carta dei diritti fondamentali dell'UE. **In tal caso, il progetto non dovrebbe essere approvato**. D'altra parte**, se un'analisi mostra che il trattamento necessario non sarà accettabile sulla base della politica degli sviluppatori del social network, dell'RGPD e/o del quadro giuridico complementare, il progetto non dovrebbe essere approvato nemmeno in questo caso.** Infine, gli sviluppatori devono valutare se il progetto è accettabile secondo gli standard etici, nonostante sia conforme agli obblighi legali (cfr. Privacy fin dalla progettazione e per impostazione predefinita nelle sezioni Azioni e Strumenti della Parte generale dei presenti Orientamenti)

Inoltre, **una chiara idea dell'uso concreto dei dati raccolti attraverso le reti sociali aiuterà i titolari del trattamento a stabilire nelle prime fasi di sviluppo alcune importanti questioni legali relative al trattamento**, come la conformità con la politica dello sviluppatore della rete sociale, l'eventuale necessità di trasferimenti internazionali di dati, l'esistenza di co-titolari o responsabili del trattamento -che devono essere attentamente selezionati-, o le misure di sicurezza e organizzative volte a minimizzare i rischi.

2.2 Attuare un programma di formazione su questioni etiche e legali per gli sviluppatori delle TIC e altre parti interessate

L'attuazione di **programmi di formazione di base** per i ricercatori/innovatori coinvolti nel trattamento potrebbe essere estremamente utile al fine di evitare problemi di protezione dei dati durante il trattamento dei dati ottenuti dai social media. Alcune risorse utili a questo scopo sono, ad esempio, disponibili presso l'Agenzia per i diritti fondamentali[11], IEEE e i suoi Orientamenti etici[12], e la Commissione europea[13]. **Questa formazione dovrebbe includere anche una profonda comprensione della politica di sviluppo della rete sociale da cui i dati saranno raccolti.**

Se la formazione non è possibile, implementare la consulenza di un **esperto esterno** sin dall'inizio del progetto potrebbe essere un'alternativa accettabile. Se i ricercatori/innovatori stanno raccogliendo dati da una determinata rete sociale, questa formazione dovrebbe includere un'attenta analisi della sua particolare politica di sviluppo. Un coinvolgimento precoce degli RPD delle istituzioni partecipanti è altamente consigliato.

È altamente raccomandabile anche l'adozione di misure adeguate a garantire la riservatezza, l'integrità e la disponibilità dei dati (cfr. la sotto-sezione "Misure a sostegno della riservatezza" nella sezione "Integrità e riservatezza" del capitolo "Principi").

---

[11] https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition e

[12] https://ethicsinaction.ieee.org/

[13] https://ec.europa.eu/justice/smedataprotect/index_en.htm

2.3 Definire i ruoli giocati da tutti gli agenti coinvolti nel trattamento

I concetti di titolare del trattamento, co-titolare e responsabile del trattamento giocano un ruolo cruciale nell'applicazione dell'RGPD, poiché stabiliscono chi è responsabile del rispetto delle diverse norme sulla protezione dei dati e come gli interessati possono esercitare i loro diritti nella pratica[14](cfr. la parte "Attori principali" dei presenti Orientamenti, soprattutto le sezioni dedicate al "Titolare del trattamento" o al "Responsabile del Trattamento"). Nel caso dell'uso dei social network per il trattamento dei dati, è altrettanto importante distinguere adeguatamente il titolare del trattamento dei dati dal responsabile del trattamento, poiché le responsabilità di ciascuno sono diverse.

Possono sorgere dubbi su quale delle parti coinvolte in questo quadro svolga il ruolo di titolare del trattamento, responsabile del trattamento o, se del caso, vi sia una situazione di controllo congiunto. **Per dissipare questi dubbi,** dobbiamo innanzitutto consultare l'elenco delle definizioni dell'RGPD, interpretate in conformità con le Linee guida CEPD 7/2020 sui concetti di titolare e responsabile del trattamento nell'RGPD e le Linee guida CEPD 8/2020 sul targeting degli utenti di social media [15]e la relativa giurisprudenza della CGUE[16].

In relazione all'uso dei social network per la ricerca, e fatte salve le precauzioni casistiche di cui sopra, si potrebbe affermare che **non esiste una situazione di titolarità congiunta, in quanto i mezzi e le finalità di ogni attività di trattamento non sono determinati congiuntamente dal social network e dall'istituzione incaricata dello sviluppo delle TIC, ma, piuttosto, il social network permette allo sviluppatore di utilizzare il suo ambiente.** La relazione tra i ricercatori e le reti sociali è, di solito, costruita sulle cosiddette Politiche dello sviluppatore. La maggior parte dei social network consente ai ricercatori/innovatori di raccogliere dati attraverso le loro Interfacce di programmazione di applicazioni (API) solo se seguono le istruzioni stabilite in tali politiche. Pertanto, i ricercatori/innovatori devono assicurarsi di procedere effettivamente in tal senso se vogliono evitare di assumersi la responsabilità di un trattamento illecito dei dati. Naturalmente, esiste una possibile eccezione a questa regola generale: se uno sviluppatore assume i servizi di un social network per il trattamento dei dati per suo conto, questo può comportare un controllo congiunto (dipenderà dalle condizioni concrete del contratto e dal modo in cui le responsabilità sui dati sono assegnate ai partner). Tuttavia, se tale eccezione non si applica:

- il social network è considerato il titolare del trattamento in relazione al trattamento dei dati che esso realizza in conformità con le finalità e gli obiettivi che persegue, e lo sviluppatore TIC è il titolare del trattamento dei dati in relazione alle attività di trattamento dei dati sotto il suo controllo;
- la relazione tra lo sviluppatore e il social network è la seguente:

[14]Linee guida CEPD 07/2020 sui concetti di titolare del trattamento e responsabile del trattamento nell'RGPD, pag. 3, disponibile all'indirizzo: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en .

[15] Linee guida CEPD (Linee guida 8/2020 sul targeting degli utenti di social media Versione 2.0 Adottate il 13 aprile 2021, disponibile all'indirizzo: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf, p. 11).

[16] Le sentenze in Wirtschaftsakademie (C-210/16), Jehovah's Witnesses (C-25/17) e Fashion ID (C-40/17) sono, qui, particolarmente rilevanti.

    - il social network svolge il ruolo di fornitore di servizi della società dell'informazione, e
    - l'istituto di ricerca il ruolo di utente del servizio della società dell'informazione.
- le attività svolte dall'istituto di ricerca a partire dal suo profilo di ricerca devono essere autorizzate dal social network, in quanto fornitore di servizi della società dell'informazione, ma ciò non implica che ci sia una situazione di titolarità congiunta né che la licenza di utilizzo dei dati garantisca una base giuridica per il trattamento dei dati personali.

Così, negli scenari più comuni, i ricercatori e gli innovatori delle TIC giocheranno il ruolo di terzo rispetto alle reti sociali e agli interessati. La rete fornirà loro i dati che appartengono agli interessati. Una volta che questi dati sono già sotto il controllo dei ricercatori/innovatori, essi diventano titolari del trattamento di quei dati e si assumono le responsabilità corrispondenti.

Sebbene non esista generalmente una situazione di titolarità congiunta, non è del tutto impossibile che una tale situazione si verifichi. Vale, quindi, la pena ricordare **le garanzie dell'Articolo 26 dell'RGPD in caso di titolarità del trattamento congiunta** (cfr. la sezione "Attore principale" della Parte generale dei presenti Orientamenti) **tra il social network e l'istituto di ricerca:**

- Sia lo sviluppatore TIC che il social network determinano in modo trasparente le rispettive responsabilità per il rispetto degli obblighi previsti dall'RGPD, in particolare per quanto riguarda l'esercizio dei diritti dell'interessato e i rispettivi obblighi di fornire le informazioni di cui agli Articoli 13 e 14, mediante **un accordo tra di loro.**
- L'accordo
    - deve essere messo a disposizione dell'interessato;
    - può designare un punto di contatto per gli interessati;
    - riflette debitamente i rispettivi ruoli e relazioni dei co-titolari del trattamento nei confronti degli interessati.
- Infine, tutti i titolari del trattamento, i co-titolari e i responsabili del trattamento devono ricordare che l'interessato può esercitare i suoi diritti ai sensi dell'RGPD (Art. 26, paragrafo 3 RGPD).

2.4 Preparare i contratti con il social network e (se del caso) con i co-titolari del trattamento, responsabili del trattamento, ecc. e documentarli

Raccogliere dati dai social network, spesso, comporta la stipula di un qualche tipo di accordo con i loro rappresentanti. Infatti, l'accesso alle loro API, o strumenti simili, probabilmente, non sarà fornito se questo accordo non è stato documentato. A volte, l'adesione alle politiche degli sviluppatori non fa nemmeno parte di questo accordo, dal momento che è chiarissimo che chiunque riceva dati dalla rete deve seguirle. Il ricercatore/innovatore dovrebbe assicurarsi, comunque, che questa architettura legale sia adeguatamente definita fin dall'inizio.

D'altra parte, è ovvio che un titolare del trattamento, spesso, affiderà alcuni dei compiti tecnici a un responsabile del trattamento, che potrebbe anche coinvolgere un sotto-responsabile. Nella pratica, tuttavia, ci saranno momenti in cui sarà difficile garantire che il

responsabile del trattamento non stia effettivamente agendo come titolare o co-titolare del trattamento.

I ricercatori e gli innovatori dovrebbero fare del loro meglio per evitare tali problemi, poiché il regolamento in materia di protezione dei dati richiede una risposta chiara alla domanda "chi è responsabile di questo trattamento?" per garantire una protezione "efficace e completa" dei diritti e delle libertà degli interessati.[17] Quindi, un requisito fondamentale di un'adeguata politica di protezione dei dati fin dalla progettazione è quello **di chiarire sin dall'inizio chi sono i titolari formali del trattamento dei dati e i responsabili del trattamento, al fine di garantire che la responsabilità legale sia chiara.**

Per raggiungere quest'obiettivo, gli **accordi scritti tra tutti gli agenti coinvolti nello sviluppo degli strumenti dovrebbero essere conclusi e documentati, quando possibile (cfr. art. 28 dell'RGPD).** Questi dovrebbero includere descrizioni chiare delle responsabilità assunte da tutti i partecipanti. Promuovere un'interazione continua tra tutti gli RPD coinvolti potrebbe essere un'ottima opzione. Possono essere adottati organi e strumenti di controllo ad hoc per garantire una supervisione regolare del trattamento dei partecipanti.

2.5 Promuovere l'impegno degli utenti finali

Poiché le TIC implicano l'uso di dati personali di diversi tipi di soggetti, è altamente raccomandabile ascoltare le voci dei rappresentanti delle collettività coinvolte, in modo da garantire che le politiche di Protezione dei dati fin dalla progettazione (cfr. la sotto-sezione "Protezione dei dati fin dalla progettazione e per impostazione predefinita" nella sezione "Concetti principali" della Parte generale dei presenti Orientamenti) siano in linea con i loro interessi, diritti e libertà. Organizzare alcune **discussioni preliminari** con questi rappresentanti garantisce l'implementazione di un quadro dal basso verso l'alto che potrebbe essere molto utile a questo scopo.

Lista di controllo: Comprensione del progetto

- ☐ L'uso dei dati raccolti tramite i social network non promuove scenari incompatibili con i valori fondamentali dell'UE.
- ☐ Lo sviluppo delle TIC non comporta un uso sproporzionato dei dati personali raccolti attraverso le reti sociali
- ☐ Il titolare del trattamento ha garantito che i membri del team che trattano i dati personali hanno ricevuto una formazione adeguata sulla politica dello sviluppatore

[17] Cfr.: Linee guida CEPD (Linee guida 8/2020 sul targeting degli utenti di social media Versione 2.0 Adottata il 13 aprile 2021, disponibile all'indirizzo: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf, p. 11)

corrispondente al social network da cui i dati saranno estratti, e sui concetti fondamentali in materia di questioni di protezione dei dati

 Fin dall'inizio del progetto sono stati implementati adeguati strumenti di valutazione sulla protezione dei dati

 I ruoli giocati da tutti i diversi agenti coinvolti nel trattamento dei dati sono stati adeguatamente chiariti attraverso gli accordi corrispondenti e il titolare del trattamento può fornirne prova.

 Lo sviluppatore TIC è ben consapevole dei termini di utilizzo dei dati raccolti dalle reti sociali

 I rappresentanti dei collettivi principali coinvolti nel trattamento dei dati sono stati consultati in merito all'impatto dell'uso dei dati raccolti e alla rete sociale concreta selezionata.

3 Ottenere l'accesso ai dati. Alcuni suggerimenti essenziali

Ai sensi dell'RGPD, un trattamento lecito richiede una base giuridica (cfr. la sotto-sezione "Liceità, equità e trasparenza" nella sezione Principi fondamentali della Parte Generale dei presenti Orientamenti). Se il trattamento coinvolge il tipo di attività incluse nel Regolamento ePrivacy, le disposizioni di questo nuovo strumento saranno applicate non appena sarà approvato. Attualmente, l'Articolo 6 dell'RGPD definisce un totale di sei possibili basi giuridiche. Nel caso del trattamento dei dati dei social network, è essenziale sottolineare che i **ricercatori o innovatori delle TIC devono essere consapevoli che avranno certamente bisogno di basi giuridiche diverse per il trattamento dei dati al momento dell'accesso ai dati e al momento di eseguire la loro ricerca o innovazione basata su quei dati.** Nel primo caso, ciò che è necessario è una base giuridica per ottenere i dati dalla rete sociale. Nel secondo caso, si tratta di trovare una base che consenta di utilizzare i dati, già legittimamente acquisiti, per finalità di ricerca. **È essenziale notare che il semplice fatto che gli interessati abbiano pubblicato i loro dati in spazi pubblici online non ne consente il trattamento.** Si tratta sempre di dati personali, anche se i dati sono accessibili al pubblico. La pubblicazione potrebbe servire per evitare il divieto incluso nell'Articolo 9, paragrafo 1 dell'RGPD, se stiamo parlando di dati di categorie particolari, ma non serve come base giuridica per il trattamento. **Per cui, le aziende non possono riutilizzare liberamente i dati, e non possono trattarli ulteriormente all'insaputa degli interessati e senza una base adeguata per un trattamento legittimo.**

3.1 Pubblico dominio non significa dati pubblici!

Il **concetto di "dominio pubblico" deve essere adeguatamente analizzato nel contesto dei social network.** Se il ricercatore o l'innovatore delle TIC ha dovuto registrarsi presso una comunità di utenti per avere accesso a dati specifici, questi dati non sono pubblici: sono dati

che gli interessati hanno voluto condividere esclusivamente con una comunità di utenti e secondo i termini e le condizioni determinati dal social network in questione, che vengono accettati nel momento in cui gli utenti creano i loro profili. Se i ricercatori sono in grado di accedere a un profilo o ad altri tipi di dati dei social media su un sito semplicemente perché sono utenti registrati, ciò non equivale a dire che quelle informazioni sono disponibili al pubblico. È, quindi, assolutamente essenziale per il ricercatore o l'innovatore TIC avere una conoscenza precisa di questi termini e condizioni, che possono differire sostanzialmente da un social network all'altro.

Inoltre, anche se i dati sono di dominio pubblico, ciò non significa affatto che possiate usarli per finalità diverse da quelle per cui sono stati resi pubblici. Ciò è estremamente importante, perché altrimenti potreste andare incontro a responsabilità legali.

Il caso Equifax: l'utilizzo di dati dello spazio pubblico non legittima necessariamente il trattamento

Equifax è una società che ha ottenuto dati dal portale d'informazione utilizzato dalle amministrazioni pubbliche per trasmettere informazioni ai cittadini. Da questi dati ha creato un archivio che, presumibilmente, trasmetteva informazioni sulla solvibilità dei cittadini. Il tutto, senza informare gli interessati di queste operazioni di trattamento e utilizzando l'interesse legittimo della società come base di legittimità. Il 26 aprile 2021, l'Agenzia spagnola per la protezione dei dati (AEPD) ha multato Equifax con 1 milione di euro per violazione delle norme sulla protezione dei dati, ha vietato l'uso continuato di quest'archivio, ha ordinato la cancellazione di tutti i dati degli interessati e ha ordinato a Equifax di notificare a tutte le aziende che hanno consultato il suo archivio il contenuto di questo Provvedimento affinché facciano lo stesso e cessino l'uso questi dati.

Questa sentenza è di grande importanza per diversi motivi. Il primo è che è la prima grande sanzione derivante dal cambiamento di criteri apportato dall'RGPD e dalla normativa nazionale (LOPDgdd) relativi all'uso di fonti accessibili al pubblico: il fatto che i dati siano accessibili al pubblico non significa che possano essere utilizzati per qualsiasi finalità e senza ulteriori spiegazioni. Nella precedente legge spagnola, la LOPD del 1999, questo criterio non era così chiaro e sembrava esprimere il contrario.

Nel suo Provvedimento, l'AEPD ha ricordato che (1) qualsiasi uso secondario dei dati deve essere compatibile con la finalità originaria per la quale sono stati raccolti (principio di limitazione della finalità del trattamento dei dati, articolo 5, paragrafo 1, lettera b) RGPD), (2) deve avere la sua base di legittimazione (non è sufficiente asserire che i dati provengono da fonti pubblicamente accessibili), e che (3) l'interessato deve essere informato dell'uso secondario dei suoi dati. La multa di 1 milione di euro era basata sulla violazione del principio di limitazione della finalità.

3.2 Ottenere l'accesso ai dati di un social network: alcuni consigli essenziali

Questi sono alcuni consigli essenziali forniti dalle informazioni etiche per la linguistica e la lingua inglese[18] che devi seguire se hai intenzione di accedere ai dati di un social network:

- Se i dati sono di dominio pubblico, è necessario rispettare tutti i requisiti dichiarati dal fornitore del corpus, anche per quanto riguarda l'anonimato, o qualsiasi altra condizione d'uso.
- Alcuni corpora possono richiedere l'approvazione etica, specialmente i corpora che includono dati sulla salute fisica o mentale, o quelli che contengono dati che potrebbero essere usati per de-anonimizzare gli individui (ad esempio, quando sono consentite risposte a testo libero).
- Se i dati non sono di dominio pubblico, devi assicurarti che il tuo uso dei dati sia conforme a qualsiasi requisito dichiarato dal fornitore del corpus. Ad esempio, i dati non devono essere condivisi in modo non autorizzato (ad esempio, pubblicati online).
- In entrambi i casi, se c'è motivo di sospettare che le persone che inizialmente hanno fornito i dati non erano consapevoli che sarebbero stati usati per finalità di ricerca, dovresti considerare attentamente le implicazioni etiche della tua ricerca, incluso se sia necessario ottenere il consenso informato.

Tutti questi consigli possono essere concretizzati nei seguenti passi:

- In primo luogo, tenere sempre presente le **ragionevoli aspettative degli interessati sull'uso dei loro dati (Considerando 47, RGPD).** Questo è essenziale nella maggior parte delle politiche degli sviluppatori di social network. Ad esempio, la politica degli sviluppatori di Twitter afferma che "vietiamo l'uso dei dati di Twitter in qualsiasi modo che non sia coerente con le ragionevoli aspettative di riservatezza delle persone. Sfruttando l'API di Twitter o accedendo ai contenuti di Twitter, hai un ruolo speciale da svolgere nella salvaguardia di questo impegno, soprattutto in termini di rispetto della privacy delle persone e fornendo loro trasparenza e controllo su come i loro dati vengono utilizzati." [19]

- In secondo luogo, ottenere l'approvazione per accedere alle API e ai contenuti di un social network non è mai sufficiente a garantire un trattamento lecito dei dati. È solo il primo passo. La maggior parte dei social network ha sviluppato **Orientamenti dettagliati per l'uso della piattaforma, che i ricercatori devono seguire rigorosamente per garantire la conformità con la politica per l'uso previsto delle piattaforme e il rispetto dei requisiti etici e legali di protezione dei dati.**

- In terzo luogo, la maggior parte dei social network ha sviluppato strumenti che **forniscono supporto ai ricercatori** che intendono utilizzare le loro Interfacce di programmazione di applicazioni (API). È sempre consigliabile che i ricercatori utilizzino questi servizi in caso di dubbi sul trattamento dei dati.

- In quarto luogo, i ricercatori e gli innovatori non dovrebbero, tuttavia, mai dimenticare che, in qualità di titolari del trattamento, hanno la responsabilità di garantire che il quadro di protezione dei dati sia adeguatamente rispettato. Così, dovresti controllare se le dichiarazioni sulla legittimità del trattamento dei dati effettuato dai social network corrispondono alla realtà. Rivedere le loro politiche di raccolta dei dati per

[18] https://resource.ppls.ed.ac.uk/lelethics/index.php/frequently-asked-questions/corpus-research/
[19] https://developer.twitter.com/en/developer-terms/policy

verificare la solidità dei consensi concessi dal punto di vista dell'RGPD sembra un requisito necessario o, almeno, prudente.

- Quinto, i ricercatori/innovatori devono tenere presente che i social network **possono modificare le loro politiche periodicamente** senza preavviso. Poiché, di solito, introducono questa precauzione nelle loro politiche, i ricercatori si assumono la responsabilità di mantenersi informati su queste possibili modifiche. Pertanto, si raccomanda vivamente di rivedere periodicamente tali politiche.
- In sesto luogo, poiché i ricercatori tratteranno dati che non sono stati ottenuti dalla persona interessata, essi devono fornire alla persona interessata le informazioni richieste dall'articolo 14, salvo che non si applichi una delle circostanze citate al punto 5.
- Infine, in caso di dubbi, consultare sempre il proprio Responsabile per la protezione dei dati e, se necessario, la corrispondente Autorità di protezione dei dati.

Riquadro: Considerare le aspettative e le preoccupazioni degli interessati. Il caso Twitter

La maggior parte dei ricercatori che utilizzano set di dati di tweet non ottengono il consenso da ogni utente di Twitter il cui tweet viene raccolto, né questi utenti sono, in genere, avvisati dal ricercatore.

Nel 2017, Fiesler e Proferes hanno elaborato un sondaggio esplorativo sulle percezioni degli utenti di Twitter in merito all'uso dei tweet nella ricerca. Al momento in cui questa ricerca è stata eseguita, la politica in materia di privacy di Twitter menzionava che gli accademici potevano usare i tweet come parte della ricerca. Tuttavia, pochi utenti erano a conoscenza di questo fatto, e la maggioranza riteneva che i ricercatori non dovessero essere in grado di utilizzare i tweet senza consenso. Tuttavia, questi atteggiamenti erano altamente contestuali e differivano in relazione a fattori quali il modo in cui la ricerca veniva condotta o divulgata, chi erano i ricercatori e di cosa trattava lo studio.

Fonte: Fiesler C, Proferes N. "Participant" Perceptions of Twitter Research Ethics. Social Media + Società. Gennaio 2018. doi:10.1177/2056305118763366

I ricercatori e gli innovatori che utilizzano i dati ottenuti dalle reti sociali sono responsabili del rispetto di tutte le politiche stabilite da quelle reti. Pertanto, è essenziale che essi esaminino e comprendano queste politiche prima di accedere alle API e ai contenuti dei social network. Il tempo impiegato a rivedere le loro politiche può far risparmiare ai ricercatori ore di lavoro ulteriore in un momento successivo e può anche aiutarli ad evitare responsabilità legali.

Lista di controllo. Ottenere l'accesso ai dati

□ Se i dati sono di dominio pubblico, i titolari del trattamento hanno rispettato i requisiti indicati dal fornitore del corpus, anche per quanto riguarda l'anonimato, o qualsiasi altra condizione d'uso.

□ Se i dati non sono di dominio pubblico, i titolari del trattamento si sono assicurati che il loro uso dei dati sia conforme ai requisiti indicati dal fornitore del corpus.

□ I titolari del trattamento conoscono gli Orientamenti per l'uso della piattaforma, che devono seguire rigorosamente per garantire la conformità alla politica per l'uso pianificato delle piattaforme e il rispetto dei requisiti etici e legali in materia di protezione dei dati.

□ I titolari del trattamento hanno considerato le ragionevoli aspettative degli interessati sull'uso dei loro dati.

□ I titolari del trattamento hanno verificato se le dichiarazioni sulla legittimità del trattamento dei dati effettuate dalle reti sociali corrispondono alla realtà

□ I ricercatori/titolari del trattamento sono consapevoli della loro responsabilità di mantenersi informati di possibili modifiche nelle politiche della piattaforma. Vengono effettuate revisioni periodiche di tali politiche

□ I titolari del trattamento forniscono agli interessati le informazioni richieste dall'articolo 14, fatta salva l'applicazione di una delle circostanze citate al punto 5

4 Scegliere una base giuridica per l'ulteriore trattamento

Quando i ricercatori/innovatori diventano i titolari del trattamento dei dati raccolti dai social network, devono decidere la base giuridica che legittimerà l'ulteriore trattamento di quei dati il più presto possibile. Tuttavia, e anche prima di selezionare la base (o le basi) giuridica per il trattamento, il titolare del trattamento deve considerare se il trattamento riguarda dati personali di categorie particolari. In tal caso, il titolare del trattamento deve essere consapevole del fatto che il trattamento è soggetto al veto dell'Articolo 9, paragrafo 1 dell'RGPD, fatta salva l'applicazione di una delle circostanze descritte nell'Articolo 9, paragrafo 2.

Una volta concluso che non sono coinvolti dati di categorie particolari o che il veto posto è stato adeguatamente affrontato, il titolare del trattamento deve selezionare la base giuridica appropriata per il trattamento dei dati. Ciò deve essere fatto con molta attenzione, poiché la base giuridica non può essere modificata durante il trattamento. Questi sono alcuni criteri che dovrebbero essere tenuti in considerazione a questo scopo:

- La necessità o l'utilità dell'uso dei dati ottenuti dai social network per il raggiungimento della finalità o dell'interesse del trattamento deve essere sufficientemente giustificata nell'ambito della base giuridica scelta.
- Il titolare del trattamento dei dati deve ponderare attentamente (1) la base di diritto utilizzata, contro (2) i possibili rischi derivanti dal trattamento dei dati.

- Inoltre, il titolare del trattamento deve considerare tutte le tutele adeguate a garantire che gli interessi, i diritti e le libertà dell'interessato siano adeguatamente preservati. Questo bilanciamento deve essere particolarmente attento se il consenso dell'interessato funge da base giuridica per il trattamento.

Le seguenti tabelle forniscono una breve panoramica delle varie basi alternative di legittimazione secondo gli Articoli 6 e le circostanze che eludono il veto creato dall'Articolo 9, paragrafo 1 dell'RGPD e la loro relazione con il trattamento dei dati provenienti da social media.

Il consenso è la base giuridica più tradizionale per il trattamento dei dati nel contesto dei social network. Tuttavia, quando un titolare del trattamento cerca di trattare dati personali per finalità di ricerca, l'interesse pubblico potrebbe essere un'ottima opzione. Sfortunatamente, essa richiede l'applicazione di certe condizioni (crf. la sotto-sezione "Protezione dei dati e ricerca scientifica" nella parte "Concetti principali" della parte generale dei presenti Orientamenti). L'interesse legittimo, d'altra parte, è una base giuridica alternativa adatta per il trattamento in questo contesto, ma non si può presumere che sarà sempre appropriato[20]. È probabile che sia più appropriato quando i titolari del trattamento utilizzano i dati delle persone in modi che essi si aspetterebbero ragionevolmente e con il minor impatto possibile sulla protezione dei dati o sulla privacy, o quando c'è una giustificazione convincente per il trattamento. [21]

Basi giuridiche possibili (Art. 6 RGPD)

Basi giuridiche per il trattamento	**Uso nel contesto dei social network**
6.1.a -consenso	Probabilmente, la base giuridica più popolare per il trattamento dei dati, anche se il suo uso diffuso è sempre più messo in discussione[22](cfr. la sezione seguente)
6.1.e - il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso con l'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Può essere applicabile, ma bisogna osservare le seguenti precauzioni: - La finalità di interesse pubblico deve essere chiaramente identificata, così come la

[20] Ad es., le autorità pubbliche possono fare affidamento su interessi legittimi solo se stanno realizzando il trattamento per un motivo legittimo diverso dall'esecuzione delle loro funzioni come autorità pubblica, quindi la "funzione pubblica" è una base giuridica migliore in queste situazioni (ICO: interessi legittimi, disponibile all'indirizzo: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/).

[21] ICO: interessi legittimi, disponibile all'indirizzo: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/).

[22] Cfr. sul trattamento dei dati a fini sanitari nel sistema americano della privacy, Charlotte A. Tschider, ´The consent myth: improving choice for the patients of the future´ (2019) 96 Washington University Law Review 1506.

	connessione con la ricerca, - Bisogna motivare perché l'uso dei dati dei social media è necessario o altamente auspicabile per gli obiettivi perseguiti. - La base del trattamento è stata stabilita dal diritto dell'Unione o dal diritto di uno Stato membro al quale è soggetto il titolare del trattamento.
6.1.f - il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore	Può essere applicabile e, in effetti, è la migliore alternativa al consenso come base di legittimità. È necessario osservare le seguenti precauzioni: - il titolare del trattamento deve effettuare e motivare un bilanciamento adeguato tra (1) l'interesse legittimo perseguito e (2) l'impatto sui diritti e le libertà fondamentali dell'interessato; questo bilanciamento deve essere effettuato con particolare attenzione se sono coinvolti dati di minori

Categorie particolari di dati personali (Art. 9 RGPD)

Base di legittimità	**Uso nel contesto delle reti sociali**
9.1.a -consenso	È ampiamente usato
9.2.e - il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato	Può essere applicabile, ma bisogna prestare particolare attenzione alle seguenti garanzie: - rispetto del principio di limitazione della finalità (art. 5, paragrafo 1, lettera b RGPD), tenendo conto delle aspettative dell'interessato e del contesto (reti sociali e impatto del profilo) in cui i dati sono stati pubblicati[23]; - misure di aggregazione per ridurre le possibilità di re-identificazione
9.2.g - il trattamento è necessario	Può essere applicabile, a condizione che il

[23] Recentemente, il Comitato spagnolo per la protezione dei dati ha multato Equifax per aver utilizzato i dati di solvibilità creditizia pubblicati da fonti ufficiali per alimentare i propri archivi, per violazione del principio di limitazione della finalità, nella misura in cui si tratta di un uso incompatibile dei dati, pur essendo dati accessibili al pubblico. Il criterio di questo Provvedimento può essere applicabile anche se vengono utilizzati dati pubblicati dalla stessa persona interessata, nella misura in cui gli usi derivati da tali dati sono incompatibili.

per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato	titolare del trattamento osservi le seguenti precauzioni: - l'interesse pubblico perseguito deve essere chiaramente identificato, così come la normativa applicabile; - deve essere sufficientemente giustificato che la ricerca attraverso i social network è necessaria o molto adatta a questa finalità; - si deve prestare particolare attenzione a sviluppare misure di protezione da impatti indebiti sui diritti fondamentali degli interessati.
9.2.j - il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato	È pienamente applicabile. Ha il vantaggio che il principio di limitazione della finalità è meno rigido (cfr. Art. 5., paragrafo 1, lettera b) RGPD) e che consente il trattamento dei dati indipendentemente dal consenso degli interessati, a condizione che il titolare del trattamento osservi le seguenti garanzie: - deve identificare chiaramente la sua finalità (archiviazione, ricerca scientifica, ricerca storica o fini statistici); - deve giustificare la proporzionalità del trattamento dei dati rispetto alla finalità perseguita; - dovrebbe giustificare l'utilità dell'uso dei social network nella ricerca; - deve sviluppare misure volte a evitare impatti indebiti sui diritti fondamentali degli interessati, concentrandosi su (1) un livello sufficiente di aggregazione e (2) altre garanzie per evitare la reidentificazione - deve seguire rigorosamente le prescrizioni dell'art. 89 RGPD

4.1 Consenso

Il consenso è la prima delle sei basi per il trattamento legittimo dei dati personali elencate nell'Articolo 6. Ai sensi dell'Articolo 6, paragrafo 1, lettera a) [24], tale trattamento è lecito se

[24] CEPD: Linee guida 05/2020 sul consenso ai sensi del Regolamento 2016/679, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità. Quindi, se i dati sono utilizzati per più finalità, il consenso deve essere prestato per ogni finalità separatamente. Il consenso specifico è la chiave per evitare un consenso non valido. Infatti, "se un trattamento di dati ha più finalità, allora il consenso deve essere richiesto per ciascuna di esse". La specificità del consenso promuove la trasparenza in quanto l'interessato conosce ogni finalità del trattamento dei dati, aumenta il suo controllo su queste finalità e protegge dal function creep." [25]

Il requisito di specificità è particolarmente importante nel caso del riutilizzo dei dati dei social network. Gli utenti finali delle reti sociali sono, spesso, inconsapevoli del fatto che i loro dati vengono utilizzati per finalità diverse da quelle che perseguono quando forniscono quei dati. Tuttavia, la maggior parte dei social network garantisce che gli interessati forniscano il consenso a questa ulteriore elaborazione e le loro politiche per gli sviluppatori copriranno sicuramente questo problema. I ricercatori e gli sviluppatori che intendono trattare i dati ottenuti dalle reti sociali per finalità di ricerca potrebbero ottenere un nuovo consenso dagli interessati. Ciò, naturalmente, è difficile e non sempre necessario. Potrebbero fare affidamento sul consenso originale fornito dall'interessato al social network. Tuttavia, **i ricercatori/innovatori dovrebbero, comunque, assicurarsi che il trattamento che intendono eseguire sia consentito dal consenso originariamente fornito dall'interessato o trovare una base giuridica alternativa (chiedendo un nuovo consenso o utilizzando il legittimo interesse o l'interesse pubblico come alternativa, ad esempio).** Consultare le condizioni d'uso della rete sociale e il consenso raccolto in origine è un ottimo modo per verificare se l'uso secondario dei dati potrebbe essere considerato compatibile con le finalità per cui i dati furono originariamente raccolti (cfr. la sotto-sezione "Principio di limitazione della finalità" nella sezione Principi della Parte generale dei presenti Orientamenti).

Se la ricerca prevede l'utilizzo di **dati raccolti da diversi social network**, i ricercatori dovrebbero concentrarsi sulla **progettazione di meccanismi di valutazione del rischio per la privacy intra-provider ed eventualmente inter-provider che tengano conto dei dati personali rivelati per tutte le attività di trattamento dei dati per una determinata rete sociale e per tutte le altre RS che un soggetto utilizza, rispettivamente.**

Infine, ma non meno importante, poiché i ricercatori tratteranno dati che non sono stati ottenuti dall'interessato, dovranno fornire a quest'ultimo le informazioni richieste dall'articolo 14, fatta salva l'applicazione di una delle circostanze citate al punto 5 (cfr. la sotto-sezione "Diritto all'informazione" nella sezione Diritti dell'interessato dei presenti Orientamenti).

Riquadro: il caso dei dati cancellati

Alcuni utenti di reti sociali pubblicano dati sulle loro piattaforme e, successivamente, li cancellano. Se quei dati sono stati recuperati da un ricercatore prima della cancellazione, non è chiaro se il consenso iniziale dell'utente per l'utilizzo dei suoi dati rimanga intatto. A seconda della sensibilità dei dati e dell'analisi, i ricercatori dovrebbero stabilire in anticipo come gestire questo problema. Ad esempio, potrebbe non essere necessario cancellare il conteggio di un post da una serie temporale, ma potrebbe essere non etico citare un singolo post che è stato poi cancellato. Tuttavia, questa è ancora una questione poco chiara. Pertanto, i ricercatori dovrebbero ancora essere cauti nell'uso dei dati cancellati.

Cfr: Social Media Research Group, Using social media for social research: An introduction esearch
Maggio 2016, pag. 17 disponibile all'indirizzo: ks and
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/524750/GSR_Social_Media_Research_Guidance_-_Using_social_media_for_social_research.pdf Cham.

Lista di controllo: consenso

 I titolari del trattamento sono in grado di dimostrare che, dopo aver valutato le circostanze del trattamento, hanno concluso che il consenso è la base giuridica più appropriata per il trattamento.

 I titolari del trattamento si sono assicurati che il consenso fornito dall'interessato alla rete sociale copra il tipo di trattamento che intendono effettuare

 Se non è questo il caso, i titolari del trattamento devono chiedere agli interessati un nuovo consenso

4.2 Interesse legittimo

L'interesse legittimo costituisce una base alternativa per il trattamento legittimo che potrebbe essere applicabile all'uso dei dati raccolti dalle reti sociali, anche se le autorità pubbliche ***non possono fare*** affidamento su questa base quando agiscono. Per chi può utilizzare questa base giuridica, devono essere soddisfatte tre condizioni cumulative[26]:

(i) il perseguimento di un interesse legittimo da parte del titolare del trattamento dei dati o del terzo o terzi a cui vengono comunicati i dati,

(ii) la necessità di trattare i dati personali per le finalità dei legittimi interessi perseguiti, e

(iii) a condizione che i diritti e le libertà fondamentali del soggetto i cui dati richiedono protezione non abbiano la precedenza.

Così, in linea di principio, l'interesse legittimo potrebbe essere la base giuridica perfetta per il trattamento in questo contesto. Tuttavia, ci sono alcune buone ragioni per ritenere che questa base non sarà sempre applicabile all'uso dei dati per la ricerca scientifica:

- In primo luogo, l'interesse legittimo dovrebbe applicarsi a tutti i co-titolari, nel caso in cui la co-titolarità si applichi al trattamento. Nel caso Fashion ID, la CGUE ha specificato che in tali circostanze "è necessario che ciascuno di questi titolari del trattamento persegua un interesse legittimo [...] attraverso queste operazioni di trattamento affinché esse siano giustificate nei confronti di ciascuno di essi".
- In secondo luogo, i titolari del trattamento dovrebbero essere in grado di dimostrare che il test di bilanciamento è stato adeguatamente eseguito (cfr. la sezione "Test di bilanciamento" nella parte "Azioni e strumenti" dei presenti Orientamenti). Ciò significa che i co-titolari sono in grado di stabilire che il trattamento è necessario per raggiungere quegli interessi legittimi. Ciò è difficile da raggiungere, poiché "necessario" richiede una connessione tra il trattamento e gli interessi perseguiti. Ciò significa che si dovrebbe considerare se sono disponibili altri mezzi meno invasivi per raggiungere la stessa finalità. Allo stesso modo, i responsabili del trattamento

[26] 9 CGUE, Sentenza in Fashion ID, 29 luglio 2019, C-40/17, par. 95 - ECLI:EU:C:2019:629.

dovrebbero essere in grado di dimostrare che i loro legittimi interessi in gioco non sono superati dagli interessi o dai diritti e dalle libertà fondamentali dell'interessato. Tutto questo è difficile da dimostrare, soprattutto se ci sono minori coinvolti nel trattamento. [27]

- In terzo luogo, l'interesse legittimo potrebbe difficilmente applicarsi come base giuridica per un trattamento legittimo se tale trattamento implica pratiche di profilazione e tracciamento intrusivo, ad esempio, quelle che implicano il tracciamento degli individui su più siti web, luoghi, dispositivi, servizi o data-brokering. [28]
- In quarto luogo, invece, se stiamo considerando i dati relativi a soggetti che hanno già avuto una precedente relazione con il ricercatore e innovatore TIC attraverso il social network, l'uso del legittimo interesse come base giuridica sembra abbastanza ragionevole. I titolari del trattamento, tuttavia, dovrebbero prendere in considerazione se la relazione precedente era simile a quella che sta per essere costruita.

Se, alla fine, viene scelto l'interesse legittimo come base giuridica per il trattamento, i titolari del trattamento devono tenere presente che i doveri di trasparenza e il **diritto di opposizione** richiedono un'attenta considerazione. **Gli interessati devono avere la possibilità di opporsi al trattamento dei loro dati per finalità mirate prima che il trattamento venga iniziato.** Gli utenti dei social media non dovrebbero solo avere la possibilità di opporsi al trattamento quando accedono alla piattaforma, ma dovrebbero anche essere dotati di controlli che garantiscano che il trattamento sottostante per finalità specifiche dei loro dati personali non avrà più luogo dopo la loro opposizione al trattamento. [29]

Lista di controllo: interesse legittimo

□ I titolari del trattamento hanno verificato che il legittimo interesse è la base più appropriata per il trattamento.

□ I titolari del trattamento hanno verificato che il trattamento è necessario e non esiste un modo meno invasivo per ottenere lo stesso risultato.

□ I titolari del trattamento hanno effettuato un test di bilanciamento, e sono sicuri che gli

[27] Cfr. il Parere 06/2014 del Gruppo di lavoro dell'articolo 29 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'Articolo 7 della Direttiva 95/46/CE, WP217, 9 aprile 2014 https://ec.europa.eu/justice/Article-29/documentation/opinion- recommendation/files/2014/wp217_en.pdf

[28] Gruppo di lavoro dell'articolo 29, Parere sulla profilazione e sul processo decisionale automatizzato, WP 251, rev. 01, pag. 15, cfr. anche Parere del Gruppo di lavoro dell'articolo 29, sull'interesse legittimo, pag. 32 e 48: "Nel complesso, vi è uno squilibrio tra l'interesse legittimo della società e la protezione dei diritti fondamentali degli utenti e l'Articolo 7, lettera f) non dovrebbe essere invocato come base giuridica del trattamento. L'articolo 7, lettera a) sarebbe una base più appropriata da utilizzare, a condizione che siano soddisfatte le condizioni per un consenso valido".

[29] Linee guida 8/2020 sul targeting degli utenti di social media Versione 2.0 Adottata il 13 aprile 2021, disponibile all'indirizzo: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf, p. 11)

interessi dell'individuo non prevalgono su quelli legittimi.

 I titolari del trattamento non stanno utilizzando i dati delle persone in modi che queste troverebbero intrusivi o che potrebbero causare loro danno, a meno che non ci sia una ragione molto buona.

 Se i titolari del trattamento prevedono il trattamento di dati di minori, si sono ulteriormente preoccupati di assicurarsi che il legittimo interesse sia una base di dati adeguata.

 I titolari del trattamento hanno preso in considerazione misure di salvaguardia per ridurre l'impatto, ove possibile.

 I titolari del trattamento hanno introdotto strumenti adeguati per garantire che il diritto di opposizione sia facile da esercitare da parte degli interessati.

 Se i titolari del trattamento hanno identificato un impatto significativo sulla protezione dei dati personali, hanno considerato la necessità di eseguire anche una DPIA.

 I titolari del trattamento includono informazioni sui loro interessi legittimi nella loro informativa sulla privacy.

4.3 L'interesse pubblico e il quadro della ricerca scientifica

Ai sensi dell'Articolo 6, lettera e) dell'RGPD, il trattamento è lecito se è necessario per l'esecuzione di un compito di interesse pubblico. Qui, bisogna tenere a mente che "ricerca scientifica" è un termine troppo ampio che si riferisce generalmente alla ricerca della conoscenza, attraverso una certa metodologia, in qualsiasi area della conoscenza umana. Così, è molto probabile che se i titolari del trattamento stanno usando una metodologia scientifica e, in qualche modo, cercando la conoscenza tramite l'uso dei dati, tale trattamento potrebbe essere legittimo sulla base della base giuridica dell'interesse pubblico.

Inoltre, l'interesse pubblico potrebbe servire a saltare il veto incluso nell'Articolo 9, paragrafo 1 dell'RGPD se si stanno utilizzando categorie particolari di dati quando altre basi giuridiche (come, ad esempio, la ricerca) non sono applicabili al caso. Tuttavia, in questo caso, il trattamento deve essere basato sul diritto dell'UE o di uno Stato membro e deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure adeguate e specifiche per salvaguardare i diritti fondamentali e gli interessi dell'interessato[30](cfr. la sotto-sezione "Protezione dei dati e ricerca scientifica" nella sezione "Concetti principali" della Parte Generale dei presenti Orientamenti**).**

[30] Cfr. EOSC-Pillar Guidelines ´D4.1: Legal and Policy Framework and Federation Blueprint´ (2021), pag. 76-77. Disponibile all'indirizzo: https://repository.eosc-pillar.eu/index.php/s/tbqe6B7rDycdFCJ#pdfviewer

D'altra parte, si deve ricordare che l'Articolo 5, lettera b) dell'RGPD stabilisce il principio di limitazione della finalità, in base al quale i dati non possono essere trattati per finalità diverse da quelle specifiche iniziali. È interessante notare che quest'articolo prevede che alcune finalità, inclusa la ricerca scientifica, sono considerate compatibili con la finalità iniziale, rendendone il successivo trattamento presuntivamente lecito. Pertanto, quando il titolare del trattamento può sostenere e documentare che la finalità del trattamento è la ricerca scientifica, gli **usi secondari dei dati personali sono, in linea di principio, considerati compatibili con lo scopo originale del trattamento dei dati personali** (cfr.a la sotto-sezione "Principio di limitazione della finalità" nella sezione Principi della Parte generale dei presenti Orientamenti).

Inoltre, è molto probabile che la rete sociale che ha originariamente raccolto i dati abbia incluso nel consenso dell'interessato una clausola che consentiva alla medesima o a un terzo un ulteriore trattamento a fini di ricerca o, almeno, ha informato l'interessato che tale trattamento sarebbe stato considerato compatibile con il suo consenso iniziale. Se questo fosse il caso, il trattamento a fini di ricerca sarebbe legittimo sulla stessa base giuridica che ha permesso al social network la raccolta dei dati.

Questa valutazione, tuttavia, deve essere effettuata prima del successivo trattamento per finalità secondarie e deve essere basata su criteri oggettivi. Il quadro giuridico su questo tema potrebbe cambiare considerevolmente tra gli Stati membri dell'UE. Pertanto, i titolari del trattamento dovrebbero essere consapevoli del quadro normativo concreto applicabile. La consultazione con i loro RPD è altamente raccomandata a questo scopo[31], così come l'inclusione di un consulente/unità etico-legale all'interno del progetto dato.

Lista di controllo: ricerca scientifica

□ I titolari del trattamento hanno verificato che il loro progetto si adatta bene al concetto di ricerca scientifica.

□ I titolari del trattamento hanno consultato i loro RPD sull'uso di questa eccezione al divieto di trattamento dei dati di categorie particolari.

□ I titolari del trattamento hanno consultato il quadro giuridico nazionale su questo argomento.

□ I titolari del trattamento hanno implementato le misure di sicurezza e organizzative volte all'allineamento con l'articolo 89 dell'RGPD e la corrispondente normativa nazionale.

□ I titolari del trattamento hanno documentato tutte le informazioni relative a questo problema nella DPIA

[31] Cfr. alcune domande e risposte pratiche sull'argomento qui: https://www.ru.nl/rdm/gdpr-research/faq-gdpr-research/

5 Questioni di equità e trasparenza

L'equità è un principio essenziale nell'RGPD. Probabilmente, tutta la protezione dei dati e, quindi, l'RGPD riguarda l'equità verso gli interessati. L'RGPD può essere considerato nell'ottica della definizione di cosa significa effettivamente *equo*. Nel caso dei dati raccolti attraverso l'uso dei social network, è particolarmente importante evitare pregiudizi relativi a sesso, razza, età, orientamento sessuale, origine nazionale, religione, salute e disabilità, ecc. Ciò potrebbe essere problematico, in quanto è possibile che alcuni dei dati raccolti attraverso le reti sociali non corrispondano a utenti reali, o che i loro dati sensibili non siano affatto precisi. Questo potrebbe creare distorsioni nascoste (cfr. la sotto-sezione "Liceità, equità e trasparenza" della sezione Concetti principali della Parte generale dei presenti Orientamenti).

La trasparenza, d'altra parte, è una strategia fondamentale per equilibrare il potere tra il titolare del trattamento e l'interessato. Funziona portando tutto alla luce e aprendolo, così, al controllo. L'obiettivo principale della trasparenza è quello di informare in anticipo **gli interessati** dell'esistenza del trattamento e delle sue caratteristiche principali. Altre informazioni (come i dati sul soggetto interessato) sono disponibili su richiesta. Gli interessati devono, inoltre, essere informati di alcuni eventi, in particolare le violazioni dei dati (nel caso in cui l'interessato sia esposto a un rischio elevato). Evidentemente, la trasparenza è un prerequisito per individuare e intervenire in caso di non conformità (cfr. la sotto-sezione "Liceità, equità e trasparenza" della sezione Concetti principali della Parte generale dei presenti Orientamenti).

Nel caso dell'utilizzo di dati dai social network, la trasparenza significa, a nostro parere, che "i soggetti di ricerca previsti dovrebbero essere informati, ad un certo punto, della ricerca che si sta svolgendo, del tipo di dati personali che i titolari del trattamento stanno raccogliendo e di come essi saranno utilizzati.+ Alcuni servizi chiariscono che ciò deve essere fatto prima di iniziare la raccolta. Per altri senza una politica specifica e quando i ricercatori/innovatori stanno conducendo una ricerca osservazionale che il previo consenso potrebbe danneggiare, dovrebbero informare gli interessati il prima possibile. I ricercatori/innovatori delle TIC dovrebbero sempre rimuovere dalla loro raccolta gli individui che non acconsentono ad essere inclusi". [32]

Nel caso di utilizzo di dati dai social network, è necessario sottolineare che, in generale, l'Articolo 14 dell'RGPD sarà applicabile ad un certo punto. Pertanto, gli interessati dovrebbero essere pienamente consapevoli del fatto che i loro dati sono condivisi con terzi (cfr. la sotto-sezione "Diritto all'informazione" nella sezione Diritti degli interessati della Parte generale dei presenti Orientamenti). Ciò può avvenire in diversi modi. Per esempio, la CNIL ha informato che i titolari del trattamento dei dati possono includere tutti i terzi in un'informativa sulla privacy esaustiva, ma periodicamente aggiornata, o inserire un link in

[32] https://info.lse.ac.uk/staff/divisions/Secretarys-Division/Assets/Documents/Information-Records-Management/Social-media-personal-data-and-research-guidance-v.1.pdf

quest'informativa e reindirizzare i soggetti alla lista con le politiche sulla privacy, proprie e di terzi. [33]

I titolari del trattamento devono garantire la trasparenza, non solo fornendo informazioni adeguate, ma anche utilizzando una serie di **strumenti complementari.** La nomina di un RPD, che poi serve come unico punto di contatto per le richieste degli interessati, è un'ottima opzione. Anche la preparazione di registri adeguati del trattamento per le autorità di controllo, o l'esecuzione di DPIA, sono misure altamente raccomandate per promuovere la trasparenza. Allo stesso modo, intraprendere analisi che valutino l'efficacia e l'accessibilità delle informazioni fornite agli interessati aiuta a garantire l'attuazione efficiente di questo principio[34].

Infine, ma non meno importante, l'implementazione dei cosiddetti Transparency Enhancing Tools (TET) [35]potrebbe essere un'ottima opzione per garantire il rispetto del principio di trasparenza, specialmente quando si prevede un trattamento massiccio o automatizzato dei dati.

5.1 Distorsioni

Le distorsioni creano pregiudizi e discriminazioni contro certi gruppi o persone. Il danno può anche derivare dallo sfruttamento intenzionale delle distorsioni (dei consumatori), o da una concorrenza sleale, come l'omogeneizzazione dei prezzi attraverso la collusione o un mercato non trasparente. L'uso di dati raccolti attraverso i social network potrebbe contribuire a esacerbare una tale situazione, soprattutto con la costruzione set di dati distorti. Ciò potrebbe accadere, per esempio, a causa di una raccolta inadeguata dei dati prodotti dagli interessati. "I dati dei social media possono essere difficili da verificare - gli utenti possono mentire sulla loro età, posizione, lavoro, o qualsiasi altra caratteristica. **I ricercatori devono essere consapevoli di questo problema e affrontare questa difficoltà, se pertinente.** Non è consigliabile intendere gli utenti come il "pubblico generale", a causa delle disuguaglianze nell'accesso a Internet, e i ricercatori dovrebbero considerare come promuovere la diversità (se del caso) nel loro campione."[36] Potrebbe anche accadere che i dati inferiti o derivati creino tali distorsioni a causa di problemi tecnici propri. Se questi dati distorti alimentano la profilazione o il processo decisionale automatizzato, ciò potrebbe portare conseguenze sociali inaccettabili. Naturalmente, se la ricerca implica l'uso di IA, questo probabilmente aumenterà il rischio legato alle distorsioni (cfr. la sotto-sezione "Liceità, equità e trasparenza" della sezione Concetti principali della Parte generale dei presenti Orientamenti).

Per evitare un tale scenario, **è necessaria una valutazione critica della provenienza dei dati**. A questo scopo, dovrebbero essere implementate misure organizzative per garantire l'accuratezza e l'affidabilità dei dati raccolti, rinviando ancora al diritto degli utenti di trattenere informazioni private (ad esempio, confermando se un registro è accurato o meno).

[33] https://www.cnil.fr/fr/transmission-des-donnees-des-partenaires-des-fins-de-prospection-electronique-quels-sont-les

Inoltre, l'esecuzione di un audit volto a individuare distorsioni nei dati grezzi o nei set di dati inferiti o derivati è necessario soprattutto quando i titolari del trattamenti utilizzano set di dati prodotti attraverso i social network.

5.2 Trasparenza

Le ricerche basate sui dati raccolti attraverso le reti sociali, spesso, implicano il trattamento di molti dati personali. Ciò crea uno scenario complesso. I titolari del trattamento devono essere consapevoli che, anche se potrebbe essere difficile da realizzare, gli interessati devono essere in grado di capire come, e per quale finalità, i loro dati personali vengono utilizzati. In generale, ciò significa che **i ricercatori dovrebbero utilizzare strumenti in grado di fornire tale conoscenza nel modo più semplice possibile.** La spiegabilità è particolarmente importante nel caso del trattamento automatico dei dati o della profilazione. "I metodi per fornire informazioni, offrire il diritto di rifiutare o richiedere il consenso **dovrebbero essere resi il più semplice possibile.** Pertanto, le politiche d'informazione devono concentrarsi su informazioni comprensibili per l'utente e non dovrebbero limitarsi a una politica generale in materia di privacy sul sito web dei titolari del trattamento". [37]

Se il titolare del trattamento "prevede" di effettuare un trattamento per scopi diversi da quelli per cui i dati sono stati raccolti dal social network, deve informare preventivamente gli utenti o gli interessati di tale ulteriore trattamento, fornendo informazioni e rispettando tutti gli altri requisiti, come avere una base giuridica per questa nuova finalità o effettuare una valutazione di compatibilità (cfr. la sotto-sezione "Principio di limitazione della finalità" della sezione Concetti principali della Parte generale dei presenti Orientamenti). Naturalmente, i requisiti di trasparenza sono chiaramente legati al principio di equità, poiché più è difficile per l'utente capire il trattamento dei dati, maggiore è la differenza tra diversi tipi di utenti. In generale, "più grande è la quantità di dati, più difficile è una panoramica chiara e comprensibile in forma di testo. I simboli offrono un modo per rappresentare le categorie di dati personali in modo snello e riconoscibile. Ciò richiede rappresentazioni grafiche significative e autoesplicative dei dati."[38]

---

[34] Cfr. EOSC-Pillar Guidelines ´D4.1: Legal and Policy Framework and Federation Blueprint´ (2021), pagg. 44 e seguenti. Disponibile all'indirizzo: https://repository.eosc-pillar.eu/index.php/s/tbqe6B7rDycdFCJ#pdfviewer

[35] Le TET possono essere suddivise in TET "ex ante" ed "ex post". Le TET ex ante guidano il processo decisionale dell'utente prima di fare la sua scelta relativa alla divulgazione di qualsiasi dato personale a un titolare del trattamento dei dati. Al contrario, le TET ex post visualizzano i dati personali divulgati, in modo tale da rendere trasparenti i processi realizzati da quando l'utente ha divulgato i suoi dati (cfr. P. Murmann; S. Fischer-Hübner, `Usable Transparency Enhancing Tools - A Literature Review´ (2017), documento di lavoro. Disponibile all'indirizzo: http://www.diva-portal.org/smash/get/diva2:1119515/FULLTEXT02.pdf).

[36] Univerity of York, **Guidelines for the Use of Social Media Data in Research**. Disponibile all'indirizzo: https://www.york.ac.uk/staff/research/governance/research-policies/social-media-data-use-research/

[37] Gruppo di lavoro dell'articolo 29 per la protezione dei dati (2014) Parere 8/2014 sui recenti sviluppi nel campo dell'Internet degli oggetti (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088

[38] Bier C., Kühne K., Beyerer J. (2016) PrivacyInsight: The Next Generation Privacy Dashboard. In: Schiffner S., Serna J., Ikonomou D., Rannenberg K. (eds) Privacy Technologies and Policy. APF 2016. Lecture Notes in Computer Science, vol 9857. Springer, Cham. https://doi.org/10.1007/978-3-319-44760-5_9

Secondo l'RGPD, le informazioni che un titolare del trattamento deve fornire agli interessati variano a seconda che queste informazioni siano state ottenute da loro o meno. Se i dati personali non sono stati ottenuti dall'utente (Art. 14 RGPD), come nel caso della ricezione dei dati da un social network, il titolare del trattamento deve essere particolarmente attento a fornire all'interessato un'informazione adeguata, soprattutto perché viene effettuata una raccolta massiccia di dati. Pertanto, i titolari del trattamento devono informare l'utente delle disposizioni di cui all'Art. 14 dell'RGPD[39].

È necessario, tuttavia, menzionare che a volte potrebbe essere estremamente difficile per un titolare del trattamento che ha raccolto i dati da un social network informare gli interessati sul trattamento. Se questo è il caso, potrebbe ricordare l'articolo 14, paragrafo 5, lettera b), che stabilisce che "la comunicazione di tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'Articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente Articolo rischi di rendere impossibile o pregiudicare gravemente il conseguimento delle finalità di tale trattamento" (cfr. la sotto-sezione "Protezione dei dati e ricerca scientifica" della sezione Concetti principali della Parte generale dei presenti Orientamenti).

In tali casi, il titolare del trattamento deve adottare misure adeguate per proteggere i diritti e le libertà dell'interessato e i legittimi interessi, compresa la messa a disposizione del pubblico delle informazioni (cfr. la sotto-sezione "Diritto all'informazione" della sezione "Diritti degli interessati" della Parte generale dei presenti Orientamenti). Quindi, in linea di principio i titolari del trattamento potrebbero evitare di fornire informazioni sul trattamento agli interessati se ciò è reso impossibile, ma solo se *adottano misure adeguate per proteggere i diritti e le libertà degli interessati e gli interessi legittimi, come rendere le informazioni disponibili al pubblico.*

Si noti con cautela, tuttavia, che uno sforzo sproporzionato può in alcune giurisdizioni essere interpretato in modo restrittivo. Ad esempio, c'è stata una recente decisione (marzo 2019) da parte dell'Autorità polacca per la protezione dei dati (DPA polacca) quando ha multato una società di data scraping con €220k per la mancata fornitura di informative sulla privacy a 5,7 milioni di persone i cui dati sono stati raschiati da un registro pubblico. L'autorità polacca per la protezione dei dati ha respinto l'argomentazione secondo cui l'inserimento di un'informativa sulla privacy sul sito web della società di scraping dei dati era sufficiente per informare gli individui, in particolare quando gli individui non erano consapevoli che i loro dati fossero stati raschiati e trattati. [40]

[39] Cfr.: CNIL, La réutilisation des données publiquement accessibles en ligne à des fins de démarchage comercial, su: https://www.cnil.fr/fr/la-reutilisation-des-donnees-publiquement-accessibles-en-ligne-des-fins-de-demarchage-commercial

[40] Campbell, Fiona, Data Scraping – Considering the Privacy Issues, disponibile all'indirizzo: https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/data-scraping-considering-the-privacy-issues

Lista di controllo: equità e trasparenza

Equità

□ I titolari del trattamento eseguono audit mirati a rilevare distorsioni nei set di dati costruiti e/o le conclusioni dell'analisi

□ I titolari del trattamento hanno implementato misure adeguate per evitare distorsioni provocate dall'uso di strumenti di IA.

Trasparenza

□ Il titolare del trattamento fornisce

- una panoramica *di quali dati personali sono stati divulgati a quale titolare del trattamento secondo quali politiche;*
- *accesso online ai dati personali e a come sono stati trattati;*
- *funzionalità di profilazione contraria che aiutano l'utente ad anticipare come i loro dati corrispondono a profili di gruppo rilevanti, che possono influenzare opportunità o rischi futuri*

□Poiché i dati personali non sono stati forniti dall'interessato, i titolari del trattamento hanno fornito tutte le informazioni elencate nell'Articolo 14, paragrafo 1 RGPD;

□ Poiché i dati personali non sono forniti dall'interessato, l'informazione è fornita:

- entro un periodo ragionevole dopo aver ottenuto i dati personali, ma non oltre un mese;
- se i dati personali devono essere utilizzati per la comunicazione con l'interessato, al più tardi al momento della prima comunicazione a tale soggetto;
- se è prevista una divulgazione a qualcun altro, al più tardi quando i dati personali sono divulgati per la prima volta

□ Le informazioni sono fornite in modo conciso, trasparente, comprensibile e facilmente accessibile. Sono chiare e redatte in un linguaggio semplice.

□Se la fornitura delle informazioni è resa impossibile, i titolari del trattamento adottano misure adeguate per proteggere i diritti e le libertà dell'interessato e gli interessi legittimi, compresa la messa a disposizione del pubblico delle informazioni.

□ I titolari del trattamento hanno documentato tutte le informazioni riguardanti questi problemi

6 Governance dei dati: principi di minimizzazione, limitazione della finalità e della conservazione

Il principio di minimizzazione (cfr. la sotto-sezione "Principio di minimizzazione" della sezione Concetti principali della Parte generale dei presenti Orientamenti) stabilisce che i dati personali devono essere **adeguati**, **pertinenti e limitati a quanto necessario in relazione alle finalità** per cui sono trattati. D'altra parte, secondo l'Articolo 5, paragrafo 1, lettera (e)

dell'RGPD, i dati personali devono essere "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati". Infine, la limitazione della finalità significa che i dati personali non possono essere trattati per finalità diverse da quelle stabilite nella politica in materia di privacy quando i dati furono raccolti, a meno che queste ulteriori finalità siano compatibili con quelle originarie e in base a garanzie adeguate (art. 6, paragrafo 4 RGPD). Ad esempio, l'ulteriore trattamento corrisponde ad attività di archiviazione di interesse pubblico, a finalità di ricerca scientifica e storica o a finalità statistiche (cfr. la sotto-sezione "Trattamento dei dati e ricerca scientifica" della sezione Concetti principali della Parte generale dei presenti Orientamenti).

La combinazione di questi tre principi crea uno strumento normativo combinato che deve essere rigorosamente seguito dai titolari del trattamento che utilizzano dati raccolti attraverso i social network. In generale, i titolari del trattamento [41]devono rendere esplicite le finalità del trattamento: "divulgate, spiegate o espresse in una forma intelligibile". In linea con il principio di minimizzazione dei dati, devono anche identificare la quantità minima di dati personali necessari per raggiungere i loro obiettivi. Inoltre, per quanto riguarda il principio di accountability (responsabilizzazione), i titolari del trattamento dei dati devono essere in grado di dimostrare che raccolgono e detengono solo i dati personali necessari, e che essi vengono utilizzati solo per le finalità specifiche comunicate in base a una base giuridica adeguata.

Riassumendo, stabilire obiettivi chiari per il trattamento aiuterà a garantire che i dati personali da trattare siano:

- adeguati: sufficienti a raggiungere la finalità dichiarata;
- pertinenti: devono avere un legame razionale con la finalità;
- limitati a quanto necessario: non devono tenere più dati di quelli necessari per la finalità dichiarata.

6.1 Principio di minimizzazione

Il principio di minimizzazione stabilisce che i dati personali devono essere **adeguati**, **pertinenti e limitati a ciò che è necessario in relazione alle finalità** per le quali sono trattati. (cfr. la sezione "Minimizzazione dei dati" nella parte Principi dei presenti Orientamenti). Secondo questo principio, i titolari del trattamento devono essere consapevoli dell'obiettivo che si intende raggiungere con il trattamento, in modo da evitare di usare più dati del necessario. Inoltre, i titolari del trattamento devono anche cercare di evitare di usare categorie particolari di dati personali se non sono strettamente necessari.

Quando i ricercatori/innovatori raccolgono dati dai social network, potrebbero finire per elaborare molti più dati personali e sensibili di quelli di cui hanno realmente bisogno per le finalità specifiche della ricerca. Ci sono modi di evitare questo tipo di scenario. In linea di principio, i titolari del trattamento **devono promuovere l'uso di dati anonimizzati**. Infatti,

[41] è importante identificare il "titolare del trattamento dei dati"; gli sviluppatori sono raramente "titolari del trattamento dei dati", poiché non sono responsabili dell'obiettivo aziendale, questo è un compito della direzione dell'azienda.

evitare l'identificazione di individui specifici dall'analisi dei big data, o la reidentificazione degli utenti i cui dati sono stati pseudonimizzati, è una salvaguardia fondamentale per evitare un impatto indebito sugli interessati causato dal trattamento dei dati [42]. Se non hanno bisogno di dati personali, potrebbero chiedere al social network di fornire loro dati anonimizzati. Naturalmente, potrebbero anche anonimizzare i dati una volta raccolti, ma, in questo caso, non dovrebbero dimenticare **che l'anonimizzazione implica il trattamento dei dati e, quindi, avrebbero bisogno di una base giuridica che la legittimi** (cfr. la sotto-sezione "Identificazione, Pseudonimizzazione e Anonimizzazione" nella sezione Concetti principali della Parte generale dei presenti Orientamenti).

Inoltre, i ricercatori/innovatori devono ricordare che l'anonimizzazione potrebbe essere difficile da ottenere. Molto spesso, l'aggregazione e le pratiche di inferenza di dati possono facilmente de-anonimizzare i set di dati. Pertanto, i **titolari del trattamento non dovrebbero presumere che i loro processi di anonimizzazione serviranno a preservare la privacy degli interessati. Infatti, dovrebbero eseguire DPIA e valutazioni del rischio per garantire tale convinzione** (cfr. l'accountability in questa parte degli Orientamenti)

Un'alternativa all'anonimizzazione in quanto tale è l'uso di **dati aggregati**. Nel contesto della protezione dei dati, bisogna distinguere due tipi di aggregazione (cfr. la sezione "Minimizzazione dei dati" nella parte Principi dei presenti Orientamenti):

- **Persona singola**: Aggregazione di elementi di dati relativi a una **singola persona**: Prendendo, ad esempio, il reddito medio mensile di una persona in un anno, si riduce il contenuto informativo relativo a quella persona.
- **Più persone**: Aggregazione di elementi di dati relativi a una **moltitudine di persone**: Prendendo, ad esempio, il reddito medio annuo di un gruppo di persone si riduce anche il contenuto informativo complessivo (minimizzazione dei dati). Inoltre, si indebolisce anche il grado di associazione tra un elemento di dati e una determinata persona. Questo tipo di aggregazione è, quindi, pertinente anche alla limitazione della conservazione

Quando la finalità del trattamento può essere raggiunta usando dati aggregati, questo è raccomandabile (cfr. la sotto-sezione "Principio di minimizzazione dei dati" della sezione Principi fondamentali della Parte generale dei presenti Orientamenti)**.** In tali circostanze, nessuno salvo l'interessato dovrebbe accedere ai dati grezzi (dati ottenuti o osservati), a meno che non si applichi una ragione estremamente rilevante (ad esempio, questioni di sicurezza nazionale interpretate in modo restrittivo). Infatti, a volte una ricerca specifica ha bisogno solo di dati aggregati e non dei dati grezzi raccolti nelle reti sociali. Pertanto, i **titolari del trattamento devono cancellare i dati grezzi non appena hanno estratto i dati necessari per il loro trattamento**. Come principio, la cancellazione dovrebbe avvenire nel punto più vicino alla raccolta dei dati grezzi (ad esempio, sullo stesso dispositivo dopo il trattamento).

[42] Le Linee guida 3/2013 del WP29 sulla limitazione delle finalità (pag. 3) evidenziano l'adozione di garanzie volte a evitare impatti indebiti sugli interessati come un fattore chiave da prendere in considerazione quando si valutano gli ulteriori usi compatibili dei dati.

6.2 Limitazione della finalità

Il principio di limitazione della finalità (cfr. la sotto-sezione "Limitazione dello scopo" nella sezione Principi principali dei presenti Orientamenti) richiede che i dati personali raccolti siano trattati solo per la finalità per cui sono stati raccolti. La limitazione della finalità è un concetto fondamentale nel trattamento dei dati ottenuti dai social network e la maggior parte delle piattaforme lo include nelle proprie Politiche per gli sviluppatori. I ricercatori e gli innovatori devono seguire rigorosamente tali politiche. D'altra parte, è, spesso, vero che gli interessati non sono veramente consapevoli dei permessi che forniscono ai social network per il trattamento. Questo è un motivo particolarmente importante per cui i titolari del trattamento che utilizzano questi dati non dovrebbero trattare i dati per finalità che potrebbero essere considerate incompatibili con il consenso iniziale.

Pertanto, i **titolari del trattamento dovrebbero implementare strumenti in grado di garantire che il trattamento non avrà luogo se gli interessati non forniscono il loro consenso, a meno che una base giuridica alternativa consenta il trattamento (**cfr. la sotto-sezione "Liceità, equità e trasparenza" della sezione Principi principali della Parte generale dei presenti Orientamenti). L'utilità dei dati conservati per la finalità prevista della ricerca dovrà essere periodicamente rivalutata per evitare un trattamento illecito dei dati.

Va notato che quando i dati vengono utilizzati per motivi di interesse pubblico o per scopi di ricerca, archiviazione o statistica, questi usi derivati non saranno considerati incompatibili con le finalità iniziali, a condizione che siano adeguatamente pseudonimizzati, ogni volta che l'ulteriore trattamento di tali dati non consente la reidentificazione degli interessati (Art. 5, paragrafo 1, lettera b) & 89, paragrafo 1 RGPD) (cfr. la sezione "Considerare se il quadro normativo relativo alla ricerca scientifica si applica all'attività" in questa parte degli Orientamenti).

6.3 Limitazione della conservazione

Il principio di limitazione della conservazione obbliga i titolari del trattamento dei dati a non conservare i dati personali "oltre il tempo necessario per il conseguimento delle finalità per le quali sono trattati" e a introdurre misure di pseudonimizzazione e anonimizzazione che riducano/eliminino l'identificabilità degli interessati non appena possibile per tali finalità. Il problema qui è che, di solito, le reti sociali potrebbero usare i dati memorizzati per finalità diverse. Inoltre, a volte i dati sono raccolti e memorizzati "per ogni evenienza" di uso futuro. I titolari del trattamento dovrebbero essere consapevoli che anche se l'RGPD consente la conservazione per periodi più lunghi, **deve esistere un motivo valido e reale per optare per un periodo così esteso (**cfr. la sotto-sezione "Principio di limitazione della conservazione" nella sezione Principi fondamentali nella Parte generale dei presenti Orientamenti). Cioè, un titolare del trattamento non dovrebbe avere la tentazione di conservare i dati oltre lo stresso necessario, con l'obiettivo di averli a disposizione nel caso in cui nuove finalità o progetti sorgano in futuro, diversi da quelli legittimamente consentiti.

Al fine di evitare la conservazione illecita, ogni singola parte coinvolta nella fornitura di un servizio specifico nella rete sociale deve effettuare un test di necessità, in quanto le finalità dei

rispettivi trattamenti possono, in effetti, essere diverse. Ad esempio, i dati personali comunicati da un utente quando si abbona a un servizio specifico nel social network dovrebbero essere cancellati non appena l'utente pone fine al suo abbonamento. Allo stesso modo, le informazioni eliminate dall'account dallo stesso utente non dovrebbero essere conservate. Quando un utente non usa il social network per un periodo di tempo determinato, il profilo utente dovrebbe essere impostato come inattivo. Dopo un altro periodo di tempo, i dati dovrebbero essere cancellati. L'utente dovrebbe essere avvisato prima di questi passi, con qualsiasi mezzo che la parte coinvolta ha a disposizione. [43]

Per riassumere, se i titolari del trattamento non hanno bisogno dei dati e non ci sono motivi legali obbligatori che impongano loro di conservarli, dovrebbero renderli completamente anonimi o cancellarli. I ricercatori dovrebbero consultare i loro RPD se desiderano conservare i dati per un periodo di tempo più lungo ed essere consapevoli della normativa nazionale applicabile.

Questo potrebbe anche essere un ottimo momento per **prevedere limiti di tempo per la cancellazione delle diverse categorie di dati, e documentare chiaramente queste decisioni** (cfr. la sotto-sezione "Principio di Accountability" nella sezione "Principi fondamentali" della Parte generale dei presenti Orientamenti). A questo proposito, deve essere preservato il giusto equilibrio tra sostenibilità della ricerca, riproducibilità, dati aperti, scienza aperta e principio di minimizzazione ai sensi dell'RGPD, considerando anche che il trattamento di set di dati pseudo/anonimizzati potrebbe generare set di dati pseudo/identificabili. A tal fine, si devono seguire i criteri di cui al Considerando 156 RGPD:

(1) il trattamento dei dati personali a fini di ricerca scientifica dovrebbe essere soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, laddove sia garantito, in particolare, che siano state predisposte misure tecniche e organizzative al fine di garantire il principio della minimizzazione dei dati;

(2) l'ulteriore trattamento dei dati personali è da effettuarsi quando il titolare del trattamento ha valutato la fattibilità di conseguire tali finalità

trattando dati personali che non consentono o non consentono più di identificare l'interessato o che forniscano garanzie adeguate di pseudonimizzazione;

(3) Le condizioni e le garanzie in questione possono comprendere procedure specifiche per l'esercizio di tali diritti da parte degli interessati, oltre a misure tecniche e organizzative intese a ridurre al minimo il trattamento dei dati personali conformemente ai principi di proporzionalità e di necessità.

Lista di controllo: governance dei dati
Minimizzazione

[43] Parere 8/2014 del Gruppo di lavoro dell'Art. 29 sulla protezione dei dati sui recenti sviluppi nel campo dell'Internet degli oggetti (SEP 16 settembre 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088

□ Il titolare del trattamento procede al trattamento dei soli dati anonimizzati o pseudonimizzati quando possibile.

□ Il titolare del trattamento tratta la quantità minima di dati necessari per raggiungere le finalità perseguite.

□ Il titolare del trattamento tratta i dati di categorie particolari solo se è strettamente necessario

Limitazione della finalità

□ I titolari del trattamento utilizzano i dati solo per finalità per cui sono stati raccolti, a meno che una base giuridica ne consenta un trattamento legittimo.

Limitazione della conservazione

□ I titolari del trattamento non conservano i dati personali "oltre il tempo necessario al conseguimento delle finalità per cui i dati personali sono trattati".

□ I titolari del trattamento verificano l'utilità dei dati memorizzati per la finalità della ricerca.

□ I dati vengono memorizzati in modo da impedire il più possibile il trattamento dei dati personali.

□ I titolari del trattamento hanno documentato tutte le informazioni relative a questi problemi.

7 Accountability e supervisione

Il principio di responsabilizzazione nell'RGPD è basato sul rischio: più alto è il rischio del trattamento dei dati per i diritti e le libertà fondamentali degli interessati, maggiori sono le misure necessarie per mitigare tali rischi (cfr. la sotto-sezione "Principio di accountability" nella sezione "Principi fondamentali" della Parte generale dei presenti Orientamenti)[44]. Poiché il trattamento dei dati personali raccolti dai social network potrebbe essere considerato ad alto rischio, [45]i ricercatori/innovatori devono anche nominare un RPD ed eseguire una DPIA. Inoltre, i titolari del trattamento devono creare una Politica in materia di protezione dei dati che consenta la **tracciabilità delle informazioni** (cfr. la sotto-sezione "Principio di accountability" nella sezione "Principi fondamentali" della Parte generale dei presenti Orientamenti)).

[44] Cfr. gli articoli 24, 25 e 32 dell'RGPD, che richiedono ai titolari del trattamento di tenere in considerazione i "rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche" quando adottano misure specifiche di protezione dei dati.

[45] Cfr., in particolare, l'Articolo 35, paragrafo 3, lettera a), secondo il quale il trattamento dei dati è considerato ad alto rischio nei casi, tra l'altro, di "una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche".

7.1 Responsabile della protezione dei dati

Nella maggior parte dei casi, la ricerca TIC basata su dati provenienti da reti sociali comporta operazioni che, per la loro natura, la loro portata e/o le loro finalità, richiedono un monitoraggio regolare e sistematico degli interessati su larga scala. Pertanto, la nomina di un RPD è obbligatoria in presenza delle condizioni stabilite dall'Articolo 37, paragrafo 1. Anche se non è questo il caso, **è sempre raccomandabile procedere in tal senso, almeno in termini di trasparenza** (cfr. la sotto-sezione "Principio di liceità, equità e trasparenza" nella sezione "Principi fondamentali" della Parte generale dei presenti Orientamenti)**.**

7.2 Valutazione d'impatto sulla protezione dei dati

L'esecuzione di una DPIA è, spesso, obbligatoria nel caso dei social network in quanto implica un monitoraggio sistematico di un'area accessibile al pubblico su larga scala (Articolo 35(3) dell'RGPD). Anche laddove non fosse questo il caso, alcune altre circostanze potrebbero renderla obbligatoria o, almeno, altamente raccomandabile (cfr. la sotto-sezione "Valutazione d'impatto sulla protezione dei dati" della sezione Azioni e strumenti principali della Parte generale dei presenti Orientamenti).

Lista di controllo

- Il titolare del trattamento ha effettuato una DPIA per l'attività di trattamento. Ha assicurato che:
  - È iniziata il più presto possibile (seguendo il principio della Protezione dei dati fin dalla progettazione).
  - Ha fornito una chiara panoramica di ciò che è una DPIA.
  - Ha utilizzato la guida e i modelli forniti dall'Autorità di controllo per la protezione dei dati (DPA) competente, ove possibile. In caso contrario (ad esempio, se la DPA non fornisce tale materiale o deve soddisfare molte aree di competenza di diverse DPA), ha seguito la guida fornita dal Gruppo di lavoro dell'articolo 29 in wp248rev.01.
  - Ha assemblato il team necessario per condurre la DPIA.
  - Ha considerato i modi per facilitare il suo lavoro.

7.3 Progettazione della politica sulla privacy e preparazione della documentazione del trattamento

La Politica sulla Privacy è il documento pubblico che spiega come un progetto di ricerca tratta i dati personali e come applica i principi di protezione dei dati, secondo gli articoli 12-14 dell'RGPD. Tutti gli interessati devono avere accesso a questa Politica sulla Privacy. Dovrebbe essere documentata. Un modello non ufficiale, ma raccomandabile, può essere trovato qui: https://gdpr.eu/wp-content/uploads/2019/01/Our-Company-Privacy-Policy.pdf

I titolari del trattamento devono sempre ricordare che, nel caso di dati raccolti dai social network, potrebbero finire per mescolare diversi set di dati o creare dati inferiti o derivati. I registri devono garantire la tracciabilità del trattamento, le informazioni sul possibile riutilizzo dei dati e l'uso di dati appartenenti a diversi set di dati nella stessa o in diverse fasi del ciclo di vita. Chiunque tratti dati personali (compresi sia i titolari del trattamento che i responsabili del trattamento) deve documentare le proprie attività principalmente ad uso delle Autorità di controllo qualificate/pertinenti. Ciò deve avvenire tramite registri delle attività di trattamento tenuti a livello centrale dall'organizzazione per tutte le sue attività di trattamento, così come documentazione aggiuntiva che riguarda una singola attività di trattamento dei dati (cfr. la sotto-sezione "Documentazione del trattamento" nella sezione "Azioni e strumenti principali" della Parte generale dei presenti Orientamenti).

Le prime fasi di sviluppo del progetto sono il momento perfetto per impostare un modo sistematico di raccolta della documentazione necessaria, poiché sarà il momento in cui l'organizzazione concepisce e pianifica l'attività di trattamento[46].

Infine, ma non meno importante, i titolari del trattamento devono ricordare che i comitati etici giocheranno, probabilmente, un ruolo fondamentale nel trattamento dei dati personali. Tuttavia, questo potrebbe cambiare considerevolmente in base ai settori e ai paesi. I titolari del trattamento devono consultare il loro RPD su questo argomento.

Infine, i titolari del trattamento non devono dimenticare che potrebbero esistere implicazioni etiche al di là della conformità legale. La consultazione con un esperto in etica delle reti sociali è sempre raccomandata.

Lista di controllo. Politica sulla privacy

- □ Il titolare del trattamento ha contattato l'ufficio/la persona che tiene i registri del trattamento per l'organizzazione.
  - Se necessario, il responsabile della protezione dei dati può aiutare a stabilire questo contatto.
- □ Il titolare del trattamento ha informato in anticipo l'ufficio/la persona di cui sopra

[46] L'articolo 25, paragrafo 1 dell'RGPD lo definisce "il momento della determinazione dei mezzi di trattamento".

della sua intenzione di trattare dati personali.

- La sua attività di trattamento deve essere inserita nei registri prima di iniziare il suddetto trattamento.

□ Il titolare del trattamento ha seguito le sue istruzioni su

- quali informazioni deve fornire per i registri del trattamento,
- quando ha bisogno di inviare aggiornamenti di queste informazioni.

Documentazione aggiuntiva relativa a una singola attività di trattamento).

I seguenti elementi devono essere documentati:

□ Valutazione sul se l'attività di trattamento comporta un rischio elevato per i diritti e le libertà delle persone fisiche.

□ Una valutazione d'impatto sulla protezione dei dati quando la valutazione di cui sopra dà un risultato affermativo.

□ Potenziale consultazione dell'autorità di controllo competente prima del trattamento.

□ Requisiti e test di accettazione per l'acquisto e/o lo sviluppo del software, dell'hardware e dell'infrastruttura impiegati.

□ Misure tecniche e organizzative implementate.

□ Verifiche periodiche, valutazione e accertamento dell'efficacia delle misure tecniche e organizzative

□ Requisiti e test di accettazione per la selezione dei responsabili del trattamento.

□ Contratti stipulati con i responsabili del trattamento.

□ Possibili ispezioni e audit del responsabile del trattamento.

□ Metodi di raccolta del consenso.

□ Dimostrazioni di espressioni individuali di consenso.

□ Informazioni fornite agli interessati.

□ Attuazione dei diritti degli interessati.

□ Gestione effettiva dei diritti degli interessati.

□ Eventuali notifiche di violazione all'autorità di controllo competente.

□ Possibile comunicazione delle violazioni di dati all'interessato.

Qualsiasi altra comunicazione con l'autorità di controllo competente.

8 Integrità e riservatezza

Ai sensi dell'RGPD, i dati personali devono essere trattati in modo da **garantire un'adeguata sicurezza** dei dati personali, compresa la protezione contro il **trattamento non autorizzato** o **illecito** e contro la **perdita accidentale, la distruzione** o **danno**, utilizzando misure tecniche o organizzative adeguate ("*integrità e riservatezza*"). (Cfr. la sotto-sezione "Integrità e riservatezza" nella sezione "Principi fondamentali" della Parte generale dei presenti Orientamenti).

Questo principio coinvolge tre questioni principali: integrità, riservatezza e disponibilità. La disponibilità e l'integrità sono in qualche modo collegate, poiché solo i dati che sono adeguatamente conservati possono essere resi disponibili al soggetto interessato. La riservatezza, invece, è una questione più complessa che merita misure complesse a causa del tipo di processi coinvolti e dei rischi inerenti a tali processi.

8.1 Disponibilità e integrità

La ricerca alimentata dall'uso di dati provenienti dai social network comporta talvolta la raccolta di una quantità impressionante di dati. Il trattamento di questi dati avviene, di solito, in luoghi remoti nel cloud e, per poterli raggiungere, è necessario utilizzare reti condivise, reti pubbliche, ecc. In tali circostanze**, di solito, è estremamente difficile rendere tutti i dati disponibili per gli interessati.** D'altra parte, vale la pena notare che l'integrità dei dati potrebbe essere compromessa dal modo in cui sono condivisi e conservati. Potrebbe accadere che uno dei responsabili del trattamento o co-titolari del trattamento, a un certo punto, cancelli o danneggi i dati. Al fine di prevenire tali scenari, sono altamente raccomandate le copie di backup. La loro creazione dovrebbe essere prevista fin dalle prime fasi della ricerca.

8.2 Eseguire un'analisi dei rischi per la sicurezza

In base al principio di riservatezza, i titolari del trattamento dovrebbero ridurre al minimo i rischi per i diritti, gli interessi e le libertà degli interessati. A questo scopo, dovrebbero lavorare su un approccio basato sul rischio (cfr. la sotto-sezione "Integrità e riservatezza" nella sezione "Principi fondamentali" della Parte generale dei presenti Orientamenti). In tutti i casi, i titolari del trattamento devono garantire il rispetto dei requisiti di protezione dei dati e di essere in grado di dimostrarlo, ad esempio attraverso la documentazione (cfr. la sotto-sezione "Responsabilità" nella sezione "Principi fondamentali" della Parte generale dei presenti Orientamenti).

Per gestire i rischi per gli individui derivanti dal trattamento dei dati personali raccolti dai social network, è importante che i titolari del trattamento sviluppino una comprensione e un'articolazione matura dei diritti fondamentali, dei rischi e di come bilanciare questi e altri interessi. In definitiva, è necessario che i titolari del trattamento valutino i rischi per i diritti degli individui che l'uso dei dati pone, e stabiliscano come devono affrontarli e determinando

l'impatto che ciò ha sul loro uso per scopi di ricerca. A questo scopo, ci sono due fattori fondamentali da considerare: [47]

- Rischi derivanti dal trattamento in sé, come l'emergere di distorsioni associate alla profilazione o a sistemi decisionali automatizzati.
- Rischi derivanti dal trattamento in relazione al contesto sociale, e gli effetti collaterali indirettamente legati all'oggetto del trattamento che possono verificarsi.

Al fine di ridurre al minimo tali rischi, i titolari del trattamento devono garantire l'implementazione di misure tecniche e organizzative appropriate per eliminare, o almeno mitigare, il rischio di sicurezza, riducendo la probabilità che le minacce identificate si materializzino, o riducendone l'impatto. È necessario prendere in considerazione gli standard di sicurezza che già esistono sul mercato, così come gli standard di conformità in relazione alla protezione dei dati che si applicheranno al trattamento. Inoltre, gli sviluppatori dovrebbero sempre ricordare che l'Articolo 32, paragrafo 4 RGPD chiarisce che un elemento importante della sicurezza è garantire che "qualsiasi persona fisica che agisca sotto l'autorità del titolare del trattamento o del responsabile del trattamento e abbia accesso a dati personali non li tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri." (cfr. la sotto-sezione "Integrità e riservatezza" nella sezione "Principi fondamentali" della Parte generale dei presenti Orientamenti).

La descrizione generale delle misure di sicurezza tecniche e organizzative deve diventare parte dei registri del trattamento, se possibile (Articolo 30, paragrafo 1, lettera g) per i titolari del trattamento, e 30, paragrafo 2, lettera d) per i responsabili del trattamento) e tutte le misure implementate devono far parte della DPIA, come misure di rimedio di supporto per limitare il rischio. Infine, una volta implementate le misure selezionate, il rischio residuo rimanente dovrebbe essere valutato e tenuto sotto controllo. Sia l'analisi del rischio che la DPIA sono gli strumenti da applicare. La valutazione del rischio e le decisioni prese "devono essere documentate al fine di rispettare il requisito della protezione dei dati fin dalla progettazione" (dell'Articolo 25 dell'RGPD) (cfr. la sotto-sezione ' (**Protezione dei dati fin dalla progettazione e per impostazione predefinita- Data Protection by Design and by Default, DPbDD**-)' nella sezione "Concetti e strumenti" della Parte generale dei presenti Orientamenti").

Infine, i titolari del trattamento devono sempre essere consapevoli che, secondo l'Articolo 32, paragrafo 1, lettera d) dell'RGPD, la protezione dei dati è un processo. Pertanto, **dovrebbero testare, definire e valutare l'efficacia delle misure tecniche e organizzative periodicamente**. Le procedure che aiutano i titolari del trattamento a identificare i cambiamenti che farebbero scattare una revisione della DPIA dovrebbero essere create in questo momento. Quando possibile, i titolari del trattamento devono cercare di imporre un modello dinamico di sorveglianza delle misure in gioco (cfr. la sotto-sezione "Integrità e

[47] AEPD (2020) Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción. Agencia Espanola Proteccion Datos, Madrid, pag.30. Disponibile all'indirizzo: www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf (consultato il 15 maggio 2020).

riservatezza" nella sezione "Principi fondamentali" della Parte generale dei presenti Orientamenti).

Lista di controllo: integrità e riservatezza

□ I titolari del trattamento hanno introdotto le procedure necessarie per garantire che i diritti degli interessati siano adeguatamente soddisfatti, indipendentemente dal se gli interessati siano gli utenti finali o terzi.

□ I titolari del trattamento hanno introdotto le procedure necessarie per garantire che i diritti degli interessati siano soddisfatti in tempo (massimo un mese dopo la richiesta).

□ I titolari del trattamento hanno introdotto strumenti efficaci per garantire che gli interessati siano in grado di esercitare i loro diritti in modo pratico, ad esempio introducendo standard di interoperabilità dei dati.

□ Gli interessati sono in grado di avere accesso a tutti i loro dati personali, compresi i dati grezzi che sono raccolti dalle reti sociali

□ I titolari del trattamento hanno implementato strumenti per leggere, editare e modificare localmente i dati prima di trasferirli a qualsiasi titolare del trattamento dei dati. Inoltre, i dati personali trattati da un dispositivo sono memorizzati in un formato che consente la portabilità dei dati

□ I titolari del trattamento hanno introdotto strumenti in grado di comunicare i dati rettificati ad ogni destinatario a cui sono stati divulgati i dati personali, salvo che ciò si riveli impossibile o comporti uno sforzo sproporzionato.

□ I titolari del trattamento hanno introdotto strumenti in grado di garantire che tutti i dati siano efficacemente cancellati su richiesta degli interessati se non ci sono motivi legittimi per opporsi a tale richiesta.

□ I titolari del trattamento hanno assicurato che gli schemi di revoca dovrebbero essere a grana fine e dovrebbero coprire:

(1) qualsiasi dato raccolto con un mezzo specifico;

(2) un tipo specifico di dati raccolti con qualsiasi mezzo;

(3) un trattamento di dati specifico

□ I titolari del trattamento hanno documentato tutte le informazioni relative a questi problemi.

9 Diritti degli interessati

Il capitolo III dell'RGPD prevede una serie di diritti che gli interessati possono esercitare per salvaguardare i loro dati personali. Sebbene ogni diritto abbia dettagli e questioni specifiche che potrebbero riguardare ed essere influenzate dalla ricerca e sviluppo nelle TIC (cfr. la sotto-sezione "Protezione dei dati e ricerca scientifica" nella parte "Concetti principali" della Parte generale dei presenti Orientamenti), tutti condividono alcune caratteristiche generali riguardanti le proprie informazioni trasparenti, la comunicazione e le modalità di esercizio (Articolo 12 RGPD). In questa sezione, analizziamo ogni diritto specifico alla luce di un trattamento che utilizza dati raccolti dai social network. Tuttavia, poiché abbiamo già analizzato il diritto all'informazione (cfr. la sezione "Trasparenza" di questa parte degli Orientamenti), e il diritto a non essere sottoposti a un processo decisionale automatizzato è stato ampiamente trattato nella sezione "Intervento umano" di questa parte degli Orientamenti, ci concentreremo ora sui diritti rimanenti.

9.1 Diritto di accesso

L'articolo 12, lettera a) stabilisce che gli interessati hanno il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che li riguardano e, in tal caso, l'accesso ai dati personali (cfr. la sotto-sezione "Diritto di accesso" nella sezione "Diritti degli interessati" della Parte generale dei presenti Orientamenti). In poche parole, l'interessato ha il diritto di ottenere dal titolare del trattamento informazioni su (1) i dati personali memorizzati, così come le loro categorie, (2) la fonte e i destinatari dei dati personali a cui i dati sono comunicati, (3) la conoscenza della logica coinvolta nel trattamento automatico dei dati riguardanti l'interessato, e (4) la finalità del trattamento dei dati personali. L'intero requisito è incluso nell'articolo 15 RGPD. **Questo diritto è particolarmente importante nel caso di dati raccolti dai social network, poiché gli interessati, di solito, non sono consapevoli dell'esistenza di tali dati. Inoltre, il titolare del trattamento potrebbe creare dati inferiti e questi dati potrebbero essere di particolare interesse per l'interessato.** Pertanto, i titolari del trattamento devono accertarsi di aver implementato strumenti adeguati per soddisfare l'esigenza degli interessati secondo le precisazioni incluse nell'RGPD.

9.2 Diritto di rettifica

Come stabilito dall'Articolo 16 dell'RGPD, gli interessati hanno il diritto di ottenere la rettifica dei loro dati personali (cfr. la sotto-sezione "Diritto di rettifica" nella sezione "Diritti degli interessati" della Parte generale dei presenti Orientamenti). Ciò è particolarmente rilevante nel caso di dati raccolti dai social network, poiché gli interessati possono fornire informazioni false o inesatte a causa di una mancanza di comprensione delle implicazioni che potrebbero avere. I titolari del trattamento sono obbligati a comunicare i dati rettificati a ogni destinatario a cui sono stati divulgati i dati personali, salvo che ciò non si riveli impossibile o comporti uno sforzo sproporzionato. I titolari del trattamento non possono sostenere che la gestione di grandi set di dati è troppo complessa per garantire la rettifica al fine di evitare questo requisito.

9.3 Diritto alla cancellazione

Gli interessati hanno il diritto di chiedere ai titolari del trattamento la cancellazione dei loro dati personali (cfr. la sotto-sezione "Diritto alla cancellazione" nella sezione "Diritti degli interessati" della Parte generale dei presenti Orientamenti). Tuttavia, l'uso del cloud computing, l'esistenza di diversi server e repository, la possibilità che i dati siano trattati da diversi responsabili del trattamento e titolari del trattamento, rende difficile garantire che tutte le copie di backup e i dati personali -e non solo le loro chiavi di crittografia- siano cancellati. Per evitare tali risultati, i titolari del trattamento dovrebbero monitorare attentamente le procedure.

Infine, i titolari del trattamento devono tenere presente che questo diritto non copre il trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" o quando "lede i diritti e le libertà altrui". Se la cancellazione di alcuni dati potrebbe causare gravi danni ai diritti e alle libertà altrui, la cancellazione non dovrebbe essere consentita. Inutile dire che questo comporta la necessità di bilanciare i diversi interessi coinvolti.

9.4 Diritto di limitare il trattamento

Secondo l'Articolo 18 dell'RGPD, l'interessato ha il diritto di ottenere dal titolare del trattamento una limitazione del trattamento quando si verifica una delle circostanze descritte in questo articolo (vale a dire: l'accuratezza dei loro dati è contestata; il trattamento è illecito e l'interessato si è opposto alla cancellazione dei suoi dati personali; il titolare del trattamento non ha più bisogno dei dati personali, ma è tenuto a conservarli; o l'interessato si oppone altrimenti al trattamento).

Dal momento che nel trattamento è coinvolto un titolare del trattamento diverso dal social network che ha originariamente raccolto i dati, potrebbe essere utile ricordare che questo diritto deve essere esercitato attraverso uno qualsiasi degli attori coinvolti, che dovrebbe informare il resto della richiesta e procedere di conseguenza. In questo contesto, può essere molto utile sviluppare accordi di condivisione dei dati che aiutino a chiarire le responsabilità attribuite a ciascuno di questi ruoli nell'esecuzione delle specifiche attività di trattamento dei dati da svolgere, se le politiche di sviluppo non chiariscono questo aspetto.

9.5 Diritto di opposizione

Gli interessati devono avere la possibilità di revocare qualsiasi consenso prestato in precedenza a un trattamento specifico di dati e di opporsi al trattamento dei dati che li riguardano (cfr. la sotto-sezione "Diritto di opposizione" nella sezione "Diritti degli interessati" della Parte generale dei presenti Orientamenti). L'esercizio di tale diritto deve essere possibile senza alcun vincolo tecnico o organizzativo e gli strumenti forniti per registrare questa revoca devono essere accessibili, visibili ed efficaci. Pertanto, i ricercatori/innovatori devono rendere questa opzione disponibile per gli interessati non appena iniziano a trattare i dati raccolti dai social network.

9.6 Diritto alla portabilità dei dati

Secondo l'RGPD, gli interessati hanno diritto alla portabilità (cfr. la sotto-sezione "Diritto alla portabilità" nella sezione "Diritti degli interessati" della Parte generale dei presenti Orientamenti). Per far fronte a questo requisito, i titolari del trattamento devono conservare i dati in formati standardizzati che consentano agli interessati di trasmettere i dati che hanno fornito da un'applicazione automatizzata, come un social network, a un'altra. [48]

In ogni caso, è necessario sottolineare che il diritto alla portabilità dei dati si applica solo ai dati "riguardanti" l'interessato e ai dati che hanno "fornito" al titolare del trattamento. Di conseguenza, sia i dati anonimizzati che quelli inferiti o derivati non sono inclusi nel diritto alla portabilità, poiché i dati anonimizzati non riguardano l'interessato e i dati inferiti o derivati non sono stati forniti dall'interessato.

Lista di controllo: diritti degli interessati

□ I titolari del trattamento hanno introdotto le procedure necessarie per garantire che i diritti degli interessati siano adeguatamente soddisfatti, indipendentemente dal fatto che si tratti degli utenti finali o di terzi.

□ I titolari del trattamento hanno introdotto le procedure necessarie a garantire che i diritti degli interessati siano soddisfatti in tempo (entro un mese dalla richiesta, prorogabile di altri due mesi in relazione alla complessità del compito e al numero di richieste).

□ I titolari del trattamento hanno introdotto strumenti efficaci per garantire che gli interessati siano in grado di esercitare i loro diritti in modo pratico, ad esempio introducendo standard di interoperabilità dei dati.

□ Gli interessati sono in grado di avere accesso a tutti i loro dati personali, compresi i dati osservati, ottenuti, inferiti e dedotti

□ I titolari del trattamento hanno fornito agli interessati l'accesso remoto ai loro dati personali. In particolare, i titolari del trattamento che forniscono servizi online basati su dati personali hanno fornito uno strumento online a questo scopo.

□ I titolari del trattamento hanno introdotto strumenti in grado di comunicare i dati rettificati ad ogni destinatario a cui sono stati divulgati i dati personali, salvo che ciò si riveli impossibile o comporti uno sforzo sproporzionato.

□ I titolari del trattamento hanno introdotto strumenti in grado di garantire che tutti i dati siano efficacemente cancellati su richiesta degli interessati se non ci sono motivi

[48] Cfr. I. GRAEF, Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union (22 luglio 2013). Telecommunications Policy 2015, Vol. 39, N. 6, pag. 502-514.

legittimi per opporsi a tale richiesta.

 I titolari del trattamento hanno introdotto interfacce di uso agevole per gli utenti che intendono ottenere dati aggregati e/o dati grezzi che ancora conservano. Questi strumenti consentono agli interessati di esportare facilmente i loro dati in un formato strutturato e di uso comune.

 I titolari del trattamento hanno documentato tutte le informazioni relative a questi problemi.