Incaricato cantonale della protezione dei dati
6501 Bellinzona
www.ti.ch/protezionedati

05.05.2025

Dati Social e amministrazione pubblica: Riflessioni su vincoli legali e costituzionali

L'analisi dei Social media da parte delle istituzioni pubbliche può comportare rischi significativi sotto il profilo legale e costituzionale, poiché può implicare il trattamento di dati personali meritevoli di particolare protezione. Tale pratica deve rispettare i principi della Legge sulla protezione dei dati e della Costituzione, in particolare la libertà di espressione e il divieto di discriminazione. I dati social, pur utili in alcuni casi, possono non essere giuridicamente affidabili né sempre ammissibili in sede legale, e verificarne l'attendibilità richiede risorse sproporzionate. Il loro utilizzo istituzionale può contrastare con la finalità originaria della comunicazione tra privati, violando il principio di buona fede e minando la fiducia verso lo Stato. L'impiego dell'intelligenza artificiale per automatizzare queste analisi amplifica i rischi, sollevando questioni legate a privacy, giurisdizione e sicurezza. In sintesi, l'uso dei social media a fini di monitoraggio istituzionale è incompatibile con i principi dello Stato di diritto e rischia di compromettere la legittimità e la trasparenza dell'azione amministrativa.

Condizioni costituzionali e legali

La Costituzione federale della Confederazione Svizzera (Cost; RS 101), la Costituzione della Repubblica e Cantone Ticino (Cost./TI; RL 101.000) e la Legge cantonale sulla protezione dei dati (LPDP; RL 163.100) quale normativa di attuazione pongono i seguenti limiti cumulativi all'analisi dei Social media da parte delle istituzioni pubbliche, a prescindere dalle tecnologie di analisi utilizzate (intelligenza artificiale o altro) e da eventuali differenze di qualità dei dati dei Social media analizzati. Il presente documento non entrerà, per contro, nel merito di altre esigenze della protezione dei dati – non di rilievo, a conseguenza dei motivi che verranno esposti di seguito - quali la buona fede (informazione, art. 7 cpv. 2 LPDP), la sicurezza dei dati (art. 17 LPDP) e la garanzia dei diritti di accesso, di rettifica, di blocco e d'interruzione (art. 23 segg. LPDP).

1. Motivo giustificativo (base legale per elaborazioni sistematiche di dati personali, oppure, in singoli casi, necessità per l'adempimento di un compito legale o consenso, art. 6 LPDP)
2. Liceità (art. 7 cpv. 1 LPDP)
3. Proporzionalità (art. 7 cpv. 3 LPDP)
4. Finalità (art. 7 cpv. 4 LPDP)
5. Esattezza (art. 7 cpv. 5 LPDP)

1. Motivo giustificativo (art. 6 LPDP)

L'esplorazione dei Social media del cittadino, sia esso di nazionalità svizzera o straniera, può implicare l'elaborazione di dati meritevoli di particolare protezione ai sensi dell'art. 4 cpv. 2 LPDP. La sfera privata, familiare, professionale, intima, così come le opinioni politiche, filosofiche o religiose, lo stato psichico, mentale o fisico, possono essere svelate. Ciò, in particolare se l'autorità non espone i criteri – categorie di dati personali ricercati, filtri, ecc. – che intenderebbe, se del caso, applicare. Una simile elaborazione di dati – premesso che adempia i criteri della proporzionalità e dell'interesse pubblico e

che venga poi, se del caso, chiarita in tutti i suoi elementi costitutivi (organo responsabile, categorie di dati elaborati, scopo, eventuale trasmissione a terzi, durata di conservazione dei dati, misure di sicurezza, ecc.) - sarebbe soggetta all'obbligo della base legale in senso formale ai sensi dell'art. 6 cpv. 1 LPDP, a prescindere dalla sistematicità o meno della stessa (art. 4 cpv. 4 LPDP). A ragione della sensibilità dei dati e della incisività nei diritti fondamentali che potrebbe implicare, una simile elaborazione di dati non potrebbe, infatti, in alcun caso avvenire senza che sia adempiuta la condizione della base legale posta dalle Costituzioni federale e cantonale per la violazione lecita dei diritti fondamentali (combinati art. 13 cpv. 2 e 36 cpv. 1 Cost., art. 8 cpv. 2 lett. d) e cpv. 3 Cost./TI).

L'analisi dei profili Social sulla base del consenso deve essere esclusa. Il consenso, infatti, non sarebbe sempre libero, poiché il cittadino, pur di evitare possibili effetti negativi sulla pratica amministrativa che lo concerne, si troverebbe di fatto obbligato, almeno in singoli casi, a concedere il suo assenso, anche se in totale contrasto con la sua volontà. A causa dell'indistinguibilità delle diverse tipologie di consenso (giuridicamente valido/non valido), quest'ultimo risulterebbe, per presunzione legale, sempre e soltanto un'accettazione delle condizioni indispensabili per ottenere quanto auspicato nei confronti dello Stato, priva di validità giuridica, poiché non libera essendo ottenuta sotto la pressione di una condizione coercitiva ("senza consenso, niente prestazione statale"). Ciò contrasta con il principio di libertà che dovrebbe caratterizzare ogni accordo in materia di trattamento dei dati personali.

Quanto al motivo giustificativo della necessità per l'adempimento di un compito legale, è da escludere per i motivi di cui alle considerazioni al p.to 3 (proporzionalità).

2. Liceità (art. 7 cpv. 1 LPDP)

Il principio della liceità implica la conformità dell'elaborazione dei dati con l'insieme del diritto. Questo principio solleva problematiche e mette in discussione l'analisi dei Social media da parte delle istituzioni pubbliche, non solo a causa dei principi e delle condizioni della LPDP qui esposti, ma anche in virtù del diritto costituzionale, in particolare della libertà di opinione e di espressione (art. 16 Cost., art. 8 cpv. 2 lett. c) Cost./TI), nonché della proibizione dell'arbitrio e della discriminazione (art. 8 e 9 Cost., art 7 Cost./TI). Tutti questi valori costituzionali sono messi sotto pressione dall'analisi dei Social media, al punto da risultare potenzialmente compromessi in modo arbitrario, a causa della violazione dei principi giuridici qui esposti.

3. Proporzionalità (art. 7 cpv. 3 LPDP)

Secondo il principio della proporzionalità, l'elaborazione di dati deve essere *a)* idonea, *b)* necessaria allo scopo perseguito e *c)* deve sussistere un rapporto ragionevole tra scopo perseguito e violazione della personalità che ne deriva (proporzionalità in senso stretto).

Idoneità

I dati sui Social media, sebbene possano contenere informazioni utili e talvolta precise, non sono generalmente considerati giuridicamente certi e affidabili come fonte ufficiale per scopi legali o amministrativi. Ciò, innanzitutto, poiché i dati pubblicati sui social media possono essere facilmente manipolati o falsificati, sia dalla persona interessata, sia da terzi non autorizzati. Le persone interessate o terzi non autorizzati possono pubblicare informazioni errate o intenzionalmente fuorvianti, e la piattaforma stessa potrebbe non essere in grado di garantire l'autenticità dei contenuti in tutti i casi. Ad esempio, attraverso falle nella sicurezza dei dati, post, commenti e immagini possono essere modificati o alterati dopo la pubblicazione, rendendo difficile garantirne la veridicità, l'autenticità e l'integrità nel tempo. In secondo luogo, molti dei contenuti sui Social media sono informali e non

sottoposti a un processo di verifica come accadrebbe per documenti o dati ufficiali. Non essendo sottoposti a una revisione giuridica o a una certificazione, non possono essere considerati come fonti certe e serie di prova in un contesto legale. In un contesto giudiziario, tali mezzi di prova potrebbero essere considerati inammissibili, con la conseguenza che la rispettiva decisione potrebbe essere considerata nulla oppure annullabile. In terzo luogo, su molte piattaforme social, gli utenti possono scegliere di utilizzare pseudonimi o identità non verificabili. Questo rende difficile attribuire con certezza i contenuti a una persona specifica, aumentando il rischio di errori nell'identificazione e di utilizzo improprio di dati non verificati. I contenuti sui Social media possono, poi, essere influenzati da bias (pregiudizi) individuali o collettivi o da emozioni o sentimenti delle istituzioni pubbliche che visualizzano le informazioni, senza consistenza nel tempo. Le persone interessate o terzi non autorizzati che ne hanno preso le veci possono, per di più, pubblicare opinioni, affermazioni o emozioni in modo che non riflettano necessariamente fatti oggettivi. Le informazioni sui social media sono poi spesso espressione di visioni personali, che potrebbero non essere neutrali o accurate. In definitiva, i dati sui Social media non possono essere considerati giuridicamente certi, attendibili e utilizzabili per scopi ufficiali senza una conferma o verifica adeguata. La loro ammissibilità in giudizio è soggetta a ponderazione, dove appare evidente che la stessa risulti nella stragrande maggioranza dei casi favorevole alla tutela dei diritti delle persone interessate. In altre parole, la loro solidità come mezzo di prova non è, di principio, data. Una loro ipotetica affidabilità dipenderebbe tra l'altro dal contesto, dalle circostanze specifiche e, soprattutto, dalla capacità di verificarne l'autenticità. Quest'ultimo aspetto potrebbe implicare, però, un dispendio di risorse completamente sproporzionato rispetto agli scopi amministrativi perseguiti, già di norma garantiti da documentazione e chiarimenti ufficiali. Per questi motivi, l'idoneità dei dati social quale elemento del principio della proporzionalità non è, di principio, data.

Necessità

Poiché i dati in questione sono inidonei, non possono essere considerati nemmeno necessari per il raggiungimento di scopi amministrativi. La mancanza di necessità è ulteriormente confermata dalla documentazione ufficiale, di regola ampiamente sufficiente. La documentazione ufficiale prevale comunque e in ogni caso su qualsiasi informazione rinvenuta su internet, la cui veridicità e attendibilità giuridica, come già sottolineato, è tutto fuorché garantita.

Rapporto ragionevole equilibrato tra scopo perseguito e violazione della personalità che ne risulta

Alla luce di quanto sopra esposto, è evidente il netto squilibrio tra gli obiettivi istituzionali perseguiti e la violazione dei diritti fondamentali che ne risulta.

4. Finalità (art. 7 cpv. 4 LPDP)

Secondo il principio della finalità, i dati personali non possono essere utilizzati o trasmessi per uno scopo che, secondo la buona fede, sarebbe incompatibile con quello per il quale originariamente erano stati raccolti. Questo principio rappresenta un fondamento essenziale nella protezione dei diritti degli individui, garantendo che l'utilizzo dei loro dati avvenga sempre in modo coerente e conforme agli scopi dichiarati al momento della raccolta. Di regola non vi è lesione della personalità se la persona interessata ha reso i suoi dati personali accessibili a chiunque e non si è opposta espressamente al trattamento. Ciò vale anche per l'elaborazione di dati meritevoli di particolare protezione. Questa presunzione giuridica può tuttavia essere rovesciata dalla persona interessata, per il tramite della prova della violazione della sua personalità, segnatamente qualora venga comprovato che l'elaborazione non è conforme con lo scopo per il quale le informazioni erano state pubblicate. Così, anche qualora la persona interessata non si sia espressamente opposta all'elaborazione, il principio

della finalità può essere violato, se l'elaborazione viola i principi generali della protezione dei dati e, in particolare, se l'elaborazione non rientra nello scopo di pubblicazione deducibile dalle circostanze. Può in questo senso, ad esempio, violare la personalità, la raccolta sistematica e consolidata di tutte le informazioni su una persona, reperibili in rete o altrove, per poi essere riutilizzate per scopi diversi[1]. L'analisi dei Social media in questione può perciò essere lesiva al principio della finalità, poiché è evidente che, sebbene i dati sui Social media siano parzialmente o totalmente "tecnicamente" accessibili al pubblico (perlomeno quando i profili sui Social media sono aperti), tale accessibilità è originariamente finalizzata alla socializzazione e alla comunicazione tra persone private, nell'esercizio della loro libertà di opinione e di espressione, e non all'uso istituzionale. L'utilizzo dei dati nel contesto istituzionale travalicherebbe i limiti della buona fede e risulterebbe in una violazione delle aspettative legittime delle persone interessate nei confronti dello Stato di diritto.

5. Esattezza (art. 7 cpv. 5 LPDP)

La presenza di profili falsi, come spiegato in precedenza, che in un contesto digitale possono essere una realtà, rende problematico l'uso delle informazioni reperite sui Social media per fini ufficiali. Non solo l'esattezza dei dati può non essere garantita, ma si può esporre il processo istituzionale a un margine di errore potenzialmente elevato, con il rischio di penalizzare ingiustamente il cittadino sulla base di informazioni inutili, fuorvianti, non aggiornate o sbagliate.

Conclusioni

L'analisi dei profili Social del cittadino per scopi istituzionali risulta incompatibile con i principi fondamentali su cui si fonda la protezione dei dati e con lo Stato di diritto in generale. Se attuata, rischia di minare il rapporto di fiducia tra le istituzioni e il cittadino, che non può essere ridotto a oggetto di monitoraggio indiscriminato. Introdurrebbe inoltre una dinamica di sfiducia reciproca anche tra le autorità coinvolte nei processi decisionali, con il rischio di compromettere l'integrità delle procedure amministrative e di erodere la legittimità delle decisioni prese, alimentando un clima di sospetto. Rischierebbe di ingaggiare la responsabilità civile dello Stato e potrebbe dare adito a raccomandazione dell'Incaricato cantonale della protezione dei dati (art. 30*b* LPDP).

Ciò in particolare perché si esporrebbe il processo istituzionale a un margine di errore potenzialmente molto elevato, con il rischio di penalizzare ingiustamente il cittadino sulla base di informazioni personali sensibili e nel contempo irrilevanti e/o errate, e di esporre di conseguenza la decisione all'azione giudiziaria. Un particolare punto di preoccupazione riguarda l'uso dell'intelligenza artificiale per l'analisi dei Social media. L'introduzione di tecnologie automatizzate iper-performanti per scandagliare i dati privati del cittadino, oltre a presentare un rischio elevato d'invasione nei diritti fondamentali, solleverebbe problemi nella gestione dei dati stessi. Non sarebbe affatto chiaro in quale Paese verrebbero salvati questi dati personali, con tutte le implicazioni che ciò comporta in termini di giurisdizione e protezione delle informazioni sensibili. Salvo casi eccezionali previsti dal diritto, è perciò imperativo evitare di legittimare e attuare l'analisi dei profili Social a scopi istituzionali e ribadire che la protezione dei diritti fondamentali deve prevalere su ogni tentativo di sorveglianza indiscriminata e di controllo sociale.

[1] CORRADO RAMPINI/REHANA C. HARASGAMA, Basler Kommentar, Datenschutzgesetz/Öffentlichkeitsgesetz, Blechta/Vasella (editori), Basilea 2024, art. 30 N 24 segg.; JOSÉPHINE BOILLAT/STÉPHANE WERLY, Commentaire romand, Loi fédérale sur la protection des données, Meier/Métille (editori), Basilea 2023, art. 30 N 34; THOMAS STEINER/CHRISTIAN LAUX, DSG Kommentar zum Schweizerischen Datenschutzgesetz mit weitern Erlassen (Orell Füssli Kommentar OFK), Bieri/Powell (editori), Zurigo 2023, art. 30 N 37 segg.