Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Incaricato federale della protezione dei dati e della trasparenza
IFPDT

LINEE GUIDA[1]

del 1° dicembre 2022

delle autorità per la protezione dei dati di Confederazione e Cantoni

per l'applicazione del diritto in materia di protezione dei dati al trattamento digitale di dati personali in relazione a elezioni e votazioni in Svizzera

Ai fini di migliorare la leggibilità e la chiarezza, nel documento non sono utilizzati rinvii specifici ai testi di legge.

[1] Questo aggiornamento sostituisce la versione del 1° giugno 2019.

Feldeggweg 1, 3003 Berna
Tel. 058 463 74 84, fax 058 465 99 96
www.edoeb.admin.ch/edoeb/it/home.html

Indice

1 Di cosa si tratta?

La società digitale è una realtà globale in cui si svolgono anche elezioni e votazioni a tutti i livelli federali della Confederazione. In questo contesto si presentano fenomeni sempre nuovi concernenti il trattamento dei dati, che possono avere conseguenze sul comportamento connesso a elezioni e votazioni. La comunicazione online offre agli attori del processo di formazione dell'opinione politica l'opportunità di trasmettere messaggi agli aventi diritto di voto o di entrare in comunicazione con loro in modo rapido ed economico, in particolare anche se questi evitano i media tradizionali per motivi di costi o per altre ragioni e utilizzano soprattutto le piattaforme digitali di dati per le informazioni e lo scambio sociale.

Nel settore dell'e-commerce grandi quantità di dati personali sono ottenute ed elaborate in modo automatizzato. L'analisi di questi dati consente di offrire a clienti potenziali o già esistenti merci e servizi adeguati al loro profilo utilizzando messaggi pubblicitari personalizzati. I metodi di trattamento automatizzati di «big data», «analytics», definizione di un profilo e «microtargeting» sono impiegati anche per rivolgersi in modo mirato agli aventi diritto di voto al fine di trasmettere informazioni con cui i partiti e i gruppi di interesse tentano di influenzare la formazione dell'opinione politica nel periodo precedente a votazioni ed elezioni.

Secondo la Costituzione federale, la garanzia dei diritti politici protegge la libera formazione della volontà e l'espressione fedele del voto. Le autorità per la protezione dei dati contribuiscono a un andamento del processo politico conforme alla Costituzione, incoraggiando gli attori coinvolti a rispettare la tutela della sfera privata e del diritto all'autodeterminazione delle cittadine e dei cittadini in materia di informazione e i principi che ne derivano per il trattamento dei dati personali. Chi tratta dati nel contesto di elezioni e votazioni deve essere consapevole del fatto che il diritto in materia di protezione dei dati sottopone i dati relativi a opinioni politiche e ideologiche a un livello di protezione più elevato rispetto a dati comparabili in un contesto commerciale e che il responsabile deve pertanto soddisfare requisiti maggiori per il trattamento consentito.

2 Autorità di sorveglianza competenti e diritto applicabile

Se stabiliscono riferimenti a persone identificate o identificabili e provengono da privati o da autorità federali, i metodi di trattamento sono soggetti alla legge federale sulla protezione dei dati (LPD) e all'attività di sorveglianza dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT). Se il trattamento dei dati personali è invece svolto da autorità dei Cantoni o Comuni che si occupano di elezioni e votazioni, sono determinanti le legislazioni cantonali sulla protezione dei dati e le norme di sorveglianza vigenti a livello locale. Per questa ragione le presenti linee guida sono redatte congiuntamente dall'IFPDT e dalla Conferenza degli incaricati cantonali per la protezione dei dati (privatim).

A livello federale, il 1° settembre 2023, quindi poco prima delle elezioni per il rinnovo del Parlamento, entreranno in vigore la legge sulla protezione dei dati del 25 settembre 2020, completamente rivista, e le relative ordinanze esecutive. Per maggiori informazioni a questo proposito si rimanda alla nostra pubblicazione «La nuova legge sulla protezione dei dati dal punto di vista dell'IFPDT». Anche varie leggi cantonali sulla protezione de dati sono attualmente in fase di revisione (cfr. anche il n. 8.1 di seguito).

3 Destinatari e scopo delle linee guida

Le linee guida si rivolgono a tutti i partiti politici, nonché ad altri attori di formazione dell'opinione.

Le autorità per la protezione dei dati redigono queste linee guida in adempimento del proprio compito legale che consiste nell'offrire consulenza a privati e organi pubblici nonché nel sensibilizzare l'opinione pubblica sui rischi sistemici del trattamento dei dati personali. Le linee guida hanno lo scopo di offrire un ausilio per l'interpretazione del diritto cantonale e federale applicabile che permetta ai destinatari di valutare quali metodi di trattamento sono autorizzati ai sensi del diritto in materia di protezione dei dati dal punto di vista delle autorità competenti nel contesto della formazione della volontà politica nello spazio digitale, nonché quali sono i requisiti da soddisfare.

Le linee guida intendono incoraggiare gli attori della formazione dell'opinione politica ad applicare metodi di trattamento digitali riconoscibili e comprensibili per gli elettori. Occorre tuttavia ben distinguere il diritto alla trasparenza conformemente alla legislazione in materia di protezione dei dati dalla nozione di veridicità dei contenuti, affrontata nel dibattito pubblico a proposito delle cosiddette «fake news», la quale non è oggetto della legislazione in materia di protezione dei dati né può essere tematizzata nelle presenti linee guida. Anche la questione del voto elettronico non è affrontata in questa sede.

4 Attori

4.1 Partiti politici e gruppi d'interesse

Il trattamento dei dati nel processo politico e il relativo obiettivo legittimo di influire sulla formazione dell'opinione politica sono voluti innanzitutto da partiti politici e gruppi d'interesse, che perseguono scopi politici, religiosi, sociali, scientifici o altri ideali sotto forma di istituzioni di diritto privato come associazioni o fondazioni.

Nel contesto del processo politico, i partiti e i gruppi d'interesse sono liberi di coinvolgere terzi nel trattamento dei dati, trasferendo del tutto o in parte il processo a questi ultimi o avvalendosi di dati di terzi.

I partiti politici e i gruppi d'interesse, in quanto «responsabili» o, secondo il diritto vigente, «detentori privati di collezioni di dati», si assumono la responsabilità globale della raccolta, della conservazione, della gestione e dell'ulteriore utilizzo dei dati ivi elaborati (cfr. tabella A).

4.2 Titolari del trattamento o responsabili del trattamento

Secondo la legislazione in materia di protezione dei dati il trattamento dei dati personali può essere effettuato in due ruoli: come titolare del trattamento (nell'attuale legge federale anche «detentore di una collezione di dati») o come responsabile del trattamento. Il responsabile è un privato o organo federale che, singolarmente o insieme ad altri, determina lo scopo e i mezzi del trattamento (cfr. tabella A) Il responsabile del trattamento è il privato o l'organo federale che trattata dati personali per conto del titolare del trattamento (cfr. tabella C). Quest'ultimo mantiene la competenza, o appunto la responsabilità, per il rispetto delle disposizioni in materia di protezione dei dati, anche quando il trattamento dei dati personali è trasferito a un terzo (responsabile del trattamento). È possibile inoltre che la responsabilità sia ripartita fra più attori che trattano dati.

> *Esempio: l'elettore A visita il sito Internet di un partito e ne consulta il programma, senza aderirvi. Il partito intende, attraverso i social media, rivolgersi in modo mirato agli elettori che hanno visitato il sito Internet senza aderirvi, vale a dire elettori come A.*
>
> *A tale scopo il partito ha inserito nel proprio sito Internet un cosiddetto baco invisibile (tracking pixel), che viene letto dai social media. Si tratta di un componente aggiuntivo che il proprietario*

di un sito Internet può integrare nello stesso. Quando un elettore visita tale sito, il suo browser stabilisce automaticamente un collegamento con i server dei social media, inviando loro una serie di informazioni sull'elettore. In questo modo i social media possono di norma sorvegliare ogni visita del sito. Questo avviene, ad esempio, per aggregare gli elettori a un determinato gruppo di destinatari della pubblicità nei social media. Quindi A, dopo aver lasciato il sito Internet del partito e visitato i social media, vedrà la pubblicità del partito sui social media.

Il partito e i social media hanno una responsabilità comune.

Se il responsabile del trattamento si trova, dal punto di vista del diritto in materia di protezione dei dati, in un Paese terzo non sicuro, dovranno essere adottate misure speciali. Una situazione di questo tipo si verifica ad esempio quando i dati personali sono salvati su un server statunitense. Maggiori informazioni a tale proposito sono pubblicate sul sito Internet dell'IFPDT (link: Trasmissione all'estero (admin.ch)

4.3 Registri pubblici

I Comuni tengono un registro degli aventi diritto di voto – il catalogo elettorale, la cui base è costituita dal controllo abitanti. Ai sensi della legislazione concernente la dimora e il domicilio, le persone in arrivo o in partenza sono tenute a notificare questi eventi presso il Comune esibendo un documento ufficiale e sono così iscritti o radiati dal controllo abitanti. Il controllo abitanti consente pertanto di determinare l'inizio e la fine della legittimazione al voto e di registrare correttamente gli aventi diritto nel catalogo elettorale. I cataloghi elettorali fungono da base per elezioni e votazioni sia federali sia cantonali e comunali. Il diritto federale prescrive che il catalogo elettorale sia pubblicamente accessibile agli aventi diritto di voto. I Cantoni determinano le modalità di tale accesso (visione sul posto, consegna di elenchi cartacei, consegna in forma digitale) e disciplinano anche se e in quale forma concedere l'accesso al controllo abitanti.

Alcuni Cantoni raccolgono i controlli abitanti comunali in un registro comprendente tutti gli abitanti del Cantone. Non di rado questi registri centralizzati sono integrati con ulteriori dati (p. es. indirizzo e-mail e numero di cellulare tratti dalla dichiarazione delle imposte).

Nel quadro della propria responsabilità globale di detentori di collezioni di dati statali, gli enti pubblici competenti per i registri pubblici devono assicurarsi che i dati ivi elaborati siano conservati in modo sicuro e trasferiti a terzi solo se consentito dalla legge. Devono garantire che i dati non siano utilizzati in modo inadeguato e non siano diffusi in modo incontrollato (cfr. tabella B).

Le misure tecniche e organizzative adottate dagli enti pubblici per proteggere questi dati centralizzati sono varie. I dati relativi a indirizzi e contatti sono dati personali che rientrano nella legislazione in materia di protezione dei dati, ma in linea di principio non sono considerati degni di particolare protezione.

Il diritto cantonale può prevedere che i controlli abitanti dei Comuni possano rendere noti su richiesta di privati, partiti o altri terzi interessati dati concernenti gli indirizzi di abitanti ordinati secondo determinati criteri (vale a dire sotto forma di elenchi, p. es. giovani cittadini). Di norma questi elenchi possono essere utilizzati dai richiedenti per scopi precisi e spesso di natura ideale e non possono essere trasmessi a terzi. Il servizio competente del Comune verifica che i presupposti di legge per rendere noti i dati siano soddisfatti e può infine comunicarli al richiedente. Gli abitanti dei Comuni che desiderano proteggere i propri dati personali presso il controllo abitanti hanno la possibilità di bloccarne la diffusione sotto forma di elenchi o in generale la trasmissione a terzi. Ciò presuppone che il Comune informi le persone interessate in merito alle condizioni e alla portata della comunicazione nonché alle possibilità di bloccare la trasmissione. Finora, le autorità hanno offerto raramente possibilità specifiche di bloccare la pubblicità politica. Nella pratica si cerca di adottare provvedimenti adeguati affinché le misure di protezione date

a livello di controllo abitanti o di catalogo elettorale, come ad esempio il diritto di blocco nell'ambito del controllo abitanti, non siano aggirate dalla possibilità di visionare l'altro registro e viceversa.

4.4 Imprese di analisi dei dati

Le imprese di analisi dei dati possono essere incaricate di gestire e analizzare i dati rilevanti di partiti o gruppi d'interesse. Si può trattare ad esempio di agenzie di comunicazione o di altre imprese che si sono specializzate in determinati processi di analisi (ad es. analisi di siti Internet, agenzie crawler).

Le imprese che si occupano di analisi dei dati possono essere nel contempo anche fornitori di dati, che si procurano in autonomia informazioni da diverse fonti, le valutano e poi le mettono a disposizione dei gruppi interessati dietro compenso.

I fornitori privati di dati trattano i dati personali nel contesto del processo politico come detentori con responsabilità globale (cfr. tabella A) oppure come responsabili del trattamento (cfr. tabella C).

4.5 Fornitori di dati

Fornitori di indirizzi professionali e di servizi simili raccolgono informazioni di ogni tipo consultabili secondo caratteristiche personali, che trattano e commercializzano in modo sistematico e per quanto possibile strutturato. I dati offerti provengono da una serie di richieste, registrazioni, ordinazioni e dichiarazioni compilate nel contesto di ordinazioni di merci e prestazioni, condizioni di contratto o concorsi. Sono utilizzate come fonti di dati anche le informazioni pubblicate dalle autorità come statistiche su risultati elettorali o tassi di disoccupazione nonché pubblicazioni, registri di commercio ed elenchi di debitori. Altri dati sono rilevati effettuando sondaggi presso i consumatori o raccolti valutando le fonti pubblicamente accessibili. Combinando i dati provenienti da varie fonti, questi fornitori professionali integrano ad esempio gli indirizzi privati con varie informazioni supplementari come il comportamento in termini di consumo, la demografia sociale o la situazione abitativa e di vita.

I fornitori privati di dati trattano i dati personali nel contesto del processo politico come detentori con responsabilità globale (cfr. tabella A) oppure come responsabili del trattamento (cfr. tabella C).

4.6 Piattaforme di dati

Piattaforme di dati di gestori di motori di ricerca come Google o reti sociali che facilitano comunicazione e incontri virtuali come Facebook o Twitter raccolgono attributi personali come nome, sesso ed età, forniti dagli utenti registrati che dispongono di un conto. A ciò si aggiungono ampie serie di dati archiviate automaticamente, lasciate da utenti di Internet (registrati o meno) quando visitano le piattaforme di dati. Tra queste vi sono dati tecnici come indirizzi IP o numeri di dispositivi nonché informazioni su pagine contrassegnate con «mi piace», messaggi condivisi ecc. Oltre a queste sono raccolte anche informazioni di pagine web esterne o app, legate alle rispettive piattaforme da partenariati pubblicitari.
Altre piattaforme specializzate nella raccolta di firme per delle votazioni raccolgono grandi quantità di dati di contatto, tra cui indirizzi e-mail, indirizzi residenziali e preferenze politiche. Queste piattaforme possono essere gestite dai partiti o dai gruppi d'interesse stessi o mettere a disposizione i loro servizi e dati in qualità di fornitori terzi.
Se le piattaforme di dati private trattano i dati personali nel contesto del processo politico come detentori con responsabilità globale, devono essere osservate le indicazioni di cui alla tabella A e alla tabella D. Se invece trattano o trasmettono tali dati su mandato, andranno osservate le indicazioni riportate alla tabella C.

4.7 Singole persone

La popolazione avente diritti elettorali e di voto è la destinataria di informazioni trattate allo scopo di formare l'opinione politica nel periodo precedente a elezioni e votazioni. Mentre la pubblicità politica attraverso radio e televisione è vietata e i media stampati pubblicano inserzioni politiche senza aver prima interagito con i singoli lettori, le piattaforme di dati offrono la possibilità di trasmettere messaggi politici mirati a singole persone o gruppi di persone. Questi possono poi commentare e diffondere i messaggi ricevuti. Lo scambio tra miliardi di utenti a livello globale sulle principali piattaforme consente non solo ai gestori delle reti, ma anche alla loro clientela, di accumulare grandi quantità di dati quali indirizzi, testi, suoni e immagini riferiti a famiglie, amici e conoscenti e che consentono di identificare ideologie e preferenze politiche. Tali informazioni sono salvate con gli account utente ad esse collegati nei centri di calcolo dei gestori delle piattaforme e in parte anche su smartphone e altri dispositivi degli utenti. Con la trasmissione mirata o la diffusione pubblica, gli utenti mettono sé stessi e soggetti terzi in condizione di influenzare l'espressione delle opinioni politiche o il comportamento elettorale o di voto di altre persone. Come i detentori professionali di collezioni di dati, anche i singoli destinatari come le persone private hanno una responsabilità relativa al trattamento dei dati personali da loro elaborati nel contesto politico (cfr. tabella A). Per assumersi tale responsabilità devono innanzitutto essere consapevoli di questo fatto.

5 Dati personali nel contesto di elezioni e votazioni

5.1 Dati personali

Sono definiti dati personali tutte le informazioni relative a una persona identificata o identificabile. Dati puramente tecnici senza riferimenti a persone identificate o identificabili non rientrano nel campo di applicazione del diritto in materia di protezione dei dati. Ne deriva che la veridicità dei contenuti politici e la questione dell'influenza esercitata sugli aventi diritto di voto mediante le cosiddette «fake news» non sono oggetto di tale diritto. Se contenuti palesemente scorretti si ripercuotono negativamente sulla personalità e sull'onore di singole persone, si rinvia alle pertinenti disposizioni del Codice civile e del Codice penale (segnatamente all'art. 28 CC nonché all'art. 173 segg. e all'art. 261bis CP)

5.2 Dati personali degni di particolare protezione e profili della personalità

I dati che consentono di risalire a opinioni politiche o ideologiche sono considerati degni di particolare protezione e la legge definisce pertanto requisiti particolari per il loro trattamento. Il trattamento di dati di per sé non sensibili può generare, attraverso ulteriori fasi di elaborazione come l'analisi dei dati o l'arricchimento, dati personali degni di particolare protezione o profili della personalità che diventano degni di particolare protezione per la legge secondo la giurisprudenza del TAF ai sensi della sentenza Moneyhouse.

Benché su questo punto non vi sia ancora una giurisprudenza esaustiva, è lecito supporre che il trattamento digitale dei dati in relazione al processo politico sia di norma soggetto al livello di protezione applicabile ai dati personali degni di particolare protezione, anche solo in ragione della finalità del trattamento di influenzare le opinioni ideologiche di molte persone. Ciò in particolare quando sono impiegati metodi di analisi automatizzati che, abbinando una serie di dati sensibili e non sensibili, permettono di

allestire profili della personalità, per i quali, secondo la giurisprudenza del Tribunale amministrativo federale (TAF) nella questione Moneyhouse[2], è indicata una protezione più elevata degli interessati.

6 Principi del trattamento dei dati

Ogni attore che tratta dati personali nel contesto di elezioni e votazioni deve attenersi ai principi generali della legislazione in materia di protezione dei dati. Per gli organi pubblici è applicato altresì il principio di legalità, secondo cui ogni trattamento di dati personali deve fondarsi su una base legale sufficiente.

6.1 Buona fede e trasparenza

Il trattamento dei dati personali deve avvenire innanzitutto secondo il principio della buona fede. Questo significa che i dati non possono essere rilevati né trattati in un modo che la persona non possa aspettarsi dalle circostanze e con il quale non sarebbe probabilmente d'accordo.

Il principio di trasparenza richiede che la raccolta e qualsiasi tipo di trattamento dei dati devono essere riconoscibili dalla persona interessata. Questo vale anche per le finalità di qualsiasi trattamento dei dati, l'identità di chi tratta i dati e – in caso di trasmissione di dati a terzi – le categorie di possibili destinatari dei dati. Anche la raccolta di dati personali presso terzi come ad esempio i fornitori di dati deve essere riconoscibile per le persone interessate. Solo in questo modo gli aventi diritto di voto possono comprendere con quali metodi di trattamento e tecnologie digitali sono chiamati in causa e influenzati a livello politico. Allo stesso modo, i partiti e i gruppi di interesse possono sostenere che i metodi di trattamento dei dati che utilizzano sono accettati dai cittadini solo se sono riconoscibili e comprensibili.

Gli organi statali che mettono a disposizione dati nel contesto di elezioni e votazioni soddisfano il principio di trasparenza prescritto dal diritto in materia di protezione dei dati attenendosi, nell'adempimento dei loro compiti, alle basi legali pubblicamente accessibili e a eventuali prescrizioni particolari sull'obbligo d'informazione.

6.2 Proporzionalità

Il trattamento dei dati deve continuare a rifarsi al principio della proporzionalità per quanto concerne la quantità di dati personali e la sua durata. Per proporzionalità s'intende che chi tratta i dati possa elaborare solo quelli adatti e obiettivamente necessari a raggiungere uno scopo (legittimo). In tale contesto, tra l'obiettivo perseguito e i mezzi utilizzati deve sussistere un rapporto ragionevole e i diritti delle persone interessate devono essere garantiti. Il trattamento dei dati deve essere ragionevole per le persone interessate in termini sia di finalità sia di mezzi.

6.3 Principio della finalità

Secondo il principio della finalità i dati personali possono essere trattati soltanto per lo scopo indicato all'atto della loro raccolta, risultante dalle circostanze o previsto da una legge. Senza una particolare giustificazione, i dati non possono essere trattati a posteriori in modo non conciliabile con una di queste finalità. Il principio della finalità vale in particolare anche per l'integrazione di servizi o applicazioni di terzi (ad es. servizi di newsletter o programmi per la pianificazione e la gestione di visite porta a porta) che non sono autorizzati a utilizzare i dati per i propri scopi.

[2] Sentenza TAF A-4232/2015 del 18 aprile 2017

6.4 Correttezza dei dati

Chi dispone di una collezione di dati deve anche assicurarsi che i dati in essa contenuti siano corretti, fintantoché questi mostrano una rilevanza personale. Chi tratta i dati deve adottare le misure adeguate affinché i dati personali non corretti o incompleti per quanto concerne le finalità della loro raccolta siano corretti o eliminati.

6.5 Sicurezza dei dati

In ultima analisi, secondo il principio della sicurezza dei dati, i dati personali devono essere tutelati da un trattamento non autorizzato mediante adeguate misure tecniche e organizzative. Devono attenersi a questa tutela non solo i detentori di una collezione di dati, ma anche chiunque tratti i dati, in particolare anche se i dati personali in questione non rappresentano una collezione di dati. L'obbligo riguarda pertanto ogni attore che tratta dati personali nel contesto di elezioni e votazioni. I rischi specifici a livello organizzativo, tecnico e di diritto in materia di protezione dei dati devono essere valutati al fine di adottare misure di tutela appropriate. Questo presuppone che esista una documentazione interna dalla quale emergano le modalità di rispetto degli obblighi menzionati riguardo alle varie categorie di dati trattati.

7 Lesione della personalità e giustificazioni

7.1 Lesione della personalità

Chi tratta i dati personali nel ruolo di responsabile privato non può ledere illecitamente la personalità delle persone interessate. Una lesione della personalità sussiste ad esempio quando è violato un principio del trattamento dei dati (cfr. n. 6), dati personali sono trattati contro la volontà esplicita oppure dati personali degni di particolare protezione o profili della personalità sono resi noti a terzi.

> *Esempio: un partito politico invia una newsletter a persone che si sono abbonate ad essa. Questo trattamento dei dati non lede la personalità delle persone interessate. Non appena una persona cancella la propria iscrizione alla newsletter, un ulteriore invio rappresenterebbe una lesione della personalità in quanto il relativo trattamento dei dati avverrebbe contro la volontà esplicita della persona.*

> *Esempio: un avvocato indipendente si candida per una carica politica e invia pubblicità elettorale ai propri clienti. Non vi è una finalità comune tra la sua attività di avvocato e la pubblicità in vista della sua elezione. Non sussiste nemmeno un collegamento logico tra i due scopi. Inoltre la modifica dello scopo del trattamento non corrisponde alle legittime aspettative dei clienti. L'avvocato non può quindi utilizzare i dati di contatto dei propri clienti senza prima aver ottenuto il loro consenso.*

Una lesione della personalità non è illecita se giustificata mediante il consenso della parte lesa, da un interesse preponderante privato o pubblico o da una legge. Di seguito non è ulteriormente approfondita la base legale come motivo giustificativo (per i relativi esempi si rimanda al n. 4.3).

7.2 Interessi preponderanti privati o pubblici

Una lesione della personalità può essere giustificata da interessi preponderanti privati o pubblici. La ponderazione degli interessi nel singolo caso determina se siano preponderanti gli interessi privati o quelli pubblici. È necessario pertanto valutare quanto peso abbiano effettivamente la lesione della personalità o le potenziali lesioni della personalità e se gli interessi privati o pubblici dietro al trattamento dei dati siano invece così seri da far apparire oggettivamente giustificato e ragionevole per la persona interessata che la protezione della sua personalità debba passare in secondo piano.

Il trattamento dei dati nel contesto politico può giustificare un legittimo interesse privato o pubblico e i diritti politici sono garantiti dalla Costituzione. In quale misura questo interesse abbia la precedenza sulla protezione della personalità e sia quindi da definire prevalente dipende segnatamente da quali dati sono trattati in tale contesto e con quali modalità avviene questo trattamento.

> *Esempio: un partito politico acquista da un fornitore di indirizzi una base di destinatari originariamente rilevata per scopi di marketing. Il partito utilizza poi questi indirizzi per inviare raccomandazioni di voto. Anche se in questo caso è ipotizzabile una violazione del principio della finalità, la relativa lesione della personalità sarà probabilmente classificata come minore, in modo da essere di norma giustificata dall'interesse prevalente del partito.*

7.3 Consenso

Se non vi è alcun interesse preponderante o se chi tratta i dati non vuole esporsi al rischio che tale interesse non venga riconosciuto in una controversia legale, un trattamento dei dati che lede la personalità degli interessati deve essere giustificato mediante il consenso di questi ultimi. Il consenso deve essere libero e informato.

Il consenso è fornito con autodeterminazione se le persone interessate possono acconsentire in modo differenziato all'attivazione o alla disattivazione di singoli aspetti e funzionalità delle applicazioni digitali (p. es. spuntando la relativa casella), scegliendo così effettivamente non solo se, ma anche come e in quale misura mettere a disposizione i propri dati. Gli interessati devono inoltre avere in ogni momento la possibilità di revocare il proprio consenso e di richiedere la cancellazione dei propri dati. Per soddisfare questi requisiti gli attori devono investire in tecnologie che favoriscono la protezione dei dati.

Un consenso informato presuppone che le persone interessate siano informate prima della registrazione in modo onesto e completo in merito al trattamento dei loro dati e al funzionamento dei metodi di analisi utilizzati, inclusi programmi automatici e intelligenza artificiale. Le persone dovranno essere informate anche in merito ai propri diritti, come ad esempio quello di revocare il consenso in ogni momento. Per onesto si intende che l'informazione deve essere facilmente comprensibile a livello linguistico, reperibile in modo rapido e trasmessa in modo chiaro. Sono considerati completi i testi online che rendono accessibili le finalità e gli effetti delle tecnologie e dei metodi di trattamento dei dati digitali a più livelli di profondità esplicativa adeguati ai destinatari e, in particolare, informano sulla durata del trattamento e sull'eventuale trasmissione dei dati. La catena di informazioni inizia con un messaggio breve e ben visibile sulla pagina di registrazione, che spiega i punti più importanti riguardanti il trattamento dei dati. Ciascuno di questi punti contiene link di approfondimento che conducono il lettore ai passaggi rilevanti dei regolamenti sul trattamento dei dati e delle disposizioni in materia di protezione dei dati vigenti. Soprattutto nel contesto politico, un'informazione onesta prevede che gli interessati non siano tratti in inganno da dati fuorvianti o errati su fonti o mittenti e, in caso di comunicazione personale, che sia loro chiaro se stanno interagendo con una persona o con un programma automatico. Inoltre, devono poter riconoscere se un'attribuzione di informazioni online è personalizzata o rivolta a tutti. Se del caso, deve essere possibile comprendere sulla base delle condizioni di utilizzo quali tecnologie e quali criteri sono

applicati per le attribuzioni personalizzate. Un'informazione completa prevede anche indicazioni in merito al trattamento dei dati che sono arricchiti e valutati con informazioni tratte dai social media («social match»).

7.4 Consenso esplicito

Inoltre, per il trattamento di dati degni di particolare protezione o di profili della personalità, il consenso (fornito con autodeterminazione e avendo ricevuto informazioni sufficienti) deve essere anche esplicito. Per ottenere un consenso informato è necessario che l'interessato compia attivamente un'azione di consenso. Un consenso esplicito è dato segnatamente quando le persone interessate si sono registrate sul sito Internet di un attore e hanno espressamente (p. es. spuntando la relativa casella) acconsentito al trattamento dei dati registrati. Dichiarazioni nelle quali le persone si limitano ad accettare le condizioni generali di utilizzo non sono invece considerate consensi espliciti. Lo stesso vale per dichiarazioni con cui le persone si abbonano a richieste o contenuti degli attori o li commentano ad esempio sulle piattaforme sociali. Inoltre, i consensi possono essere riferiti solo ai propri dati. Il trattamento dei dati di persone terze presuppone il loro consenso.

8 Il processo di trattamento dei dati nel contesto politico

Il trattamento dei dati da parte di responsabili privati è facilmente consentito dal diritto svizzero, a condizione di non ledere la personalità degli interessati. Se sussiste una lesione, questa deve essere giustificata (cfr. su tutto questo tema il n. 7). In tale contesto, la legittimità deve essere garantita per l'intero processo di trattamento dei dati. Per illustrare il significato di questo concetto in un contesto politico, il processo può essere suddiviso a livello funzionale in raccolta, analisi, attribuzione di informazioni e contatto con gli interessati.

8.1 Raccolta di dati personali

Se i dati sono raccolti direttamente presso la persona interessata, il relativo processo può essere allestito in modo da garantire il rispetto dei diritti della personalità degli interessati (cfr. a tale proposito quanto sopra esposto al n. 7). In questo contesto è cruciale rispettare la trasparenza e la finalità nonché l'obbligo d'informazione nella raccolta di dati personali degni di particolare protezione e nell'elaborazione di profili della personalità. Gli interessati devono pertanto essere informati soprattutto in merito a quali dati sono trattati, con quali scopi e con quali modalità. Con l'entrata in vigore la nuova legge sulla protezione dei dati nel settembre 2023, l'obbligo d'informazione sarà applicato anche alla raccolta di dati personali non degni di particolare protezione («La nuova legge sulla protezione dei dati dal punto di vista dell'IFPDT»).

Se sono altresì rispettati gli altri principi di trattamento e non sono comunicati a terzi né dati personali degni di particolare protezione né profili della personalità, la personalità delle persone interessate non è violata, per cui non è necessario giustificare il trattamento dei dati.

> *Esempio: un partito integra l'insieme di dati rilevati nell'ambito dell'invio della newsletter con informazioni ottenute mediante raccolte di firme o rivolgendosi personalmente alla popolazione con stand, visite a domicilio o telefonate. Si procura inoltre dati da fonti pubblicamente accessibili come elenchi telefonici o registri pubblici. Il partito raccoglie la gran parte dei dati*

presso le persone interessate e, al momento della raccolta, dovrebbe pertanto informarle che i dati saranno utilizzati per un contatto personale e che questi saranno eventualmente integrati con altri dati pubblicamente accessibili.

Se il trattamento dei dati rischia di costituire una violazione dei diritti della personalità, è raccomandabile ottenere il consenso degli interessati, anche perché, in situazioni simili, ciò è possibile senza grossi sforzi.

Quando i dati personali sono ottenuti da terzi, è molto più difficile proteggere i diritti della personalità degli interessati. Soprattutto quando sono trattati dati relativi a un gran numero di interessati, il rispetto del principio di trasparenza, ad esempio, diventa praticamente impossibile o richiederebbe un grande carico di lavoro. Pertanto, in tali situazioni o se è previsto di rendere noti a terzi dati personali degni di particolare protezione o profili della personalità, è necessario fornire un motivo giustificativo sufficiente.

Esempio: un gruppo di interesse politico raccoglie dati personali con l'ausilio del «web mining» da siti e portali Internet, incarica terzi di farlo oppure ottiene le informazioni acquistandole. A tale scopo sono impiegati servizi di «web crawler», che possono effettuare ricerche sistematiche di contenuti di siti Internet o indirizzi e-mail e raccogliere le informazioni desiderate. Il rispetto del principio di trasparenza o anche l'informazione attiva degli interessati in questi casi non sono di fatto possibili. In questo modo si corre anche il rischio di violare il principio della finalità. Per trattamenti dei dati di questa natura deve quindi sussistere un interesse preponderante. Se le raccolte si basano su palesi violazioni del diritto, come ad esempio nei casi dei servizi di «web crawler» che non rispettano i termini di utilizzo dei social network, l'invocazione di interessi preponderanti raggiunge il suo limite.

La gestione dei dati raccolti con l'ausilio di un software realizzato per le campagne è al limite di quanto può essere giustificato da un interesse preponderante. Questi software funzionano come un sistema flessibile di gestione dei contenuti (CMS) e collegano tutti i social network comuni ad un sistema unico che permette interazioni con determinati gruppi di persone. Una volta in possesso di un indirizzo e-mail, il gruppo d'interesse può utilizzare una certa funzione («social match») per cercare la persona attiva nei social network e arricchire la sua raccolta dati con le informazioni pertinenti (cfr. n. 7). In determinate circostanze, questo trattamento dei dati interferisce fortemente con i diritti della personalità degli interessati, cosicché spesso non è più possibile giustificare il trattamento con un interesse preponderante. In questo caso è necessario chiedere il consenso degli interessati.

8.2 Analisi

La definizione di un profilo nel contesto politico deve fare in modo non solo che ciascun gruppo di profili si distingua dagli altri gruppi per gli interessi comuni, ma anche che le persone all'interno dei gruppi abbiano posizioni e idee politiche più simili tra loro rispetto a persone di gruppi diversi.

La segmentazione delle persone basata sulle loro caratteristiche demografiche, ideologiche, socioeconomiche e mentali nonché vari metodi di intelligenza artificiale sono utilizzati per prevedere il comportamento degli individui. Questi profili possono essere inoltre utilizzati per rivolgere messaggi politici mirati alle persone interessate.

Già nella fase di raccolta dei dati, i detentori di tali collezioni devono fare in modo che una serie di dati sensibili – vale a dire degni di particolare protezione – o di dati in sé non sensibili si aggreghino per formare profili della personalità ai sensi della legge sulla protezione dei dati. Questi sottostanno a una protezione legale qualificata o più elevata. Nella sentenza Moneyhouse (n. 5), il TAF si è espresso approfonditamente in merito. La protezione qualificata si applica inoltre, per volontà del legislatore, anche al trattamento di dati sensibili come le opinioni politiche o ideologiche (n. 5.2).

Per quanto è dato constatare, non vi sono basi legali che consentirebbero a un organo pubblico di effettuare analisi politiche di dati personali.

8.3 Attribuzione di informazioni

Partendo dal presupposto che persone appartenenti a un gruppo di profili comune reagiranno in modo particolarmente accentuato a determinati messaggi, i partiti e i gruppi d'interesse trasmettono ai singoli gruppi di cui hanno allestito un profilo informazioni mirate attraverso mailing list o social media. In questo modo, partiti e gruppi d'interesse cercano di influenzare la formazione dell'opinione politica nel periodo precedente a votazioni ed elezioni. Il cosiddetto «microtargeting» consente di personalizzare non solo messaggi o contenuti, ma anche le modalità di contatto. Ciò presuppone che la conoscenza dei destinatari sulla base dei dati raccolti sia così precisa da consentire di trasmettere loro i messaggi politici adeguati utilizzando i canali di comunicazione da loro preferiti. Il «microtargeting» può incidere sull'effetto voluto in particolare nelle votazioni, in quanto l'esperienza evidenzia che in questi casi una grande quantità di aventi diritto di voto non si è ancora formata un'opinione consolidata su un determinato tema.

I messaggi politici personalizzati non hanno sempre lo scopo di influenzare il voto in sé. Talvolta mirano a promuovere o ostacolare l'esercizio dei diritti politici, a seconda che i dati indichino che i destinatari condividono l'opinione del mittente. Possono anche essere finalizzati esclusivamente a incoraggiare i destinatari a votare a favore del mittente: i messaggi vengono quindi inviati solo ai sostenitori del mittente e gli avversari politici vengono deliberatamente esclusi..

8.4 Contatto con le persone interessate

Spesso l'invio di un messaggio politico è la prima occasione in cui gli interessati vengono a conoscenza del trattamento dei dati effettuato (cfr. n. 8.1 – 8.3), soprattutto quando il trattamento si fonda su un interesse preponderante. Per questo, tale mancanza deve essere colmata al momento dell'invio del messaggio politico alle persone interessate. Queste devono essere informate, indicando chi è responsabile del messaggio ricevuto, dove sono disponibili ulteriori informazioni sul relativo trattamento dei dati e quali diritti possono far valere gli interessati. Questi ultimi devono essere informati nel modo più chiaro possibile in merito al trattamento dei dati effettuato (cfr. n. 8.1 – 8.3), in modo che il contesto del messaggio politico possa essere compreso e correttamente classificato. Inoltre, è necessario offrire una possibilità di revoca semplice e rapida.

8.5 Ottenere un consenso valido

Per i presupposti relativi a un consenso valido si rimanda a quanto illustrato in precedenza ai n. 7.3 e 7.4.

8.6 Diritti delle persone interessate

I responsabili hanno l'obbligo di garantire in modo semplice i diritti degli interessati in materia di protezione dei dati siano garantiti. Ogni persona interessata ha pertanto il diritto di chiedere informazioni al detentore di una collezione di dati trattati che la riguardano, di correggere i dati personali errati e di farli cancellare.

Tutte le persone interessate devono quindi poter esercitare i propri diritti di informazione, rettifica e cancellazione. Innanzitutto devono quindi essere informati in merito ai loro diritti e al modo in cui esercitarli. Strumenti idonei a tale scopo sono il sito Internet del titolare del trattamento e il contatto con le persone interessate. Se il trattamento dei dati è effettuato da contitolari o se si ricorre a terzi come responsabili del trattamento, deve essere facile per le persone interessate identificare l'attore presso il quale far valere i propri diritti.

Per le persone interessate, esercitare i propri diritti deve essere facile e di norma gratuito.

9 Requisiti del sito Internet

Se sono previsti il trattamento dei dati personali e la gestione di un sito Internet, devono essere rispettati i principi di trattamento dal punto di vista del diritto in materia di protezione dei dati; gli organi pubblici devono inoltre attenersi al principio della legalità. Le seguenti domande di controllo hanno lo scopo di fungere da ausilio al fine di rispettare i principi di trattamento per quanto concerne il sito Internet.

- I siti Internet informano i visitatori in modo evidente, semplice, accessibile e con un linguaggio comprensibile in merito ai vari strumenti impiegati e allo scopo della raccolta (cfr. n. 6.1)?
- Per le persone che necessitano di maggiori informazioni, è presente una spiegazione a più livelli, vale a dire: oltre alle spiegazioni sintetiche e facilmente comprensibili sono presenti anche delucidazioni più dettagliate da un punto di vista tecnico?
- I visitatori possono decidere singolarmente («in modo granulare») a quali strumenti di tracciamento intendono acconsentire?
- Nell'ambito dell'integrazione di «Facebook social plugin» o di servizi simili, sono impiegate tecnologie volte a garantire che il tracciamento o la trasmissione dei dati avvengono solo dopo aver ottenuto l'eventuale consenso (cfr. n. 7.3 e 7.4)?
- Le persone interessate sono informate sui propri diritti, in particolare sul diritto all'informazione? Sono state adottate le necessarie misure tecnologiche e organizzative al fine di rispondere alle richieste di informazioni (cfr. n. 8.6)?
- Il tracciamento effettuato raccoglie solo dati necessari all'impiego previsto (cfr. n. 6.1 e 6.3)?
- Per il tracciamento e l'analisi web sono state scelte soluzioni che escludono un utilizzo da parte di terzi per i loro scopi, ad esempio mediante l'impiego di strumenti di analisi installati presso il detentore stesso dei dati o che abbreviano l'indirizzo IP (cfr. n. 6.3)?
- Se l'incarico è affidato a terzi: le persone interessate sono state informate? I terzi incaricati devono dimostrare di aver adottato misure organizzative e tecniche al fine della sicurezza dei dati e queste sono controllate (cfr. n. 4.2 e 6.5)?

- Un eventuale trasferimento di dati (p. es. modulo di contatto) avviene in modo criptato?

- Le persone interessate sono informate in anticipo in merito a un eventuale ulteriore utilizzo dei loro indirizzi e-mail ad esempio per il «social matching» e viene ottenuto a tale scopo un consenso separato (cfr. n. 6.1; 7.3 e 7.4)?

10 Esempi pratici

Esempio 1

Un partito politico raccoglie membri come associazione durante manifestazioni e sul proprio sito Internet. Qui i visitatori hanno la possibilità di abbonarsi alla newsletter fornendo il proprio indirizzo e-mail. L'associazione intende mettere a disposizione del gestore di un social network tutti gli indirizzi e-mail così ottenuti, al fine di sfruttare le tecniche di targeting e rinforzo di tale network per inviare la propria pubblicità politica a persone con un profilo della personalità simile.

Non vi è alcun collegamento logico evidente tra lo scopo di fornire ai visitatori informazioni aggiornate sul partito con contenuti generici e lo scopo aggiuntivo di inviare in modo mirato messaggi politici orientati sui profili della personalità contenenti aspetti ideologici. Lo scopo aggiuntivo non corrisponde nemmeno alle legittime aspettative dei destinatari della newsletter. L'associazione non può far valere interessi preponderanti privati o pubblici che possano giustificare la lesione della personalità.

L'associazione non può quindi utilizzare gli indirizzi e-mail per lo scopo aggiuntivo della pubblicità politica mirata e personalizzata senza aver prima informato i destinatari della newsletter e averne ottenuto l'esplicito consenso.

Esempio 2

Un'agenzia pubblicitaria operante per un partito politico offre attraverso i social media un test di idoneità professionale che comprende una valutazione psicologica.

Con la compilazione del test i gestori dei social media ottengono informazioni su formazione, attività professionale, situazione occupazionale, età, hobby nonché l'indirizzo e-mail e i contatti delle persone che si sottopongono al test. L'agenzia acquista queste informazioni dai gestori dei social media per poter inviare in modo più mirato possibile la pubblicità politica del proprio committente.

Il trattamento dei dati mediante tali tecniche di targeting viola i principi della finalità e del trattamento in buona fede. Dal momento che non possono essere fatti valere interessi preponderanti privati o pubblici, gli interessati in quanto potenziali elettori devono essere informati prima della raccolta delle informazioni richieste, che queste saranno trattate anche per scopi di marketing politico mirato e che devono acconsentire in modo esplicito a questo ulteriore trattamento.

11 Riepilogo

A **Partiti e gruppi di interesse**	Nella misura in cui i partiti e i gruppi di interesse si assumono la responsabilità generale nel senso di un detentore di una ***collezione di dati*** (responsabile) (n. 4.1 e 4.2) devono tenere conto delle informazioni di seguito riportate. • Il trattamento avviene indipendentemente dal coinvolgimento di terzi ***in modo conforme alla legge*** e nel rispetto dei principi generali della LPD (n. 6). • ***I terzi incaricati*** **come contitolari** devono dimostrare di rispettare tutte le disposizioni del diritto in materia di protezione dei dati (n. 6) • ***I terzi incaricati*** come responsabili del trattamento sono tenuti per contratto a rispettare tutte le disposizioni del diritto in materia di protezione dei dati, dimostrando in particolare di adottare misure organizzative e tecniche adeguate al fine della sicurezza dei dati (n. 6.5) e di trattare i dati personali solo per gli scopi stabiliti dal contratto. • Il diritto degli aventi diritto di voto alla ***trasparenza*** (n. 6.1 e 9) è soddisfatto mediante ***informazioni basate sul sito Internet*** in merito a - identità del detentore responsabile della collezione; - categorie dei dati trattati; - raccolta dei dati con indicazione di fonti terze; - finalità attuale e, se necessario, giustificazione del trattamento; - metodi di trattamento inclusi lo scopo e il funzionamento dei metodi di analisi utilizzati, compresa l'intelligenza artificiale; - le categorie degli eventuali destinatari dei dati; - i ruoli, gli obblighi e le responsabilità di fornitori di dati, di imprese che si occupano di analisi dei dati o di piattaforme di dati; - le condizioni di utilizzo determinanti concernenti terzi e il luogo dove reperirle. • Il trattamento dei dati avviene nel rispetto dei principi di ***finalità*** (n. 6.3) e della ***proporzionalità*** (n. 6.2), secondo cui un trattamento ulteriore deve sempre avvenire nei limiti dello scopo alla base della raccolta e della durata fino al raggiungimento di tale scopo; • ***I consensi*** necessari per il trattamento dei dati personali nel contesto del processo politico sono ottenuti ***in modo esplicito*** (n. 7.4); • ***la correttezza dei dati*** è garantita anche nel caso di coinvolgimento di terzi e i dati non più necessari sono cancellati (n. 6.4); • i ***rischi*** organizzativi, tecnici e relativi al diritto in materia di protezione dei dati ***sono stimati*** e adeguate misure di protezione sono adottate (n. 6). • È presente una ***documentazione*** interna dalla quale si evince come è garantita la sicurezza delle varie categorie di dati da trattare (n. 6); • Nell'utilizzo di servizi o applicazioni di terzi (p. es. servizi di newsletter o pianificazione e gestione di visite porta a porta) valgono le norme vigenti in materia di trasmissione dei dati a terzi e di trasferimento di dati personali all'estero. Cfr. a tale proposito soprattutto le informazioni sul sito Internet dell'IFPDT (link: Trasmissione all'estero (admin.ch) e almeno i documenti indicati di seguito

	- Parere sulla trasmissione di dati personali negli Stati Uniti e in altri Stati che non garantiscono un livello di protezione dei dati adeguato conformemente all'articolo 6 capoverso 1 LPD (link: PDF del parere) - Guida per l'esame dell'ammissibilità della comunicazione di dati all'estero (link: PDF della Guida) • Sono rispettati i diritti all'informazione delle persone interessate nonché eventuali obblighi di notifica per le collezioni di dati od obblighi d'informazione per la trasmissione di dati personali all'estero nei confronti delle autorità per la protezione dei dati.
B **Registri pubblici**	Per la gestione ***del registro degli abitanti e del catalogo elettorale*** (n. 4.3) le autorità responsabili si assicurano • che il trattamento dei dati non vada oltre le ***disposizioni di legge*** per quanto concerne finalità, contenuto, portata e durata; • che la trasmissione dei dati personali avvenga solo in presenza di una base legale sufficiente o che i dati siano prima pseudonimizzati in modo efficace; • che le persone registrate possano avvalersi di ***possibilità di blocco*** se una trasmissione dei dati ai fini della pubblicità politica non è esclusa per legge fin dall'inizio; • i ***rischi*** concernenti la sicurezza tecnica e organizzativa, inclusi i rischi legati alla re-identificazione, siano ***valutati e documentati*** e che siano adottate le misure di protezione necessarie (n. 6.5); • che la perdita di dati sia notificata immediatamente alle autorità per la protezione dei dati.
C **Fornitori di dati e imprese che si occupano di analisi dei dati**	Se trattano dati nel contesto del processo politico come ***detentori*** con responsabilità globale, le imprese di analisi dei dati (n. 4.4) o i fornitori di dati (n. 4.5) devono tenere conto delle indicazioni di cui alla tabella A. Se invece sono ***processori d'ordine*** e trattano dati nel contesto del processo politico • si attengono agli obblighi stabiliti nel contratto dal titolare del trattamento; • si assicurano prima della conclusione del contratto che il committente sia in grado a livello tecnico e organizzativo di trattare ulteriormente i dati ottenuti conformemente alla legge e al contratto; • osservano la giurisprudenza ai sensi di Moneyhouse per quanto concerne la combinazione di dati provenienti da varie fonti ai fini della definizione di un profilo (n. 5); • garantiscono la sicurezza dei dati secondo gli obblighi stabiliti dal contratto (n. 6.5); • garantiscono la sicurezza dei dati valutando e documentando i rischi nonché adottando le necessarie misure di protezione. Chiariscono i seguenti elementi nelle proprie condizioni di utilizzo o condizioni di contratto scritte • come, da quali fonti, con quali metodi e con quali finalità hanno raccolto i dati trasmessi; • se, e in caso affermativo, per quali finalità e in quale forma le persone interessate hanno potuto acconsentire a una trasmissione e a un ulteriore trattamento dei dati.

D **Piattaforme di dati**	Indipendentemente dal fatto che le piattaforme private di dati (n. 4.6) trattino informazioni nel contesto del processo politico come detentori con responsabilità globale o come responsabili del trattamento, il trattamento deve in ogni caso rispettare le condizioni generali di contratto e le condizioni di utilizzo. • Tengono conto del diritto degli aventi diritto di voto a un ***trattamento trasparente dei dati*** (n. 6.1 e 8.4) e investono pertanto costantemente in ***tecnologie che favoriscono la protezione dei dati***, al fine di offrire agli utenti ***informazioni*** a più livelli e ***vere possibilità di scelta digitali adeguate agli utenti***. • Nominano ***persone di contatto*** sufficientemente informate e autorizzate al fine di comunicare con le autorità competenti in materia di protezione dei dati, che siano disponibili per informazioni in caso di perdite di dati o di altri incidenti rilevanti per la protezione dei dati con possibili ripercussioni su votazioni ed elezioni. Se trattano le informazioni come ***detentori con responsabilità globale***, le piattaforme di dati rispettano inoltre le indicazioni di cui alla tabella A. Se sono ***responsabili del trattamento*** rispettano le indicazioni della tabella C.
E **Singole persone**	Prima di pubblicare, valutare o diffondere opinioni e contenuti politici, le persone singole, in quanto destinatari, fanno in modo di rispettare la sfera privata e altri aspetti dei diritti della personalità come l'onore o la vita familiare degli interessati. ***Prima di trasmettere informazioni*** riferite ad amici, familiari o altre persone identificabili a partiti, gruppi d'interesse, fornitori di dati, imprese che si occupano di analisi dei dati e piattaforme di dati, si procurano il loro ***consenso esplicito***. Si assicurano che il software che accede a questi dati provenga da fonti affidabili.