Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB
Préposé fédéral à la protection des données et à la transparence PFPDT
Incaricato federale della protezione dei dati e della trasparenza IFPDT
Incumbensà federal per la protecziun da datas e per la transparenza IFPDT

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

LINEE GUIDA

del 1° giugno 2019

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

Stato: 1° giugno 2019

Queste linee guida sono state redatte in collaborazione con gli esperti Urs Maurer-Lambrou, avvocato, LL.M. e Prof. Dr. Adrian Vatter, politologo.

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

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

Indice

1 Scopo e destinatari delle linee guida

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.

Se stabiliscono riferimenti a persone identificate o identificabili e provengono da privati o da autorità federali, questi 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 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).

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 della popolazione 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 opinioni politiche e ideologiche a un livello di protezione più elevato rispetto a dati comparabili in un contesto commerciale.

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 ai rischi sistemici del trattamento dei dati personali. Le presenti linee guida devono essere intese quale ausilio per l'applicazione della LPD, risalente al 1992, nel dinamico contesto della digitalizzazione sul trattamento dei dati in ambito di elezioni e votazioni. Si rivolge agli attori della formazione dell'opinione politica e intende incentivarli a rendere riconoscibili e comprensibili i metodi di trattamento digitali dei dati. Questa esigenza di trasparenza nell'ambito del diritto in materia di protezione dei dati deve essere separata da due ambiti tematici differenti: dalla problematica della veridicità dei contenuti conosciuta dal pubblico con il termine di «fake news», che non è oggetto della legislazione in materia di protezione dei dati né può essere tematizzata nelle presenti linee guida, come pure dal tema del voto elettronico in Svizzera, che non è soggetto di questa guida.

2 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.

Benché su questo punto non vi sia ancora una giurisprudenza esaustiva, è lecito presupporre che il trattamento digitale dei dati in relazione al processo politico sia di norma soggetto al livello di protezione vigente per i dati personali degni di particolare protezione solo per il fatto di avere lo scopo di influenzare le opinioni ideologiche di molte persone. Ciò in particolare quando sono impiegati metodi di analisi automatizzati, che mediante comparazione di una serie di dati sensibili o anche non sensibili costituiscono profili della personalità che secondo la giurisprudenza del Tribunale amministrativo federale (TAF) nella questione Moneyhouse[1] depongono anch'essi per una protezione più elevata degli interessati. Partiti politici e gruppi d'interesse, in quanto «detentori» privati di collezioni di dati, devono così assumersi la responsabilità globale per la raccolta, la conservazione, la cura e l'ulteriore utilizzo dei dati ivi elaborati (cfr. tabella A), orientandosi in tale contesto al principio fondamentale della trasparenza (n. 7). Rendendo riconoscibili e comprensibili i metodi di trattamento che applicano, i partiti e i gruppi d'interesse potranno ottenere l'accettazione da parte dei cittadini.

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. Nell'ambito della propria responsabilità globale di detentori, rendono trasparente l'inserimento e il ruolo dei terzi, che a seconda delle circostanze possono essere anch'essi detentori o semplicemente responsabili del trattamento. Inoltre, si assicurano che questi ultimi rispettino le prescrizioni della legislazione in materia di protezione dei dati (cfr. tabella C).

3 Registri pubblici

I Cantoni 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 (ad 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

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

sicuro e trasmessi 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, ad 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 Processo di trattamento dei dati

La legge definisce il trattamento dei dati come qualsiasi operazione relativa a dati, indipendentemente dai mezzi e dalle procedure impiegati. Nel contesto di elezioni e votazioni questo processo si suddivide a livello funzionale in raccolta, analisi e attribuzione delle informazioni.

4.1 Raccolta

Ai fini del trattamento dei dati nel processo politico, partiti e gruppi d'interesse possono innanzitutto ricorrere all'insieme di dati da essi raccolti come indirizzi di membri, elenchi di indirizzi e-mail di abbonati alle newsletter e informazioni simili. Spesso questi dati propri sono integrati da informazioni che partiti e gruppi d'interesse ottengono mediante raccolte di firme o rivolgendosi personalmente alla popolazione con stand, visite a domicilio o telefonate. Tramite questi contatti diretti, oltre ai dati di contatto delle persone interpellate, è possibile che i partiti o i gruppi di interesse richiedano anche le preferenze politiche individuali e altre informazioni. Possono inoltre procurarsi i dati da fonti pubblicamente accessibili come elenchi telefonici o registri pubblici.

Con l'ausilio del «web mining» possono utilizzare portali Internet o pagine web statistiche per la raccolta dei dati, incaricare terzi di svolgere queste operazioni oppure ottenere le informazioni acquistandole. I servizi di «web crawler» possono effettuare ricerche sistematiche di pagine web o indirizzi e-mail e raccogliere le informazioni desiderate. Un'ulteriore possibile fonte di dati sono le piattaforme di dati.

I dati raccolti vengono raggruppati dai partiti o dai gruppi d'interesse e possono essere gestiti con un software realizzato per le campagne. 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, i partiti e i gruppi d'interesse possono utilizzare una certa funzione per cercare la persona attiva nei social network e arricchire la loro raccolta dati con le informazioni pertinenti ("social match", cfr. sezione 7).

Il software per la campagna supporta il partito o il gruppo d'interesse nella pianificazione e nell'implementazione delle azioni e permette di combinare il potenziale dei dati raccolti con le possibilità offerte dai social network, consentendo al software di utilizzare queste possibilità di analisi e di selezione..

In qualsiasi forma di raccolta di dati a fini politici, i responsabili sono tenuti a rispettare in particolare il principio di trasparenza (sezione 7). Le informazioni sulle opinioni filosofiche o politiche sono soggette a una protezione giuridica qualificata (sezione 7).

4.2 Analisi

Nel contesto dei «big data», nel settore dell'e-commerce grandi quantità di dati eterogenei sono trattati per un periodo prolungato, aggregati e messi insieme a scopi analitici. Con l'ausilio di sistemi informatici altamente performanti e metodi analitici, i dati possono essere valutati permettendo di identificare gli interessi di singoli o di piccoli gruppi di persone con opinioni simili. Modelli statistici consentono di prevedere quali prodotti e servizi sono adatti a determinati gruppi di profili di clienti nuovi o già esistenti («predictive analytics»). I clienti già acquisiti o potenziali ricevono quindi messaggi pubblicitari su misura per il proprio profilo o trovano ad esempio in un negozio online proposte di prodotti adatti a loro.

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. 2), il TAF si è espresso approfonditamente in merito. La protezione qualificata vale anche per il trattamento di dati sensibili come opinioni politiche o ideologiche che il legislatore ha sottoposto a una particolare protezione (n. 7).

4.3 Attribuzione di informazioni

Partendo dal presupposto che persone appartenenti a un gruppo di profili comune reagirà in modo particolarmente accentuato a determinati messaggi, ai singoli gruppi dovranno essere trasmesse 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 si è ancora formata un'opinione consolidata su un determinato tema. Nelle elezioni proporzionali come le elezioni del Consiglio nazionale si osserva invece spesso un comportamento consolidato fondato su tradizioni e abitudini. Comportamenti ancora diversi possono essere identificati nell'ambito delle elezioni per il Consiglio degli Stati, quando i candidati sono sostenuti da più partiti.

I messaggi personalizzati nel contesto politico non devono sempre mirare a influenzare il comportamento in sede di votazioni o elezioni a livello di contenuto. Possono invece avere l'effetto di promuovere o inibire la consapevolezza dei diritti politici, a seconda che i dati valutati dei destinatari li designino come provenienti da alleati o da avversari politici. Un'ulteriore possibilità risiede richiamare la consapevolezza del diritto elettorale e di voto inviando i messaggi in modo selettivo, ovvero tralasciando i presunti avversari politici.

5 Altri attori del trattamento dei dati

5.1 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).

5.2 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 web, 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.

Le imprese di analisi dei 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).

5.3 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.

5.4 Singole persone (destinatari)

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 E). Per assumersi tale responsabilità devono innanzitutto essere consapevoli di questo fatto.

6 Principi generali del trattamento dei dati

Ogni attore che tratta dati nel contesto di elezioni e votazioni deve attenersi ai principi generali del trattamento dei dati della legislazione in materia di protezione dei dati.

Sono definiti dati personali tutte le informazioni relative a una persona identificata o identificabile. I dati che consentono di risalire a opinioni politiche o ideologiche sono considerati degni di particolare

protezione e il loro trattamento è pertanto particolarmente tutelato dalla legge. 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 (n. 2).

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

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.

Secondo il principio di 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 di finalità vale in particolare anche per l'integrazione di servizi o applicazioni di terzi (ad es. servizi di newsletter o software per la pianificazione e la gestione di visite porta a porta) che non sono autorizzati a utilizzare i dati per i propri scopi (cfr. anche sezione 7).

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. Semplici dati tecnici senza riferimenti a persone identificate o identificabili non rientrano nel campo di applicazione del diritto in materia di protezione dei dati. La veridicità di contenuti politici e la problematica delle cosiddette «fake news» non sono oggetto di tale diritto.

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 Diritto alla trasparenza degli aventi diritto di voto

Gli attori devono altresì tenere presente la particolare rilevanza del principio della trasparenza, che conferisce agli aventi diritto di voto la possibilità, nell'ambito del diritto in materia di protezione dei dati,

di determinare sulla base di quali metodi di trattamento e tecnologie digitali sono contattati e influenzati dal punto di vista politico.

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 al quadro delle basi legali pubblicamente accessibili.

Come base per il trattamento di dati personali da parte di **attori privati** come partiti o gruppi d'interesse possono valere il consenso degli interessati o un interesse preponderante privato o pubblico. Nella pratica, nel contesto politico trova applicazione di norma solo il consenso degli interessati, valido solamente se concesso volontariamente e dopo aver ricevuto informazioni adeguate. Come già menzionato, nel contesto politico di norma sono trattati dati personali concernenti opinioni politiche o ideologiche che rientrano nella categoria dei dati degni di particolare protezione. Collegando tra loro i dati che le persone interessate lasciano ad esempio su pagine web e piattaforme sociali è possibile definire profili della personalità. Se non vi sono né una giustificazione secondo la legge né un interesse preponderante privato o pubblico, il trattamento di dati personali degni di particolare protezione o profili della personalità presuppone un consenso esplicito delle persone interessate. Nel contesto politico i dati sulle persone possono quindi essere trattati solo se queste acconsentono al loro utilizzo in modo esplicito, esercitando il diritto all'autodeterminazione ed avendo ricevuto informazioni sufficienti.

Gli attori del processo di formazione dell'opinione politica elaborano i dati solo secondo finalità, portata e metodi per i quali esiste un consenso. Un consenso esplicito è dato segnatamente quando le persone interessate si sono registrate sulla pagina web di un attore e hanno espressamente (ad 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 a sua volta il loro consenso.

Il consenso è fornito con autodeterminazione se le persone interessate posso acconsentire in modo differenziato all'attivazione o alla disattivazione di singoli aspetti e funzionalità delle applicazioni digitali (ad 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»).

8 Riepilogo

A **Partiti e gruppi d'interesse**	Se i partiti e i gruppi d'interesse si assumono una responsabilità globale nel ruolo di ***detentori*** di un ***catalogo di dati*** (n. 2), devono tenere conto delle indicazioni seguenti. • Il trattamento avviene indipendentemente dal coinvolgimento di terzi ***in modo conforme alla legge*** e nel rispetto dei principi generali della LPD (n. 6). • Ai ***terzi incaricati*** è richiesto di provare il ricorso a misure adeguate a livello organizzativo e tecnico in materia di protezione dei dati (n. 6). • Il diritto alla ***trasparenza*** (n. 7) degli aventi diritto di voto è soddisfatto da ***informazioni basate sulla pagina web*** in merito a - identità del detentore responsabile della collezione; - categorie dei dati trattati; - raccolta dei dati con indicazione di fonti terze; - finalità attuale e 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) e di ***proporzionalità*** (n. 6), secondo cui un ulteriore trattamento deve sempre avvenire entro la finalità alla base della raccolta e la durata che permette di raggiungere lo scopo. • I ***consensi*** necessari per il trattamento dei dati personali nel contesto del processo politico devono essere ottenuti in modo ***esplicito*** (n. 7). • La ***correttezza dei dati*** è garantita anche se sono coinvolti terzi e i dati non più necessari sono cancellati (n. 6). • I ***rischi*** a livello organizzativo, tecnico e di diritto in materia di protezione dei dati ***sono valutati*** e sono adottate misure di protezione adeguate (n. 6). • È presente una ***documentazione*** interna dalla quale emergono le modalità con cui è garantita la sicurezza delle varie categorie di dati trattati (n 6). • Nell'utilizzo di servizi o applicazioni di terzi (ad 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 (vedi il promemoria "La

	trasmissione di dati all'estero in breve" e le "Spiegazioni concernenti la comunicazione di dati a carattere personale all'estero"); • 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. 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 un'esplicita base legale o che i dati siano prima pseudonimizzati; • che le persone registrate possano avvalersi di ***possibilità di blocco*** se una trasmissione dei dati ai fini della pubblicità politica non è esclusa fin dal principio a norma di legge; • che 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); • che la perdita di dati sia notificata in tempo utile 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, i fornitori di dati privati (n. 5.1) o le imprese che si occupano di analisi dei dati (n. 5.2) devono tenere conto delle indicazioni di cui alla tabella A. Se invece sono **processori d'ordine** nel contesto del processo politico • si assicurano prima della conclusione del contratto che il committente sia in grado a livello tecnico e organizzativo di effettuare il trattamento da concordare secondo la legge e il contratto; • osservano la giurisprudenza ai sensi di Moneyhouse (n. 2) per quanto concerne la combinazione di dati provenienti da varie fonti ai fini della definizione di un profilo (n. 4.2); • garantiscono la sicurezza dei dati valutando e documentando i rischi nonché adottando le necessarie misure di protezione (n. 6); • sostengono il committente su desiderio di quest'ultimo nella rilevazione dei rischi e gli notificano eventuali perdite di dati. 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 di dati (n. 5.3) 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. 7) 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 anche 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.