COMMISSIONE
EUROPEA

Bruxelles, 12.9.2018
COM(2018) 638 final

Elezioni libere e corrette

DOCUMENTO DI ORIENTAMENTO

Orientamenti della Commissione sull'applicazione del diritto dell'Unione in materia di protezione dei dati nel contesto elettorale

Contributo della Commissione europea all'incontro dei leader di Salisburgo del 19-20 settembre 2018

ORIENTAMENTI DELLA COMMISSIONE SULL'APPLICAZIONE DEL DIRITTO DELL'UNIONE IN MATERIA DI PROTEZIONE DEI DATI NEL CONTESTO ELETTORALE

L'impegno nei confronti dell'elettorato è alla base del processo democratico. È prassi costante dei partiti politici adattare le proprie comunicazioni elettorali al pubblico dei destinatari, tenendo conto dei loro interessi specifici. È quindi naturale che i soggetti coinvolti nelle elezioni studino le possibilità di usare i dati per ottenere voti. La diffusione degli strumenti digitali e delle piattaforme online ha creato molte opportunità nuove per coinvolgere le persone nel dibattito politico.

Tuttavia, lo sviluppo del *micro-targeting* degli elettori basato sul trattamento illecito dei dati personali, come emerso dalle rivelazioni su Cambridge Analytica, è di natura diversa. Esso mette in luce le sfide poste dalle tecnologie moderne e nel contempo dimostra la grande importanza della protezione dei dati nel contesto elettorale. Il *micro-targeting* è diventato una questione fondamentale non solo per le persone fisiche, ma anche per il funzionamento delle nostre democrazie, in quanto costituisce una grave minaccia alla correttezza e alla democraticità del processo elettorale e può compromettere l'apertura, la correttezza e la trasparenza del dibattito, elementi essenziali di una democrazia. La Commissione ritiene che sia della massima importanza affrontare la questione, per ripristinare la fiducia dei cittadini nella correttezza del processo elettorale.

Le prime relazioni dell'autorità britannica per la protezione dei dati (*Information Commissioner's Office* - ICO) sull'uso delle tecniche di analisi dei dati nelle campagne politiche[1] e il parere del garante europeo della protezione dei dati sulla manipolazione online e sui dati personali[2] hanno confermato la crescente incidenza nel contesto elettorale del *micro-targeting*, inizialmente sviluppato per fini commerciali.

Più in generale, varie autorità per la protezione dei dati hanno affrontato la questione della protezione dei dati nel contesto elettorale[3].

Il regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio (regolamento generale sulla protezione dei dati)[4], che è diventato direttamente applicabile in tutta l'Unione

[1] Relazioni dell'autorità britannica per la protezione dei dati (*Information Data Protection Office* - ICO) del 10 luglio 2018: *"Investigation into the use of data analytics in political campaigns - Investigation update"* (Indagine sull'uso delle tecniche di analisi dei dati nelle campagne politiche - aggiornamento) e *"Democracy Disrupted? Personal information and political influence"* (Democrazia sovvertita? Informazioni personali e influenza politica).

[2] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

[3] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3013267 "Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale" del Garante per la protezione dei dati personali pubblicato nella Gazzetta Ufficiale italiana n. 71 del 26 marzo 2014 [doc. web n. 3013267]; https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux *"Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?"*, documento pubblicato dalla *Commission Nationale de l'informatique et des libertés* (Commissione nazionale Informatica e libertà) l'8 novembre 2016; https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf *Information Commissioner's Office "Guidance on political campaigning"* (Orientamenti sulle campagne politiche) [20170426].

[4] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

il 25 maggio 2018, fornisce all'Unione gli strumenti necessari per affrontare i casi di uso illecito dei dati personali nel contesto elettorale. Tuttavia, solo un'applicazione rigorosa e coerente delle norme contribuirà a proteggere l'integrità del quadro politico democratico. Poiché è la prima volta che saranno applicate nel contesto elettorale europeo in occasione delle prossime elezioni del Parlamento europeo, è importante fornire chiarezza ai soggetti coinvolti nei processi elettorali, quali le autorità elettorali nazionali, i partiti politici, gli intermediari di dati, gli analisti di dati, le piattaforme dei media sociali e le reti pubblicitarie online. L'obiettivo dei presenti orientamenti è pertanto sottolineare gli obblighi in materia di protezione dei dati che hanno pertinenza per le elezioni. Le autorità nazionali per la protezione dei dati, in quanto autorità incaricate di far rispettare il regolamento generale sulla protezione dei dati, devono esercitare appieno i loro poteri rafforzati per reagire ad eventuali violazioni, in particolare quelle riguardanti il *micro-targeting* degli elettori.

1. Il quadro dell'Unione in materia di protezione dei dati

La protezione dei dati personali è un diritto fondamentale sancito dalla Carta dei diritti fondamentali dell'Unione europea (articolo 8) e dai trattati (articolo 16 del TFUE). Il regolamento generale sulla protezione dei dati rafforza il quadro per la protezione dei dati, dotando l'Unione di mezzi più appropriati per trattare in futuro i casi di abuso di dati personali e facendo in modo che tutti i soggetti rendano maggiormente conto del loro operato e siano più responsabili in relazione alle modalità di trattamento dei dati personali.

Esso conferisce alle persone fisiche nell'Unione diritti aggiuntivi e rafforzati che sono particolarmente rilevanti nel contesto elettorale. Il sistema di protezione dei dati in vigore nell'Unione negli ultimi 20 anni ha risentito in particolare dell'applicazione frammentata delle norme da parte degli Stati membri, dell'assenza di meccanismi formali di cooperazione tra le autorità nazionali per la protezione dei dati e dei limitati poteri di esecuzione di tali autorità. Il regolamento generale sulla protezione dei dati colma tali lacune: basandosi sui principi collaudati in materia di protezione dei dati, armonizza concetti chiave come il consenso, rafforza il diritto delle persone fisiche a ricevere informazioni sul trattamento dei loro dati, chiarisce le condizioni alle quali i dati personali possono essere ulteriormente condivisi, introduce norme sulla violazione dei dati personali, istituisce un meccanismo di cooperazione tra le autorità per la protezione dei dati nei casi transfrontalieri e rafforza i loro poteri di esecuzione. In caso di violazione delle norme dell'UE sulla protezione dei dati, le autorità per la protezione dei dati hanno il potere di condurre indagini (ad esempio ordinando di fornire informazioni, effettuando ispezioni nei locali dei titolari del trattamento e dei responsabili del trattamento) e di correggere comportamenti (ad esempio rivolgendo avvertimenti e ammonimenti o disponendo la sospensione temporanea o definitiva del trattamento). Esse possono inoltre imporre sanzioni fino a 20 milioni di EUR o, nel caso delle imprese, fino al 4 % del fatturato mondiale dell'impresa interessata[5]. Nel decidere in merito all'imposizione di sanzioni e al loro livello, le autorità per la protezione dei dati esamineranno le circostanze del

[5] Orientamenti della Commissione sul regolamento generale sulla protezione dei dati, consultabile al seguente indirizzo: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_it

caso e fattori quali la natura, la portata o la finalità del trattamento, il numero di persone interessate e l'entità dei danni subiti[6]. Nel contesto elettorale è probabile che la gravità della violazione e il numero di persone interessate saranno elevati. Ciò potrebbe comportare l'imposizione di sanzioni elevate, tenuto conto in particolare dell'importanza della questione della fiducia dei cittadini nel processo democratico.

Il comitato europeo per la protezione dei dati di recente istituzione, che raggruppa tutte le autorità nazionali per la protezione dei dati e il garante europeo della protezione dei dati, svolge un ruolo fondamentale nell'applicazione del regolamento generale sulla protezione dei dati, pubblicando linee guida, raccomandazioni e migliori prassi[7]. Le autorità nazionali per la protezione dei dati, in quanto autorità incaricate di far rispettare il regolamento generale sulla protezione dei dati e fungendo da punti di contatto diretto per le parti interessate, sono in una posizione idonea per assicurare ulteriore certezza giuridica in merito all'interpretazione del regolamento. La Commissione sostiene attivamente tale attività.

La direttiva 2002/58/CE del Parlamento europeo e del Consiglio[8] (direttiva relativa alla vita privata e alle comunicazioni elettroniche o direttiva e-privacy) completa il quadro dell'Unione in materia di protezione dei dati ed è di rilievo nel contesto elettorale, poiché il suo ambito di applicazione comprende le norme sull'invio elettronico di comunicazioni indesiderate, anche a fini di marketing diretto. La direttiva e-privacy stabilisce inoltre norme in materia di archiviazione delle informazioni e di accesso alle informazioni già archiviate - ad esempio mediante *cookie* che possono essere utilizzati per tenere traccia del comportamento online degli utenti - nelle apparecchiature terminali, ad esempio smartphone o computer. La proposta di regolamento sulla vita privata e le comunicazioni elettroniche ("regolamento e-privacy")[9], presentata dalla Commissione e attualmente in fase di negoziazione, si basa sugli stessi principi della direttiva e-privacy. Il nuovo regolamento estenderà l'ambito di applicazione al di là degli operatori di telecomunicazione tradizionali per includere i servizi di comunicazione elettronica basati su internet.

2. Principali obblighi dei vari soggetti

Il regolamento generale sulla protezione dei dati si applica a tutti i soggetti attivi nel contesto elettorale, come i partiti politici europei e nazionali (di seguito: "partiti politici"), le fondazioni politiche europee e nazionali (di seguito: "fondazioni"), le piattaforme, le società di analisi dei dati e le autorità pubbliche responsabili del processo elettorale. Tali soggetti devono trattare i dati personali (ad esempio nomi e indirizzi) in modo lecito, corretto e trasparente e solo per finalità specifiche, e non possono servirsene successivamente in modo incompatibile con le finalità per le quali i dati sono stati inizialmente raccolti. In linea di

[6] Articolo 83 del regolamento generale sulla protezione dei dati.
[7] Il garante europeo della protezione dei dati inoltre emette pareri.
[8] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).
[9] Proposta di regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche) (COM(2017) 10 final).

principio il trattamento a scopi giornalistici rientra anch'esso nell'ambito di applicazione del regolamento generale sulla protezione dei dati ma, data l'importanza del diritto alla libertà di espressione e di informazione in una società democratica, può beneficiare delle esenzioni e deroghe previste dal diritto nazionale[10].

La nozione di dati personali ha un ampio significato. I "dati personali" sono tutti i dati riguardanti una persona fisica identificata o identificabile. I dati trattati nel contesto elettorale comprendono spesso categorie particolari di dati personali ("dati sensibili"), quali le opinioni politiche, l'appartenenza a un sindacato, l'origine etnica, la vita sessuale e così via, che beneficiano di un regime di maggiore tutela[11]. Inoltre, le tecniche di analisi dei dati consentono di desumere "dati sensibili" (ad esempio le opinioni politiche, le convinzioni religiose o l'orientamento sessuale) da una serie di dati non sensibili. Anche il trattamento dei dati desunti rientra nell'ambito di applicazione del regolamento generale sulla protezione dei dati e dovrebbe pertanto essere effettuato nel rispetto di tutte le norme in materia di protezione dei dati.

In conclusione, il regolamento generale sulla protezione dei dati si applica praticamente a tutte le operazioni di trattamento dei dati nel contesto elettorale.

Tenendo conto della necessità di assicurare chiarezza ai soggetti coinvolti nel processo elettorale e considerate le prime risultanze nel caso Cambridge Analytica, le sezioni che seguono evidenziano gli obblighi in materia di protezione dei dati che risultano di particolare rilevanza nel contesto elettorale. Tali obblighi sono sintetizzati in allegato.

2.1 Titolari del trattamento e responsabili del trattamento

La nozione di responsabilità per il proprio operato in relazione al titolare e al contitolare del trattamento è un elemento fondamentale del regolamento generale sulla protezione dei dati. Il titolare del trattamento è il soggetto che decide, da solo o in collaborazione con altri, le finalità e le modalità del trattamento dei dati personali; il responsabile del trattamento tratta i dati personali unicamente per conto del titolare del trattamento e secondo le sue istruzioni (e il rapporto tra questi due soggetti è stabilito in un contratto o altro atto giuridico vincolante). Il titolare del trattamento deve adottare sin dall'inizio misure adeguate ai rischi e attuare la protezione dei dati fin dalla progettazione ed essere in grado di comprovare il rispetto del regolamento generale sulla protezione dei dati (principio di responsabilizzazione).

Il ruolo di titolare del trattamento o di responsabile del trattamento deve essere valutato caso per caso. Nel contesto elettorale vari soggetti possono essere titolari del trattamento: i partiti politici, i singoli candidati e le fondazioni politiche sono, nella maggior parte dei casi, titolari del trattamento; le piattaforme e le società di analisi dei dati possono essere (con)titolari del trattamento o responsabili del trattamento per un determinato trattamento a seconda del grado

[10] Articolo 85, paragrafo 2, del regolamento generale sulla protezione dei dati.
[11] Articolo 9, paragrafo 1, del regolamento generale sulla protezione dei dati.

di controllo che esercitano sullo stesso[12]; le autorità elettorali nazionali sono titolari del trattamento per i registri elettorali.

Quando le loro attività di trattamento riguardano l'offerta di beni e servizi a persone fisiche nell'Unione o il monitoraggio del loro comportamento nell'Unione, anche le società aventi sede al di fuori dell'Unione devono conformarsi al regolamento generale sulla protezione dei dati. È questo il caso di una serie di piattaforme e società di analisi dei dati.

2.2 Principi, liceità del trattamento e condizioni speciali per i "dati sensibili"

I soggetti coinvolti nelle elezioni sono tenuti a trattare i dati personali, compresi quelli ottenuti da fonti pubbliche, nel rispetto dei principi relativi al trattamento dei dati personali e per il numero limitato di motivi chiaramente indicati nel regolamento generale sulla protezione dei dati[13]. I principali motivi di trattamento lecito nel contesto elettorale sono il consenso espresso dall'interessato, l'adempimento di un obbligo legale ai sensi della normativa dell'Unione o nazionale, l'esecuzione di un compito svolto nel pubblico interesse e il legittimo interesse di uno dei soggetti. Tuttavia, i soggetti nel contesto elettorale possono invocare il motivo del legittimo interesse solo se gli interessi o i diritti e le libertà fondamentali delle persone interessate non prevalgono sui loro interessi.

Inoltre, l'archiviazione delle informazioni nelle apparecchiature terminali (computer, smartphone, ecc.) e l'accesso alle informazioni ivi archiviate devono essere conformi alle prescrizioni della direttiva e-privacy in materia di protezione delle apparecchiature terminali, il che significa che l'interessato deve fornire il suo consenso.

Quando come motivo legale è invocato il consenso, il regolamento generale sulla protezione dei dati prescrive che esso sia prestato mediante azione positiva inequivocabile[14] e sia libero e informato.

Le autorità pubbliche coinvolte nel processo elettorale trattano i dati personali per adempiere a un obbligo legale o per svolgere un compito di interesse pubblico. Gli altri soggetti coinvolti nel contesto elettorale possono trattare i dati sulla base del consenso o di un legittimo interesse[15]. I partiti politici e le fondazioni politiche possono trattare i dati anche per motivi di interesse pubblico se previsto dal diritto nazionale[16].

Le autorità pubbliche possono divulgare ai partiti politici determinate informazioni, ad esempio il nome e l'indirizzo, sulle persone fisiche figuranti nelle liste elettorali o nei registri

[12] La recente giurisprudenza della Corte di giustizia dell'Unione europea (sentenza del 10 luglio 2018, Testimoni di Geova, causa C-25/17) ha chiarito che, in determinate circostanze, un soggetto che esercita un'influenza sull'attività di raccolta e trattamento dei dati personali può essere considerato titolare del trattamento.
[13] Articoli 5 e 6 del regolamento generale sulla protezione dei dati.
[14] Articolo 7 e articolo 4, paragrafo 11, del regolamento generale sulla protezione dei dati.
[15] Purché non vi siano gravi ripercussioni sui diritti e le libertà degli interessati.
[16] Cfr. il considerando 56 del regolamento generale sulla protezione dei dati, che recita: "Se, nel corso di attività elettorali, il funzionamento del sistema democratico presuppone, in uno Stato membro, che i partiti politici raccolgano dati personali sulle opinioni politiche delle persone, può esserne consentito il trattamento di tali dati per motivi di interesse pubblico, purché siano predisposte garanzie adeguate".

dei residenti solo se espressamente autorizzate dalla normativa dello Stato membro e solo a fini di pubblicità nel contesto elettorale e nella misura necessaria a tal fine.

Il trattamento nel contesto elettorale riguarda spesso "dati sensibili". Il trattamento di tali dati, compresi i "dati sensibili" desunti, è generalmente vietato, tranne che per i motivi specifici previsti dal regolamento generale sulla protezione dei dati[17]. Il trattamento dei "dati sensibili" richiede il soddisfacimento di condizioni specifiche più rigorose: la persona interessata deve aver prestato il proprio consenso esplicito[18] o aver reso pubblici i dati in questione[19]. I partiti politici e le fondazioni politiche possono trattare i "dati sensibili" anche per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri e se sono state previste adeguate misure di tutela[20]. Il regolamento generale sulla protezione dei dati stabilisce che i partiti politici e le fondazioni politiche possono procedere al trattamento dei "dati sensibili" anche nella misura in cui il trattamento riguarda esclusivamente i membri, gli ex membri o le persone che hanno regolari contatti con loro, ma unicamente affinché siano comunicati all'interno del partito politico o della fondazione politica[21]. Tale disposizione specifica tuttavia non può essere utilizzata da un partito politico per trattare i dati di potenziali membri o elettori.

Le finalità del trattamento dei dati dovrebbero essere specificate al momento della raccolta (principio della "limitazione delle finalità")[22]. I dati raccolti per una determinata finalità possono essere trattati ulteriormente solo per finalità compatibili, altrimenti è necessario un altro motivo previsto dal regolamento generale sulla protezione dei dati, ad esempio il consenso, per procedere al trattamento dei dati per la nuova finalità. In particolare, i dati raccolti a fini commerciali dagli intermediari o dalle piattaforme di dati sugli stili di vita non possono essere successivamente trattati nel contesto elettorale.

A meno che applichino la dovuta diligenza e verifichino che i dati siano stati ottenuti in modo lecito, i partiti politici e le fondazioni politiche non possono utilizzare tali dati ricevuti da terzi.

2.3 Obblighi di trasparenza

Il caso Cambridge Analytica ha dimostrato l'importanza di combattere l'opacità e di informare adeguatamente gli interessati. Spesso le persone non sanno chi tratta i loro dati personali e a quali fini. I principi di trattamento corretto e trasparente implicano che le persone siano informate dell'esistenza del trattamento e delle sue finalità[23]. Il regolamento generale sulla protezione dei dati chiarisce gli obblighi dei titolari del trattamento al riguardo. Essi sono

[17] Articolo 9 del regolamento generale sulla protezione dei dati.
[18] Articolo 9, paragrafo 2, lettera a), del regolamento generale sulla protezione dei dati.
[19] Articolo 9, paragrafo 2, lettera e), del regolamento generale sulla protezione dei dati.
[20] Articolo 9, paragrafo 2, lettera g), del regolamento generale sulla protezione dei dati.
[21] Articolo 9, paragrafo 2, lettera d), del regolamento generale sulla protezione dei dati. I partiti politici o le fondazioni politiche non possono condividere con terzi i dati relativi ai propri membri o ex membri, o a persone che hanno regolari contatti con loro, senza il consenso della persona interessata.
[22] Articolo 5, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati.
[23] Articolo 5, paragrafo 1, lettera a), del regolamento generale sulla protezione dei dati.

tenuti a informare le persone sui principali aspetti relativi al trattamento dei loro dati personali, ad esempio:

- l'identità del titolare del trattamento;
- le finalità del trattamento;
- i destinatari dei dati personali;
- la fonte dei dati quando non sono raccolti direttamente presso l'interessato;
- l'esistenza di un processo decisionale automatizzato e
- ogni altra informazione necessaria per assicurare un trattamento corretto e trasparente[24].

Inoltre, il regolamento generale sulla protezione dei dati impone di fornire le informazioni in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro[25]. Ad esempio, un avviso breve e poco chiaro sulla protezione dei dati stampato unicamente in caratteri piccoli nel materiale elettorale non sarebbe conforme agli obblighi di trasparenza.

Secondo le risultanze preliminari, informazioni incomplete circa la finalità per la quale i dati erano stati raccolti hanno costituito una delle principali lacune nel caso Cambridge Analytica, il che mette peraltro in dubbio la validità del consenso prestato dalle persone interessate. Tutte le organizzazioni che trattano dati personali nel contesto elettorale devono assicurarsi che le persone comprendano pienamente come e per quali finalità i loro dati personali saranno utilizzati, prima che le persone esprimano il proprio consenso o che il titolare del trattamento inizi a trattare i dati sulla base di qualsiasi altro motivo.

Le persone devono essere informate in ogni fase del trattamento, non solo al momento della raccolta dei dati.

In particolare, quando trattano dati ottenuti da terzi (ad esempio da liste elettorali nazionali, intermediari di dati, analisti di dati e altre fonti) i partiti politici devono di norma informare e spiegare alle persone interessate il modo in cui combinano e utilizzano i dati per assicurarne un trattamento corretto[26].

2.4 Profilazione, processo decisionale automatizzato e *micro-targeting*

La profilazione è una forma di trattamento automatizzato dei dati utilizzata per analizzare o prevedere aspetti concernenti ad esempio le preferenze personali, gli interessi, la situazione economica e così via[27]. La profilazione può essere utilizzata per sottoporre le persone a *micro-targeting*, ossia per analizzare i dati personali (ad esempio la cronologia di ricerca su internet) allo scopo di individuare gli interessi particolari di un determinato pubblico o di una determinata persona con l'intento di influenzarne le azioni. Il *micro-targeting* può essere

[24] Articoli 13 e 14 del regolamento generale sulla protezione dei dati.
[25] Orientamenti del comitato europeo per la protezione dei dati in materia di trasparenza.
[26] Articolo 14 del regolamento generale sulla protezione dei dati.
[27] Come definita all'articolo 4, paragrafo 4, del regolamento generale sulla protezione dei dati.

utilizzato per offrire un messaggio personalizzato a una persona o a un pubblico che utilizza un servizio online, ad esempio i media sociali.

Il caso Cambridge Analytica ha messo in luce le sfide specifiche poste dai metodi di *micro-targeting* sui media sociali. Le organizzazioni possono estrarre mediante *data mining* i dati raccolti dagli utenti dei media sociali per creare profili degli elettori. Ciò potrebbe permettere a tali organizzazioni di identificare gli elettori più facilmente influenzabili e quindi di influenzare l'esito delle elezioni.

A tale trattamento dei dati si applicano tutti i principi generali e le norme del regolamento generale sulla protezione dei dati, quali i principi di liceità, correttezza e trasparenza e la limitazione delle finalità. Le persone molto spesso non sanno di essere sottoposte a profilazione: non comprendono il motivo per cui ricevono annunci pubblicitari in modo chiaramente collegati alle ultime ricerche effettuate o perché ricevono messaggi personalizzati da diverse organizzazioni. Il regolamento generale sulla protezione dei dati obbliga tutti i titolari del trattamento, ad esempio i partiti politici o gli analisti di dati, ad informare le persone circa il ricorso a tali tecniche e le loro conseguenze[28].

Il regolamento generale sulla protezione dei dati riconosce che il processo decisionale automatizzato, compresa la profilazione, può avere gravi conseguenze. Esso stabilisce che una persona ha il diritto di non essere sottoposta a una decisione basata unicamente sul trattamento automatizzato che produca effetti giuridici che la riguardano o che incida in modo analogo significativamente sulla sua persona, a meno che il trattamento avvenga nel rispetto di condizioni rigorose, vale a dire se si basa sul consenso esplicito dell'interessato o è autorizzato dal diritto dell'Unione o dello Stato membro, che precisa altresì adeguate misure di tutela[29].

Le pratiche di *micro-targeting* nel contesto elettorale rientrano in questa categoria quando producono effetti sufficientemente significativi sulle persone. Il comitato europeo per la protezione dei dati ha dichiarato che ciò si verifica quando la decisione può influenzare in modo significativo le circostanze, il comportamento o le scelte delle persone o ha un impatto prolungato o permanente sulle persone[30]. Il comitato ritiene che la pubblicità mirata online in talune circostanze potrebbe influire in modo sufficientemente significativo sulle persone quando, ad esempio, è invasiva o sfrutta le loro vulnerabilità note. Data l'importanza dell'esercizio del diritto democratico di voto, i messaggi personalizzati che potrebbero avere come effetto, ad esempio, quello di spingere le persone a non votare o a votare in un determinato modo potrebbero soddisfare il criterio degli effetti significativi.

Nel contesto elettorale pertanto i titolari del trattamento devono assicurare che qualsiasi trattamento dei dati mediante il ricorso a tali tecniche sia legittimo e conforme ai principi sopra menzionati e alle condizioni rigorose del regolamento generale sulla protezione dei dati.

[28] Articolo 13, paragrafo 2, del regolamento generale sulla protezione dei dati.
[29] Articolo 22 del regolamento generale sulla protezione dei dati.
[30] Orientamenti del comitato europeo per la protezione dei dati sul processo decisionale automatizzato, WP251rev.01, rivisto e adottato il 6 febbraio 2018.

2.5 Sicurezza ed esattezza dei dati personali

La sicurezza è particolarmente importante nel contesto elettorale, date le dimensioni dei set di dati coinvolti, e tenuto conto del fatto che tali set di dati spesso contengono "dati sensibili". Il regolamento generale sulla protezione dei dati impone agli operatori che trattano dati personali (sia ai titolari del trattamento che ai responsabili del trattamento) di mettere in atto adeguate misure tecniche e organizzative per garantire un livello di sicurezza proporzionato ai rischi che il trattamento dei dati può comportare per i diritti e le libertà delle persone fisiche[31].

Il regolamento generale sulla protezione dei dati impone ai titolari del trattamento di notificare le violazioni dei dati personali all'autorità di controllo competente senza ingiustificato ritardo ed entro 72 ore. Quando la violazione dei dati personali potrebbe presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento è tenuto altresì a informare le persone interessate dalla violazione dei dati senza ingiustificato ritardo[32].

I partiti politici e gli altri soggetti coinvolti nel processo elettorale devono prestare particolare attenzione per garantire l'esattezza dei dati personali nel caso dei grandi set di dati e quando i dati sono compilati a partire da fonti differenti ed eterogenee. I dati inesatti devono essere immediatamente cancellati o rettificati e, ove necessario, aggiornati.

2.6 Valutazione d'impatto sulla protezione dei dati

Il regolamento generale sulla protezione dei dati introduce un nuovo strumento per la valutazione del rischio prima di iniziare il trattamento: la valutazione d'impatto sulla protezione dei dati, da effettuare necessariamente quando è probabile che il trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche[33]. È il caso del contesto elettorale, quando i titolari del trattamento valutano, sistematicamente e in modo approfondito, aspetti personali delle persone (profilazione compresa) che incidono in modo significativo sulle stesse, e quando trattano "dati sensibili" su vasta scala. Nello svolgimento dei loro compiti di servizio pubblico le autorità elettorali nazionali potrebbero non dover effettuare la valutazione d'impatto sulla protezione dei dati, se è già stata effettuata nel contesto dell'adozione della normativa.

Le valutazioni d'impatto che i vari soggetti sono tenuti ad effettuare nel contesto delle elezioni dovrebbero includere gli elementi necessari a far fronte ai rischi connessi a tale trattamento, in particolare la liceità del trattamento anche per i set di dati ottenuti da terzi e gli obblighi di trasparenza.

[31] Articolo 32 del regolamento generale sulla protezione dei dati.
[32] Articoli 33 e 34 del regolamento generale sulla protezione dei dati e orientamenti del comitato europeo per la protezione dei dati in materia di notifica delle violazioni dei dati personali.
[33] Articoli 35 e 36 del regolamento generale sulla protezione dei dati e orientamenti del comitato europeo per la protezione dei dati in merito alla valutazione d'impatto sulla protezione dei dati.

3. Diritti delle persone fisiche

Il regolamento generale sulla protezione dei dati conferisce alle persone fisiche nell'Unione diritti aggiuntivi e rafforzati che sono particolarmente rilevanti nel contesto elettorale:

- il diritto di accedere ai loro dati personali;
- il diritto di chiedere la cancellazione dei loro dati personali se il trattamento si basa sul consenso e tale consenso è revocato, se i dati non sono più necessari o se il trattamento è illecito; e
- il diritto alla correzione dei dati personali inesatti, imprecisi o incompleti.

Le persone hanno inoltre il diritto di opporsi al trattamento dei loro dati (ad esempio dei dati figuranti nelle liste elettorali trasmesse ai partiti politici) se è effettuato per motivi di "legittimo interesse" o di "interesse pubblico".

Le persone hanno il diritto di non essere sottoposte a decisioni basate unicamente sul trattamento automatizzato dei loro dati personali. In tal caso, esse possono chiedere l'intervento di una persona fisica e hanno il diritto di esprimere il proprio punto di vista e di contestare la decisione.

Per consentire alle persone di esercitare tali diritti, tutti i soggetti coinvolti devono fornire gli strumenti e le impostazioni necessari. Il regolamento generale sulla protezione dei dati prevede la possibilità di elaborare un codice di condotta approvato da un'autorità per la protezione dei dati che specifichi l'applicazione del regolamento in ambiti specifici, incluso il contesto elettorale.

Il regolamento generale sulla protezione dei dati conferisce alle persone il diritto di proporre reclamo a un'autorità di controllo e il diritto al ricorso giurisdizionale. Esso conferisce inoltre alle persone il diritto di incaricare un'organizzazione non governativa a proporre reclamo per conto loro[34]. In alcuni Stati membri la legislazione nazionale consente alle organizzazioni non governative di proporre reclamo senza essere incaricate da una persona. Ciò è di particolare rilevanza nel contesto elettorale, tenuto conto del gran numero di persone potenzialmente interessate.

[34] Articolo 80, paragrafo 1, del regolamento generale sulla protezione dei dati.

Aspetti fondamentali relativi alla protezione dei dati nel processo elettorale[35]

<table>
<tr><td rowspan="2">Partiti politici e fondazioni politiche</td><td colspan="2">I partiti politici e le fondazioni politiche sono titolari del trattamento dei dati</td></tr>
<tr><td colspan="2">• rispettano il principio di limitazione delle finalità, procedendo a un ulteriore trattamento solo per finalità compatibili (ad esempio, per la condivisione dei dati con le piattaforme)
• scelgono la base giuridica corretta per il trattamento dei dati (anche per i dati desunti): consenso, legittimo interesse, compito di interesse pubblico (se previsto dalla legge), condizioni specifiche per i "dati sensibili" (ad esempio: parere politico)
• effettuano la valutazione d'impatto sulla protezione dei dati
• informano le persone dello scopo di ciascun trattamento (obblighi di trasparenza), sia quando raccolgono i dati direttamente sia quando li ottengono da terzi
• assicurano l'esattezza dei dati, in particolare per i dati provenienti da fonti diverse e per i dati desunti
• verificano se i dati ricevuti da terzi sono stati ottenuti in modo lecito e per quale finalità (per esempio: se le persone interessate hanno prestato il loro consenso informato per una determinata finalità)
• tengono conto dei rischi specifici della profilazione e adottano adeguate misure di tutela
• rispettano condizioni specifiche se utilizzano il processo decisionale automatizzato (per esempio, ottengono il consenso esplicito e forniscono garanzie adeguate)
• indicano chiaramente chi ha accesso ai dati
• assicurano la sicurezza del trattamento attraverso misure tecniche e organizzative; segnalano le violazioni dei dati
• chiariscono gli obblighi con i responsabili del trattamento, come le società di analisi dei dati, in contratti o in altri atti giuridici vincolanti
• cancellano i dati non più necessari per le finalità iniziali per le quali erano stati raccolti</td></tr>
<tr><td rowspan="2">Intermediari di dati e società di analisi dei dati</td><td colspan="2">Gli intermediari di dati e le società di analisi dei dati sono titolari (o contitolari) o responsabili del trattamento a seconda del grado di controllo che esercitano sul trattamento</td></tr>
<tr><td>In qualità di titolari del trattamento</td><td>In qualità di responsabili del trattamento</td></tr>
</table>

[35] Le informazioni di cui sopra non sono affatto esaustive. Esse intendono evidenziare una serie di obblighi fondamentali connessi ai dati a norma del regolamento generale sulla protezione dei dati che sono pertinenti nell'ambito del processo elettorale. Le informazioni presentate corrispondono a uno scenario in cui i partiti politici raccolgono i dati autonomamente (da fonti pubbliche, attraverso la loro presenza sui media sociali, direttamente dagli elettori, ecc.) e utilizzano i servizi di intermediari di dati o di società di analisi dei dati per rivolgersi in modo mirato agli elettori attraverso le piattaforme dei media sociali. Le piattaforme possono anche essere una fonte di dati per i soggetti sopra citati. Pertinenti possono essere anche altre disposizioni, quali le norme sull'invio di comunicazioni indesiderate e le norme in materia di protezione delle apparecchiature terminali della direttiva e-privacy.

	• rispettano il principio di limitazione delle finalità, procedendo a un ulteriore trattamento solo per finalità compatibili (soprattutto per la condivisione dei dati con terzi) • scelgono la base giuridica appropriata per il trattamento: consenso, interesse legittimo. Nel caso dei "dati sensibili", il trattamento è possibile solo nel caso in cui venga espresso il consenso esplicito o i dati siano resi manifestamente pubblici • effettuano la valutazione d'impatto sulla protezione dei dati • informano le persone sulle finalità di ciascun trattamento (obblighi di trasparenza), in particolare quando è richiesto il consenso poiché generalmente i dati saranno venduti a terzi • rispettano condizioni specifiche se utilizzano il processo decisionale automatizzato (per esempio, ottengono il consenso esplicito e forniscono garanzie adeguate) • prestano particolare attenzione alla liceità del trattamento e all'esattezza quando combinano diversi set di dati • assicurano la sicurezza del trattamento attraverso misure tecniche e organizzative; segnalano le violazioni dei dati	• rispettano gli obblighi derivanti dal contratto o da un altro atto giuridico vincolante con il titolare del trattamento • assicurano la sicurezza del trattamento attraverso misure tecniche e organizzative • assistono il titolare del trattamento nella valutazione d'impatto sulla protezione dei dati o nell'esercizio dei diritti degli interessati o comunicano senza indugio al titolare del trattamento le violazioni dei dati di cui vengono a conoscenza
	Le piattaforme sono in genere titolari del trattamento dei dati che avviene sulle piattaforme stesse ed eventualmente contitolari del trattamento con altre organizzazioni	
Piattaforme di media sociali/reti pubblicitarie online	• scelgono la base giuridica appropriata per il trattamento: contratto sottoscritto con le persone interessate, consenso, legittimo interesse. Nel caso dei "dati sensibili", il trattamento è possibile solo nel caso in cui venga espresso il consenso esplicito o i dati siano resi manifestamente pubblici • utilizzano solo i dati necessari per la finalità individuata • effettuano la valutazione d'impatto sulla protezione dei dati • garantiscono la liceità quando condividono i dati degli utenti con terzi • rispettano gli obblighi di trasparenza, in particolare per quanto riguarda i termini e le condizioni, ad esempio se i dati sono successivamente condivisi con terzi • rispettano condizioni specifiche se utilizzano il processo decisionale automatizzato (per esempio, ottengono il consenso esplicito e forniscono garanzie adeguate)	

	• assicurano la sicurezza del trattamento attraverso misure tecniche e organizzative; segnalano le violazioni dei dati • forniscono controlli e impostazioni affinché le persone possano esercitare effettivamente i loro diritti, compreso il diritto di non essere sottoposte a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione
	Le autorità elettorali nazionali sono titolari del trattamento dei dati
Autorità elettorali nazionali	• Base giuridica per il trattamento: obbligo giuridico o compito di interesse pubblico previsto per legge • effettuano la valutazione d'impatto sulla protezione dei dati se l'impatto non è già stato valutato nella relativa legge