

Metodo democratico, partiti politici, nuove tecnologie e basi giuridiche per il trattamento dei dati personali: alcuni spunti di riflessione

di Gianluca Bellomo

Abstract: Democratic method, political parties, new technologies and legal bases for the processing of personal data: some food for thought – The entry into force of Regulation (EU) no. 679/2016 has deeply affected the personal data process, setting strict rules. This changed legal framework has produced direct and indirect consequences also on the “democratic method” of parties as well as in their internal activities, due to the new technologies’ increasing influence on democratic life. As the present essay will try to discuss, the possibility that incorrect process of voters or supporters’ personal data could affect individual rights and freedoms increases the party juridical responsibility in terms of respect for data treatments.

Keywords: Democratic method; political parties; Regulation (EU) n. 2016/679; data protection.

1. Dati personali, ruolo, funzioni e diritti *dei* e *nei* partiti politici

I partiti politici rappresentano delle libere associazioni di cittadini non riconosciute, di natura privatistica, previste direttamente in Costituzione all’art. 49¹. Già la stessa natura di questi soggetti implica che le persone ed

¹ Su cui per approfondimenti cfr. M. Luciani, *Partiti e forma di governo*, in *Nomos*, n. 3/2018, 1-11; F. Bilancia, *La Costituzione dello Stato e i partiti politici: l’attualità del noto saggio di Heinrich Triepel*, in *Costituzionalismo.it*, n. 1/2015, 1-14; ma anche G. Pasquino, V. Vidotto, P. Ridola, *Voce “Partiti politici”*, Enciclopedia Italiana Treccani, V Appendice, 1994, Roma, reperibile in www.treccani.it/enciclopedia/partiti-politici_%28Enciclopedia-Italiana%29/, S. Curreri, G. Stegheer, *I partiti politici in Italia*, in *Federalismi.it*, n. 23/2018, 3 s., ma anche i molteplici interventi pubblicati in Associazione italiana dei costituzionalisti, *Partiti politici e società civile a sessant’anni dall’entrata in vigore della Costituzione*, Napoli, 2009; e più risalenti E. Cheli, *Intorno alla regolazione dei partiti politici*, in *Studi senesi*, 1958; Aa.Vv., *Dibattito sulla disciplina legislativa del partito politico*, in *Rassegna parlamentare*, 1962; V. Crisafulli, *La Costituzione della Repubblica italiana e il controllo democratico dei partiti*, in *Studi politici*, 1967; C. Rossano, *Considerazioni sulla democrazia e sullo stato dei partiti*, in *Scritti degli allievi offerti a A. Tesaurò*, Milano, 1968. Con profili di comparazione tedesca e spagnola invece cfr. C. Pinelli, *Discipline e controllo sulla democrazia interna dei partiti*, Padova, 1984. Inoltre sulla necessità di una disciplina legislativa cfr. anche A. Pace, *Problematica delle libertà costituzionali*, Padova, 1988, II; S. Ceccanti, *Regolamentazione legislativa dei partiti ed elezioni primarie: un esempio del possibile ruolo del diritto comparato nell’iniziativa legislativa*,

il trattamento dei dati a queste collegati rappresentino uno degli elementi essenziali per la propria costituzione, affermazione e stessa esistenza in vita.

La raccolta, l'interpretazione e il continuo aggiornamento dei dati legati alle persone sia iscritte al partito, sia al di fuori di questo, non solo sono necessari per tali organizzazioni, ma anche connaturati alla stessa concezione classica della democrazia rappresentativa. È di tutta evidenza, infatti, che la traduzione dei bisogni degli elettori implica per i partiti il trattamento di dati personali collegati a questi ultimi. Così tradizionalmente i partiti politici hanno avuto il ruolo di soggetti intermedi tra società ed istituzioni fungendo da mediatori sia nella selezione della classe dirigente, sia nella formulazione delle priorità politiche da portare in primo piano sulla scena istituzionale ed in particolare con riferimento alla funzione legislativa prima ed esecutiva dopo².

Detta funzione negli anni, ed in particolare negli ultimi decenni, ha subito profondi mutamenti sotto la spinta delle nuove tecnologie³ che hanno fornito ai partiti e ai cittadini innovativi strumenti di comunicazione tra le

in *Diritto pubblico comparato ed europeo*, 1999; G. Cerrina Feroni, *Partiti politici: una regolazione giuridica?*, in *Rassegna parlamentare*, 2007.

² Su cui per approfondimenti cfr. S. Curreri, G. Stegheer, cit., 3.

³ Come era stato già autorevolmente notato «Se si esce dalla logica strettamente conservatrice di una lettura statica e chiusa del dettato costituzionale, e, come ci è stato insegnato, si accetta di guardare oltre la realtà fattuale che i Costituenti conoscevano per cogliere il senso “forte” dell’art. 49 quale norma che tutela le “cerniere” tra cittadini e politica, tra elettori e eletti, tra società civile e società politica, tra comunità e istituzioni, allora tutto cambia.

Il “*prius*” non è più il partito e la sua struttura organizzativa, ma la funzione alla quale esso è chiamato. Il valore tutelato non è più il partito pesante del novecento ma la partecipazione politica dei cittadini. L’analisi degli effetti delle nuove tecnologie non è più ristretta solo nei confini di una organizzazione partitica vista come un “*prius*” ma diventa essenziale per comprendere se siamo in presenza di mutamenti tecnologici che possono offrire opportunità di partecipazione politica impensate e impensabili nel passato e tali da poter consentire un superamento delle forme partitiche senza per questo mettere a repentaglio la partecipazione alla politica nazionale vista, come il Costituente la vide, quale elemento fondamentale di una società democratica.

In questa prospettiva, peraltro, si può persino giungere, come qualcuno ha fatto, a caricare le nuove tecnologie di una portata ancora più espansiva, fino ad individuare in esse, nelle opportunità che offrono e nei loro effetti, nuove forme di organizzazione politica. Non a caso spesso le duplici e duplicemente ambigue etichette della *e-democracy* e della *e-participation*, sono utilizzate tanto per indicare forme nuove di democrazia e di partecipazione quanto nuove forme di organizzazione politica.

In sostanza, mentre nella versione che muove dall’esperienza del partito le tecnologie rischiano di essere considerate soltanto in modo strumentale, fino a trascurare il loro stesso potenziale innovativo o a ridurlo a mero aspetto marginale di una realtà sostanzialmente immutata, nella seconda impostazione le tecnologie vengono viste come potenzialmente portatrici di nuove e più moderne forme di organizzazione diffusa, capaci di dar vita, per il solo fatto di esistere, a forme di partecipazione alla vita politica alternative e sostitutive degli stessi partiti.» F. Pizzetti, *Partiti politici e nuove tecnologie*, in *Federalismi.it*, 21/2008, 3 s. Ma anche per approfondimenti sul tema cfr. i contributi pubblicati in N. Urbinati (cur.), *Democrazie in transizione*, Milano, 2016, reperibile in fondazionefeltrinelli.it/app/uploads/2016/06/Democrazie-in-transizione-A-cura-di-Nadia-Urbinati-1.pdf.

parti, sempre più raffinati e spesso sempre più invasivi della sfera privata dei cittadini. Così, si è passati dall'iniziale rapporto personale tra politici ed elettori intercorso da principio nelle piazze o comunque in modo più o meno regolare *de visu*, all'impiego di sondaggi su varia scala per poter acquisire informazioni su numeri elevati di persone (o meglio elettori), fino a giungere al ricorso a strumenti volti all'analisi comportamentale dei singoli utenti sulla Rete attraverso tecniche di profilazione "elettorale"⁴, possibili grazie all'impiego proprio di nuove tecnologie e all'uso di sofisticati strumenti di analisi dei c.d. *Big Data*⁵. Da ultimo, ed i recenti fatti di cronaca ne sono un tangibile esempio⁶, si registra un ulteriore "salto" nell'evoluzione del rapporto tra politica ed elettori che sta conducendo alla predisposizione di vere e proprie campagne di condizionamento del voto attuate su vasta scala in particolare all'interno di piattaforme informatiche di tipo "social"⁷.

A tale evoluzione, resa possibile dall'avvento di nuove tecnologie e dai cambiamenti da queste innescate nella società, è corrisposto un vero e proprio processo di *leaderizzazione* nei partiti politici che hanno visto un accentramento dei rapporti tra cittadini elettori e leader dei singoli partiti che sempre più si rivolgono direttamente all'opinione pubblica attraverso le nuove piattaforme di comunicazione di massa⁸ (canali social quali *Facebook* o

⁴ Su cui cfr. R. Montaldo, *Le dinamiche della rappresentanza tra nuove tecnologie, populismo, e riforme costituzionali*, in *Quaderni costituzionali*, 4/2019, 789-810.

⁵ Per approfondimenti con riguardo ai rapporti con la democrazia rappresentativa cfr. M. Betzu, G. Demuro, *I big data e i rischi per la democrazia rappresentativa*, in *Media Laws*, 1/2020, 218-223.

⁶ Con riferimento a quest'ultimo "salto evolutivo" nelle azioni in ambito elettorale si pensi al noto caso di Facebook/Cambridge Analytica.

⁷ Su cui cfr. L. Califano, *Autodeterminazione vs. eterodeterminazione dell'elettore: voto, privacy e social network*, in *Federalismi.it*, 7 agosto 2019, 1-12; G. Grasso, *Social network, partiti politici e lotta per il potere*, in *Media Laws*, n. 1/2020, 211-216.

⁸ Tale fenomeno è anche direttamente e facilmente rilevabile a livello periferico. Si pensi ai sindaci dei comuni che ormai si sono dotati in gran numero di uno o più *account* su piattaforme social attraverso le quali hanno creato un canale diretto non istituzionale di contatto con i cittadini. Se tale fenomeno presenta degli indubbi vantaggi in termini di velocità di diffusione delle informazioni in senso biunivoco, trasformando di fatto ogni utente in "occhi del politico/amministratore" sul territorio, consentendo di segnalare a chiunque in tempo reale eventuali problematiche e potendo così avere risposte immediate; va anche rilevato che tale pratica ormai ampiamente diffusa pone una serie di problematiche riconducibili, tra le altre ad esempio, all'uso di strumenti e di *account* sostanzialmente privati per finalità istituzionali, ma anche al pericolo di esclusione di rilevanti porzioni di popolazione con un livello di competenze informatiche non sufficiente o prive di adeguati strumenti tecnologici tra i quali *in primis* l'accesso alla Rete. Un ulteriore rischio per l'esercizio del principio democratico è riconducibile ai condizionamenti che i soggetti politici possono subire con riferimento alle priorità sia in sede di formulazione che di attuazione delle proprie scelte amministrative. Infatti i soggetti politici, soprattutto a livello periferico, potrebbero incorrere nel rischio concreto di percepire orientamenti politici minoritari dei cittadini come prevalenti, ciò a causa di ripetuti interventi di pochi ed assidui attivisti costantemente impegnati nel sostenere tali posizioni all'interno di determinate comunità incidendo così in modo rilevante sulle scelte della classe politica eletta.

Twitter; ma anche gruppi più ristretti tramite strumenti chiusi e riservati di comunicazione di gruppo quali *Whatsapp*⁹).

Per converso, va notato che a tale collegamento diretto tra leader dei singoli partiti politici ed elettori è corrisposto un parallelo incrementarsi di sempre più stretti rapporti tra parlamentari e partiti politici e sempre meno tra eletti ed elettori. Si è così iniziato a parlare di “Repubblica dei partiti”¹⁰, si è affermato come il concetto tradizionale di partito sia ormai in crisi¹¹, si è anche arrivati a parlare di «degrado della democrazia dei partiti»¹².

Ma quali sono le principali situazioni giuridiche che si esplicano attraverso i partiti o quando si viene in contatto con un partito oggi e che possono produrre effetti negativi sulla garanzia del metodo democratico *dei* e *nei* partiti, senza dimenticare che i partiti politici non sono costituiti solo ed esclusivamente dagli iscritti¹³?

Per quanto attiene ai diritti che vengono in rilievo in connessione con i partiti politici si possono qui segnalare, almeno, il diritto: di costituire un partito; di aderire a un partito, in base alle regole e ai limiti fissati all'interno degli stessi; di recedere da un partito; di non iscriversi a nessun partito; ma anche, di voto per gli iscritti nelle assemblee politiche nazionali; di espulsione

⁹ Si pensi che l'uso di *Whatsapp* caratterizzato da una tecnologia che cripta i messaggi in prima dell'invio e li decifra sul dispositivo del destinatario in fase di ricezione facendo “viaggiare” i messaggi protetti da codice. Se da una parte tale tecnologia rende molto più sicura la conversazione, dall'altra la rende anche meno intercettabile in caso di indagini giudiziarie a differenza delle normali telefonate o in caso di ricorso all'invio di sms. Inoltre la facilità di reinoltro dei contenuti ricevuti attraverso l'app (che si tratti di messaggi di testo, di file audio o video) a molteplici destinatari o a gruppi costituiti anche da un numero rilevante di partecipanti rende tale strumento particolarmente idoneo a diffondere in pochissimo tempo dati personali anche ad un numero elevato di soggetti che possono essere di volta in volta selezionati dal singolo mittente del messaggio in modo esatto, anche se dopo l'invio non si potrà predeterminare i soggetti ai quali questi a loro volta dovessero decidere di inviare detto file.

¹⁰ Su cui per approfondimenti cfr. P. Scoppola, *La repubblica dei partiti. Evoluzione e crisi di un sistema politico 1945-1996*, Bologna, 1997.

¹¹ «Erano organismi collettivi, caratterizzati dal condividere idee e valori di fondo circa la società, dall'elaborare e portare avanti programmi conformi a quei valori, e dall'orientare, attraverso l'elaborazione e la partecipazione costante, le scelte istituzionali. Certamente oggi i partiti sembrano in crisi, anzi sembrano quasi scomparsi, perché le ideologie non hanno più presa e non è chiaro quali sono i valori di fondo dei diversi gruppi che si confrontano, e i programmi sono spesso visti come specchietti per le allodole. Tentativi di attirare il consenso attraverso promesse irrealizzabili o solleticando gli interessi immediati ed egoistici dei singoli gruppi, invece che come progetti concreti e realistici in funzione del bene della collettività. E quindi i partiti hanno perso anche la capacità di orientare le scelte istituzionali.», P. Springhetti, *Nelle forme tradizionali la partecipazione è in crisi. Ma non possiamo farne a meno*, intervista a Valerio Onida, 09/01/2019, reperibile in www.retisolidali.it/crisi-della-partecipazione-valerio-onida/.

¹² Su cui cfr. S. Merlini, *I partiti politici, il metodo democratico e la politica nazionale*, in *Partiti politici e società civile a sessant'anni dall'entrata in vigore della Costituzione*, Atti del XXIII Convegno annuale AIC, 17-18 ottobre 2008, Napoli, 2009, 51-110.

¹³ Circostanza, questa, che amplifica notevolmente il numero di soggetti interessati e la dimensione delle problematiche coinvolte.

di iscritti per i quali dovesse essere accertata la violazione delle regole interne.

Passando invece alle funzioni che i partiti sono chiamati ad assolvere, si possono individuare tra le altre: la selezione delle candidature e l'organizzazione di eventuali elezioni primarie; la gestione del partito a livello centrale e periferico; l'attivazione di processi decisionali interni e di dibattito tra gli iscritti; la fidelizzazione degli iscritti; il reperimento di fondi; la formazione e l'istruzione (politica, amministrativa, ecc.) dei propri iscritti, la raccolta e l'analisi dei bisogni del proprio bacino elettorale, con la scrematura delle istanze da promuovere in sede politica; l'acquisizione di nuovi iscritti e soprattutto del voto di nuovi elettori.

Un non corretto esercizio di dette situazioni giuridiche da parte dei partiti politici rischierebbe di portare ad una deriva nel corretto esercizio del metodo democratico *dei* partiti e *nei* partiti che potrebbe far sì che, come rilevato in Dottrina¹⁴, «persone che emergono non si sa come, occupano uno spazio televisivo, sviluppano idee per lo più banali e prive di approfondimento, abbassando il dibattito politico ad uno scambio di slogan e insulti» con ovvie nefaste conseguenze sulla vita delle istituzioni e dei cittadini.

2. Nuove tecnologie e partiti politici

L'avvento sempre più massivo ed intensivo delle nuove tecnologie e dei nuovi strumenti da queste messi a disposizione dei partiti hanno inciso ed incideranno sempre di più sulla vita dei partiti e in particolar modo sull'esercizio dei citati diritti e funzioni delle quali questi si dovrebbero fare portatori¹⁵.

Così, si pensi a mero titolo di esempio: alla raccolta e all'utilizzo a fini elettorali di dati recuperati su internet e *social network* da parte dei partiti (tramite operazioni di *webcrawling* possibili grazie a programmi che analizzando la Rete reperiscono dati in modo massivo; ma anche all'impiego spregiudicato di *Facebook*, *Twitter* o altre piattaforme *social*); all'uso delle comunicazioni di gruppo selettive e mirate (si pensi ad esempio al citato

¹⁴ Su ci cfr. R. Bin, *Partiti politici: un diritto che ci è sottratto*, in *lacostituzione.info*, 27 dicembre 2019, 1.

¹⁵ Va rilevato con riguardo al tema infatti, come affermato dal già *Garante privacy*, che sempre più oggi «la nostra più effettiva e reale dimensione di vita è paradossalmente quella digitale: densa di opportunità ma anche di insidie», A. Soro, *Persona, diritti, innovazione*, Discorso del Presidente dell'Autorità garante per la protezione dei dati personali, Relazione 2016, reperibile in www.garanteprivacy.it/documents/10160/0/Relazione+2016+-+Discorso+del+Presidente+Antonello+Soro.pdf/0e39e415-51fc-4461-9ab0-5ccc5cc75d0c?version=1.2.

Per ulteriori approfondimenti sul tema cfr. Aa.Vv., *Il Forum: Le sfide della democrazia digitale*, in Gruppo di Pisa, n. 3/2019, 231-284, invece per alcuni spunti critici, in particolare sull'evoluzione nel rapporto tra grandi lobby, mass media e sistema politico, cfr. C. Crouch, *Postdemocrazia*, Laterza, Bari 1-148.

ricorso intensivo all'uso di *Whatsapp* fatto a tutti i livelli politici anche nei partiti); alla già ricordata profilazione “elettorale”; all'uso dei *Big Data*, ma anche di programmi di *Intelligenza Artificiale* e di *Machine learning* in ottica predittiva, ma purtroppo anche manipolativa (es. uso mirato di *fake news* a fini di condizionamento elettorale)¹⁶.

Va rilevato, peraltro, che sovente i dati trattati dai partiti politici possono essere rivelatori dell'orientamento politico di un interessato e quindi rientrare pienamente tra quella particolare categoria di dati che una volta veniva definita come “dati sensibili” che gode di particolare tutela proprio in quanto potenzialmente maggiormente lesiva dei diritti e delle libertà dei cittadini ove tali dati non godano di adeguate tutele. Si pensi già solo banalmente all'iscrizione di un soggetto ad un'associazione partitica, ma anche semplicemente alla ricezione di una pubblicazione periodica inviata da un partito o alla pubblicizzazione di un contributo in denaro versato da un soggetto ad un Partito. Proprio quest'ultimo caso ha posto il problema del corretto bilanciamento tra un principio di trasparenza e di tutela dei dati personali che ha trovato una soluzione nella fissazione di una serie di regole sui contributi erogati in favore dei partiti e delle fondazioni politiche che hanno dato vita alla legge 9 gennaio 2019, n. 3 «*Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici*» con il quale sono state introdotte misure per la trasparenza dei partiti e dei movimenti politici e delle fondazioni, con particolare riferimento al loro finanziamento. Successivamente sulla materia è intervenuto il D.L. n. 34/2019 «*Misure urgenti di crescita economica e per la risoluzione di specifiche situazioni di crisi*», principalmente per ridefinire gli obblighi di trasparenza posti in capo alle fondazioni politiche¹⁷.

Da quanto rilevato dovrebbe risultare quindi evidente che oggi più che mai anche la democrazia *dei* partiti e *nei* partiti risente degli effetti dell'avvento delle nuove tecnologie e, considerato che ormai praticamente tutte le attività ad elevato contenuto tecnologico richiedono per il proprio funzionamento il trattamento in via diretta o indiretta di dati personali (registrazioni di account; installazione di *app* che per funzionare richiedono l'accesso a dati personali quali la posizione, il numero di telefono, l'elenco dei contatti, ecc.), ne consegue che si assiste ad un aumento esponenziale del

¹⁶ Anche per tali ragioni, in considerazione dei potenziali rischi che l'uso illecito dei dati personali può comportare per i processi elettorali e la democrazia, lo stesso legislatore europeo ha di recente previsto «sanzioni pecuniarie nei casi in cui i partiti politici europei o le fondazioni politiche europee sfruttino le violazioni delle norme in materia di protezione dei dati al fine di influenzare l'esito delle elezioni del Parlamento europeo», v. Regolamento UE, Euratom n. 1141/2014, del 22 ottobre 2014, relativo allo statuto e al finanziamento dei partiti politici europei e delle fondazioni politiche europee, come modificato dal Regolamento UE, Euratom 2019/493 del 25 marzo 2019.

¹⁷ Su cui per un primo quadro d'insieme cfr. Servizio studi della Camera dei Deputati, *Disciplina e trasparenza dei partiti politici e delle fondazioni*, 22 aprile 2020, 1-5 reperibile in www.camera.it/temiap/documentazione/temi/pdf/1104961.pdf.

rischio di ledere quel principio di autodeterminazione informativa preconizzato da Rodotà già venti anni fa¹⁸ e del quale l'attuale quadro normativo in materia di protezione dei dati personali è portatore. Così il corretto trattamento dei dati riferibili alle persone fisiche assume oggi nei partiti e per i partiti politici un ruolo sempre più strategico e cruciale per la loro stessa sopravvivenza e garanzia del ruolo e delle funzioni costituzionalmente loro assegnate. Ma il corretto trattamento, da ultimo, deve fare i conti con l'attuale quadro normativo in materia, profondamente innovato dalla piena entrata in vigore avutasi il 25 maggio 2018 del Regolamento (UE) n. 679/2016 (GDPR nell'acronimo inglese).

3. Regolamento (UE) n. 679/2016 (GDPR) e partiti politici

Con il Regolamento n. 679/2016, da un lato, si è assistito a un vero e proprio *tsunami* per le organizzazioni pubbliche e private che trattano dati personali e quindi anche per i partiti politici, e dall'altro si sono messi a sistema, all'interno di una norma generale comune di rango europeo, una serie di diritti, tutele e istituti con rilevanti ricadute sui cc.dd. *interessati*¹⁹.

Il Regolamento ha riscritto per tutti i Paesi membri la disciplina, originariamente introdotta con la direttiva 95/46. In particolare, esso ha rimodellato (ma in gran parte sostituito) la normativa italiana in materia abrogando tutte le norme previste nel precedente decreto legislativo 30 giugno 2003, n. 196²⁰ (*Codice della privacy*) incompatibili. Si è venuto così a

¹⁸ «Non metteremo la mano su di te». Questa era la promessa della Magna Charta: rispettare il corpo nella sua integralità: “*Habeas corpus*”. Questa promessa sopravvive ai mutamenti tecnologici. Ogni trattamento di singoli dati dev'essere considerato come se si riferisse al corpo nel suo insieme, ad una persona che deve essere rispettata nella sua integrità fisica e psichica. È nata una nuova concezione integrale della persona, alla cui proiezione nel mondo corrisponde il diritto al pieno rispetto di un corpo che ormai è, al tempo stesso, “fisico” ed “elettronico”. In questo nuovo mondo la *data protection* adempie alla funzione di assicurare que“*habeas data*” che i tempi mutati esigono, diventando così, com'è avvenuto con l'*habeas corpus*, un elemento inscindibile dalla civiltà ... Non ho timore di usare parole troppo impegnative. Ma sono convinto che la riflessione sulla protezione dei dati, su *privacy* e dignità, sia un passaggio ineludibile per comprendere la condizione dell'uomo in questo millennio e per definire i caratteri che la democrazia sta assumendo», S. Rodotà, *Privacy, libertà, dignità*, 26a Conferenza Internazionale sulla Privacy e sulla Protezione dei Dati Personali, Wroclaw (PL), 14, 15, 16 settembre 2004, reperibile in www.privacy.it/archivio/rodo20040916.html.

¹⁹ Per *interessato* si intende, come desumibile dallo stesso GDPR all'art. 4, 1), qualsiasi persona fisica identificata o identificabile alla quale sono riconducibili uno o più dati personali.

²⁰ Decreto legislativo 30 giugno 2003, n. 196 recante il «Codice in materia di protezione dei dati personali» (in S.O. n. 123 alla G.U. 29 luglio 2003, n. 174); successivamente modificato dal decreto legislativo 10 agosto 2018, n. 101, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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

positivizzare un nuovo rapporto nel bilanciamento tra diversi diritti fondamentali²¹. Contemporaneamente si è assistito, in Italia, a una convulsa azione di adeguamento della normativa interna incompatibile con la disciplina regolamentare europea, attraverso l'approvazione ed emanazione del d.lgs. 10 agosto 2018, n. 101²².

Il Regolamento, insieme alle singole discipline interne predisposte dagli Stati membri in sede di adeguamento normativo nel rispetto dei margini di autonomia da questo delegati agli ordinamenti nazionali, oggi, quindi, rappresenta uno dei modelli più avanzati, a livello globale, di tutela della *privacy* e dei dati personali²³. Il Regolamento, infatti, si propone nell'attuale conformazione come possibile archetipo per una costituzionalizzazione mondiale dei principi relativi alla tutela dei dati personali verso i quali l'UE sembrerebbe essersi prefissa di far convergere

Generale sulla Protezione dei Dati – GDPR in lingua inglese)” (in G.U. 4 settembre 2018 n. 2).

²¹ Su cui v. C. Docksey, *Four fundamental rights: finding the balance*, in *Int. Data Priv. Law*, n. 3/2016, Vol. 6, 195-209.

²² Va evidenziato che il legislatore italiano ha preferito, non senza critiche, percorrere la strada di modifica del pregresso *Codice della privacy*, invece di emanare un nuovo Codice che sostituisse il precedente. Ciò ha portato da una parte, forse, a un passaggio di adeguamento meno traumatico per gli operatori coinvolti, ma dall'altra alla attuale formulazione del *Codice della privacy* che, quanto meno dal punto di vista del *drafting* normativo, risulta di non facile lettura. Si pensi solo, a titolo di esempio: da una parte all'art. 2 del Codice novato, che introduce ben sedici articoli dopo l'art. 2 fino al 2-*septiesdecies*; e dall'altra all'abrogazione in sequenza di tutte le disposizioni dall'art. 3 fino all'art. 45, oltre a molte altre nel prosieguo del testo in quanto incompatibili con il Regolamento, su cui per maggiori dettagli v. V. Cuffaro, *Quel che resta di un codice: il D.Lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati*, in *Corr. giur.*, n. 10/2018, 1181-1185, che ha efficacemente parlato di «intervento demolitorio».

Un'evidenza empirica della confusione generata dalla scelta presa è rinvenibile nel fatto che ancora oggi può capitare di leggere su documenti ufficiali o su moduli prestampati anche di pubbliche amministrazioni, formulazioni che, nell'adeguare i richiami alle nuove normative introdotte in materia di *privacy*, richiamano esclusivamente il d.lgs. n. 101/2018, come se questo avesse abrogato, e non esclusivamente modificato, il precedente Codice del 2003.

²³ Il Regolamento cerca di rispondere alle nuove sfide dettate dalla crescita esponenziale di Internet e dei servizi a questo collegati, «Internet, infatti, è ormai a pieno titolo un *advertisement supported service* che si basa in larghissima parte sulla profilazione dell'utenza: in questo contesto, come ebbe ad affermare nel 2009 il Commissario europeo per la tutela dei consumatori Meglena Kuneva, «*[p]ersonal data is the new oil of the internet and the new currency of the digital world*»: i dati personali, insomma, sono divenuti un vero e proprio carburante per lo svolgimento dell'attività di numerosissimi operatori. Per altro verso, gli stessi utenti di servizi online rendono universalmente pubbliche innumerevoli informazioni personali: una pratica, questa, che è divenuta quasi un *modus vivendi* per gran parte della popolazione mondiale e che ha finito con il trasformare le stesse relazioni sociali, specialmente per i c.d. *nativi digitali*. Conseguenza di tutto ciò è l'esponenziale aumento del rischio che il potenziale “invasivo” del sistema informativo telematico nell'esistenza umana divenga strumento per nuove e sempre più sofisticate forme di controllo sociale». Così E. Lucchini Guastalla, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e impresa*, n. 1/2018, 108.

gli altri standard, ove presenti, degli ordinamenti extraeuropei²⁴. Sul punto va però rilevato che ove il modello europeo²⁵ non dovesse trovare, almeno nei principi fondamentali, la diffusione sperata, il rischio opposto potrebbe essere quello che la normativa adottata in UE per la tutela dei dati personali si possa trasformare in un *unicum* nello spazio globale che porti all'isolamento dell'Unione e quindi a una contestuale diminuzione dei propri livelli di competitività nei regionalismi macroeconomici mondiali in continua trasformazione. Peraltro, va anche rilevato che il ruolo della Corte di giustizia sta influenzando e non poco sulla conformazione di tale modello e sui limiti di applicabilità dello stesso, si pensi a quanto statuito in materia di diritto all'oblio e nello specifico circa il diritto alla deindicizzazione²⁶.

²⁴ In forza dell'interpretazione estensiva che con il tempo, la Corte di Giustizia ha iniziato a fornire relativamente all'*ambito di applicazione della Direttiva* originaria e, in particolare, del suo art. 4 (rubricato «Dritto nazionale applicabile»), la Corte ha assicurato l'applicabilità della normativa europea anche nel caso in cui il trattamento dei dati personali fosse effettuato da soggetti non europei e i dati venissero trattati prevalentemente fuori dall'Europa. Così con tali decisioni, la Corte «assume che il livello di protezione dei dati personali adottato in Europa sia più elevato rispetto al livello di protezione dei dati personali adottato altrove nel mondo e si fa promotrice del modello europeo del diritto alla protezione dei dati personali», cfr. *amplius* C. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, cit., 8 s., citando in nota G. Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Scherms*, in G. Resta – V. Zeno-Zencovich (cur.), *La protezione transnazionale dei dati personali. Dai "Safe harbour principles" al "Privacy shield"*, Roma, 2016, 116, ma da ultimo sia anche consentito il rinvio a G. Bellomo, *Trasferimento di dati personali verso paesi terzi: la Corte annulla il «Privacy Shield», amplia i poteri delle autorità di controllo e responsabilizza ulteriormente i data exporters*, in *DPCE on line*, n. 4/2020, 5337-5345.

²⁵ «Le leggi certo non mancheranno, e già oggi vi sono molte leggi "simil-GDPR" o versioni "light" del GDPR in giro per il mondo. Il GDPR deve vedersela con vari concorrenti che aspirano a fungere da modelli per la disciplina della protezione dei dati. Vi è chi dubita che l'influenza del GDPR possa essere duratura, ritenendo che sia maggiore il potenziale attrattivo della versione "modernizzata" della Convenzione 108. Il concetto di "Data Free Flow with Trust", ossia di libera circolazione dei dati in un ambiente fidato, promosso dal G20 di giugno 2019, non corrisponde esattamente al sistema GDPR basato su diritti e responsabilizzazione. Quale che sia il modello adottato, devono esserci in ogni caso la volontà e le risorse per assicurarne l'attuazione. Singoli e gruppi devono disporre degli strumenti per far valere i propri diritti, e avere il diritto di farlo. Un Internet balcanizzato, frammentato, ovvero uno "splinternet", non è auspicabile, ma forse è inevitabile se alcune regioni del mondo non riusciranno a tutelare la dignità umana e i valori democratici», C. D'Cunha, *L'UE può farcela*, in Aa.Vv., *"Privacy 2030": Una nuova visione per l'Europa, Un manifesto per il nostro futuro. Il manifesto del pensiero di Giovanni Buttarelli*, IAPP e Garante per la protezione dei dati personali italiano, 27, reperibile in www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9456977.

²⁶ Su tali dinamiche cfr. G. Finocchiaro (dir.), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 897; ma anche, in particolare con riferimento al diritto all'oblio e alla sua evoluzione alla luce delle pronunce della Corte di giustizia v. O. Pollicino, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della carta di Nizza nel reasoning di Google Spain*, in *Dir. Inf.*, 2014, 569-590, e più nello specifico Id., *Limitare il diritto all'oblio è un rischio*,

A ben vedere, però, il Regolamento ha una portata di gran lunga più ampia rispetto ai confini normativi legati alla mera nozione di tutela della riservatezza, giacché esso detta disposizioni inerenti alla tutela dei dati personali anche quando questi ultimi non sono direttamente collegabili alla vita privata degli interessati (potenziali elettori o iscritti al partito), o ad aspetti di tipo strettamente personale²⁷.

Non può non evidenziarsi, peraltro, che il Regolamento, già a partire dalla sua denominazione, è espressivo di un duplice livello di tutela da bilanciare e cioè: da una parte la protezione delle persone fisiche, con riguardo al trattamento dei dati personali; ma, dall'altra, la maggiore libera circolazione di tali dati²⁸, che trova spesso una scarsa valorizzazione nella fase applicativa. La *ratio* regolamentare va quindi individuata primariamente nella tutela delle libertà e dei diritti fondamentali dei cittadini, e quindi nella riduzione effettiva dei livelli di rischiosità per i soggetti coinvolti²⁹; dall'altra però, non si prefigge lo scopo di bloccare la circolazione dei dati personali, ma di fornire un contesto normativo generale e uniforme a livello europeo caratterizzato da maggiori margini di certezza, che consenta di coniugare le istanze ora evocate, favorendo al contempo un elevato livello di effettività in una realtà sempre più tecnologizzata³⁰.

in *Ilsole24ore*, 24 settembre 2019, reperibile in www.ilsole24ore.com/art/limitare-diritto-all-oblio-e-rischio-ACiINem?refresh_ce=1; e Id., *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in *Federalismi.it*, n. 3/2014, 27.

²⁷ Così, come affermato in dottrina «I dati personali costituiscono il tema disciplinato anche se non si riferiscono a vicende private, intime o familiari. Qualunque informazione, quale che sia il suo contenuto, è oggetto del Regolamento. Il diritto alla protezione dei dati personali deve essere considerato distinto dalla libertà negativa di non subire interferenze nella propria vita privata, al cuore del diritto alla riservatezza, costituendo invece il fondamento della libertà positiva di esercitare un controllo sul flusso delle proprie informazioni», G. Finocchiaro, cit., 896.

²⁸ Un esempio di come il Regolamento cerchi di favorire la circolazione dei dati è rappresentato dall'introduzione del «diritto alla portabilità dei dati», previsto all'art. 20. Tale diritto sancito nel GDPR nasce proprio con l'intento di rimuovere quegli ostacoli che non consentono il rapido trasferimento dei dati di clienti tra operatori. Si pensi, ad esempio, a un utente che intenda cambiare operatore telefonico o internet service provider. Troppo spesso, infatti, sono stati utilizzati presunti ostacoli al trasferimento di questi al fine di scoraggiare il passaggio da un fornitore di un servizio a un altro creando di fatto delle distorsioni alla libera concorrenza tra operatori con conseguenze negative in particolare a carico dei consumatori.

²⁹ Va evidenziato che la tutela dei dati personali, essendo potenzialmente lesiva di diritti fondamentali in via diretta o indiretta, può essere considerata oggi a pieno titolo come *esercizio di attività pericolosa* posta in essere dal titolare del trattamento (o dal responsabile) ai sensi dell'art. 2050 «Responsabilità per l'esercizio di attività pericolose» del Codice Civile con tutte le relative conseguenze giuridiche.

³⁰ Tale intento è già presente nel *considerando 7 al Regolamento UE 2016/679* dove si può leggere «Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che le riguardano e che la certezza giuridica e operativa sia

All'interno del quadro appena tratteggiato il Regolamento, quindi, incide ed inciderà sempre di più sulla vita *dei* e *nei* partiti politici proprio a causa dello spostamento delle attività che li riguardano dal mondo fisico a quello digitale. Ciò, infatti, comporterà un netto aumento nella mole di dati personali trattati dai partiti politici in quanto il ricorso ai nuovi strumenti tecnologici da parte di questi richiede quasi sempre il trattamento di dati personali di persone fisiche (creazione di un account, accreditamento preventivo all'uso o concessione di privilegi di accesso a piattaforme informatiche ecc.). A questo si aggiunga, e la cosa dovrebbe indurre ad una maggiore riflessione, che proprio in ambito *privacy* i partiti politici maneggiano dati personali che sono sottoposti di norma ad un regime giuridico maggiormente restrittivo. Ciò si spiega perché detti dati sono potenzialmente «idonei a rivelare le opinioni politiche» degli utenti-cittadini, e quindi rientrano in quelli che una volta venivano identificati come c.d. «dati sensibili» ai sensi dell'art. 4, lettera d), del vecchio *Codice privacy* e oggi come «particolari categorie di dati» dall'articolo 9 del Regolamento, essendo potenzialmente maggiormente lesivi dei diritti e delle libertà fondamentali dei cittadini.

4. Presupposti di liceità nel trattamento dei dati personali e partiti politici

Volendo analizzare con maggior dettaglio i presupposti di liceità nei trattamenti di dati personali attuati da parte dei partiti politici ed i limiti generali imposti dall'attuale disciplina in materia, si dovranno necessariamente distinguere, in prima battuta, le attività di trattamento svolte nei confronti dei propri membri o di persone che hanno regolari contatti con i singoli partiti, dalle attività di trattamento che dovessero invece coinvolgere soggetti terzi. Inoltre, vanno considerate le specifiche finalità per le quali i dati coinvolti vengono trattati.

Va rilevato, infatti, che il GDPR per i dati personali che non rientrano nelle particolari categorie previste dall'art. 9, individua all'art. 6 una serie di basi giuridiche che consentono il trattamento dei dati personali da parte di altri soggetti. Tra queste quelle che possono trovare applicazione, con specifico riferimento ai partiti politici, sono sostanzialmente tre: il *consenso* al trattamento dei dati da parte dei singoli interessati; il trattamento sulla base

rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche».

Un esempio applicativo di tale tensione e di come non sia facile trovare un ragionevole bilanciamento nell'azione di *enforcement* della normativa può essere rintracciato nel contemperamento tra tutela della *privacy* e protezione dei dati personali, da una parte, e, necessità di assicurare un adeguato livello di sicurezza pubblica e di integrità del sistema finanziario europeo dall'altra, su cui per approfondimenti cfr. L. Borlini, *Tutela della privacy e protezione dei dati personali a fronte della sicurezza pubblica e dell'integrità del sistema finanziario europeo*, in *Dir. um. dir. int.*, n. 1/2017, 23-49.

di un interesse pubblico; ed infine il perseguimento di un interesse legittimo del titolare o di terze parti.

Ogni base giuridica presenta delle date condizioni di applicabilità.

La prima base giuridica (art. 6, 1, a) impone che il consenso dell'interessato abbia dei caratteri specifici, pena la sua invalidità. Così deve essere libero, specifico, informato, il mancato consenso non deve prevedere conseguenze negative sull'interessato e deve essere chiaro che quest'ultimo è d'accordo al trattamento dei propri dati personali per le specifiche finalità e con le modalità che gli sono state comunicate. Il ricorso a tale base giuridica comporta per i partiti politici elevati rischi di incorrere nell'inosservanza di quanto previsto dal GDPR e comunque implica un elevato sforzo gestionale con tutti i relativi costi a questo collegati, oltre che in molti casi una vera e propria impossibilità al rispetto di tutto quanto previsto dalla normativa a riguardo, in particolare quando i dati personali sono trattati con il ricorso a strumenti informatici o su vasta scala. L'uso di tale base giuridica, pertanto e molto verosimilmente, sarà, ove possibile, residuale da parte dei partiti politici.

La seconda base giuridica in analisi (art. 6, 1, e) prevede che ove il titolare sia investito di una funzione di pubblico interesse possa, limitatamente alle funzioni affidate, evitare di ricorrere al consenso per il trattamento dei dati personali coinvolti. Va rilevato a riguardo però che affinché si rientri nel concetto di funzione di pubblico interesse, detta funzione deve essere esplicitamente contemplata da norme europee, o di legge emanate dai singoli Stati membri e alle quali ogni partito politico è soggetto. Si aggiunga, inoltre, che la norma deve rispondere ad obiettivi di pubblico interesse, essere proporzionata alle finalità da raggiungere, ferma la discrezionalità degli Stati membri di introdurre previsioni più specifiche per gli scopi previsti dal Regolamento. Il ricorso a tale base giuridica da parte dei partiti politici sembrerebbe legittimo sia alla luce delle finalità pubbliche che materialmente questi organismi espletano in base alle disposizioni costituzionali dei singoli Paesi membri (ad esempio nell'art. 49. Cost. It. «concorrere con metodo democratico a determinare la politica nazionale»); sia in base a quanto previsto dalle singole leggi elettorali dei Paesi membri; sia, ancora, in base a quanto affermato dalla stessa Commissione europea che, in un rapporto sull'applicazione al contesto elettorale delle norme in materia di tutela dei dati personali, ha esplicitamente ammesso il ricorso a tale base giuridica a condizione che le leggi nazionali lo prevedano³¹, lasciando così di fatto ampi margini di applicazione di tale principio ai partiti politici da parte dei legislatori dei singoli Stati membri.

L'ultima base giuridica tra quelle applicabili ai partiti politici per il trattamento dei dati personali prevista (art. 6, 1, f) consente anch'essa, come la seconda, di evitare il ricorso al *consenso* è rappresentata, come ricordato,

³¹ Commissione europea, Free and Fair Elections: Guidance on the Application of Union Data Protection Law in the Electoral Context, COM(2018) 638 final, 5.

dall'interesse legittimo del titolare o di terze parti. Il ricorso a tale base giuridica però non è certo banale. Infatti, il Regolamento prevede una serie di limitazioni³² e criteri nel legittimo ricorso a tale base di trattamento che costringono di volta in volta i partiti a svolgere con riguardo ad ogni singolo caso un'operazione di corretto bilanciamento tra i legittimi interessi del titolare e gli interessi ed i diritti fondamentali degli interessati³³. Così in tale bilanciamento sarà indispensabile valutare i livelli di compressione e di prevalenza nel rapporto tra diritto alla *privacy* e alla protezione dei dati personali da una parte e gli altri diritti fondamentali così come previsti nella Carta di Nizza, incluso il diritto alla libertà di espressione e di informazione dall'altra³⁴.

Passando al caso affatto raro in cui i partiti politici si trovino invece a trattare particolari categorie di dati³⁵, che quindi in potenza potrebbero maggiormente danneggiare i singoli interessati in caso di non corretto trattamento degli stessi, il Regolamento prevede all'art. 9, come anticipato, un regime specificamente dedicato al legittimo trattamento dei dati che prende le mosse da un obbligo di divieto generale di trattamento di dette categorie.

Nel medesimo articolo, però, sono rinvenibili le eccezioni che consentono di superare tale generale divieto. Tra queste quelle di maggiore interesse, con specifico riferimento ai partiti politici, sono individuabili: nel consenso al trattamento fornito dall'interessato per scopi specifici; nei trattamenti effettuati nell'ambito delle legittime attività svolte da una fondazione, associazione o altro organismo senza scopo di lucro che persegua

³² Così l'*interesse legittimo* dovrà essere "pertinente" e cioè dovrà, ai sensi dell'articolo 7, lettera f): essere lecito (ossia conforme al diritto nazionale e unionale applicabile); essere articolato in maniera sufficientemente chiara da consentire di eseguire il test comparativo valutando l'interesse legittimo del responsabile del trattamento rispetto agli interessi e ai diritti fondamentali dell'interessato (ossia sufficientemente specifico); rappresentare un interesse concreto ed effettivo (ossia non deve essere teorico), Gruppo di lavoro Art. 29, cit., 30.

³³ Su cui cfr. Gruppo di lavoro Art. 29, Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE, 844/14/IT WP217, 28-43 in cui, tra l'altro, vengono riportati gli elementi da prendere in considerazione a tal fine: se è coinvolto l'esercizio di diritti fondamentali; se sono coinvolti ulteriori interessi legittimi pubblici e privati; l'estensione del livello di riconoscimento della legittimità dell'interesse coinvolto; la magnitudo dell'impatto sia positivo che negativo in termini di conseguenze del trattamento; la natura dei dati coinvolti; il modo in cui i dati sono trattati; le ragionevoli aspettative degli interessati ecc. (punti da I a V del provvedimento).

A riguardo il Garante italiano è entrato molto in dettaglio anche stabilendo in modo chiaro quali siano i dati non utilizzabili in assenza di consenso in particolare con il provvedimento emanato nell'aprile 2019 al quale sia consentito rinviare per approfondimenti, Garante per la protezione dei dati personali, *Provvedimento in materia di propaganda elettorale e comunicazione politica*, doc. web n. 9105201, 18 aprile 2019, reperibile in www.privacy.it/2019/04/18/provvedimento-propaganda-elettorale-comunicazione-politica/.

³⁴ *Ibidem*, 30 s.

³⁵ Così come previste all'art. 9 del GDPR.

finalità politiche; in trattamenti necessari per motivi di interesse pubblico rilevante.

Per quanto attiene al tema del consenso al trattamento da parte degli interessati con riferimento a quanto previsto dall'art. 9 del Regolamento³⁶, va rilevato che sostanzialmente non vi sono rilevanti differenze rispetto a quanto previsto per i caratteri del consenso richiesti per l'art. 6, che di fatto si ripetono³⁷. Ovviamente anche in questo caso, in particolare nell'ipotesi di un elevato numero di interessati coinvolti, per i partiti politici dover ricorrere a tale base giuridica per il trattamento di questa particolare categoria di dati personali comporterà uno sforzo non indifferente in termini di predisposizione di adeguate informative, di raccolta e conservazione dei singoli e specifici consensi, ecc. Ne conseguirà che il ricorso a tale base giuridica da parte dei partiti sarà molto verosimilmente residuale.

Passando alla seconda eccezione di particolare interesse per i partiti politici sulla quale il Regolamento consente di fondare il trattamento di particolari categorie di dati³⁸, evitando di ricorrere al consenso, va rilevato che, affinché ciò sia possibile, si devono verificare tre condizioni: che il trattamento sia effettuato dai partiti politici nel corso delle loro legittime attività e con appropriate garanzie per gli interessati; che il trattamento sia relativo unicamente ai membri, agli ex membri o alle persone che hanno regolari contatti con il singolo Partito per le finalità di quest'ultimo; che i dati personali non siano comunicati all'esterno del Partito senza il consenso dell'interessato.

Ovviamente tale esimente riguarderà tutte le particolari categorie di dati ricomprese nell'art. 9 e non esclusivamente quella relativa all'orientamento politico. Quindi i partiti politici potranno trattare sulla base di questa base giuridica in assenza di consenso anche ulteriori categorie di dati personali quali ad esempio quelle legate alla salute, all'orientamento sessuale, ecc.

Con riferimento a quanto appena rilevato, va evidenziato quindi che ai partiti politici non sarà consentito trattare in assenza di esplicito consenso tali categorie di dati con riguardo a possibili sostenitori del singolo partito, o di interessati che hanno contatti occasionali con il partito (si pensi al riguardo ad una persona che *una tantum* decida di dare un modesto contributo

³⁶ Art. 9, c. 2 GDPR «a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1».

³⁷ Il consenso dovrà dunque essere libero, specifico, informato, ecc.

³⁸ Art. 9, c. 2 GDPR «d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato».

in denaro ad un partito politico per esempio), o ancora con riguardo ad elettori anche nel caso in cui il partito ritenga che siano simpatizzanti o lo abbiano votato³⁹. Così il ricorso a tale base giuridica presenterà un doppio limite: la portata soggettiva dei trattamenti di tali categorie di dati, che dovranno necessariamente riguardare solo gli interessati che hanno già contatti regolari con i partiti politici e non i terzi; ma anche l'ambito di applicazione oggettivo per cui tali dati possono essere trattati in assenza di consenso solo all'interno del partito e non da parte di soggetti terzi.

Venendo alla terza e ultima esimente relativa alle attività di trattamento di *particolari categorie* di dati di specifico interesse per i partiti politici, resta da analizzare il trattamento per *motivi di interesse pubblico rilevante*⁴⁰. Affinché si possa ricorrere a tale base giuridica però, così come visto anche per l'analogo comma 1 lett. e) dell'art. 6 del Regolamento, si dovrà valutare se l'interesse coinvolto sia un interesse pubblico rilevante o meno per l'ordinamento europeo o del singolo Stato membro. Inoltre dovrà essere rispettato un principio di proporzionalità nel bilanciamento tra gli interessi in gioco, nel rispetto dell'essenza del principio alla protezione dei dati personali e adottando misure specifiche per la tutela dei diritti e degli interessi degli interessati. Va però rilevato che l'art. 9 non prevede la possibilità in capo agli Stati membri di introdurre previsioni più specifiche per incidere sull'applicazione delle regole così riducendo i margini di flessibilità applicativa del Regolamento da parte di questi ultimi con riferimento a tali particolari categorie di dati⁴¹. Nonostante ciò, questa terza base giuridica può rappresentare per i partiti un'importante esimente per il trattamento di tali particolari categorie di dati. Infatti, a determinate condizioni essa consente alle associazioni partitiche di non dover richiedere il consenso agli interessati e quindi di aumentare notevolmente i propri margini operativi.

5. La tutela dei dati personali rappresenta un nuovo parametro per “il metodo democratico” dei partiti e nei partiti?

³⁹ Sul concetto di “regolarità” nei contatti si è espresso il Garante francese che ha fornito una serie di indicazioni a riguardo (es. non è sufficiente per rientrare in tale categoria mettere un *like* su di una pagina Facebook di un Partito politico). Su cui per approfondimenti cfr. CNIL, *Elections 2016/2017: quelles règles doivent respecter les candidats et partis?*, 08 novembre 2016, reperibile in www.cnil.fr/fr/elections-2016-2017-queelles-regles-doivent-respecter-les-candidats-et-partis.

⁴⁰ Art. 9, c. 2, GDPR «g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato».

⁴¹ Su cui per approfondimenti cfr. M. McDonagh, M. Donnelly, *Putting the Fox in Charge? Political Parties and the GDPR: An Irish Perspective*, in *European Public Law*, 26, n. 2/2020, 375 s.

Da quanto qui brevemente accennato si può iniziare a provare a trarre qualche prima breve considerazione sul tema.

Da una parte va rilevato che l'evoluzione delle nuove tecnologie ed i cambiamenti nel rapporto tra iscritti ai partiti politici ed elettori innescato dalle prime sta profondamente incidendo sulle dinamiche democratiche *nei* partiti che stanno sempre più accentrando i ruoli decisionali interni su sempre meno soggetti; e *dei* partiti, che stanno sempre più trasferendo le proprie tradizionali attività dalla realtà fisica a quella digitale. Tutto ciò rischia di influire negativamente sui livelli di democrazia interna ai partiti, ma anche di amplificare le ripercussioni sulle libertà fondamentali di coloro che vengono in contatto con i partiti politici a causa dei rischi di non conformità con il nuovo quadro normativo europeo in materia di tutela dei dati personali che necessariamente vengono sempre più impiegati nel ricorso proprio alle nuove tecnologie.

I partiti politici, anche alla luce delle particolari categorie di dati personali che possono trattare, potenzialmente rivelatori dell'orientamento politico di un numero rilevante di interessati, devono e dovranno sempre più gestire queste nuove problematiche alla luce dei profondi cambiamenti che si sono avuti nel quadro normativo di riferimento, in particolare con la piena entrata in vigore del Regolamento (UE) n. 679/ 2016 avutosi nel marzo 2018. Proprio in detto Regolamento vengono definite le basi giuridiche lecite per il corretto trattamento sia di "normali" categorie di dati personali (es. dati anagrafici, legati all'identità o alla residenza, ecc.), sia di quelle che sono state definite dal Regolamento come "particolari categorie" (es. dati identificativi dell'orientamento sessuale, religioso, dello stato di salute, ecc.) tra le quali appunto rientrano anche quelle rivelatrici dell'orientamento politico degli interessati.

Con riguardo proprio al trattamento delle *particolari categorie di dati*, come visto sopra, in particolare con riferimento a soggetti terzi rispetto ai partiti politici, sanciti all'articolo 9 del Regolamento va rilevato, in prima battuta, che difficilmente sono rinvenibili presupposti validi e applicabili nel coinvolgimento di dati personali di terzi da parte dei partiti politici che non siano il *consenso* dei soggetti con i quali di volta in volta i singoli partiti vengono in contatto dal momento, peraltro, che proprio l'articolo 9 non prevede alcun esonero contrattuale a riguardo. Si aggiunga a ciò, come visto, che per detta tipologia di dati non si può nemmeno ritenere applicabile il presupposto di liceità connesso al trattamento dei dati da parte di fondazioni, partiti politici o associazioni senza scopo di lucro con finalità politiche. Infatti, tali soggetti possono lecitamente trattare questa particolare categoria di dati ma limitatamente ai loro membri o a persone che hanno con essi regolari contatti, e peraltro solo all'interno dell'ambito politico/associativo, poiché per la divulgazione di tali dati all'esterno la norma richiede espressamente il consenso. A riguardo va evidenziato che non è un caso che proprio alla luce di detti presupposti il Garante per la

tutela dei dati personali sia intervenuto con provvedimenti specifici ad esempio proprio sul *webcrawling*, sulle attività di profilazione e sulle campagne di c.d. *micro-targeting*⁴².

Va però rilevato, alla luce dell'analisi condotta che, almeno con riguardo alle basi giuridiche per il trattamento dei dati personali, resta però in via indiretta in capo ai partiti politici (attraverso l'azione legislativa dei gruppi parlamentari) comunque un importante margine di intervento. Infatti, come visto, a determinate condizioni, i singoli Stati membri in base al Regolamento possono incidere legittimamente sui confini (in misura maggiore per le basi giuridiche di trattamento relative a categorie di dati personali c.d. "normali", e minore per le "particolari categorie" previste all'art. 9) entro i quali possono essere fatte valere basi giuridiche esimenti rispetto all'obbligo di richiesta del "consenso" nel trattamento dei dati personali di possibili elettori o soggetti comunque terzi rispetto ai partiti. Si noti, infatti, che, se da una parte è ovvio che il legislatore sostanzialmente è costituito dagli esponenti dei partiti politici eletti e quindi questi ultimi a livello nazionale ben possono incidere sulle scelte dei singoli legislatori dei Paesi membri europei incidendo in via estensiva sui confini dei trattamenti per i quali valgono le esimenti dalla richiesta del consenso⁴³; dall'altra è altrettanto vero che nell'esercitare tale potere il singolo legislatore nazionale dovrà sia tener conto di quanto previsto dal Regolamento stesso circa gli elementi minimi da includere in tali regolazioni in termini di definizione di tutta una serie di parametri richiesti dallo stesso Regolamento, sia richiedere il parere preventivo sulle normative in approvazione da parte delle singole Autorità garanti per la protezione dei dati personali nazionali che potranno ben vigilare e segnalare a livello europeo all'EDPB⁴⁴ eventuali abusi da parte dei singoli legislatori nazionali e quindi anche al legislatore europeo. Così sarebbe possibile in qualsiasi momento l'intervento immediato dell'EDPB, che con eventuali provvedimenti potrebbe esercitare un rilevante potere di conformazione materiale ad un unico indirizzo ermeneutico europeo; o, nei casi più gravi, quest'ultimo ben potrebbe sollecitare l'intervento direttamente del legislatore europeo al quale spetterà la decisione se emanare o meno modifiche di rango regolamentare.

Alla luce di quanto sopra dovrebbe risultare maggiormente evidente che sempre più, quindi, anche sul terreno della tutela della *privacy* e dei dati

⁴² Su cui per approfondimenti cfr. Garante per la protezione dei dati personali, *Provvedimento in materia di propaganda elettorale e comunicazione politica*, cit.

⁴³ Peraltro, ciò anche con possibili rilevanti distorsioni interne allo spazio eurounitario tra i singoli paesi membri.

⁴⁴ *European Data Protection Board* (Comitato europeo per la protezione dei dati) rappresenta l'organo europeo indipendente, che contribuisce all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione europea e promuove la cooperazione tra le autorità di controllo competenti per la protezione dei dati dell'UE. Il Comitato europeo per la protezione dei dati è composto dai rappresentanti delle autorità nazionali per la protezione dei dati (i Garanti *privacy*) e dal Garante europeo della protezione dei dati (GEPD).

personali *nei* partiti, e *dei* soggetti che vengono in contatto con i partiti, si gioca e si giocherà l'estrinsecazione materiale di quel "metodo democratico" previsto all'art. 49 Cost. it. la cui corretta applicazione risulta indispensabile per il fluire della vita dei cittadini e delle istituzioni nel rispetto dei principi costituzionalmente garantiti dall'ordinamento.

Gianluca Bellomo

Dipartimento di scienze giuridiche e sociali
Università degli studi "G. d'Annunzio" Chieti-Pescara
gianluca.bellomo@unich.it