SUDEUROPA

Quadrimestrale di civiltà e cultura europea

Seconda serie – Anno di fondazione 1978 | ISSN 2532-0297 | n. 1 gennaio/marzo 2022

1

Centro di documentazione europea
Istituto Superiore Europeo di Studi Politici
Rete dei CDE della Commissione europea

SUDEUROPA

Quadrimestrale di civiltà e cultura europea

Seconda serie – Anno di fondazione 1978 | ISSN 2532-0297 | n. 1 gennaio/marzo 2022

1

Centro di documentazione europea
Istituto Superiore Europeo di Studi Politici
Rete dei CDE della Commissione europea

Direzione, redazione e amministrazione di SUDEUROPA sono presso l'ISESP – Istituto superiore europeo di studi politici, proprietario della testata, Via Nino Bixio, 14 - 89127 Reggio Calabria; email cde@isesp.eu, sito internet www.isesp.eu

LARUFFA EDITORE
via dei Tre Mulini, 14
89124 Reggio Calabria
tel.: 0965.814954
www.laruffaeditore.it
segreteria@laruffaeditore.it

Registrato presso il Tribunale di Reggio Calabria, n. 7 del 10/11/2016
ISSN 2532-0297

La casa editrice Laruffa cura la stampa e la distribuzione
La rivista è pubblicata dal ***Centro di documentazione europea*** dell'ISESP
e fa parte delle pubblicazioni della rete CDE della Commissione europea.

Commissione europea

europe direct
Rete italiana dei CDE

SUDEUROPA viene realizzata anche con il contributo scientifico di

Dipartimento di Giurisprudenza, Economia e Scienze Umane

Centro di Ateneo per i Diritti umani Antonio Papisca

Università degli Studi di Padova

CRIOS. Center for Research Innovation Organization and Strategy

Università Commerciale Luigi Bocconi

LUISS Università Guido Carli

Sapienza Università di Roma
Cattedra Religion and Law

SOMMARIO

Social Media Targeting vs Consumer Data Protection? Le Linee-Guida EDPB n. 8/2020 (parte seconda)

*Angela Busacca**

Introduzione.

Il targeting costituisce oggi una componente essenziale di diversi modelli di business e viene utilizzato per individuare, a seguito delle operazioni di segmentazione della domanda, gruppi di utenti/consumatori ai quali proporre, sul web, contenuti in linea con le preferenze ed i gusti ed in grado di orientare le scelte di consumo di beni e servizi ma altresì le scelte in tema di informazione ed accesso alla conoscenza[1]. Proprio in considerazione della moltiplicazione delle offerte e delle possibilità di accesso presenti sul web, si è reso necessario, in termini di competitività sul mercato, poter disporre di informazioni e dati sulle preferenze dei gruppi di utenti/consumatori per ottimizzare le strategie di digital engagement[2] e modellare proposte di servizi, beni e contenuti in grado di attrarre l'utente/consumatore, ma altresì di fidelizzarlo. Attraverso le strategie di targeting, infatti, ai diversi gruppi-obiettivo vengono sottoposte offerte diversificate, in grado di soddisfare le differenti opzioni di consumo e di informazione, ed al contempo vengono predisposti meccanismi per orientate la scelta tra le opzioni proposte e fidelizzare l'utente/consumatore.

* *Università Mediterranea.*

[1] In argomento si segnala il recentissimo G. D'Ippolito, *Profilazione e pubblicità targettizzata on line. Real Time Bidding e behavioural adverstising*, Napoli, 2022.

[2] Il *digital engagement* rappresenta una delle più recenti modalità di strategia e pianificazione del marketing contemporaneo e prevede il coinvolgimento, sempre più progressivo, dell'utente/consumatore sui canali di comunicazione e vendita dell'operatore commerciale (o della comunicazione): informare, coinvolgere, profilare e convertire (in consumatore fidelizzato) sono i quattro livelli della strategia di digital engagement che possono essere utilizzate in tutti i campi: a titolo puramente esemplificativo si pensi alla vendita di beni e servizi collegati al settore sportivo, al fashion, all'agroalimentare, ai viaggi e turismo, fino alle esperienze digitali/virtuali (quali ad esempio il gaming di ruolo o le nuove attività nel metaverso). In argomento, cfr. C. Drummond, T. O'Toole, H. Mc Garth, *Digital engagement strategies and tactics in social media marketing*, in "European Journal of Marketing", 2020, p. 1247; I. Dodson, *L'arte del marketing digitale*, Ed. Apogeo, 2020.

Elemento essenziale delle attività di targeting sono i dati, personali e non personali, degli utenti/consumatori, considerati sia nella forma grezza che in quella (anche minimamente) strutturata: per una corretta classificazione dei diversi gruppi-obiettivo appaiono necessari indicatori ed informazioni che permettano di specificare al meglio i caratteri dei diversi gruppi e dei (correlati) diversi contenuti offerti. Su queste considerazioni non stupisce che la fonte privilegiata per acquisire i dati da trattare per finalità di targeting siano i social media ed in particolare i social network generalisti (quali, ad esempio, Facebook, Instagram e, più recentemente, TikTok e Telegram) che permettono la creazione di comunità di utenti e di reti di comunicazioni per la condivisione di informazioni e contenuti digitali. Da alcune recenti statistiche[3], risulta che siano attivi più di 4 miliardi di profili social media e che, particolarmente negli Stati membri UE, gli utenti attivi trascorrano (in media) più di tre ore al giorno dedicandosi ai social per motivi non professionali o lavorativi; quest'ultimo dato, peraltro, aumenta con riferimento agli utenti di età inferiore ai 18 anni, evidenziando così come proprio i minori siano i soggetti più esposti ai rischi delle attività di raccolta e trattamento dei dati, inclusa la profilazione, che possono essere realizzati attraverso i social media[4].

L'enorme massa di dati che quotidianamente circola sui social media è oggetto di diverse attività che dal semplice monitoraggio coinvolge poi più complessi strumenti di *web analysis* e trattamento dei dati, tra i quali anche il targeting, che interessano differenti tipologie di dati, fra i qua-

[3] Il riferimento è ai dati del report dell'agenzia "We are social" diffusi nel gennaio del 2022. L'intero report è liberamente consultabile all'indirizzo https://wearesocial.com/it/blog/2022/01/digital-2022-i-dati-globali .

[4] In argomento, cfr. I. Caggiano, *Protecting minors as technologically vulnerable persons through data protection: An analysis on the effectiveness of law,* in "European Journal of Privacy Law & Technologies" , 2022, p. 27; C. Perlingieri, *La tutela dei minori di età nei social networks*, in "Rassegna di diritto civile", 2016, p. 1324; A. Thiene, *L'inconsistente tutela dei minori nel mondo digitale*, in "Studium Iuris", 2012, p. 528. In tema di tutela dei minori, appare opportuno evidenziare come il Regolamento Europeo sui Servizi Digitali (Digital Services Act) attualmente in fase di discussione, preveda un regime molto stringente sulla pubblicità rivolta ai minori e sulle attività di profilazione dei dati dei minori per finalità pubblicitarie; nell'ottica di una maggiore responsabilizzazione delle piattaforme per la veicolazione dei contenuti e per le attività sui dati degli utenti, viene previsto un generale divieto di pubblicità mirata nel corso della navigazione dei minori ed un divieto di trattamento dei dati, realizzando così una tutela che trova le sue basi nel GDPR ma oltrepassa alcuni limiti del regolamento con riferimento ai profili di responsabilità degli operatori.

li soprattutto dati personali (come definiti dall'art. 4 GDPR) e categorie particolari di dati (come definiti dall'art.9 GDPR) per i quali risulta necessario assicurare una valida base giuridica e la tutela dei diritti degli interessati.

Nell'ambito dell'articolata strategia europea indirizzata alla costituzione di un completo quadro regolamentare in tema di circolazione, utilizzazione e tutela dei dati[5], le Linee-Guida dell'*European Data Protection Board* (EDPB) 8/2020[6] costituiscono attualmente il punto di riferimento per l'individuazione dei più opportuni standard di condotta per il trattamento dei dati e per la tutela degli interessati che siano titolari di pagine social[7] ed al contempo dei profili di responsabilità dei soggetti coinvolti nella realizzazione delle attività di targeting on social media.

[5] Al momento attuale sono in discussione diversi provvedimenti che, una volta emanati ed attuati all'interno della UE, permetteranno di avere un quadro regolamentare (tendenzialmente) completo, in grado di superare alcune incertezze e criticità interpretative del GDPR ed al lungo tempo trascorso dalla emanazione della Direttiva 2000/31 sui servizi della società dell'informazione, ed altresì in grado di rispondere al meglio alle esigenze di un mercato digitale sempre più attento alla dimensione economica ed al valore di scambio dei dati (personali e non personali) ed alle potenzialità legate al riutilizzo dei cd. open data. In particolare, il Regolamento n.2022/868 relativo alla governance europea dei dati (Data Governance Act), di recentissima adozione da parte del Parlamento EU, incoraggia alla condivisione ed alla circolazione dei dati pubblici ed alla possibilità di sfruttare il potenziale insito nel trattamento dei cd. Big Data anche mediante utilizzo di strumenti AI. La questione presenta molteplici profili di interesse che, tuttavia, esulano dall'economia delle presenti considerazioni; in argomento, nell'ambito di una vasta bibliografia, per una prima lettura del Regolamento, cfr. S. Tranquilli, *Il nuovo citoyen européen nell'epoca del Data Governance Act*, in "Rivista di Digital Politics", 2022, p. 179.

[6] Linee Guida 8/2020 sul targeting degli utenti dei social media; testo consultabile in lingua italiana all'indirizzo https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_it.

[7] Sul punto, appare opportuno specificare che esulano dall'ambito di operatività delle Linee-Guida tutte le questioni relative alle persone fisiche che non sono registrate sui social media e che, pertanto, non hanno un rapporto definito con il social media provider; per individuare gli appartenenti a questa ultima categoria, A titolo esemplificativo possono considerarsi coloro che hanno possibilità di accedere ai contenuti della rete social pur senza avere un account oppure coloro che interagiscono con il social attraverso altri siti/pagine web; anticipando quanto sarà poi oggetto di più approfondita considerazione nel paragrafo seguente, gli utenti "registrati" sono quelli che hanno un account/profilo per l'interazione e la condivisione dei contenuti con gli altri utenti del social media e che, a tal fine, hanno stipulato un contratto con il gestore del social media. Proprio in forza del contratto stipulato, utente e social media provider acquistano diritti ed obblighi correlati alla propria posizione contrattuale.

Ponendosi in linea di continuità con il precedente studio[8] dedicato all'ambito di applicazione, ai rischi delle attività di targeting rispetto ai diritti ed alle libertà degli interessati ed ai profili soggettivi degli autori dei trattamenti finalizzati al targeting, il presente lavoro si indirizza all'analisi degli ulteriori profili delle Linee-Guida 8/2020 in relazione alle tipologie di dati ricavati ed utilizzati per le attività di targeting on line, ai limiti di utilizzabilità dei dati (soprattutto se afferenti alle categorie particolari ex art.9 GDPR), agli obblighi dei titolari in ordine alle ipotesi di alto rischio nonché agli accordi tra titolari e/o contitolari ed ai conseguenti profili di responsabilità; in relazione a questo ultimo profilo, infatti, può osservarsi sin da subito come il ruolo di titolare/contitolare si rifletta sulla ripartizione di responsabilità tra social media provider e targeter ed in caso di contitolarità la determinazione delle responsabilità nei riguardi dell'applicazione del GDPR debba costituire oggetto dell'accordo con riferimento a tutti i trattamenti congiunti, dal momento che una previsione parziale o superficiale comporterebbe già una violazione dell'art.26 GDPR e, conseguentemente, una prima ipotesi di responsabilità a carico di entrambi. Proprio in considerazione dell'importanza di tale questione, le Linee-Guida si soffermano, particolarmente nell'ultima parte, sui profili di responsabilità, indicando alcune ipotesi di possibile illecito e suggerendo alcune buone prassi per evitare situazioni di criticità.

Circolazione dei dati sui social network sites e modelli di targeting

L'enorme flusso di dati che circola quotidianamente sui social network non ha una fonte univoca: non tutti i dati, infatti, sono volontariamente immessi dagli utilizzatori e "consegnati" consapevolmente alle attività di trattamento; la raccolta di dati avviene anche da attività di profilazio-

[8] *Social Media Targeting vs Consumer Data Protection? Le Linee-Guida EDPB n. 8/2020 (parte prima),* pubblicato in questa Rivista, fasc. 1-2/2021, p.87.

ne[9] realizzate analizzando le tracce di navigazione o attraverso la raccolta dei cookie[10]. Su queste considerazioni, l'EDPB ha indicato una classificazione delle differenti tipologie di dati che possono essere oggetto di targeting, secondo diverse modalità di raccolta e trattamento: dai dati inseriti direttamente tramite *form* ai dati raccolti in conseguenza dell'utilizzo di un servizio o di un dispositivo connesso od ancora a quelli derivati dal monitoraggio delle attività social dell'interessato. Accanto alla enunciazione delle regole applicabili, peraltro, l'EDPB ha altresì indicato una serie di esempi tratti dalla vita quotidiana (dall'uso di una app per acquistare cibo con consegna a domicilio alla consultazione di tabelle per

[9] L'attività di profilazione viene definita dall'art.4 comma 1 n.4 GDPR come "*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*". In relazione ai trattamenti automatizzati deve considerarsi anche l'art.22 GDPR, in tema di decisioni automatizzate e diritto di opposizione; in argomento è intervenuto anche il Gruppo di Lavoro art.29, emanando le Linee-Guida in materia di processi decisionali automatizzati e profilazione, adottate il 3 ottobre 2017, revisionate ed adottate il 6 febbraio 2018 (WP251rev01; testo italiano disponibile sub https://www.garanteprivacy.it/regolamentoue/profilazione). Nella dottrina italiana, nell'ambito di una vasta bibliografia sul tema, anche in considerazione dell'incidenza della profilazione sulla sfera della persona e sul grado di tutela dei dati personali, si segnalano, senza alcuna pretesa di completezza, V. Guggino – B. Banorri, *L'advertising ai tempi dell'Intelligenza Artificiale: algoritmi e marketing personalizzato,* in U. Ruffolo (a cura di) *Intelligenza artificiale, Il diritto, i diritti, l'etica*, Milano, 2020, p. 625 ss (ma spec. 630: *la profilazione in ambito digitale*); F. Lagioia, G. Sartor, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in "Federalismi.it", 11/2020, p. 85 ss; E. Pellecchia, *Privacy, decisione automatizzate e algoritmi*, in E. Tosi (a cura di) *Privacy digitale*, Milano, 2019, p. 417 ss; D. Messina, *Piattaforme "online", profilazione e intelligen za artificiale: nuove sfide per il GDPR e, in particolare, per il consenso dell'interessato informato e non ambiguo*, in "MediaLaws - Rivista di diritto dei media", 2019, p. 159 ss; F. Caia, *Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione,* in G. M. Riccio, G. Scorza, E. Belisario (a cura di) *GDPR e normativa privacy.Commentario*, Milano, 2018, p. 219 ss; O. Sesso Sarti, *Profilazione e trattamento dei dati personali*, in L. Califato – C. Colapietro (a cura di) *Innovazione tecnologica e valore della persona*, Napoli, 2017, p. 573.

[10] In argomento, anche in questo caso con mero valore indicativo e non esaustivo, G. Marino, *Internet e tutela dei dati personali: il consenso ai cookie*, in "Jus Civile" 2020, p. 398 ss; R. Cabazzi, *Utilizzo dei "cookie" e (nuova) tutela dell'utente interessato: la presa di posizione della Corte di giustizia nel caso "Planet49"* in "MediaLaws - Rivista di diritto dei media", 2020/2, pp. 316 ss; A. Mantelero, *Si rafforza la tutela dei dati personali: "data breach notification" e limiti alla profilazione mediante i "cookies"*, in "Il Diritto dell'informazione e dell'informatica", 2012, p. 781; C. Rossi Chauvenet, E. Stefanini, *Internet e privacy: il recepimento in Italia della Direttiva sulla "Cookie Law"*, in "Responsabilità civile e previdenza", 2012, p. 1806.

orari e prezzi di voli aerei[11]) evidenziando, nelle diverse ipotesi, le modalità di trattamento realizzate sui dati immessi dagli utenti/interessati nonché gli obblighi e le responsabilità dei titolari.
Seguendo quanto indicato dalle Linee-guida, possiamo individuare tre diverse macrocategorie di dati che possono essere oggetto di attività di targeting:

- "*provided data*" (dati forniti): cioè dati forniti direttamente (e con-

[11] La scelta di inserire una varietà di esempi tratti dalla vita quotidiana risulta particolarmente felice con riferimento all'analisi dei diversi meccanismi di targeting poiché permette un approccio immediato ed evidenzia la pluralità di questioni, dall'identificazione del titolare alla base giuridica di riferimento, al grado di tutela dei diritti dell'interessato ed alla possibilità di far valere pretese ed azioni nei confronti dei titolari/contitolari. Si è già detto che la finalità delle Linee-Guida è principalmente quella di fornire uno strumento agli operatori e proprio per questo, l'EDPB ha attinto alla casistica delle Corti e delle Autorità di controllo per individuare una serie di ipotesi da prendere in considerazione come esemplificative. Il primo degli esempi proposti (al paragrafo 41) ipotizza una attività di targeting per promuovere prodotti in saldo che venga realizzata sulla base di dati forniti dagli utenti attraverso la compilazione del form del profilo social e veicolata con messaggi postati in determinate fasce orarie di maggior condivisione; nel caso proposto, l'oggetto è costituito da dati forniti; social media provider e targeter assumono il ruolo di contitolari (poiché partecipano entrambi alla determinazione delle modalità e delle finalità del trattamento); la base giuridica sarà quella del consenso dell'interessato e del legittimo interesse del titolare (art. 6 lett.a e lett f GDPR) mentre non potrà invocarsi l'esecuzione del contratto (art.6 lett. b GDPR) né da parte del targeter né da parte del social media provider. L'esempio n.1 rappresenta la più semplice ed intuitiva ipotesi di dati forniti dall'interessato al social media provider in fase di compilazione del proprio profilo utente; altri esempi, come vedremo, prendono in considerazione le ipotesi di targeting realizzati sulla base di dati forniti dall'interessato al targeter o sulla base di dati osservati e di dati desunti.

sapevolmente) dall'utente al social media provider[12] od al targeter[13];

- "*observed data*" (dati osservati): cioè dati forniti dall'interessato in relazione all'utilizzo di un servizio o di un dispositivo mobile connesso (ad es. i servizi GPS, una recensione su di un sito web od ancora la condivisione di contenuti tra piattaforme diverse); in questo caso i dati possono essere raccolti dal provider o dal targeter attraverso social plug-in o pixel posti su siti esterni ma in grado di ricondurre

[12] Come può leggersi al paragrafo 41, *"le persone fisiche possono comunicare attivamente una quantità notevole di informazioni su se stesse quando utilizzano i social media"* ed a seconda della struttura e dell'architettura del social media, accanto ai dati quali nome, data di nascita, sesso e luogo di residenza, possono figurare anche informazioni quali lo stato civile e/o lo stato sentimentale, l'orientamento sessuale, gli interessi e la situazione lavorativa, le preferenze in ordine ad una serie di situazioni che spaziano dal tempo libero alle scelte di vita. Rinviando al paragrafo successivo per le questioni relative alle informazioni riconducibili alle categorie particolari di dati ex art.9 GDPR, appare opportuno evidenziare che l'utente che compila il proprio profilo social dovrebbe essere informato al meglio sulle privacy policies relative ai suoi dati per comprendere quali dati condividere (e quindi rendere conoscibili) e quali invece mantenere riservati. L'attività di targeting sui dati forniti direttamente dall'interessato al social media provider non può che trovare base giuridica nel consenso dell'interessato e, solo in via residuale, nell'interesse legittimo del titolare, secondo quanto stabilito dalla Corte Europea di Giustizia nella sentenza Fashion ID.

[13] Esempio tipico in argomento è il cd. targeting basato su elenchi, cioè l'ipotesi di attività che possono comportare dati forniti dall'interessato al targeter, che poi utilizzerà gli stessi per rivolgersi in maniera mirata all'interessato sui social media (in questi termini si esprime il paragrafo 60); i dati che l'interessato ha fornito al targeter vengono confrontati e strutturati con quelli già in possesso del social media provider, realizzando così una clusterizzazione che può meglio rispondere alle esigenze di comunicazione di entrambi i contitolari; a titolo esemplificativo, si consideri un elenco di indirizzi di posta elettronica raccolti da un operatore commerciale previa informazione (agli interessati) del possibile utilizzo degli stessi per finalità di marketing e della possibilità di fare opposizione a tale utilizzo. Anche in questo caso social media provider e targeter assumeranno i ruoli di contitolari solo nei limiti dei trattamenti per i quali agiranno in sinergia nel determinare finalità e mezzi e potranno utilizzare quale base giuridica principalmente il consenso dell'interessato; per provare l'interesse legittimo del titolare, infatti, dovrà aversi attenzione al contesto della raccolta dei dati ed al contesto dell'utilizzo degli stessi per l'attività di targeting.

all'account social[14];
•"*inferred data*" o "*derived data*" (dati desunti): cioè dati derivati che vengono creati dal titolare sulla base dei dati forniti e dall'osservazione del comportamento e dalla navigazione social degli interessati[15].

L'eterogeneità delle fonti di raccolta e della tipologia di dati evidenzia come le attività di targeting non possano basarsi tutte unicamente sul consenso dell'interessato, dal momento che, particolarmente per l'ultima categoria, siamo in presenza di trattamenti che avvengono all'insaputa dell'interessato e, talvolta, anche del primo titolare (che ha raccolto

[14] In particolare, il sito web del targeter può incorporare dei pixel di tracciamento (definiti dalle stesse LineeGuida come "piccoli frammenti di codice" che viene scaricato, previa autorizzazione, sul browser dell'utente/consumatore, permettendo così il monitoraggio della sessione di navigazione); diversamente, i plug-in social permettono il collegamento dal quale poter attingere i dati. In tutti questi casi è essenziale il livello di informazione e di trasparenza che il targeter ed il social media provider devono garantire: l'utente deve ricevere una informativa sulla presenza e sulle (possibili) conseguenze dell'utilizzo dei plug-in social e la semplice presenza di un banner non implica accettazione se non in conseguenza della pressione del tasto di accettazione. La finalità di marketing deve essere manifesta ed inequivocabile ed in assenza di un consenso da parte dell'interessato, le attività di raccolta e trattamento dei dati derivati saranno considerate illecite (per violazione del principio di finalità del trattamento) con responsabilità del targeter e del social media provider, considerati contitolari. L'utilizzo dei pixel di tracciamento, peraltro, può permettere altresì di impostare dei cookies e questo determina il richiamo alla normativa in materia, con particolare riferimento alla Direttiva 2002/58/EU (cd. direttiva e-privacy) in combinato con il GDPR; a titolo esemplificativo si consideri che in presenza di dispositivi di tracciamento, il consenso deve essere manifesto e libero ed essere manifestato come richiesto dall'art.7 GDPR con modalità opt-in e non con modalità opt-out su impostazione di accettazione predefinita.

[15] I dati desunti rappresentano, per certi versi, delle informazioni (nel senso di dati più strutturati) create dal titolare combinando categorie di dati forniti e di dati osservati: si pensi alle interazioni social con pagine tematiche ed alle preferenze espresse in fase di compilazione della propria pagina social od ancora all'utilizzo di applicazioni sui dispositivi mobili in combinato alle preferenze di navigazione od alle impostazioni su un dispositivo utilizzato sia per attività lavorative che per attività nel tempo libero. Social media provider e targeter sono entrambi titolari e chiamati a rispondere in caso di comportamenti illeciti nel trattamento dei dati. Si tratta della categoria che comporta le maggiori criticità, soprattutto perché implica, come peraltro indicato nel prosieguo del testo, una attività di profilazione e quindi risulta essere il risultato di una attività di trattamento finalizzata ad una ulteriore attività di trattamento.

il consenso al trattamento[16]).

I dati desunti sono, infatti, il risultato delle attività di trattamento del titolare (o dei contitolari), principalmente attività di profilazione, che possono avere la propria base sia nei dati forniti che nei dati osservati; il targeting sui dati desunti è l'attività che non solo pone le maggiori criticità in ordine alla tutela degli interessati ma, da ottica, differente, è quella che ripone maggiore affidamento sulla qualità dei dati di input e potrebbe restituire risultati falsati in presenza di erronee analisi su questi ultimi. Il richiamo alla profilazione rende opportuno, secondo quanto indicato dall'EDPB, il rinvio alla disciplina dell'art.22 GDPR[17] ed alle

[16] Al riguardo viene in considerazione quanto indicato al paragrafo 76, laddove si prevede che: *"il consenso che dovrebbe essere raccolto dal gestore del sito web per la trasmissione di dati personali attivata dal suo sito web (integrando un plug-in sociale) si riferisce soltanto all'operazione o all'insieme di operazioni che comportano il trattamento di dati personali per le quali il gestore determina effettivamente le finalità e i mezzi"*, sicché anche in presenza di consenso raccolto dal titolare del sito e poi trasmesso, tramite plug-in ad un social network, il social media provider deve *"assicurarsi che l'interessato abbia fornito un consenso valido per il trattamento di cui è responsabile in qualità di contitolare, nonché per qualsiasi trattamento successivo o ulteriore effettuato da tale fornitore e per il quale il gestore del sito web non determina congiuntamente le finalità e i mezzi (ad esempio operazioni successive di profilazione per finalità di targeting)"*. In tema di trasferimento dei dati e trattamenti da parte di titolari successivi, la dottrina ha evidenziato le criticità di una regolamentazione eccessivamente stringente, che potrebbe portare a limitazioni delle attività economiche ed ha suggerito la possibilità di rendere ammissibili i trattamenti in presenza di finalità "non incongruente" (in questo senso cfr. P. F. Giuggioli, *Tutela della privacy e consumatore*, in E. Tosi (a cura di), *Privacy digitale*, cit., p. 263 ed altresì G. De Gregorio, R. Torino, *Privacy, protezione dei dati personali e Big data*, *ivi*, p. 447).

[17] L'art.22 GDPR è espressamente richiamato al paragrafo 85, laddove viene evidenziato come nel caso di un processo decisionale automatizzato che produca effetti giuridici nella sfera dell'interessato o che incida significativamente sulla sua persona, i titolari del trattamento possono avvalersi di alcune eccezioni, quali il consenso esplicito dell'interessato, la necessità del processo decisionale automatizzato ai fini della stipula o dell'esecuzione di un contratto e, da ultimo, l'autorizzazione conferita dal diritto dello Stato membro cui è soggetto il titolare del trattamento. In relazione all'art. 22 GDPR, nell'ambito di una vasta dottrina, possono richiamarsi: E. Falletti, *Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche*, in "Il diritto dell'informazione e dell'informatica", 2020, p. 169; E. Pellecchia, *Privacy, decisioni automatizzate ed algoritmi*, in E. Tosi (a cura di), *Privacy digitale, cit*., p. 417; R. Messinetti, *La tutela della persona umana "versus" l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in "Contratto e Impresa", 2019, p. 861.

Linee-Guida WP29 sul processo decisionale automatizzato[18], soprattutto al fine della determinazione della soglia di "significativa incidenza" dei processi decisionali automatizzati sulla sfera personale dell'interessato ed alla, possibile, conseguente "significativa incidenza" del targeting realizzato sulla base di tali processi[19].

Accanto al consenso, pertanto, devono individuarsi gli altri criteri di liceità e basi giuridiche del trattamento: EDPB fa riferimento agli artt. 5 e 6 del GDPR ed in particolar modo all'interesse legittimo del titolare (art. 6 lett f). Sul punto, peraltro, l'EDPB manifesta una serie di preoccupazioni in ordine alla possibile mancanza di trasparenza e di controllo/conoscenza da parte degli utenti nonché alla possibilità di utilizzi imprevisti o non desiderati dei dati personali che possono comportare dei pericoli per i diritti e le libertà degli interessati; viene evidenziato altresì come sarebbe bene che le diverse attività di trattamento poste in essere con finalità di targeting avessero le stesse basi giuridiche dal momento che, sebbene non vi sia un esplicito divieto di far riferimento a basi giuridiche diverse, tuttavia la frammentazione sarebbe negativa per gli interessati che avrebbero maggiori difficoltà a far valere i propri diritti.

In relazione al quadro normativo di riferimento, il richiamo alle disposizioni del GDPR viene considerato come prioritario: non solo per le norme relative al consenso ed alla base giuridica del trattamento, ma altresì per quelle relative ai criteri di liceità (delle attività di trattamento) ed alla ripartizione delle responsabilità tra i diversi soggetti che interagiscono nelle attività di targeting ed assumono il ruolo di titolari. In riferi-

[18] Gruppo di lavoro, Art. 29 Linee-Guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, WP 251 rev. 01; il testo è consultabile all'indirizzo: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_it.

[19] Richiamando quanto affermato nelle Linee-Guida sul processo decisionale automatizzato, il WP29 ha evidenziato come, sebbene in numerosi casi non si possa parlare di "significativa incidenza", tuttavia possono presentarsi casi di incidenza, tra i quali: l'invasività del processo di profilazione, compreso il tracciamento delle persone su siti web, dispositivi e servizi diversi; le aspettative e le volontà delle persone interessate; il modo in cui viene reso disponibile l'annuncio pubblicitario; lo sfruttamento della conoscenza di vulnerabilità degli interessati coinvolti. Sulla base di queste considerazioni, nelle Linee-Guida 8/2020, al paragrafo 87, si prevede che: *"il titolare del trattamento (o i contitolari del trattamento, a seconda del caso) dovrà (dovranno) effettuare una valutazione dell'eventualità che il targeting "[incida] in modo analogo significativamente" su un interessato, in ogni caso tenendo conto delle caratteristiche concrete del targeting"*. Alla valutazione di impatto preventiva ed ai correlati obblighi, come previsti dal GDPR, è dedicato il successivo paragrafo 7.

mento ai criteri di liceità, particolare attenzione deve essere prestata alla finalità della raccolta, dal momento che gli scopi devono essere specifici, espliciti e legittimi e l'informativa dovrà essere completa (indicando le diverse tipologie di trattamento) ed espressa con linguaggio chiaro e comprensibile per gli interessati; a titolo di esempio, viene indicato come la semplice parola "advertising" non possa considerarsi comprensiva delle attività di targeting, dal momento che le attività di promozione e pubblicità generiche sono ben diverse dall'attività di trattamento finalizzata alla definizione dei gruppi target.

La divisione tra "dati forniti" "dati osservati" e "dati derivati" si riferisce alle fonti della raccolta, ed alla presenza, o meno, di un valido consenso espresso dall'interessato; tuttavia, sottesa ad essa deve considerarsi la basilare divisione tra dati personali (art. 4 GDPR) e categorie particolari di dati (art.9 GDPR), dal momento che per questi ultimi è necessario avere come base giuridica il consenso dell'interessato, come previsto dall'art.9 comma 2.

Trattamenti su categorie particolari di dati

L'EDPB dedica particolare attenzione alle ipotesi di targeting realizzato sulla base del trattamento dei dati appartenenti alle categorie particolari previste dall'art.9 del GDPR[20], cioè tutti quei dati personali "*che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*", comunemente indicati come "dati sensibili", secondo la terminologia della direttiva 96/45/CE e del nostrano d.lgs.196/2003. Le categorie particolari di dati personali, proprio per la loro afferenza (ed inferenza) con la sfera più intima della persona, ricevono dal legislatore europeo una partico-

[20] Sulle categorie particolari di dati contemplate dall'art.9 DGPR, nell'ambito di una vasta letteratura, cfr. G. Druetta, J. Purificati, *Art.9 – Trattamento di categorie particolari di dati personali* in G.M. Riccio, G. Scorza, E. Belisario, *GDPR e normativa privacy. Commentario*, cit., p. 111; A. Thiene, *Art.9 – Trattamento di categorie particolari di dati personali*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta, *Codice della Privacy e Data Protection*, Milano, 2021; M. Granieri, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, in NGCC, 2017, p. 166; si consentito altresì il rinvio a A. Busacca, *Le "categorie particolari di dati" ex art. 9 GDPR. Divieti, eccezioni e limiti alle attività di trattamento*, in "OIDU - Ordine Internazionale e Diritti Umani", 2018, p.36.

lare tutela che prevede un generale divieto di trattamento (art.9 par.1)[21] ed una serie di ipotesi eccezionali (art.9 par.2)[22], in presenza delle quali il trattamento può essere posto in essere, sempre nel rispetto dei generali principi indicati dall'art.5 GDPR[23]. Ancora, la presenza di categorie

[21] Il comma 1 prevede un generale divieto di trattamento per le cd. "categorie particolari di dati" individuati come quei dati che *"rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona"*; con questa scelta si realizza un rafforzamento ed una sorta di stratificazione della tutela dei dati dell'interessato, per i quali vengono, appunto, posti diversi livelli di tutela, anche e soprattutto in considerazione della diversa afferenza alla sfera sanitaria, esistenziale e relazionale del soggetto.

[22] Il comma 2 indica una serie di ipotesi nelle quali il divieto generale previsto al comma 1 non trova applicazione; riprendendo la classificazione già proposta (in *Le "categorie particolari di dati" ex art. 9 GDPR. Divieti, eccezioni e limiti alle attività di trattamento, cit.*, p.48) le ipotesi indicate possono dividersi in tre macro-categorie collegate all'interesse per la realizzazione/tutela del quale le attività di trattamento vengono consentite: interessi individuali del soggetto interessato (presenza di un valido consenso al trattamento, dati resi manifestamente pubblici e interessi vitali in ipotesi di interessato impossibilitato ad esprimere il proprio consenso) interessi del titolare e dell'interessato (trattamento necessario per "assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale" o trattamento effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali con il duplice limite dell'agire per finalità proprie ed offrendo idonee garanzie ed ancora con il limite di trattamenti che riguardino soggetti che abbiano od abbiano avuto rapporti con l'ente), e, da ultimo, interessi generali della collettività (attività collegate all'amministrazione della giustizia, esistenza di un interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, comunque nel rispetto dei principi di finalità e non eccedenza; attività svolte a fini "di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici"; tutela di interessi correlati alla tutela della salute, sia in dimensione individuale che collettiva, anche come prevenzione per il rischio di epidemie o diffusione di nuove patologie; finalità di archivio per interessi di ricerca scientifica o storica o per statistiche, nel rispetto dei principi di proporzionalità e finalità e con misure appropriate e specifiche per tutelare i diritti fondamentali).

[23] Al riguardo, come afferma M. Granieri (*Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679, cit.*, p. 166): " le categorie particolari di dati si inseriscono nel quadro complessivo di una disciplina che cerca al meglio di conciliare la tutela della persona fisica, riguardo alle informazioni sensibili che la riguardano, con l'esigenza che siano poste in essere attività rilevanti a livello economico e non (molte delle quali tipiche dello stato sociale e, dunque, rivolte a beneficio degli stessi cittadini dei cui dati si tratta), talora incidenti sulla ricerca scientifica, sulle prestazioni sanitarie e previdenziali, nonché su altre libertà fondamentali di chi svolge il trattamento".

particolari di dati risulta elemento pertinente ai fini della valutazione sulla opportunità della valutazione di impatto preventiva (come prevista dall'art.35 GDPR) nonché della nomina di una *data protection officer* (come previsto dall'art.37 GDPR) ed è determinante per la valutazione di adeguatezza delle "misure appropriate" di sicurezza (previste dagli artt. 24, 25, 28 e 35 GDPR).

Nelle ipotesi di social media targeting che sia basato su categorie particolari di dati appare di primaria importanza verificare non soltanto chi, tra social media provider e targeter (o entrambi) ricopra il ruolo di titolare, ma altresì quale sia la base giuridica che legittima il trattamento e che deve potersi ricondurre ad una delle ipotesi dell'art.9 pr.2 GDPR per superare il generale divieto posto dall'art.9 par.1.

In relazione ai dati circolanti sui social network che costituiscono la base sulla quale viene strutturata l'attività di targeting e di comunicazione, assumono rilevanza principalmente il consenso dell'interessato e l'ipotesi che il dato sia stato reso manifestamente pubblico dallo stesso interessato; proprio quest'ultima ipotesi, tuttavia, pur nell'apparente semplicità della formulazione, costituisce una delle maggiori criticità interpretative, soprattutto se rapportata all'ambiente complesso dei social media. L'espressione "manifestamente" sottesa alla consapevolezza, da parte dell'interessato, di rendere pubblici i propri dati personali deve essere interpretata come consapevolezza di rendere i dati personali disponibili e quindi conoscibili ad una platea potenzialmente sconfinata di altri utenti tra i quali anche istituzioni, pubbliche amministrazioni e autorità: in questo senso si è espresso il Gruppo di Lavoro Art.29 nel parere reso nel 2017 in relazione ad alcune questioni interpretative sulla direttiva 2016/680/UE[24], chiarendo altresì che nei casi dubbi, debba prevalere, proprio in regione della tutela della persona, una interpretazione restrittiva.

Le Linee-Guida indicano, sul punto, la necessità di una analisi casistica, evidenziando come l'attività di immissione dei propri dati personali sulle pagine dei social media non possa univocamente interpretarsi come consapevolezza della potenziale divulgazione indiscriminata; peraltro i dati afferenti alle categorie particolari ex art.9 possono essere inseriti sia nella compilazione del "profilo" oppure essere contenuto di post e/o contenuti multimediali postati sulla bacheca/diario ed aperti, a seconda delle impostazioni privacy, alla visione e condivisione da parte di altri utenti secondo il meccanismo di collegamento delle pagine social.

[24] Working Paper 258 del 29.11.2017, p.11, richiamato dalle Linee-Guida, p.40 nt.104

Ne deriva che, ai fini della consapevolezza sulla maggiore o minore potenzialità di circolazione dei dati assumono rilievo diverse circostanze, tra le quali la struttura e le impostazioni predefinite della piattaforma social, l'accessibilità delle pagine e delle sezioni nelle quali sono rinvenibili i dati personali "particolari", la presenza di adeguati strumenti informativi sulla pubblicità ed accessibilità dei dati personali "particolari". Proprio in considerazione della pluralità di circostanze da considerare, l'EDPB indica una serie di elementi che vengono indicati come "pertinenti" ai fini della riconducibilità del dato personale ex art.9 par.1 GDPR alla categoria dei dati personali resi manifestamente pubblici e quindi oggetto di trattamento lecito ex art.9 par.2 lett.e GDPR, specificando tuttavia che non è sufficiente la presenza di uno solo degli elementi ma deve aversi la concorrenza di più elementi per escludere ogni profilo di responsabilità per i titolari/contitolari del trattamento. Gli elementi indicati sono: le impostazioni predefinite della piattaforma di social media[25]; la natura della piattaforma di social media[26]; l'accessibilità della pagina dove sono reperibili i dati appartenenti alle categorie particolari[27]; la visibilità dell'informazione relativa alla natura pubblica dei post e dei contenuti immessi sulla piattaforma[28]; la circostanza che i dati siano stati immessi dallo stesso interessato o piuttosto da un soggetto terzo o, ancora, siano dati

[25] In particolare, il riferimento è alla presenza di impostazioni predefinite sulle quali l'interessato sia intervenuto modificando, ad esempio, le impostazioni "private" in impostazioni "pubbliche". In questo caso, la condotta dell'interessato, pur non riferita espressamente ai dati personali appartenenti alle categorie ex art.9, acquista, tuttavia, valore generale.

[26] Le diverse finalità delle piattaforme di social media si riflettono sul grado di condivisibilità e pubblicità delle informazioni: si considerino, al riguardo, un social media professionale come Linkedin o una piattaforma di incontri finalizzata alla creazione di relazioni intime od ancora una piattaforma di microblogging o un social generalista quale Instagram o Facebook.

[27] Il riferimento è alla libera accessibilità, ad es. attraverso motori di ricerca, od alla necessaria (preventiva) iscrizione al social network per poter visualizzare e condividere i contenuti.

[28] In particolare, il riferimento è alla presenza di banner o altra segnalazione che permetta all'interessato di avere cognizione della diffusione e dell'accessibilità del contenuto che sta immettendo in piattaforma; tra le altre modalità di segnalazione, può indicarsi anche la presenza di informazioni collegate al click di pubblicazione, sul modello delle cd. *button solution* adottate nell'ambito della legislazione consumeristica europea per tutelare i consumatori dalla presenza di costi occulti.

desunti[29]. Particolarmente interessante, sul punto, è l'esempio proposto dalle Linee-Guida: si immagina un soggetto che, nell'aprire un account su di una piattaforma social di micro-blogging, abbia compilato i dati relativi al profilo (con impostazione predefinita in modalità "privata" non modificata) indicando anche il proprio orientamento sessuale e che, informato della pubblicità dei messaggi scambiati sulla piattaforma, abbia iniziato a seguire e scambiare messaggi con gruppi di orientamento politico conservatore. La questione sottesa riguarda la liceità di una attività di targeting svolta per conto di un partito politico conservatore che intenda rivolgersi a soggetti con il medesimo orientamento sessuale e la risposta dell'EDPB è in senso negativo, dal momento che sebbene sia presente l'elemento della informazione sulla pubblicità dei post e dello scambio di messaggi tramite il social media, non possono dirsi "resi manifestamente pubblici dall'interessato" né l'appartenenza politica (di fatto, ha solo scambiato messaggi e partecipato a forum di discussione con orientamento politico, ma non ha dichiarato una appartenenza né una affiliazione politica), né l'orientamento sessuale (dal momento che i dati del profilo mantengono impostazione privata, non essendo intervenuta alcuna attività di modificazione da parte dello stesso interessato). Dall'esempio illustrato appare chiaro come targeter e social media provider, che rivestono il ruolo di contitolari del trattamento, debbano valutare tutte le circostanze del caso e non possono procedere ad attività di raccolta e trattamento in assenza di una valida (e comprovata) base giuridica.

Si è detto che tra gli elementi rilevanti ai fini della valutazione sulla liceità della base giuridica per effettuale il trattamento dei dati "resi manifestamente pubblici dall'interessato" viene annoverata anche l'ipotesi che i dati siano "desunti" cioè dati che appartengono alle categorie particolari ex art.9GDPR ma che l'interessato non fornisce direttamente ma vengono ricavati dal titolare sulla base dei dati forniti e dei dati osservati.

In considerazione della enorme mole di dati che circola sui social media e che costituisce oggetto di trattamenti, tra i quali principalmente

[29] Quest'ultimo elemento riguarda le ipotesi di contenuti immessi da terzi che tuttavia permettano di trarre dati personali afferenti alle categorie ex art.9 GDPR: si pensi ad una foto durante un rito religioso privato od ancora durante una riunione politica privata od ancora presso una struttura sanitaria per la cura di determinate dipendenze. In tutti questi casi, così come anche nell'ipotesi di dati desunti, il trattamento non potrà considerarsi lecito dal momento che, a meno che non si dimostri l'esistenza di un consenso dell'interessato (quindi la circostanza ex art.9 per.2 lett a GDPR), non può ravvisarsi alcuno stato di consapevolezza da parte dell'interessato.

trattamenti automatizzati e profilazione, è ben possibile che vengano creati cluster di targeting sulla base di categorie particolari di dati risultanti dal trattamento di dati personali non appartenenti, in origine, alle categorie particolari ex art.9 GDPR.

Viene, cioè, a realizzarsi una sequenza di dati che, dalla raccolta dei dati personali non riferibili alle categorie particolari può portare a dati derivati che, invece, sono riferibili a tali categorie e, pertanto, ripropongono le limitazioni di trattamento dell'art.9 par.1 GDPR; a titolo esemplificativo, si considerino i dati relativi alla geo-localizzazione dell'interessato presso la sede di un determinato movimento/partito politico o alla raccolta dei suoi like espressi in relazione a post di una data congrega religiosa od ancora alla raccolta dei cookie di navigazione ed alla cronologia delle visite su siti che individuano un determinato stile alimentare come espressione di un credo filosofico: i dati in questione non possono riferirsi all'art.9 GDPR, tuttavia il social media provider potrebbe, nell'ambito dell'attività di profilazione, incrociare/strutturare gli stessi con altri dati, desumendone altri dati appartenenti alle categorie particolari, quali, ad es., le convinzioni politiche, religiose e filosofiche. Il dato emergente dall'attività di trattamento, peraltro, potrebbe essere non rispondente alla realtà, dal momento che l'agente software preposto all'attività di profilazione (o comunque al trattamento automatizzato) potrebbe giungere ad un risultato di clusterizzazione erroneo[30]. Su questo aspetto, tuttavia, le Linee-Guida EDPB evidenziano come, in ogni caso, il profilo di illiceità rilevante si appunti principalmente sul trattamento dei dati personali riconducibili alle categorie ex art.9 GDPR, tralasciando di soffermarsi sulla veridicità o meno del dato desunto (e sul conseguente pregiudizio ai diritti dell'interessato). Da ultimo, in relazione al profilo delle responsabilità, appare opportuno evidenziare che social media provider e targeter possono rivestire il ruolo di contitolari del trattamento quando entrambi si trovino ad operare sui dati

[30] Riprendendo quanto proposto come esempio: l'interessato frequenta abitualmente i locali di un movimento/partito politico, acquista on line una serie di testi sulla storia del partito e sulle dottrine politiche ad esso riconducibili, ordina on line la stampa di foto di manifestazioni del movimento/partito in questione: sono elementi dai quali potrebbe ricavarsi l'appartenenza dell'interessato al movimento/partito politico. Tuttavia, tale risultato, in assenza di una affiliazione espressa o di dichiarazioni univoche, potrebbe non corrispondere alla realtà e quindi determinare non soltanto un trattamento di dati personali riferibili all'art.9 e quindi vietato, ma altresì un trattamento che determina un travisamento dell'identità dell'interessato. In questo caso vengono in considerazione gli ulteriori profili della affidabilità e della qualità del dato e delle interpretazioni dello stesso: tutti elementi che possono alterare la validità del trattamento e del risultato.

desunti; diversamente, quando le attività di trattamento che portano alla creazione dei dati desunti ed al successivo utilizzo degli stessi siano poste in essere solo dal targeter, ugualmente solo a questi dovranno riferirsi ruolo e responsabilità di titolare, dal momento che il social media provider non potrà essere chiamato a rispondere di attività non poste in essere (e delle quali potrebbe anche ignorare l'esistenza). Sul punto l'EDPB afferma efficacemente come la sola circostanza di trattare grosse quantità di dati personali, dai quali possono poi desumersi categorie particolari di dati, non implica automaticamente il trattamento delle categorie particolari di dati; l'applicazione dell'art.9 GDPR, infatti, viene espressamente esclusa *"se il trattamento da parte del socia media provider non comporta inferenze su categorie particolari di dati e se il social media provider ha adottato misure per evitare che dati inferenze siano possibili o che i dati appartenenti a tali categorie siano utilizzati per il targeting"*.

"Rischio elevato" sulla protezione dei dati ed obbligo della valutazione di impatto preventiva sulla protezione dei dati

Tra gli obblighi che le Linee-Guida 8/2020 pongono a carico dei contitolari del trattamento possono ricondursi anche quelli relativi alla valutazione di impatto preventiva sulla protezione dei dati (DPIA)[31] per tutti

[31] La valutazione di impatto preventiva è uno strumento di analisi del rischio in base al quale è possibile, per il titolare, evidenziare l'indice di rischio delle diverse tipologie di trattamento ed adottare le più adeguate misure tecniche ed organizzative (per eliminare/ridurre i rischi) calibrando le stesse sui diversi trattamenti posti in essere. Costituisce uno dei principali adempimenti inquadrabili nel principio di accountability del titolare e, come indicato dal Gruppo di Lavoro art.29 (WP29), rappresenta uno "*strumento importante per la responsabilizzazione in quanto sostiene i titolari del trattamento non soltanto nel rispettare i requisiti del Regolamento (...) ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del Regolamento*" (in questi termini WP29, Linee-Guida in materia di valutazione di impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del Regolamento (UE) 2016/679 (WP248); il testo completo può leggersi sub http://www.interlex.it/2testi/autorit/wp248dpia.pdf). In argomento cfr. G. Giannone Codiglione, *Risk-based approach e trattamento dei dati personali*, in S. Sica, V. D'Antonio, G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Padova, 2016, p. 55 ss. (spec. p.70 ss.); A. Mantelero, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (Artt. 32-39)*, in Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 307; L. Tarullo, *La gestione del rischio nel trattamento dei dati personali*, in F. Di Resta (a cura di), *La nuova "privacy europea". I principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, Torino, 2018, p. 113 s. (spec. p. 125 s.); presenta un approccio più pratico, R. Rapicavoli, *Come applicare il GDPR negli studi e nelle aziende*, Rimini, 2018, p.77 s.

quei trattamenti di dati personali che risultano funzionali all'attività di targeting e che possono presentare un grado di "rischio elevato per i diritti e le libertà delle persone fisiche"[32]. In argomento, gli indici normativi di riferimento sono dati dall'art.35 e dai Considerando nn.71,75 e 91 del GDPR[33], ai quali è opportuno affiancare, in un'ottica di sistema, le Linee-Guida del WP29 "in materia di valutazione di impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del regolamento n.679/2016"[34], adot-

[32] In questi termini l'art.35 comma 1 GDPR: *"quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali"*; sul punto, è stato osservato in dottrina come l'espressione appaia indeterminata, potendo creare una serie di problemi soprattutto in considerazione della eterogeneità dei rischi e delle scale e metodologie di valutazione che possono essere utilizzate: possono allora ipotizzarsi, quali trattamenti suscettibili di determinare un rischio elevato quelli che "verosimilmente possono determinare conseguenze negative significative per l'interessato, nel suo esercizio e godimento delle libertà e diritti fondamentali, quali discriminazioni, furto o usurpazione d'identità, perdita finanziaria, pregiudizio alla reputazione, decifratura non autorizzata dalla pseudonimizzazione" e, in linea generale, tutti quelli che hanno un indice elevato di rischio "insito" nel trattamento stesso (in questi termini, F. Cecamore, *Art.35 – Valutazione di impatto sulla protezione dei dati*, in G.M. Riccio, G. Scorza, E. Belisario, *GDPR e normativa privacy. Commentario*, *cit*., p. 408)

[33] Nell'ambito dell'ampia bibliografia sull'art.35 GDPR, cfr. il recentissimo A. Mantelero, *Art.35 - Valutazione di impatto sulla protezione dei dati*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta, *Codice della privacy e data protection*, *cit*., p. 530 ss.; proprio con riferimento ai Considerando ed alle Linee-Guida WP 248 del WP29, l'autore evidenzia il ruolo che "la gravità del rischio" riveste in uno schema graduale e progressivo quale quello proposto dal GDPR, sottolineando come il Considerando n.75 identifichi ben sei criteri da utilizzare per la valutazione dei rischi ai diritti ed alle libertà degli interessati, spaziando dalla natura dei dati trattati alla specifica finalità dei trattamenti fino alle condizioni personali dell'interessato: ne deriva che, proprio per la delicatezza del tema e delle implicazioni, "la valutazione delle potenziali conseguenze negative non riguarda solo le ipotesi di rischio elevato in cui (...) è richiesta una valutazione formalizzata di impatto, bensì costituisce un modus operandi generalizzato" (p.538)

[34] WP29, Linee-Guida in materia di valutazione di impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del Regolamento (UE) 2016/679 (WP248), cit sub. nt.1. Il documento del Gruppo di Lavoro art.29, nella versione aggiornata ed emendata del 4 ottobre 2017, è stato approvato dal Comitato Europeo per la Protezione dei Dati (EDPB) nella prima riunione plenaria del 2018. Sul contenuto delle Linee-Guida ed in particolare sulle ipotesi di esenzione dall'obbligo della DPIA, cfr. F. Bravo, *La nuova "privacy europea"*, *cit*., p. 131.

tate, nella versione aggiornata e modificata, del mese di ottobre 2017. Prima di procedere all'analisi dei paragrafi 105-112, relativi alla DPIA per le attività di targeting, tuttavia, appaiono opportune alcune brevissime considerazioni di carattere generale sulla DPIA, come prevista dal GDPR. La DPIA rappresenta una significativa innovazione del GDPR, contribuendo a rappresentare "la più recente fase evolutiva" del modello europeo in materia di trattamento dei dati[35], e si pone come un rinnovato modello di analisi del rischio i cui elementi basilari sono indicati dall'art.35 comma 7 GDPR (descrizione sistematica dei trattamenti, valutazione della necessità e proporzionalità in relazione alle finalità, valutazione dei rischi per i diritti e le libertà degli interessati, misure previste per affrontare i rischi e dimostrare la conformità al regolamento) e risultano altresì funzionali e collegati al principio della cd. privacy by design dell'art.25[36], dal momento che, come affermato in dottrina, anche dal punto di vista operativo, la DPIA deve integrarsi sin dal principio con il processo di sviluppo del prodotto/servizio nell'ambito del quale sarà effettuato il trattamento

[35] L'espressione è di A. Mantelero (*Art.35, cit*., p. 534), il quale sottolinea altresì come si assista, specie nel contesto italiano, al "passaggio da un modello di valutazione generalizzato (...) e con soglie minime di sicurezza (...) ad un modello di valutazione caso per caso e privo di tali soglie"; sul punto, peraltro, appare opportuno ricordare come in tema di trattamenti che possono comportare rischi per gli interessati, infatti, la disciplina previgente prevedeva l'obbligo di istanza all'autorità di controllo (quindi in Italia, l'Autorità Garante per il trattamento dei dati personali) che aveva il compito di verificare caratteri e rischi del trattamento ed autorizzare, o meno, l'attuazione dello stesso con l'eventuale indicazione delle misure da adottare per limitare/ridurre i rischi. Il D.lgs. 196/2003 prevedeva al riguardo l'istituto della cd. verifica preliminare (art.17) oggi abrogato. L'intervento dell'autorità di controllo è oggi previsto nella diversa ipotesi della "Consultazione preventiva" (art.36 GDPR) che assume valore residuale in caso di valutazione di impatto preventiva che evidenzi la presenza di rischi elevati in caso di trattamento posto in essere in assenza di misure, predisposte dal titolare, per attenuare il rischio; si tratta di ipotesi nelle quali le misure predisposte dal titolare non risultino sufficienti e/o non si riescano a trovare misure in gradi di ridurre l'indice di rischio.

[36] Nell'ambito della vasta letteratura sul tema, cfr. M. Ratti, *Art.25 - Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita*, in *R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta, Codice della privacy e data protection, cit*., p. 410 ss; L. Bianchi, G D'Acquisto, *Art.25 - Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita*, in G.M. Riccio, G. Scorza, E. Belisario, *GDPR e normativa privacy. Commentario, cit*., p.245 ss.; R. D'Orazio, *Protezione dei dati by default e by design,* in S. Sica, V. D'Antonio, G.M. Riccio, *La nuova disciplina europea della privacy, cit*., p. 79 ss.

dei dati personali[37]; in caso di pluralità di "trattamenti simili che presentano rischi elevati analoghi", l'art.35 prevede che possa essere effettuata una singola valutazione che esamini tutti i trattamenti simili[38].

Sebbene la DPIA costituisca uno dei principali e più utili strumenti in riferimento alle *accountability policies*, il GDPR non pone un obbligo generalizzato in capo al titolare per qualsiasi tipologia di trattamento, ma piuttosto indica, all'art.35 comma 1, alcuni requisiti di carattere generale (trattamento effettuato "in particolare con l'uso di nuove tecnologie[39] che considerati la natura, l'oggetto, il contesto e le finalità del trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"); successivamente, al comma 3 indica una serie di ipotesi che richiedono "particolarmente" la DPIA (trattamento effettuato in modo automatico, trattamento che può comportare la profilazione, trattamento su larga scala di categorie particolari di dati o di dati giudiziari, trattamento che comporta la sorveglianza sistematica su larga scala di zone accessibili al pubbli-

[37] Le interazioni tra DPIA e principio *privacy by design* previsto dall'art.25 GDPR sono state ripetutamente evidenziate dalla dottrina, anche in considerazione del riferimento all'impiego delle nuove tecnologie come elemento in grado di influire sull'indice di rischio; in argomento, è stato osservato come "l'obiettivo della DPIA è quello di fornire requisiti progettuali costituendo di fatto il "capitolato" tecnico del progetto di compliance" coinvolgendo tutti gli stakeholder interni ed esterni (F. Bravo, *La nuova privacy europea, cit.* p. 127)

[38] La scelta di permettere la realizzazione di una singola DPIA per gruppi di trattamenti che presentino caratteristiche comuni e rischi analoghi risponde all'esigenza di evitare un'inutile aggravio, in termini di attività e costi, per il titolate che intenda realizzare diverse tipologie di trattamento o per i trattamenti realizzati da più soggetti in veste di contitolari; sul punto deve considerarsi anche quanto indicato dal Considerando n.92 che ipotizza la realizzazione di una DPIA su base comune in ipotesi di contitolarità in trattamenti finalizzati alla realizzazione di prodotti/servizi utilizzati su larga scala o di una piattaforma di trattamenti comuni a tutto un settore o segmento professionale.

[39] Sul punto afferma F. Cecamore (*Art. 35, cit.*): "la novità tecnologica, come elemento determinante, trova origine dalla constatazione che spesso solo dopo qualche tempo rispetto all'introduzione di una tecnologia innovativa, se ne conosce effettivamente la portata di rischio in ordine alla sicurezza dei dati (...) una DPIA da parte del fornitore di un nuovo prodotto tecnologico, come ad esempio un software, appare utile a stimare l'impatto sulla protezione dei dati; ma ciò non fa venir meno l'obbligo per ciascun titolare, che può utilizzare le informazioni fornite nell'ambito della DPIA del fornitore, di svolgere la propria valutazione in relazione all'utilizzo del prodotto effettuato in concreto".

co)[40]; da ultimo agli artt.4 e 5 demanda alle autorità di controllo nazionali la compilazione di elenchi contenenti l'indicazione delle tipologie di trattamenti che devono obbligatoriamente essere oggetto di DPIA (art.4) nonché la compilazione, in questo secondo caso solo eventuale, di elenchi di tipologie di trattamenti che sono esentati dalla DPIA (art.5), con l'ulteriore previsione della pubblicità di tali elenchi e della comunicazione degli stessi all'EDPB. A margine delle previsioni dell'art.35, tuttavia, appare opportuno evidenziare come pur in presenta di una tipologia di trattamento non rientrante tra quelle oggetto di obbligo, sarebbe tuttavia sempre preferibile, per il titolare, porre in essere la DPIA, anche perché il modello di valutazione del rischio proposto non si presenta come statico, bensì dinamico, dal momento che il GDPR pone in capo al titolare l'obbligo di effettuare la DPIA (art.35 comma 1) e di procedere a periodici riesami in ipotesi di variazioni del rischio (art.35 comma 11), identificando così un modello circolare in grado di offrire non solo le maggiori garanzie all'interessato, ma altresì una l'accountability e la conformità al Regolamento per il titolare.

In relazione alla DPIA per le attività di targeting, mantengono il ruolo di contitolari sia il fornitore di social media che il targeter, sicché entrambi saranno tenuti alla verifica della tipologia dei trattamenti per il confronto con gli elementi previsti dall'art.35 comma 1 e (soprattutto) comma 3 nonché con gli elenchi stilati dalle autorità nazionali secondo quanto previsto dal comma 4. Richiamando le citate Linee-Guida del WP29, peraltro, è opportuno che i contitolari definiscano con precisione le proprie competenze e realizzino conseguentemente la DPIA secondo quanto previsto nell'accordo e con ogni opportuno scambio di informazioni e collaborazione[41]. In particolare, i contitolari potrebbero anche

[40] Nell'indicare una serie di ipotesi che richiedono la realizzazione di una DPIA, l'art.35 si propone come esemplificativo e non esaustivo, sicché l'elencazione deve intendersi aperta e non tassativa; sul punto, peraltro, le Linee-Guida del WP29 evidenziano come nel dubbio sull'obbligatorietà o meno della DPIA, il titolare dovrebbe comunque optare per la realizzazione, proprio perché da essa può derivare la conferma della conformità alle previsioni del regolamento o l'avvertimento sulla mancata conformità e sull'esposizione a rischi che permetterebbe al titolare, in questa ultima ipotesi, di predisporre le misure correttive e non restare esposto alla eventualità di sanzioni.

[41] In argomento, il paragrafo 112 prevede che: "Qualora sia necessaria una valutazione d'impatto sulla protezione dei dati, l'accordo di contitolarità dovrebbe disciplinare le modalità di svolgimento della stessa da parte dei titolari del trattamento e assicurare che avvenga un pertinente scambio di conoscenze. In questo esempio può essere che la piattaforma di social media si trovi in una posizione migliore per valutare determinati trattamenti, nella misura in cui il partito politico si limiti a selezionare criteri generali di targeting".

stabilire che sia uno solo dei due a realizzare, operativamente[42], la DPIA ma ciò non esime da responsabilità (verso gli interessati) anche l'altro contitolare dal momento che l'accordo tra i contitolari non può intendersi derogatorio della disciplina generale e degli obblighi ex art.26 GDPR.

Le attività di targeting, peraltro, siano esse correlate al mercato o alla propaganda (ad es., politica o sindacale) od ancora all'influenza dell'opinione pubblica, devono essere valutate non soltanto in relazione al contenuto del messaggio, ma altresì alle caratteristiche della comunicazione ed alle fasce di pubblico destinatarie, alle finalità della comunicazione, alla tempistica della stessa (il paragrafo 105 parla, non a caso, di "invasività") nonché alla tipologia di dati personali utilizzati (osservati, desunti o derivati). La DPIA assume particolare rilievo quando l'attività di veicolazione dei messaggi sia indirizzata a fasce di popolazione e/o categorie particolarmente deboli o vulnerabili, quali ad esempio anziani o fanciulli, proprio in ragione della maggior tutela che deve essere garantita a tali soggetti a fronte di comunicazioni che potrebbero rappresentare un rischio elevato. In relazione alla DPIA, l'esempio indicato dalle Linee-Guida (esempio 9) riguarda l'ipotesi di un partito politico che voglia incoraggiare al voto per un determinato candidato una ben precisa di categoria di utenti di social media che abbiano le seguenti caratteristiche: anziani, abitanti in zone rurali, regolari frequentatori della chiesa e che non abbiano viaggiato all'estero negli ultimi due anni; come si può notare, il targeter individua un ben preciso profilo di "potenziale elettore" al quale saranno indirizzati messaggi in linea con quelle che si ritiene siano le opinioni corrispondenti allo stile ed al contesto di vita; in un caso come questo è possibile che fornitore di social media e targeter effettuino operativamente insieme la DPIA avendo entrambi sufficienti conoscenze in ordine alle tipologie di trattamenti, come è anche possibile che il targeter, cioè il partito politico, si limiti ad indicare le caratteristiche della categoria dei destinatari della comunicazione e che sia solo il fornitore di social media a svolgere operativamente la DPIA, avendo una

[42] Tale possibilità è prevista al paragrafo 109: *"i contitolari del trattamento possono stabilire che spetti a uno di loro eseguire la valutazione d'impatto sulla protezione dei dati (...) ciò dovrebbe poi essere specificato nell'accordo di contitolarità, facendo salva la responsabilità congiunta dei titolari in quanto tale"*; la possibilità di indicare un solo soggetto per l'esecuzione della DPIA può essere determinata dalla circostanza che *"uno dei titolari del trattamento si trovi in una posizione migliore per valutare determinati trattamenti (...) ad esempio tale titolare del trattamento può essere, a seconda del contesto, quello che dispone del grado di controllo e di conoscenze più elevato in merito al trattamento di targeting - in particolare sul back-end del sistema distribuito o sui mezzi di trattamento"*.

posizione migliore per valutare quali tipologie di trattamenti mettere in atto e quale impatto (essi) possano avere sulla categoria di destinatari; sul punto appare opportuno ricordare, ancora una volta, che le scelte in ordine alle modalità operative della DPIA devono essere definite nell'accordo, ferma restando, in ogni caso, la contitolarità nelle attività di trattamento e la (conseguente) responsabilità nei confronti degli interessati.

La DPIA relativa al targeting per una attività di comunicazione mirata deve comprendere "le misure previste per affrontare i rischi, le misure di sicurezza ed i meccanismi per garantire la protezione dei dati e dimostrare la conformità al GDPR" (in questi termini il paragrafo 110); qualora, nonostante la predisposizione delle misure di sicurezza e dei meccanismi di data protection, residuino ulteriori rischi di grado elevato, sarà obbligo dei contitolari, ciascuno (almeno) per la parte di competenza, consultare le autorità di controllo. Peraltro, in presenza di rischi non individuati o di rischi che non siano previsti/attenuati in modo sufficiente, l'attività di targeting non dovrebbe essere realizzata in quanto verrebbe a porsi in contrasto con il GDPR[43] e costituirebbe una fonte di responsabilità per i contitolari.

Rapporti tra social media provider e targeter: accordi di contitolarità e profili di responsabilità

Come evidenziato nei paragrafi precedenti, social media provider e targeters possono assumere il ruolo di contitolari in relazione alle attività di trattamento finalizzate al targeting; tale ruolo determina, in accordo con la normativa del GDPR che viene richiamata, una serie di obblighi: nei confronti degli utenti/interessati (entrambi devono essere in grado di garantire la trasparenza, la legittimità e l'informazione sui trattamenti che saranno posti in essere) e, con carattere di reciprocità nei confronti del partner commerciale (con riferimento ai rapporti interni, obbligo di stipulare un accordo per la definizione delle responsabilità "in merito all'osservanza" del regolamento). L'art. 26 del GDPR prevede, infatti,

[43] La possibilità di una attività di targeting in violazione del GDPR viene implicitamente prevista dall'ultimo inciso del paragrafo 110 (qualora violi il GDPR, in particolare perché i rischi non sono stati identificati o attenuati sufficientemente, il targeting non dovrebbe avere luogo, con una formulazione verbale che riprende l'originale testo inglese "*the targeting should not take place*") che potrebbe interpretarsi come una ipotesi di responsabilità aggravata, posto che l'attività viene realizzata pur in presenza di una esplicita indicazione in senso contrario. La stessa formulazione testuale della norma, infatti, potrebbe apparire come una indicazione più che come un diniego imperativo.

che i contitolari determinino mediante accordo interno i rispettivi ruoli e le responsabilità in relazione al rispetto dei diritti degli interessati e degli obblighi in materia di trasparenza e legittimità del trattamento[44]; in relazione questo punto, l'EDPB richiede che l'accordo tra targeters e social media provider debba contemplare tutte le differenti attività di trattamento finalizzate al targeting, dal momento che un accordo solo superficiale ed incompleto, o indirizzato genericamente alle attività di trattamento senza specificazioni, sarebbe in contrasto con l'art. 26 GDPR e, dunque, fonte di responsabilità.

Sia il targeter che il social media provider dovranno, pertanto, avere a disposizioni sufficienti informazioni relative alle diverse attività di trattamento (incluse quelle di profilazione) che saranno realizzate e nell'accordo dovrà essere presente un esplicito riferimento a tutti i dati e le informazioni che permettono di rispettare gli obblighi ed i principi ex art.5 par. 1 e la conformità ex art.5 par.2 GDPR.

Particolare attenzione viene dedicata al tema della base giuridica del trattamento ex art.6 par.1 GDPR con la raccomandazione di utilizzare una unica base giuridica per tutti i trattamenti funzionali ad uno strumento di targeting ed una finalità precisa: la presenza di diverse basi giuridiche e l'indicazione di diverse finalità, infatti, sebbene astrattamente rispondenti alle previsioni del GDPR potrebbero tradursi in una serie di difficoltà ed ostacoli per l'interessato che volesse far valere i suoi diritti (e che, come indicato al par 134 potrebbe trovarsi ad invocare la

[44] F. Pizzetti – L. Greco, *Art. 26 - Contitolari del trattamento*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta, *Codice della privacy e data protection, cit.*, p.422; M. L. Salvati, *Art. 26 – Contitolari del trattamento,* in G.M. Riccio, G. Scorza, E. Belisario, *GDPR e normativa privacy. Commentario, cit.,* p. 326; D. Farace, *Il titolare e il responsabile del trattamento*, in V. Cuffaro, R. *D'Orazio, V. Ricciuto (a cura di) I dati personali nel diritto europeo, Milano, 2019, p. 731; V. Ricciuto, Titolarità e contitolarità nel trattamento dei dati personali tra Corte di Giustizia e Regolamento privacy*, in *NGCC*, 2018, p. 1805; E. Pelino, *I soggetti del trattamento*, in L. Bolognini (a cura di) *Il Regolamento privacy europeo*, Milano, 2016, p. 136.

tutela di situazioni diverse in relazione ai singoli trattamenti[45]). Ancora, l'art.26 par.1 del GDPR prevede che siano oggetto dell'accordo anche "le funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14" ed il successivo par.2 che "il contenuto essenziale dell'accordo è messo a disposizione dell'interessato": si tratta di obblighi che si riflettono sui diritti dell'interessato e sono finalizzati a garantirne la tutela. Dal combinato delle due disposizioni emerge, infatti, che i contitolari dovranno predisporre l'informativa ed ogni altra comunicazione richiesta dagli artt.13 e 14 utilizzando un linguaggio chiaro e comprensibile, ma al contempo fornendo informazioni complete ed esaurienti "riguardo al trattamento a cui si riferisce con spiegazioni, se del caso, sulle varie fasi del trattamento e sui vari soggetti coinvolti nello stesso"[46]. Le informazioni dovranno essere fornite agli interessati prima della raccolta dei dati e devono riguardare anche le finalità condivise o strettamente collegate, nonché l'eventualità del trasferimento a terzi; nell'accordo interno, peraltro, potrà essere prevista anche una suddivisione degli obblighi di informazione, senza tuttavia che tale suddivisione si rifletta sul regime di responsabilità che si manterrà comune. Il contenuto dell'accordo deve essere messo a disposizione degli interessati attraverso una esplicita indicazione nell'ambito delle privacy policies di ciascun contitolare e, eventualmente, un collegamento ipertestuale che ne permetta la diretta accessibilità.

[45] Tra gli esempi riportati, può essere preso in considerazione quello di una impresa di dating che voglia rivolgere pubblicità mirata a soggetti di sesso maschile che hanno indicato uno status di single e che abbiano età compresa tra i 30 ed i 45 anni; acquisendo i pattern di dati (già oggetto di trattamento e/o di profilazione) dal social media provider, l'impresa di dating potrà invocare come base giuridica del trattamento l'interesse legittimo, ma dovrà acquisire una serie di informazioni sui trattamenti effettuati dalla piattaforma social e sulle misure aggiuntive, quali ad esempio la possibilità di una opposizione preventiva. E' necessario, infatti, che il targeter accerti che la propria base giuridica, qualora diversa da quella del social media provider, non si ponga in contrasto con diritti e le libertà fondamentali dell'interessato. Quest'ultimo, peraltro, in presenza di trattamenti effettuati su basi giuridiche diverse ed altresì effettuati per finalità diverse, dovrà far valore i propri diritti verso ciascuno dei contitolari in ragione della base giuridica e della finalità di ciascun trattamento, anche a costo di una eventuale duplicazione delle azioni esperibili.

[46] Sul punto, le Linee-Guida richiamano il parere del WP29 n. 1/2010 - WP169 sui concetti di "responsabile del trattamento" e "incaricato del trattamento": il testo completo del parere può leggersi all'indirizzo https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

Sebbene le Linee-Guida non offrano un elenco tipizzato, i richiami alle disposizioni del GDPR sparsi in diversi paragrafi, permettono di identificare una sorta di "contenuto obbligatorio dell'accordo": le informazioni sulla tipologia di trattamento, l'ambito di applicazione, la base giuridica le finalità del trattamento (conformandosi a quanto previsto dagli artt. 5 e 6 GDPR), le indicazioni sui diritti dell'interessato e sulle modalità di esercizio (con particolare attenzione al diritto di accesso), la sicurezza del trattamento, le disposizioni in merito al rispetto dei principi ex art.25 GDPR (privacy by design e privacy by default), le modalità di notifica e di comunicazione in caso di violazione dei dati personali, la (eventuale) valutazione di impatto preventiva, la presenza di responsabili del trattamento e/o altri soggetti coinvolti nelle attività, l'eventualità di trasferimento dati verso paesi terzi[47].

In margine alle considerazioni esposte, appare opportuno sottolineare come, in relazione ai trattamenti, social media provider e targeter possano altresì assumere la qualifica di titolare esclusivo: è il caso dei trattamenti che la piattaforma social potrebbe realizzare prima di quelli previsti dall'accordo e per finalità proprie e non condivise; in queste, come nelle altre ipotesi di trattamenti esclusivi da parte del targeter, l'EDPB rileva che non sussiste alcun obbligo informativo a carico dei contitolari per tutti i trattamenti ulteriori rispetto al rapporto di contitolarità per i quali sarà il social media provider, o il targeter, in via esclusiva, a dover adempiere gli obblighi ex artt.13 e 14 del GDPR.

La qualifica di contitolari determina significative ricaduta anche in tema di responsabilità per le attività di trattamento svolte; in particolare, il paragrafo 130 delle Linee-Guida richiama l'obbligo, ex art.26 GDPR, di definire, nell'accodo interno, *"le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR"*, esplicitando poi, ai paragrafi successivi, che entrambi sono responsabili *"di assicurare il rispetto del principio di limitazione delle finalità"* (e che, al riguardo, dovrebbero esse-

[47] La questione dell'eventuale trasferimento verso paesi terzi pone particolari questioni soprattutto per quegli stati extra UE per i quali non c'è una dichiarazione di adeguatezza ai sensi dell'art.45 GDPR e si rende necessario il ricorso ad una delle altre garanzie previste dagli artt. 46 e 47 GDPR. Sul tema, nell'ambito di una vasta bibliografia, cfr. C. Peraro, *Protezione extraterritoriale dei diritti: il trasferimento dei dati personali dall'Unione Europea verso Paesi Terzi*, in "OIDU. Ordine Internazionale e diritti umani", 2021, p. 666; G. M. Riccio, F. Pezza, *Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*, in E. Tosi (a cura di) *Privacy digitale, cit.,* p. 585; A. Barletta, *La tutela della "privacy" nello spazio (giudiziario) europeo e nel tempo (della "aterritorialità) di internet"*, in "Europa e Diritto Privato", 2017, p. 1179.

re previste adeguate disposizioni nell'accordo di contitolarità, par. 135) nonché degli altri principi in tema di legittimità del trattamento e di tutela dei diritti dell'interessato (par.136) e dell'indicazione delle modalità concrete con le quali saranno soddisfatti gli obblighi del GDPR (par 137). Lacune o inesattezze in relazione a quello che abbiamo individuato come "contenuto obbligatorio" determinano violazioni dell'art.26 GDPR comma 1 e responsabilità a carico di entrambi i contitolari[48].

In relazione all'accordo interno appare opportuno evidenziare come esso possa assumere sia la forma di un accordo negoziato tra le parti sia quella di un contratto di adesione predisposto unilateralmente e senza possibilità di modifiche e/o integrazioni; in questo caso la parte aderente, generalmente il targeter, non potrà invocare limitazioni di responsabilità dal momento che espressamente l'EDPB ritiene che tale circostanza "non infici la responsabilità congiunta". L'autonomia delle parti nel determinare il contenuto dell'accordo interno, infatti, non può prevalere sugli obblighi che derivano dalla qualifica di contitolare del trattamento dal momento che ciascuno rimane *"per principio, responsabile della conformità del trattamento"*. L'elemento sul quale l'accordo interno può influire è, invece, il grado di responsabilità: sul punto, infatti, richiamando quanto stabilito dalla EUCJ nella sentenza Wirtschaftakademie[49], viene evidenziato come il livello di responsabilità possa corrispondere al ruolo effettivo svolto nelle attività di trattamento; per riprendere le parole della EUCJ, la responsabilità congiunta non significa responsabilità equivalente. Anzi, proprio al paragrafo 142 vengono indicate una serie di circostanze che devono essere considerate nella valutazione dei profili

[48] In relazione alle eventuali lacune dell'accordo interno, il paragrafo 137 prevede che "laddove non vi sia chiarezza in merito alle modalità di soddisfacimento di tali obblighi, in particolare in relazione ai diritti degli interessati, si dovrà ritenere che tanto il targeter quanto il fornitore di social media stiano violando l'articolo 26, paragrafo 1, GDPR (...) inoltre in tali casi entrambi i (con)titolari del trattamento non avranno attuato misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento sia stato condotto in conformità con il GDPR, e quindi avranno violato i loro obblighi ai sensi dell'articolo 5, paragrafo 2, e dell'articolo 24".

[49] Il paragrafo 140 delle Linee-Guida richiama espressamente quanto indicato dalla EUCJ al paragrafo 43 della sentenza 5 giugno 2018, *Wirtschaftakademie* (C-210/16): "l'esistenza di una responsabilità congiunta non implica necessariamente una responsabilità equivalente, per un medesimo trattamento di dati personali, dei diversi soggetti che vi partecipano. [...] tali soggetti possono essere coinvolti in fasi diverse di tale trattamento e a diversi livelli, di modo che il grado di responsabilità di ciascuno di essi deve essere valutato tenendo conto di tutte le circostanze rilevanti del caso di specie"

di responsabilità e che dovrebbero corrispondere ad altrettante determinazioni contenute nell'accordo interno, quali la capacità di influire concretamente sul trattamento o la conoscenza effettiva o costruttiva di ciascuno od ancora l'effettivo svolgimento di uno o più segmenti delle attività di trattamento.

In relazione a questa ultima ipotesi, qualora il targeter utilizzi una serie di pattern di dati che siano frutto di precedenti attività di profilazione o altre attività di trattamento svolte (antecedentemente all'accordo interno) dal solo social media provider, graverà proprio su quest'ultimo l'obbligo di garantire che quei trattamenti siano stati svolti nel rispetto delle disposizioni del GDPR e, di conseguenza, sarà maggiore il grado di responsabilità nei confronti degli interessati. Può capitare, infatti, che le attività finalizzate alla raccolta e classificazione dei diversi pattern di dati, nonché alla individuazione di cluster di possibili destinatari ed ancora alla definizione dei criteri e dei diversi meccanismi di targeting, siano state poste in essere dal social media provider, il quale ha assunto autonomamente alcune decisioni, sia in ordine alla quantità e qualità dei dati che alle modalità di trattamento; successivamente, il targeter ha effettuato le proprie attività servendosi dei patter di dati ricevuti e delle attività già poste in essere dal social media provider. In tale ipotesi, sarà opportuno evidenziare nell'accordo interno ruoli e decisioni in ordine ad ogni attività di trattamento ed avere una "chiara allocazione di responsabilità" che rispecchi "il livello di responsabilità di ciascun soggetto"; in questo modo, sebbene rimangano inalterati il ruolo di contitolari per le attività di targeting e la legittimazione dell'interessato ad agire nei confronti di entrambi per la tutela dei propri diritti, tuttavia il diverso grado di responsabilità avrà riflessi sulla qualificazione degli eventuali illeciti e sulla (eventuale) quantificazione delle relative sanzioni.

L'ultimo paragrafo delle Linee-Guida richiama, sempre in ordine ai profili di responsabilità, la possibilità di accertamento da parte delle autorità di controllo alle quali siano soggette i contitolari, evidenziando che *"nella misura in cui i termini dell'accordo di contitolarità stipulato tra il fornitore di social media e il targeter non vincolano le autorità di controllo, queste ultime possono esercitare le loro competenze e i loro poteri in relazione a ciascuno dei contitolari del trattamento"*, chiaramente "nella misura in cui il contitolare del trattamento in questione è soggetto alla competenza di tale autorità di controllo".

Conclusioni… aspettando il Digital Service Package.

Da una analisi del testo adottato dall'EDPB, emerge come le Linee Guida 8/20 in materia di targeting degli utenti di social media si presentino come un documento di indubbio valore soprattutto per l'attenzione rivolta ad un fenomeno in costante crescita nel mercato ma che non sempre risulta di facile inquadramento nel sistema normativo attuale. Sebbene l'attenzione sia rivolta all'aspetto commerciale delle attività di targeting ed all'impatto delle stesse sulle dinamiche del marketing on line, tuttavia non deve trascurarsi come le stesse attività possano essere attuate anche con finalità di analisi ed orientamento dell'opinione pubblica nonché di influenza delle scelte sociali e politiche. In relazione a questi ultimi punti, l'EDPB paventa che possano verificarsi fenomeni negativi quali la discriminazione o esclusione di categorie sociali in ragione di debolezza o motivi etnici, od ancora la manipolazione degli utenti, considerati come consumatori ma altresì come cittadini.

Proprio per prevenire queste eventuali patologie, il documento dell'EDPB ha una forma molto diretta e si presenta ricco di esempi e casi pratici: infatti esso appare differente da un testo normativo rivolto solo agli addetti ai lavori e spesso di difficile comprensione per gli operatori od i diretti destinatari. Sul tema, saranno quindi i prossimi mesi a dare una risposta sulla reale efficacia delle Linee-Guida, pur nella consapevolezza che un tema delicato quale la tutela dei dati personali nelle attività di targeting, particolarmente quelle che fanno ricorso a profilazione, sistemi automatizzati e strumenti AI, richieda una continua attenzione da parte del legislatore europeo anche nell'ottica di un continuo aggiornamento del GDPR per adeguarlo alle esigenze di una società sempre più "connessa" ed alle esigenze di tutela di un interessato sempre più esposto all'automazione ed agli strumenti AI.

Proprio nell'ottica degli interventi del legislatore europeo sarà interessante verificare l'attenzione rivolta ai fenomeni di profilazione e di targeting nei provvedimenti di prossima adozione quali il nuovo Regolamento Europeo sui mercati digitali (Digital Markets Act - DMA) ed il nuovo Regolamento europeo sui servizi digitali (Digital Services Act-DSA). Entrambi i provvedimenti, considerati unitariamente come Digital

Services Package[50], si indirizzano, almeno nelle intenzioni del legislatore europeo, alla responsabilizzazione delle piattaforme ed all'enforcement della posizione degli utenti/cittadini europei anche con riferimento alla tutela dei dati nei rapporti commerciali e di consumo.

Accanto ai provvedimenti normativi del Digital Services Package, tuttavia, non deve trascurarsi l'aspetto legato all'utilizzo del targeting per finalità di comunicazione e propaganda e, sul punto, l'attenzione è rivolta ai lavori della Commissione che sta procedendo alla revisione del Codice Europeo di condotta contro la disinformazione, che dovrebbe essere presentato nell'estate del 2022. Nella stesura della novella del testo originario del Codice, formulato nel 2018[51], il Gruppo di esperti nominato dalla Commissione ha manifestato la volontà di dedicare una particolare attenzione alle attività di propaganda politica basate su attività di profilazione e targeting, avvertendo la particolare portata invasiva che tali attività possono avere sulla sfera individuale[52]. Sebbene il Codice Europeo di condotta contro la disinformazione non sia un documento normativo ma un codice di autoregolamentazione, appare tuttavia condivisibile l'opinione di quanti vedono nel coinvolgimento di un maggior numero di firmatari/aderenti e particolarmente delle Big Companies del Web, un segnale positivo sulla concreta realizzazione di un progetto (globale) di tutela degli utenti considerati come soggetti agenti nel panorama digi-

[50] S. Scola, *"Digital Services Act": occasioni mancate e prospettive future nella recente proposta di regolamento europeo per il mercato unico dei servizi digitali*, in "Contratto e impresa. Europa", 2022 p. 127; G. M. Ruotolo, *Le proposte europee di riforma della responsabilità dei fornitori di servizi su Internet,* in "Rivista italiana di informatica e diritto", 2022, p. 17; E. M. Tripodi, *Il Regolamento comunitario sul "Digital Services Act" (Legge sui servizi digitali). Verso la revisione della disciplina del commercio elettronico,* in "Disciplina del commercio e dei servizi", 2022, p. 34; V. Falce, *Digital Markets between Regulation and Competition policy. Converging agendas*, in "European Journal of Privacy Law & Technologies", 2021, p. 9.

[51] F. Sammitto, G. Sichera, *L'informazione (e la disinformazione) nell'epoca di internet: un problema di libertà*, in "Costituzionalismo.it", 2021, p. 77; C. Vaditara, *"Fake news": regolamentazione e rimedi*, in *Il* "Diritto dell'informazione e dell'informatica", 2021, p. 257; G. Pagano, *Il "Code of Practice on Disinformation". Note sulla natura giuridica di un atto misto di autoregolazione*, in "Federalismi.it", 2019; M. Monti, *Il "Code of Practice on Disinformation" dell'UE: tentativi "in fieri" di contrasto alle "fake news"*, in "MediaLaws – Rivista di diritto dei media", 2019, p. 320.

[52] Gli "Orientamenti sul rafforzamento del codice di buone pratiche sulla disinformazione" della Commissione UE possono leggersi all'indirizzo https://digital-strategy.ec.europa.eu/it/library/guidance-strengthening-code-practice-disinformation; in particolare, cfr. Comunicazione della Commissione sulle Linee-Guida per il rafforzamento del Codice conto la disinformazione del 26.05.2021, COM(2021) 262 final.

tale e non più solo come destinatari di servizi digitale e consumatori di beni e servizi ed altresì consumatori di informazione.

Responsabilizzazione delle piattaforme e maggiore consapevolezza degli utenti in ordine ai propri diritti ed agli strumenti dei propri interessi sono le due chiavi che l'UE dovrà sviluppare nel prossimo futuro per garantire l'auspicato sviluppo digitale e l'auspicato ampio grado di partecipazione da parte dei cittadini nell'ambito della realizzazione del *Digital Decade policy programme*[53].

Abstract

L'aumento esponenziale dell'utilizzo dei social media determina la continua crescita dei flussi di dati personali circolanti on line: tali dati possono essere una preziosa fonte di informazioni per le aziende che vogliono implementare strategie di marketing diretto. Altresì, il trattamento dei dati personali degli utenti dei social media può costituire un rischio per la privacy e la tutela in ambito individuale: ogni attività di trattamento richiede il rispetto dei principi e dei criteri di liceità previsti dal GDPR. Per quanto riguarda la peculiarità delle attività di targeting, il Comitato europeo per la protezione dei dati (EDPB), a seguito di una consultazione pubblica, ha adottato nell'aprile 2021 le Linee guida 8/2020 "sul targeting degli utenti dei social media". Il testo delle Linee- Guida si presenta piuttosto completo: analizza i rischi derivanti dalle attività di trattamento dei dati personali ed individua tutti i soggetti coinvolti in tali attività (soprattutto Social Media Provider e Targeters) e le relative responsabilità; classifica inoltre le tre categorie di dati che possono essere trattati: "dati forniti" (forniti direttamente dall'utente), dati osservati (forniti utilizzando un dispositivo o un servizio) e "dati desunti/derivati" (forniti dalla profilazione e dall'osservazione del comportamento degli utenti sul web). Inoltre, le Linee Guida si concentrano sulle basi giuridiche del trattamento e sugli obblighi previsti dal GDPR.

[53] Il claim "*Europe aims to empower businesses and people in a human-centred, sustainable and more prosperous digital future*" sintetizza il *Digital Decade policy programme*; in data 26 gennaio 2022 la Commissione ha presentato una dichiarazione interistituzionale sui diritti digitali e sui principi per il prossimo "decennio digitale": si tratta di diritti che si aggiungono a quelli già esistenti e proclamati dalla Carta dei diritti fondamentali della UE e dalla legislazione sulla privacy ed arricchiranno il quadro di riferimento normativo per la tutela dei diritti digitali dei cittadini europei e potranno altresì offrire un valido orientamento per gli Stati membri della UE e per le imprese in materia di nuove tecnologie. In estrema sintesi, i nuovi diritti digitali ed i principi sottesi alla loro affermazione sono: mettere le persone e i loro diritti al centro della trasformazione digitale; sostenere la solidarietà e l'inclusione; garantire la libertà di scelta online; promuovere la partecipazione nello spazio pubblico digitale; aumentare la sicurezza, la sicurezza e l'empowerment dei soggetti; promuovere la sostenibilità del futuro digitale. Obiettivi, programmi ed itinerario del *Digital Decade policy programme* possono leggersi all'indirizzo https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en.

Parole chiave: Targeting on line – Social Media – Protezione dei dati personali – GDPR – EDPB – LineeGuida.

Abstract
The exponential increase in social media use determines a continuously growing flow of personal data, which can be a valuable source of information for companies wanting to implement direct marketing strategies. However, processing of personal data of social media users can constitute a risk for privacy and protection in the individual sphere: each process activity requires compliance with principles and criteria of lawfulness provided for by the GDPR. Regarding the peculiarity of targeting activities, the European Data Protection Board (EDPB), following public consultation, adopted the 8/2020 Guidelines in April 2021 "on the targeting of social media users". The Guideline text is quite complete, analyzing risks coming from processing activities involving personal data, identifying all subjects involved in these activities, (above all Social Media Providers and Targeters) and related responsibilities; it also identifies three data categories that can be processed: "provided data" (provided directly by the user), observed data (provided by using a device or a service) and "inferred/derived data" (provided from profiling and observing of user behavior on the web). Moreover, the Guidelines focus on the legal bases of processing and on obligations required by the GDPR.
Keywords: Targeting on line – Social Media – Personal Data Protection – GDPR – EDPB – Guidelines.