Ordine internazionale e diritti umani
International Legal Order and Human Rights
Ordenamiento Jurìdico Internacional y Derechos Humanos
Ordre Juridique International et Droits de l'Homme
Diretta da Claudio Zanghì, Lina Panella, Carlo Curti Gialdino
EDITORIALE SCIENTIFICA

3. M*ICROTARGETING* POLITICO NELL'UNIONE EUROPEA: ALCUNE RIFLESSIONI ALLA LUCE DELLA PRASSI ISTITUZIONALE E DELLA REGOLAMENTAZIONE PIÙ RECENTI.

1. Introduzione

Il *microtargeting* ha acquisito un ruolo sempre più rilevante, grazie all'uso sofisticato delle tracce digitali lasciate dagli elettori. Questo fenomeno si inserisce in un contesto più ampio, in cui le tecniche di *web marketing*, come la profilazione, il *retargeting* e gli annunci a pagamento, sono ormai dominanti in tutti i settori, compreso quello politico. In particolare, le piattaforme *online* svolgono un ruolo cruciale: attraverso tali strumenti, esse consentono la costruzione di campagne politiche mirate, capaci di identificare con precisione il pubblico di riferimento e di persuaderlo, adattando i messaggi alle caratteristiche specifiche di ciascun elettore. Questa personalizzazione del messaggio, da un lato, aumenta l'efficacia della comunicazione politica, ma, dall'altro lato, solleva anche interrogativi significativi in termini di trasparenza e tutela della *privacy* (si rimanda a N. WITZLEB, M, PATERSON, "Micro-targeting in political campaigns: political promise and democratic risk", in U. KOHL, J. EISLER (Eds.), *Data-Driven Personalisation in Markets, Politics and Law,* Cambridge University Press, 2021, pp. 223-239; v. F.J. ZUIDERVEEN BORGESIUS, J. MÖLLER, S. KRUIKEMEIER, R. Ó FATHAIGH, K. IRION, T. DOBBER, B. BODO, C. DE VREESE, *Online Political Microtargeting: Promises and Threats for Democracy*, in Utrecht Law Review, 2018, pp. 82-96; K. BAUM, O. ABRAMOVA, S. MEIßNER, H. KRASNOVA, *The effects of targeted political advertising on user privacy concerns and digital product acceptance: A preference-based approach*, in Electron Markets, 2023).

Una dimostrazione concreta di questi rischi è emersa lo scorso dicembre, quando il Garante europeo della protezione dei dati (GEPD) ha accertato che la Commissione europea ha violato le norme sulla protezione dei dati personali attraverso l'uso di *political advertising*. In particolare, la decisione ha evidenziato come la Commissione abbia sfruttato l'algoritmo di X per individuare gruppi di utenti sulla base di categorie di dati sensibili, come le opinioni politiche e le convinzioni religiose, contravvenendo così alle norme pubblicitarie della piattaforma e al Regolamento (UE) 2018/1725, che disciplina il trattamento dei dati personali da parte delle istituzioni dell'Unione. Queste violazioni sono emerse nel contesto di una campagna pubblicitaria lanciata nel settembre 2023 per promuovere la proposta di regolamento sulla prevenzione e il contrasto dell'abuso sessuale sui minori, avanzata dalla Commissione europea l'11 maggio 2022 (*Child Sexual Abuse Material Regulation, CSAM*. V. F.

DI GIANNI, *Protezione dei minori vs. tutela dei dati personali: profili critici della proposta di Regolamento sulla prevenzione e la lotta contro l'abuso sessuale sui minori online*, in Ordine Internazionale e Diritti Umani, 2023. Sullo stato di avanzamento dei lavori relativi alla proposta di regolamento vedi qui).

La vicenda ha assunto una certa rilevanza perché avvenuta in concomitanza con l'adozione del nuovo Regolamento (UE) 2024/900 che ha introdotto norme armonizzate sulla trasparenza e sul *targeting* della pubblicità politica. Il regolamento rappresenta il risultato dell'azione normativa dell'Unione europea che, negli ultimi anni, ha teso a rafforzare la tutela dei dati personali dei cittadini, soprattutto *online*. In particolare, il nuovo atto chiarisce le responsabilità di sponsor, piattaforme, inserzionisti e società di consulenza politica nella diffusione di contenuti a pagamento, integrando in tal senso il quadro normativo già esistente, compreso il Regolamento generale sulla protezione dei dati (RGPD), il Regolamento (UE) 2018/1725 e il Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali (o regolamento sui servizi digitali, *DSA*), che stabilisce norme sulla trasparenza e la responsabilità delle piattaforme *online*. Tale quadro normativo, infatti, sebbene rappresenti un importante strumento di tutela, non è sufficiente a proteggere completamente i cittadini dall'invasività delle nuove pratiche di comunicazione politica.

A partire da queste premesse, nel presente lavoro si analizzeranno, innanzitutto, le implicazioni della decisione del GEPD. Successivamente, si esamineranno i principali strumenti normativi dell'Unione in materia di pubblicità politica *online* e protezione dei dati personali, con particolare attenzione alle disposizioni del nuovo Regolamento (UE) 2024/900. Quest'ultimo introduce obblighi specifici di diligenza e trasparenza per i prestatori di servizi di pubblicità politica e pone limiti stringenti all'uso delle tecniche di *targeting*. Tuttavia, come evidenzia il caso esaminato, la costruzione di un ambiente digitale sicuro e affidabile non può limitarsi al monitoraggio delle piattaforme *online*, ma deve coinvolgere anche le autorità europee che ne definiscono le regole e ne orientano l'evoluzione. Su queste tensioni, che emergono chiaramente dal confronto tra il quadro normativo e le prassi adottate, si concentreranno le riflessioni conclusive di questa analisi

2. I fatti rilevanti all'origine del reclamo e le osservazioni della Commissione

Prima di approfondire il ragionamento seguito dal Garante europeo della protezione dei dati nel suo richiamo formale (*reprimand*), conviene soffermarsi sui caratteri della campagna pubblicitaria mirata sulla piattaforma X lanciata dalla Commissione europea che sono all'origine del ricorso.

Il caso è stato sollevato da un cittadino olandese, rappresentato dall'organizzazione noyb, associazione non-profit nota per il suo impegno nella difesa della *privacy* e dei diritti digitali, che ha contestato il trattamento dei dati personali effettuato dalla Commissione. Secondo il ricorrente, tale trattamento avrebbe comportato una profilazione basata su categorie particolari di dati personali, in violazione di diverse disposizioni del Regolamento (UE) 2018/1725, senza rientrare in nessuna delle eccezioni previste dall'art. 10, par. 2 del medesimo regolamento.

La campagna pubblicitaria in oggetto, svoltasi tra il 15 e il 28 settembre 2023 in otto Stati membri, era finalizzata a promuovere la proposta di regolamento per la prevenzione e il contrasto agli abusi sessuali sui minori, nota come *Chat Control Regulation* (punto 2.1 *reprimand*). Per la diffusione del messaggio, la Commissione ha adottato criteri di inclusione

ed esclusione basati sugli orientamenti espressi dagli utenti, distinguendo tra posizioni favorevoli all'integrazione europea in materia e posizioni euroscettiche. La campagna si è svolta attraverso la piattaforma X, sfruttando due specifiche tecniche di *microtargeting*: il *keyword targeting* e il *look-alike advertising*. Il primo consente di raggiungere utenti in base alle parole chiave presenti nelle loro ricerche, nei post pubblicati di recente o con cui hanno interagito. Attraverso questo meccanismo, la Commissione ha potuto includere o escludere destinatari in base a criteri geografici, linguistici, relativi al dispositivo utilizzato e al genere. Ad esempio, se un utente aveva interagito con un post contenente una parola chiave inclusa e soddisfaceva i criteri definiti, avrebbe ricevuto il contenuto pubblicitario. Al contrario, se l'utente aveva pubblicato o interagito con un post contenente una parola chiave esclusa, sarebbe stato automaticamente escluso dalla campagna, indipendentemente dagli altri parametri. Inoltre, i contenuti sponsorizzati non compaiono nei risultati di ricerca associati a parole chiave escluse, limitando ulteriormente la loro visibilità a determinate fasce di pubblico.

Accanto al *keyword targeting*, è stato utilizzato anche il *look-alike advertising*, una tecnica di *targeting* nella pubblicità digitale che permette di individuare nuovi utenti con caratteristiche simili a un pubblico di riferimento già definito. Introdotta inizialmente da Facebook nel 2013, questa strategia si basa sull'analisi algoritmica di un *database* esistente per identificare profili con comportamenti affini in un archivio più ampio. Tale approccio, ormai diffuso anche su piattaforme come Google, LinkedIn e la stessa X, consente di ampliare la portata della campagna raggiungendo utenti potenzialmente interessati, replicando i tratti dei destinatari originari (v. K. SUDHIR, S. Y. LEE, S. ROY, *Lookalike Targeting on Others' Journeys: Brand Versus Performance Marketing*, in *Cowles Foundation Discussion Papers*, 2644; A. POPOV, D. IAKOVLEVA, *Adaptive look-alike targeting in social networks advertising*, in *Procedia Computer Science*, 2018, pp. 255-264).

In proposito, la Commissione ha dichiarato che il pubblico di riferimento è stato selezionato sulla base di criteri demografici generali, come l'età (a partire dai 18 anni), la località (limitata ai Paesi Bassi) e la lingua (l'olandese). La campagna mirava inoltre a raggiungere persone con interessi legati all'educazione, alla tecnologia e all'informatica, individuate in base alle loro interazioni sulla piattaforma. A prima vista, nulla suggerisce un uso diretto di dati sensibili. Tuttavia, per ampliare l'impatto della campagna, sono state impiegate parole chiave legate a temi particolarmente delicati. In particolare, 36 segmenti di pubblico facevano riferimento a partiti politici (come AfD, Vox, Sinn Féin e l'English Defence League), a figure politiche specifiche (come Viktor Orbán, Marine Le Pen e Giorgia Meloni) o a posizioni euroscettiche e nazionalistiche, con termini come Brexit, Nexit e l'hashtag #EUCorruption. Altri sei segmenti riguardavano credenze religiose, con riferimenti a termini come cristianesimo, islam e persino anticristiano (punto 2.10). In questo modo, la Commissione europea, scegliendo di utilizzare la piattaforma X per una campagna pubblicitaria e definendo le modalità di raccolta e trattamento dei dati, come la selezione dei *target* e delle parole chiave, ha assunto il ruolo di titolare del trattamento, ai sensi dell'art. 3, par. 8 del Reg. 2018/1725, divenendo, di conseguenza, il responsabile del rispetto del Regolamento e il garante della protezione dei dati personali degli utenti coinvolti. A questo proposito, il GEPD ha richiamato un'analogia con il caso *Wirtschaftsakademie* (sentenza della Corte del 5 giugno 2018, causa C-210/16, *Wirtschaftsakademie/Facebook*, ECLI:EU:C:2018:388), in cui la Corte di giustizia ha stabilito che il creatore di una pagina fan sui *social media*, avvalendosi dei filtri di Facebook per definire i parametri di trattamento, ha assunto il ruolo di titolare del trattamento. Al contrario, secondo la Commissione, sarebbe

stata responsabilità della piattaforma garantire il rispetto delle proprie politiche e dei regolamenti vigenti nell'Unione, in particolare del RGPD, che stabilisce norme rigorose sulla gestione dei dati personali e sulla tutela della privacy, come previsto anche dalle policy di X.

In secondo luogo, la Commissione ha sostenuto che i trattamenti di dati personali derivanti dalla campagna sarebbero stati giustificati come necessari per l'adempimento di un compito di interesse pubblico, in conformità con l'art. 5, par. 1, lett. a) del Reg. 2018/1725 (punto 3.17). Questo compito si riferirebbe all'art. 17, par. 2 del Trattato sull'Unione europea (TUE), che attribuisce alla Commissione il diritto di iniziativa legislativa, comprese le attività di comunicazione relative a tale proposta. In altre parole, il trattamento dei dati personali nell'ambito della campagna pubblicitaria era legittimo e giustificato dalla necessità di informare il pubblico su una proposta legislativa, rientrando così nelle sue funzioni istituzionali (punto 3.16).

In ultimo, la Commissione ha sottolineato che non c'era alcuna intenzione di trattare dati sensibili e, qualora ciò fosse accaduto, sarebbe stato un evento involontario (punto 3.7).

3. Per il GEPD, la campagna di microtargeting della Commissione ha violato il diritto dell'Unione a tutela dei dati personali.

Date queste premesse, il Garante europeo si è pronunciato sulla condotta della Commissione, facendo riferimento a un consolidato orientamento giurisprudenziale della Corte di giustizia. Secondo tale giurisprudenza, l'intento del titolare del trattamento dei dati personali non costituisce un fattore determinante. Infatti, ciò che rileva è l'effettivo trattamento di dati particolari, indipendentemente dalle finalità perseguite (punto 4.46). Come sottolineato nel RGPD, il trattamento di categorie particolari di dati personali, stabilito all'art. 10, par. 1, è vietato a prescindere dalle intenzioni dichiarate, in quanto comporta significativi rischi per le libertà e i diritti fondamentali degli interessati (sentenza della Corte del 4 luglio 2023, causa C-252/21, *Meta Platforms Inc. e a. c. Bundeskartellamt* (Condizioni generali di utilizzo di un social network) EU:C:2023:537, punti 69 e 70; v. G. DE GREGORIO, O. POLLICINO, *Op-Ed: "Lessons for Digital Markets from Meta Platforms v. Bundeskartellamt (C-252/21)*" , in EULawLive, 27 July 2023).

Sugli altri aspetti del comportamento della Commissione, in merito alla necessità di svolgere un compito d'interesse pubblico (art. 5 Reg. 2018/1725) come giustificazione del trattamento dei dati che ha guidato la campagna pubblicitaria, il GEPD ha osservato che la disposizione in questione, al secondo comma, specifica come questo tipo di trattamento debba essere previsto da un atto o disposizione di diritto dell'Unione che abbia un contenuto chiaro, preciso e prevedibile (come indicato anche dal considerando 23 del regolamento). A tal proposito, il richiamo all'art. 17, par. 2 TUE non costituisce una base giuridica sufficientemente chiara e precisa per il trattamento dei dati personali nel contesto di campagne pubblicitarie mirate (punti 4.25 e 4.26). Inoltre, la citazione da parte della Commissione della sentenza *Nikolaou* (sentenza del Tribunale del 12 settembre 2007, causa T-259/03, *Nikolaou c. Commissione*, ECLI:EU:T:2007:254), al cui par. 219 si richiama anche la sentenza *Bergaderm* sentenza della Corte del 4 luglio 2000, causa C-352/98 P , *Bergaderm e Goupil c. Commissione*, ECLI:EU:C:2000:361), utilizzata per sostenere che le istituzioni europee possano svolgere attività di comunicazione anche senza una base legale esplicita è stata respinta come *case law*. Per il GEPD, il punto centrale e comune alle due cause riguarda la distinzione tra il possesso del potere di agire da parte degli organi e delle istituzioni dell'Unione e l'obbligo di rispettare le normative vigenti nell'esercizio di tale potere. In altre

parole, sebbene le istituzioni europee abbiano la facoltà di intraprendere determinate azioni, come adottare politiche di comunicazione o pubblicare comunicati stampa ufficiali, ciò non le esonera dal dovere di conformarsi alle normative applicabili, comprese quelle sulla protezione dei dati personali. Un esempio rilevante proviene dalla sentenza T-259/03, che ha stabilito che, pur avendo l'OLAF il diritto di comunicare pubblicamente le proprie attività, ciò non implicava automaticamente che avesse rispettato tutte le norme sulla protezione dei dati. Pertanto, sebbene le istituzioni abbiano la capacità di agire in ambito comunicativo, questo potere non le esime dal rispetto delle regole, soprattutto quando si tratta di trattamenti dei dati personali. Inoltre, sebbene il caso in esame differisca nei fatti, il trattamento dei dati nell'ambito di una campagna pubblicitaria mirata sui social media implica un livello di invasività decisamente maggiore rispetto alla semplice pubblicazione di comunicati stampa (punto 4.27).

Pertanto, l'unica base giuridica alternativa per il trattamento di categorie particolari di dati personali sarebbe stata il consenso esplicito dell'interessato, come previsto dall'art. 5, par. 1, lett. d) del Reg. 2018/1725. Tuttavia, la Commissione non ha raccolto tale consenso esplicito, come evidenziato dal GEPD (punto 4.34). Di conseguenza, il titolare del trattamento ha violato gli artt. 5, par. 1, lett. (a) e 5, par. 2, lett. (d) del Regolamento (UE) 2018/1725, trattando dati personali senza una base giuridica valida. Questo ha comportato la violazione del principio di liceità del trattamento, sancito dall'art. 4, par. 1, lett. a) dello stesso Regolamento (punto 4.36; sul controllo di liceità cfr. S. ORLANDO, *Sulla necessità di un controllo di liceità sostanziale per tutte le basi del trattamento dei dati personali*, in Persona e Mercato, 2024/3, p. 815 ss.). Inoltre, poiché la Commissione non è stata in grado di dimostrare la conformità del trattamento alle disposizioni del regolamento, il GEPD ha riscontrato anche una violazione degli artt. 4, par. 2 e 26 del Regolamento, che impongono al titolare del trattamento di garantire e, soprattutto, dimostrare il rispetto delle norme sulla protezione dei dati personali (punto 4.37).

Entrando nel merito dell'analisi, la questione si pone, in particolar modo, sulle deroghe all'utilizzo di categorie particolari di dati personali. La campagna pubblicitaria ha di fatto comportato il trattamento di dati sensibili, come opinioni politiche e credenze religiose. In particolare, l'art. 10, par. 1 del Reg. 2018/1725 stabilisce una proibizione generale al trattamento di tali dati, salvo che siano rispettate le specifiche deroghe previste al par. 2, che meritano di essere attentamente esaminate in quanto condizioni indispensabili per legittimare il trattamento in questione.

Da quanto precede, tra le eccezioni non applicabili alla condotta della Commissione vi sono il consenso esplicito dell'interessato (art. 10, par. 2, lett. a)), che non è stato raccolto, e il trattamento di dati manifestamente pubblici (art. 10, par. 2, lett. e)), che non risulta pertinente nel caso specifico, poiché le impostazioni di *privacy* più restrittive dell'utente non consentono di considerare i dati come manifestamente pubblici (punto 4.54). Affinché i dati possano essere qualificati come "manifestamente pubblici" (v. sentenza della Corte del 4 ottobre 2024, causa C-446/21, *Schrems c. Meta Platforms Ireland Ltd*, ECLI:EU:C:2024:834; sul concetto di dichiarazione pubblica di particolari categorie di dati, si consenta di rimandare a L. PIGNA, *Schrems c. Meta. La Corte di giustizia si pronuncia sui limiti al trattamento dei dati personali per fini di pubblicità mirata*, in Ordine Internazionale e Diritti Umani, 2024) è necessario che l'utente abbia configurato consapevolmente i parametri del proprio profilo utente in modo tale da renderli accessibili a un numero illimitato di persone; essi devono in pratica «aver esplicitamente acconsentito» (sentenza *Meta Platforms*, punto 83. Cfr. F. BATTAGLIA, *La sentenza Meta Platforms : Riflessioni in materia di valore dei dati e libera espressione del consenso*, in Ordine

Internazionale e Diritti Umani, 2023; sul consenso nel mercato digitale, si veda anche F. BATTAGLIA, *Il consumatore digitale nel diritto dell'Unione europea*, Napoli, 2023). In assenza di tali impostazioni o di un'adeguata informazione, i dati non possono essere considerati come tali.

Nel caso in questione, il ricorrente ha usato impostazioni di *privacy* più restrittive, limitando l'accesso alle proprie informazioni esclusivamente agli utenti con un account X che fossero anche suoi *followers* (punto 4.58). Inoltre, una recente sentenza della Corte di giustizia (sentenza della Corte del 4 ottobre 2024, causa C-446/21, *Maximilian Schrems/Meta Platforms Ireland Limited,* ECLI:EU:C:2024:834) ha chiarito che, anche quando i dati sono manifestamente pubblici, sebbene possano perdere il carattere di "specialità", il loro trattamento per la pubblicità politica personalizzata non è giustificato senza ulteriori garanzie legali (si veda anche *EDPS Supervisory Opinion of 09/11/2023 on the use of social media monitoring for epidemic intelligence purposes by the ECDC*, par. 65). In altre parole, una dichiarazione pubblica non equivale al consenso per il trattamento di ulteriori dati sensibili (*ibidem*, punto 82). Inoltre, la deroga prevista dall'art. 10, par. 2, lett. g), legata a un interesse pubblico sostanziale, non risulta applicabile nel caso specifico, poiché la Commissione non ha dimostrato che il trattamento fosse necessario e proporzionato a un interesse pubblico rilevante, nonostante il suo diritto di comunicare su tematiche legislative (punto 4.63).

Il Garante europeo della protezione dei dati ha quindi concluso che l'art. 10 del Reg. 2018/1725 è stato violato, in quanto il trattamento delle categorie particolari di dati personali non ha rispettato le condizioni di liceità previste (punto 4.65). In conseguenza di ciò, il GEPD ha emesso un richiamo nei confronti della Commissione europea per aver violato il Regolamento sulla protezione dei dati. Tuttavia, non sono state ritenute necessarie ulteriori misure correttive di conformità o limitazione del trattamento, in quanto la campagna pubblicitaria era stata interrotta al momento della pronuncia (punti 6.1 e ss.). La vicenda ha così messo in evidenza l'importanza di garantire che ogni trattamento di dati personali da parte delle istituzioni europee avvenga nel pieno rispetto delle normative vigenti, al fine di tutelare i diritti fondamentali dei cittadini.

4. La pubblicità politica nell'Unione europea. Gli elementi essenziali del nuovo quadro regolatorio sui servizi digitali e il Regolamento 2024/900.

Parlando di *microtargeting* politico e delle nuove sfide poste dell'uso delle tecnologie digitali, non si può fare a meno di sottolineare come, negli ultimi anni, l'Unione europea abbia compiuto significativi progressi nel cercare di regolamentare l'uso di queste tecniche, mirando a bilanciare l'innovazione tecnologica con la protezione dei diritti fondamentali dei cittadini. Ogniqualvolta gli utenti accedono alle piattaforme di *social media* o ad altri servizi digitali, i fornitori raccolgono e analizzano i dati personali. Queste informazioni vengono utilizzate per profilare le abitudini, gli interessi e le preferenze degli utenti, facilitando così il *microtargeting*, una strategia di *marketing* che sfrutta i dati raccolti per personalizzare i messaggi pubblicitari in base alle caratteristiche di ciascun individuo. La prassi ha dimostrato come attraverso la raccolta e l'analisi dei dati personali sia possibile realizzare campagne mirate che influenzano in modo capillare l'opinione pubblica. Inoltre, la targetizzazione degli elettori non solo incide sul processo democratico, ma pone anche rilevanti questioni relative alla *privacy* e alla protezione dei dati personali, così come coinvolge altri diritti e doveri fondamentali, come il diritto dei partiti politici e delle piattaforme digitali di diffondere informazioni, il diritto degli elettori di riceverle, e l'obbligo delle istituzioni di garantire elezioni libere ed eque (vedi qui).

Per regolamentare la pubblicità politica e le tecniche di profilazione basate sui dati personali, la Commissione europea, nell'ambito del piano d'azione per la democrazia, ha condotto all'adozione del regolamento sulla trasparenza e sul *targeting* della pubblicità politica. Tra gli obiettivi principali di tale piano vi è la promozione di elezioni libere ed eque, nonché la valutazione delle sfide poste dalle nuove tecnologie di indirizzamento pubblicitario.

La Commissione europea ha presentato il Regolamento come un atto giuridico innovativo e ambizioso, destinato a intervenire in un ambito tradizionalmente riservato alla competenza degli Stati membri. Fino ad oggi, infatti, l'intervento dell'Unione nei processi democratici nazionali è stato limitato e si è sostanzialmente basato su strumenti non vincolanti o, come nel caso del Regolamento Generale sulla Protezione dei Dati, su atti che trattano questioni generali senza entrare nel dettaglio della pubblicità politica (V. O. POLLICINO, *I codici di condotta tra self-regulation e hard law: esiste davvero una terza via per la regolazione digitale? Il caso della strategia europea contro la disinformazione online*, in *Riv. trim. dir. pub*, 2022). Con l'introduzione di questo nuovo regolamento, l'Unione europea compie un passo significativo verso la creazione di un quadro giuridico unificato, destinato a uniformare le diverse normative nazionali, stabilendo definizioni e regole comuni per garantire una maggiore trasparenza nel settore del *targeting* politico. (v. C. MASSA, *Proposta di regolamento sulla pubblicità politica nell'UE: più trasparenza e meno targeting,* in *il blog di AISDUE*, 2022). Adottato sulla base degli articoli 16 e 114 TFUE, il regolamento si propone di garantire una maggiore chiarezza sulle modalità di diffusione dei messaggi pubblicitari di natura politica, imponendo obblighi stringenti in materia di diligenza, utilizzo delle tecniche di *targeting* e trattamento dei dati personali. L'obiettivo dichiarato del regolamento è quindi duplice: da un lato, prevenire la frammentazione normativa tra gli Stati membri e assicurare la certezza del diritto per i prestatori di servizi di pubblicità politica; dall'altro, tutelare l'integrità del processo democratico, contrastando interferenze esterne e limitando l'uso improprio dei dati personali, in linea con i principi sanciti dal Reg. 2016/679 (RGPD) (sulla questione della scelta delle basi giuridiche si veda S. POLI, *Il rafforzamento della sovranità tecnologica europea e il problema delle basi giuridiche*, in *I Post di AISDUE*, 2021; M. INGLESE, *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno?*, in *Quaderni AISDUE*, 2024).

Per rimanere nell'ambito della presente analisi, il regolamento esclude dal suo campo di applicazione le comunicazioni effettuate dalle autorità pubbliche nazionali o dell'Unione relative alle procedure di voto, alla promozione della partecipazione alle elezioni o alla comunicazione finalizzata a fornire informazioni ufficiali al pubblico, a condizione che tali attività non siano intese a influenzare l'esito di un'elezione o di un referendum, né a condizionare un comportamento di voto o un processo legislativo o regolamentare (art. 3, par. 2, lett. i) e ii) del Reg. 2024/900). Rientra in questa fattispecie, a titolo di esempio, una campagna pubblicitaria politica, anche quando promossa dalle stesse istituzioni dell'Unione (v. E. STELLA, *La disciplina in materia di pubblicità politica del regolamento (Ue) 2024/900*, in *Eurojus.it*, 2024). Tra gli aspetti più rilevanti del regolamento, vi è il divieto di utilizzare tecniche di *targeting* che comportino il trattamento di categorie particolari di dati personali, quali l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose, l'appartenenza sindacale, nonché dati genetici, biometrici, relativi alla salute o alla vita sessuale, salvo che venga ottenuto il consenso esplicito dell'interessato (considerando 77). Il legislatore evidenzia infatti come un tale trattamento dei dati personali possa compromettere i diritti e le libertà fondamentali, come l'equità, la libertà di informazione e di scelta (artt. 11 e 21 della Carta dei diritti fondamentali dell'Unione europea) e influire negativamente sul processo democratico,

favorendo la frammentazione del dibattito pubblico, la comunicazione selettiva e la manipolazione dell'elettorato (considerando 74). In altre parole, l'uso di informazioni sensibili per finalità di profilazione pubblicitaria è vietato, a meno che l'utente non abbia prestato il proprio consenso informato e specifico, in accordo con l'art. 9 del RGPD e 10 del Reg. 2018/1725 (art. 18 Reg. 2024/900). Sebbene il RGPD vieti già il trattamento dei dati sensibili con alcune eccezioni, il regolamento riduce queste eccezioni all'ottenimento del consenso da parte del titolare del trattamento, eliminando dunque quelle non rilevanti per il *microtargeting* politico. Tuttavia, il Reg. 2022/2065 (*DSA*) introduce un divieto ancora più ampio, vietando qualsiasi forma di pubblicità mirata basata su dati sensibili (art. 26, par. 3). Di conseguenza, il Reg. 2024/900 ha il merito di includere formalmente il *microtargeting* politico nel quadro normativo europeo, non aggiungendo tutele aggiuntive o specifiche (v. M. Z. VAN DRUNEN, N. HELBERGER, R. Ó FATHAIGH, *The beginning of EU political advertising law: unifying democratic visions through the internal market*, in International Journal of Law and Information Technology, 2022, pp. 187-188).

Oltre a una serie di obblighi di trasparenza cui deve conformarsi un messaggio di pubblicità politica (contenuto, lo sponsor, il linguaggio utilizzato, il contesto, i mezzi di diffusione, il pubblico destinatario e l'obiettivo, apposizione di etichette (artt. 8 e ss. Reg. 2024/900), i titolari del trattamento sono soggetti a obblighi aggiuntivi di trasparenza, tra cui la divulgazione della logica e dei parametri dietro le tecniche di *targeting*, compreso l'uso di sistemi di intelligenza artificiale (art. 19 Reg. 2024/900). I titolari devono anche pubblicare le loro politiche interne sul *targeting* e sulla diffusione degli annunci per un periodo di sette anni.

Alle autorità di controllo nazionali sulla *privacy* e la protezione dei dati personali e al garante europeo è stato affidato il potere di monitorare la corretta applicazione delle disposizioni espressamente dedicate al *targeting* politico (art. 22, par. 1 Reg. 2024/900; si tratta degli artt. 18 e 19); sui restanti articoli il controllo è affidato alle autorità che gli Stati membri designano per l'osservanza del Reg. 2022/2065 (art. 22, par. 3 Reg. 2024/900).

Sempre in tema di *advertising* politico, merita una speciale menzione l'art. 39 del DSA, che impone alle *Very Large Online Platforms* (*VLOPs*) e ai *Very Large Online Search Engines* (*VLOSEs*), che ospitano pubblicità sulle loro interfacce *online*, l'obbligo di compilare e rendere accessibile al pubblico un registro contenente specifiche informazioni relative agli annunci pubblicitari (anche di natura politica), con l'obiettivo di garantire maggiore trasparenza e responsabilità. In particolare, bisogna indicare se la pubblicità sia destinata a specifici gruppi di destinatari, precisando i principali parametri utilizzati per la profilazione e, se presenti, quelli impiegati per escludere determinati gruppi (V. S. TOMMASI, *The liability of internet service providers in the proposed Digital Services Act*, in European Review of Private Law, 2021, pp. 925-944; P. VAN CLEYNEN-BREUGEL, *The Commission's Digital Services and Markets Act Proposal: First Step towards Tougher and more Directly Enforced EU Rules?,* in Maastricht Journal of European and Comparative Law, 2021, pp. 667-686; M.L. CHIARELLA , *Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment*, in Athens Journal of Law, 2023, pp. 33-58). A tal proposito, il Reg. 2024/900, oltre a ribadire i doveri di diligenza a carico degli editori di pubblicità digitale, come le piattaforme, istituisce un ulteriore registro europeo dei messaggi di pubblicità politica, sotto la responsabilità della Commissione europea. Questo registro consente l'accesso dei cittadini ai messaggi pubblicitari politici e prevede un servizio di hosting per tali messaggi, fino a 7 anni dalla loro prima pubblicazione. Inoltre, le *VLOPs* e le *VLOSEs* devono consentire l'accesso ai propri registri e ai messaggi di pubblicità politica *ivi* contenuti attraverso tramite il nuovo registro europeo (art. 13, par. 2 Reg. 2024/900). Questa misura ha lo scopo di rafforzare la trasparenza nel settore della

pubblicità *online*, consentendo un controllo più efficace da parte del pubblico e delle autorità di regolamentazione sulle pratiche di *targeting* e sulla diffusione dei contenuti sponsorizzati. Inoltre, favorisce un monitoraggio più approfondito delle strategie pubblicitarie adottate dalle grandi piattaforme, contribuendo a contrastare la disinformazione e a tutelare i diritti fondamentali degli utenti (Cfr. E. BIRRITTERI, *Contrasto alla disinformazione, Digital Services Act e attività di private enforcement: fondamento, contenuti e limiti degli obblighi dicompliance e dei poteri di autonormazione degli operatori*, in *mediaLAWS*, 2023; A. TURILLAZZI, M. TADDEO, L. FLORIDI, F. CASOLARI, *The digital services act: an analysis of its ethical, legal and social implications*, in *Law, Innovation and Technology*, 2023).

Il quadro normativo in tema di trasparenza e controllo della pubblicità politica *online* si completa con il riferimento all'art. 46 del Reg. 2022/2065, con cui la Commissione incoraggia l'elaborazione di codici di condotta volontari a livello di Unione da parte dei fornitori di piattaforme *online*, i quali devono perseguire un'efficace trasmissione delle informazioni, che rispetti pienamente i diritti e gli interessi di tutte le parti coinvolte, nonché un ambiente competitivo, trasparente ed equo nella pubblicità *online*, conformemente al diritto dell'Unione e nazionale (G. VASINO, *Censura 'privata' e contrasto all'hate speech nell'era delle Internet Platforms*, in *federalismi.it*, 2023, p. 147 e s.).

Già in occasione delle elezioni del Parlamento europeo del 2019, la Commissione europea aveva pubblicato il Codice di buone pratiche sulla disinformazione, basato sulla collaborazione con le principali piattaforme digitali, in seguito al caso *Facebook/Cambridge Analytica*, che aveva sollevato gravi preoccupazioni sull'impatto delle violazioni della protezione dei dati nei principali appuntamenti elettorali di quegli anni (v. T. DOBBER, R. O FATHAIGH, F. J. ZUIDERVEEN BORGESIUS, *The regulation of online political micro-targeting in Europe*, in *Internet Policy Review*, 2019, p. 12).

Il codice è stato revisionato e rafforzato nel 2022, e infine integrato alla Legge sui servizi digitali, il 13 febbraio 2025 ad opera della Commissione europea e del comitato europeo per i servizi digitali. Tra i vari impegni contenuti nel codice, i firmatari (tra cui *VLOP* e *VLOSE* come Facebook, Instagram, LinkedIn, Bing, TikTok, YouTube e Google Search) si sono impegnati a «promuovere la trasparenza nella pubblicità politica e a garantire una maggiore tutela dei dati personali utilizzati per la pubblicità politica mirata, rispettando pienamente il Regolamento generale sulla protezione dei dati e le altre normative applicabili, soprattutto in relazione all'ottenimento di un consenso valido, quando richiesto» (*Code of Conduct on Disinformation, Chapter III, lett. g*).

Tale cornice normativa è in gran parte già applicabile e con un impatto significativo sulle dinamiche di interazione tra gli attori del mercato digitale. Obiettivo primario dell'esecutivo dell'Unione è quello di proteggere i suoi cittadini, permettere loro di cogliere le nuove opportunità dell'era digitale ma allo stesso tempo costruire un futuro digitale su temi quali la fiducia e la sicurezza *online*.

5. Considerazioni conclusive

Alla luce di quanto esaminato, la portata della vicenda legata al *microtargeting* politico da parte della Commissione europea, unitamente alle conseguenze di un intervento normativo così vasto e stratificato, lascia spazio a più osservazioni di sintesi e quesiti.

In primo luogo, rimanendo sempre nel contesto di un uso "politico" o "elettorale" dei dati personali, l'ammonimento del Garante europeo della protezione dei dati nei confronti della Commissione non è certamente il primo caso di richiamo mosso nei confronti

di un'istituzione dell'Unione (si veda a tal riguardo l'inchiesta del 2019 del GEPD sull'uso da parte del Parlamento europeo della società statunitense *NationBuilder* per la raccolta e il trattamento di dati personali durante la campagna per le elezioni europee del 2019). In tal senso, vale la pena di sottolineare che, subito dopo la censura emessa da parte del GEPD, il Tribunale dell'Unione ha emesso una sentenza di risarcimento danni a carico della Commissione in favore di un cittadino tedesco (v. sentenza del Tribunale del 8 gennaio 2025, causa T-354/22, *Bindl/Commissione,* ECLI:EU:T:2025:4). La Commissione, in quanto responsabile del trattamento dei dati personali relativi al sito Internet della Conferenza sul futuro dell'Europa, ha violato le disposizioni del Reg. 2018/1725 (art. 46 e *ss.*), stavolta in relazione al trasferimento di dati personali verso Paesi terzi rispetto agli Stati membri dell'Unione. In particolare, la possibilità per gli utenti di iscriversi agli eventi *online* della *CAE* utilizzando i propri *account* Facebook attraverso il servizio di autenticazione *EU Login*, ha comportato un trasferimento dei dati degli utenti europei verso i server Meta ubicati negli Stati Uniti. Le sentenze *Schrems* (sentenza della Corte del 6 ottobre 2015, causa C-362/14, Schrems, ECLI:EU:C:2015:650; sentenza della Corte del 16 luglio 2020, causa C-311/18, *Schrems II*, ECLI:EU:C:2020:559) hanno già dimostrato che gli Stati Uniti non forniscono garanzie a tutela dei dati personali adeguate agli standard europei. Dunque, senza ulteriori garanzie, come l'utilizzo di clausole contrattuali *ad hoc* (art. 48), la Commissione si è trovata a dover rispondere di comportamenti in contrasto con il diritto dell'Unione a protezione dei dati personali.

In secondo luogo, tornando al caso in esame, la decisione del GEPD si è concentrata esclusivamente sull'analisi del trattamento dei dati attribuibile alla sola Commissione, in quanto rientrante sotto la sua diretta responsabilità. (art. 52 Reg. 2018/1725). Allo stesso tempo, il GEPD ha riconosciuto la possibilità che la piattaforma X abbia stabilito congiuntamente con la Commissione europea le finalità e i mezzi del trattamento dei dati personali, configurandosi così come contitolare del trattamento (punto 4.13 *reprimand*). In tal senso, X avrebbe violato il *Digital Services Act* (*DSA*), in particolare l'art. 26, par. 3 del Reg. 2022/2065, che vieta alle piattaforme *online* di mostrare annunci pubblicitari basati sulla profilazione automatizzata utilizzando categorie particolari di dati personali (come convinzioni politiche, religiose o orientamento sessuale), come definito nell'art. 9, par. 1 del RGPD, senza rispettare le eccezioni previste dall'art. 9, par. 2 del medesimo regolamento.

Orbene, la Commissione europea, che è responsabile della supervisione del rispetto del DSA su piattaforme come X, è stata direttamente coinvolta nella violazione. In effetti, poco dopo l'avvio della campagna di pubblicità politica, l'esecutivo ha avviato una procedura d'infrazione nei confronti di X per presunte violazioni della legge sui servizi digitali. Il procedimento riguarda, in particolare, l'uso improprio della spunta blu per la verifica degli account, la mancanza di trasparenza sui dati e sulle pubblicità, e l'efficacia del nuovo sistema di fact-checking per la moderazione dei contenuti sulla piattaforma. Questa situazione ha evidenziato, a parere dello scrivente, un ruolo ambiguo della Commissione, la quale, se da un lato ha richiesto ai propri dipendenti di interrompere la pubblicità a pagamento su X (come indicato nel punto 3.25 del *reprimand*), al fine di evitare possibili sanzioni, dall'altro non ha intrapreso, e a questo punto non ha potuto intraprendere, azioni concrete e immediate contro X per il *targeting* pubblicitario illecito (vedi qui).

In terzo luogo, risulta difficile comprendere il comportamento della Commissione europea che, proprio nello stesso periodo nel quale lanciava e gestiva la campagna di comunicazione oggetto del provvedimento del GEPD, adottava il Regolamento (UE) 2024/900 del Parlamento europeo e del Consiglio del 13 marzo 2024 relativo alla trasparenza

e al *targeting* della pubblicità politica, destinato a trovare piena applicazione a decorrere dal prossimo 10 ottobre 2025.

In conclusione, l'analisi della vicenda si inserisce nel più ampio dibattito sull'impatto delle nuove tecnologie nei processi democratici e sui rischi derivanti dall'uso non trasparente di strumenti di *microtargeting* e profilazione. La recente prassi ha dimostrato come anche le istituzioni europee possano incorrere in pratiche potenzialmente lesive della *privacy* e della trasparenza. Allo stesso tempo ha evidenziato l'importanza del ruolo delle piattaforme digitali. A tal riguardo, le recenti decisioni come quelle di YouTube e Meta (vedi qui), che hanno scelto di affidarsi prevalentemente alle segnalazioni degli utenti per il controllo dei contenuti, sollevano ulteriori dubbi sulla loro reale adesione alle disposizioni del *Digital Services Act* e sulla capacità di affrontare in modo efficace fenomeni come la disinformazione e la propaganda politica. La scelta di alcuni operatori di ridimensionare gli impegni volontari, come il ritiro di X dal Codice di condotta sulla disinformazione (vedi qui), evidenzia la difficoltà di applicare regole uniformi e stringenti in un panorama digitale in costante evoluzione. Sebbene l'uso di tecnologie avanzate, comprese quelle basate sull'intelligenza artificiale, non sia vietato, è evidente la necessità di una regolamentazione chiara e rigorosa che bilanci l'innovazione con la tutela dei diritti fondamentali (per un'analisi giuridica in proposito, si veda C. AMALFITANO, F. FERRI, *Transizione digitale e dimensione costituzionale dell'Unione europea: tra principi, diritti e valori*, in R. TORINO, S. ZORZETTO (a cura di), *La trasformazione digitale in Europa. Diritti e principi*, Torino, 2023, pp. 1-34). L'Unione europea, attraverso un sistema di co-regolamentazione con le piattaforme digitali e un quadro normativo sempre più articolato, ha avviato una risposta legislativa significativa per contrastare disinformazione e profilazione illecita. Al momento, è ancora troppo presto per valutarne l'efficacia, che molto dipenderà dalla capacità di adattare le nuove misure ai rapidi sviluppi tecnologici e dall'impegno costante da parte di tutti gli attori coinvolti, sia pubblici che privati. In questo scenario, l'ammonimento del GEPD rappresenta, dunque, non solo un richiamo alla responsabilità per le istituzioni dell'Unione, ma anche un invito più ampio a riflettere sulla tutela della democrazia nell'era digitale.

LUIGI PIGNA