

Giovanni Di Gregorio

**SOCIAL NETWORK,
CONTITOLARITÀ DEL
TRATTAMENTO E STABILIMENTO:
LA DIMENSIONE
COSTITUZIONALE DELLA TUTELA
DEI DATI PERSONALI TRA
VECCHIE E NUOVE PROSPETTIVE**

Estratto



Milano • Giuffrè Editore

**CORTE DI GIUSTIZIA UE
GRANDE SEZIONE**
**5 GIUGNO 2018
CAUSA C-210/16**
PRESIDENTE: LENAERTS

RELATORE: TIZZANO

AVV. GENERALE: BOT

PARTI: DATENSCHUTZ

SCHLESWIG-HOLSTEIN,

WIRTSCHAFTSAKADEMIE

SCHLESWIG-HOLSTEIN,

FACEBOOK IRELAND

Dati personali • Responsabile del trattamento • Social network • Amministratore di pagina • Sussiste • Responsabilità congiunta con il titolare del social network

L'articolo 2, lettera d), della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, deve essere interpretato nel senso che la nozione di «responsabile del trattamento», ai sensi di tale disposizione, include l'amministratore di una fanpage presente su un social network.

• Dati personali • Autorità per la protezione dei dati • Competenza • Filiale di impresa stabilita in altro Stato membro • Mera funzione di raccolta della pubblicità • Irrilevanza

Gli articoli 4 e 28 della direttiva 95/46 devono essere interpretati nel senso che, qualora un'impresa stabilita al di fuori dell'Unione europea disponga di varie filiali in diversi Stati membri, l'autorità di controllo di uno Stato membro è autorizzata a esercitare i poteri che le conferisce l'articolo 28, paragrafo 3, di tale direttiva nei confronti di una filiale di detta impresa situata sul territorio di tale Stato membro anche se, in base alla ripartizione delle funzioni all'interno del gruppo, da un lato, tale filiale è compe-

tente solamente per la vendita di spazi pubblicitari e per altre attività di marketing sul territorio di detto Stato membro e, dall'altro, la responsabilità esclusiva per la raccolta e per il trattamento dei dati personali grava, per l'intero territorio dell'Unione europea, su una filiale situata in un altro Stato membro.

• Dati personali • Autorità per la protezione dei dati • Responsabile del trattamento con sede in altro Stato membro • Coordinamento • Necessità • Non sussiste.

L'articolo 4, paragrafo 1, lettera a), e l'articolo 28, paragrafi 3 e 6, della direttiva 95/46 devono essere interpretati nel senso che, qualora l'autorità di controllo di uno Stato membro intenda esercitare, nei confronti di un organismo stabilito sul territorio di tale Stato membro, i poteri d'intervento di cui all'articolo 28, paragrafo 3, di tale direttiva a motivo di violazioni delle disposizioni relative alla protezione dei dati personali, commesse da un terzo responsabile del trattamento di tali dati che ha la propria sede in un altro Stato membro, tale autorità di controllo è competente a valutare, in modo autonomo rispetto all'autorità di controllo di quest'ultimo Stato membro, la liceità di un siffatto trattamento di dati e può esercitare i suoi poteri d'intervento nei confronti dell'organismo stabilito sul proprio territorio senza previamente richiedere l'intervento dell'autorità di controllo dell'altro Stato membro.

* La sentenza per esteso è pubblicata retro su questa Rivista 2018, 310.

**SOCIAL NETWORK,
CONTITOLARITÀ DEL
TRATTAMENTO E
STABILIMENTO: LA
DIMENSIONE
COSTITUZIONALE DELLA
TUTELA DEI DATI
PERSONALI TRA VECCHIE E
PROSPETTIVE PASSATE E
FUTURE**

**1. DICOTOMIE COMPLEMENTARI:
DALLA PRIVACY ALLA TUTELA DEI DATI
PERSONALI COME DALLA DIMENSIONE
ATOMICA ALLA SFERA DIGITALE.**

Il riconoscimento costituzionale della tutela della riservatezza e della protezione dei dati personali può essere considerato come il risultato di un percorso europeo partito dall'evoluzione del concetto di *privacy* di matrice statunitense, inizialmente basato esclusivamente sul diritto alla riservatezza. Da una prospettiva meramente negativa (*the right to be left alone*) connotata da una predominante caratterizzazione personalista frutto delle

istanze borghesi tipiche dello Stato liberale ¹, il diritto alla *privacy* ha conosciuto un'evoluzione che ha portato alla definizione di una sua dimensione positiva consistente nel diritto alla tutela dei dati personali ², sviluppo che può essere ricondotto principalmente all'incremento delle attività di utilizzo e trattamento dei dati consentito, in particolare, dal progresso delle nuove tecnologie digitali. Ed è qui che si comprende come la dicotomia *offline-online* si intreccia con quella *privacy-data protection*, proprio perché l'emersione della dimensione positiva del diritto alla *privacy* è strettamente collegata (seppur non esclusivamente) allo sviluppo della società dell'informazione ³. In altre parole, se il diritto alla riservatezza fino a prima dell'introduzione delle moderne tecnologie digitali bastava a soddisfare le esigenze di tutela dell'individuo, nella società dell'informazione il trattamento diffuso dei dati personali (basti pensare recentemente al tema dei Big Data) ha reso non più sufficiente tutelare esclusivamente la dimensione negativa del suddetto diritto fondamentale.

Nel caso di specie ⁴, il rapporto tra le due dicotomie emerge in modo rilevante dal momento che le scelte che hanno condotto la Corte di

¹ S. D. WARREN, L. D. BRANDEIS, *The right to privacy*, in *Harvard Law Review* 4, 1890, p. 193 ss.;

² Per alcuni riferimenti sul tema v. O. POLLICINO, M. BASSINI, *Trattamento dei dati personali e ordine di protezione europeo: alla ricerca di un punto di equilibrio*, in H. Belluta, M. Ceresa-Gastaldo (a cura di), *L'ordine europeo di protezione: La tutela delle vittime di reato come motore della cooperazione giudiziaria*, Torino, 2016, p. 122 ss.; G. F. FERRARI, *La tutela dei dati personali dopo il Trattato di Lisbona*, in ID. (a cura di), *La tutela dei dati personali in Italia 15 anni dopo. Tempo di bilanci e di bilanciamenti*, Egea, 2012, p. 19; F. PIZZETTI, *La privacy come diritto fondamentale al trattamento dei dati personali nel*

Trattato di Lisbona, in P. Bilancia, M. D'Amico (a cura di), *La nuova Europa dopo il Trattato di Lisbona*, Giuffrè, 2009, p. 83 ss.; S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, 2006; R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, 2003.

³ Sull'influenza del fattore tecnologico si v. P. COSTANZO, *Il fattore tecnologico e le sue conseguenze*, in *Rass. Parl.* 54, 2012, p. 811 ss.; O. POLLICINO, *La "transizione" dagli atomi ai bit nel reasoning delle Corti europee*, in *Ragion pratica* 44, 2015, p. 53 ss.

⁴ Corte di giustizia, sentenza *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388.

giustizia (di seguito, anche “Corte” o “CGUE”) alla decisione che verrà di seguito analizzata possono essere collocate in un filone giurisprudenziale europeo che mira a garantire un’elevata tutela del diritto alla protezione dei dati personali *online* nonché, a tale scopo, ad estendere il diritto europeo in materia di *privacy* a soggetti che offrono servizi digitali non stabiliti nell’Unione.

Tale orientamento giurisprudenziale risulta essere frutto del percorso di costituzionalizzazione del diritto alla tutela dei dati personali in Europa. A seguito del riconoscimento a livello internazionale ⁵ nonché della suddetta evoluzione del modello statunitense, il diritto alla *privacy* è approdato in Europa trovando dimora a livello regionale nella Convenzione Europea dei Diritti dell’Uomo (di seguito, anche “CEDU”) che ha riconosciuto il rispetto della vita privata e familiare quale diritto fondamentale ⁶.

Inizialmente affermatosi in Europa anche in questo caso nella sua dimensione negativa, come già accennato, il diritto alla *privacy*, pur mantenendo la sua originale connotazione di *right to be let alone*, ha conosciuto un’evoluzione che ha portato al riconoscimento costituzionale della tutela dei dati personali. Tra i fattori che hanno contribuito in questo senso, è necessario sottolineare il ruolo delle nuove tecnologie che hanno permesso il trattamento di grandi quantità di dati anche in modo automatizzato utilizzate sia dall’attore pubblico al fine di soddisfare i propri obblighi positivi derivanti dalle prestazioni sociali nonché dai soggetti privati ai fini della propria attività d’impresa ⁷. In altre parole, l’evoluzione tecnologica ha reso non più sufficiente garantire il diritto alla riservatezza richiedendo una tutela aggiuntiva che si estendesse anche alle attività riguardanti il trattamento dei dati personali. Ancora una volta, il Consiglio d’Europa ha svolto un ruolo cruciale in tale transizione attraverso l’adozione della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione n. 108/1981) il cui scopo, per la prima volta in Europa, non mirava esclusivamente a garantire la tutela della vita privata ma anche dei dati personali ⁸.

⁵ In particolare, v. la Dichiarazione Universale dei Diritti dell’Uomo adottata dall’Assemblea Generale delle Nazioni Unite il 10 dicembre 1948. In particolare, l’art. 12 prevede: “Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesioni del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni”. In seguito occorre menzionare la Convenzione internazionale sui diritti civili e politici del 1966, il cui art. 17 para. 1 sancisce “Nessuno può essere sottoposto ad interferenze arbitrarie o illegittime nella sua vita privata, nella sua famiglia, nella sua casa o

nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione”.

⁶ L’art. 8, para. 1 CEDU prevede: “Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza”. In merito v. V. ZENO-ZENCOVICH, *Art. 8*, in S. Bartole, B. Conforti, G. Raimondi (a cura di), *Commentario alla convenzione europea per la tutela dei diritti dell’uomo e delle libertà fondamentali*, Cedam, 2001, p. 307 ss.

⁷ Si v. O. Pollicino, M. Bassini, op cit., p. 128.

⁸ Secondo l’art. 1 della Convenzione: “Scopo della presente Convenzione è quello di garantire, sul territorio di ogni Parte, ad ogni persona fisica, qualunque siano la sua cittadinanza o residenza, il rispetto dei di-

Se, in quel periodo, il Consiglio d'Europa poteva essere considerato il promotore dello sviluppo della dimensione costituzionale del diritto alla tutela dei dati personali, tale considerazione non può essere estesa all'Unione europea, dove la Direttiva 95/46/CE (di seguito, "Direttiva Privacy")⁹ ha disciplinato il trattamento dei dati personali prima che la relativa tutela costituzionale fosse riconosciuta dalla Carta di Nizza¹⁰ nel 2000, seppur senza alcuna vincolatività fino all'entrata in vigore del Trattato di Lisbona nel 2009¹¹. Al fine di comprendere il motivo di tale differente approccio, è sufficiente analizzare il testo della Direttiva Privacy che mette in luce il carattere funzionale (e non fondamentale) della tutela dei dati personali al consolidamento e al buon funzionamento del mercato unico e, di conseguenza, come strumento al fine di garantire le libertà fondamentali dell'Unione¹².

In questo scenario basato sulla prevalenza della dimensione economico-funzionale della tutela dei dati personali, il ruolo della Corte è stato fondamentale nel processo di consolidamento ed emancipazione del diritto alla tutela dei dati personali come autonomo diritto fondamentale, da un lato, riconoscendo la sua rilevanza costituzionale nel caso *Promusicae*¹³, seppur funzionale a garantire la tutela della vita privata¹⁴, dall'altro, rafforzando la tutela di tale diritto fondamentale come appare particolarmente chiaro nelle decisioni in materia di *digital privacy*¹⁵ nello scenario successivo all'entrata in vigore del Trattato di Lisbona.

ritti e delle libertà fondamentali, ed in particolare del diritto alla vita privata, nei confronti dell'elaborazione automatizzata dei dati di carattere personale che la riguardano ("protezione dei dati")".

⁹ Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, OJ L 281, 23.11.1995, p. 31.

¹⁰ L'art. 8, para. 1 della Carta prevede: "Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano".

¹¹ Art. 6 TUE.

¹² Prendendo ad esempio il Considerando 3 della Direttiva Privacy, questo recita: "considerando che l'instaurazione e il funzionamento del mercato interno, nel quale, conformemente all'articolo 7 A del trattato, è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali, esigono non solo che i dati personali possano circolare liberamente da uno Stato membro all'altro, ma che siano altresì salvaguardati i diritti fondamentali della persona".

¹³ Corte di giustizia, sentenza *Promusicae*, C-275/06, ECLI:EU:C:2008:54. In questo caso, la Corte ha osservato: "Tuttavia, occorre rilevare che nella controversia in relazione alla quale il giudice del rinvio ha sollevato tale questione risulta coinvolto, oltre ai due suddetti diritti, anche un altro

diritto fondamentale, vale a dire quello che garantisce la tutela dei dati personali e, quindi, della vita privata" (punto 63). Occorre però considerare una successiva pronuncia in cui la Corte ha basato la sua decisione soltanto sulla tutela della riservatezza, v. sentenza *Satamedia*, C-73/07, ECLI:EU:C:2008:727. In particolare: "Una siffatta conciliazione è prevista all'art. 9 della direttiva. Come emerge in particolare dal trentasettesimo 'considerando' della direttiva, l'art. 9 di quest'ultima persegue la finalità di conciliare due diritti fondamentali, vale a dire, da un lato, la tutela della vita privata e, dall'altro, la libertà di espressione" (punto 54). Sul percorso di costituzionalizzazione della tutela dei dati personali v. O. LYNKEY, *Deconstructing data protection: the 'added value' of a right to data protection in the EU legal order*, in *International and Comparative Law Quarterly* 63, 2014, p. 569 ss; P. DE HERT, S. GUTWIRTH, *Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action*, in S. GUTWIRTH, Y. POULLET, P. DE HERT, J. NOUWT, C. DE TERWANGNE (Eds.), *Reinventing Data Protection*, Dordrecht, 2009.

¹⁴ J. KOKOTT, C. SOBOTTA, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, in *IDPL* 3, 2013, p. 222 ss.

¹⁵ Sul punto v. Corte di giustizia, sentenza *Digital Rights Ireland*, cause riunite C-293/12 e C-594/12, ECLI:EU:C:2014:238;

Il processo di costituzionalizzazione della protezione dei dati personali sembra aver trovato compimento non solo nell'inclusione in un *bill of rights* quale la Carta di Nizza e nel riconoscimento nel diritto primario dell'Unione¹⁶ ma anche nell'adozione del Regolamento (UE) 679/2016 (di seguito, "Regolamento" o "GDPR")¹⁷ il cui scopo primario è proprio quello di garantire la tutela dei dati personali quale diritto fondamentale dell'interessato¹⁸.

Avendo a mente le considerazioni fin qui svolte, occorre concentrarsi con maggiore attenzione sulla decisione in epigrafe che merita di essere analizzata attraverso due profili distinti. La Corte si è focalizzata, da un lato, sulla qualificazione soggettiva dell'amministratore di una *fanpage* su Facebook in base alla Direttiva Privacy riconoscendo una contitolarità del trattamento tra l'amministratore e il *social network* motivata fonda-

sentenza *Google Spain*, C-131/12, ECLI:EU:C:2014:317; sentenza *Schrems*, C-362/14, ECLI:EU:C:2015:650. In dottrina tra i numerosi contributi sul caso *Schrems v. O. POLLICINO, M. BASSINI, Bridge Is Down, Data Truck Can't Get Through...A Critical View of the Schrems Judgment in the Context of European Constitutionalism*, in G. ZICCARDI CAPALDO (ed.), *The Global Community Yearbook of International Law and Jurisprudence 2016*, Oxford, 2017, p. 245 ss.; G. FINOCCHIARO, *La giurisprudenza della Corte di giustizia in materia di dati personali. Da Google Spain a Schrems*, in *Dir. Inf.* 4-5, 2015, p. 779 ss. Sul caso *Google Spain*, v. G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015. O. POLLICINO, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale, in federalismi.it*, 24 novembre 2014; ID., *Diritto all'oblio e conservazione di dati. La Corte di giustizia a piedi uniti: verso un digital right to privacy*, in *Giur. Cost.* 3, 2014, p. 2949 ss.; T.E. FROSINI, *Diritto all'oblio e Internet, in federalismi.it*, 10 giugno 2014; F. PIZZETTI, *La decisione della Corte di giustizia sul caso Google Spain: più problemi che soluzioni*, ivi, 10 giugno 2014; G.E. VICEVANI, *Identità, oblio, informazione e memoria in viaggio da Strasburgo a Lussemburgo, passando per Milano*, in *Danno e resp.* 7, 2014, p. 731 ss.; O. POLLICINO, M. BASSINI, *Reconciling Right to Be Forgotten and Freedom of Information: Past and Future of Persona Data Protection in Europe*, in *DPCE* 2, 2014, p. 641 ss.; M. BASSINI, *Il diritto all'oblio ai tempi di Internet: la Corte di giustizia sui motori di ricerca*, in *Quad. cost.* 3, 2014, p. 730 ss. Sul caso *Digital Rights Ireland*, v. L. TRUCCO, *Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giur. it.*, 2014, 8-9, 1850 ss.; F. FABBRINI, *The European Court of Justice Ruling in the*

Data Retention Case and its Lessons for Privacy and Surveillance in the U.S., *Harvard Human Rights Journal* 28, 2015, p. 65 ss.; A. VEDASCHI, V. LUBELLO, *Data retention and its implications for the fundamental right to privacy: a European perspective*, in *Tilburg Law Review* 20, 2014, p. 14 ss.; R. FLOR, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. «data retention» contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Riv. Trim. Dir. Pen. Contemp.* 2, 2014, p. 178 ss.

¹⁶ Art. 16 TFUE.

¹⁷ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), OJ L 119, 4.5.2016, p. 1.

¹⁸ Secondo i Considerando 1-2: "(1) La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. (2) I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche".

mentalmente dalla necessità di tutelare l'interessato, garantendo quindi, una maggiore protezione del suo diritto fondamentale alla protezione dei dati in ambito digitale.

Dall'altro, la Corte si è trovata a dover interpretare la nozione di stabilimento di cui all'art. 4 della Direttiva Privacy al fine di rispondere al quesito se l'autorità di controllo di uno Stato membro potesse esercitare i propri poteri nei confronti di una filiale di un'impresa stabilita al di fuori dell'Unione europea che disponga di varie filiali in diversi Stati membri tra cui lo Stato membro dell'autorità di controllo, anche se, in base alla ripartizione delle funzioni all'interno del gruppo, da un lato, tale filiale è competente solamente per la vendita di spazi pubblicitari e per altre attività di *marketing* sul territorio di detto Stato membro e, dall'altro, la responsabilità esclusiva per la raccolta e per il trattamento dei dati personali grava, per l'intero territorio dell'Unione europea, su una filiale situata in un altro Stato membro. In questo caso, come si avrà modo di sottolineare nel proseguo, la decisione è stata essenzialmente giustificata dalla necessità di estendere l'applicazione del diritto alla *privacy* di matrice europea anche a soggetti non residenti nell'Unione, tutto ciò nuovamente al fine di garantire una tutela effettiva, e non solo formale, del diritto alla protezione dei dati personali che verrebbe altrimenti frustrato se, specialmente nel contesto digitale, un soggetto potesse sottrarsi dal rispetto delle regole europee soltanto in virtù della propria collocazione geografica.

Occorre, inoltre, preliminarmente osservare che, seppur tale decisione sia basata *ratione temporis* sull'applicazione delle regole previste dalla Direttiva Privacy, tuttavia risulta opportuno inquadrare sia l'istituto della contitolarità sia la nozione di stabilimento alla luce del Regolamento al fine di poter comprendere i profili evolutivi della questione ¹⁹.

2. I FATTI OGGETTO DI CAUSA

La vicenda che sta alla base della decisione della Corte qui commentata prende le mosse dalle attività di una società tedesca (Wirtschaftsakademie) impegnata a offrire servizi di formazione attraverso una *fanpage* di Facebook.

Il problema era sorto dal momento che all'epoca dei fatti né la Wirtschaftsakademie né Facebook Ireland avevano informato gli utenti della *fanpage* del fatto che il *social network* raccoglieva attraverso l'impiego di *cookie* le informazioni personali dei visitatori elaborandole in un momento successivo. Ed è per questo motivo che l'autorità di controllo tedesca competente ordinava alla società tedesca di disattivare la *fanpage* nel novembre 2011.

¹⁹ Per un commento analitico del Regolamento v., tra gli altri, G. FINOCCHIARO (diretto da), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017; S. SICA, V. D'ANTONIO, G. M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Assago, 2016; L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il*

Regolamento Privacy europeo, Milano, 2016. F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali: Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016; ID., *Privacy e il diritto europeo alla protezione dei dati personali: Il Regolamento europeo 2016/679*, Torino, 2016.

Sebbene il successivo reclamo di quest'ultima non venisse accolto dall'autorità competente, il Tribunale amministrativo (*Verwaltungsgericht*) a cui la Wirtschaftsakademie aveva fatto intanto ricorso annullava la suddetta decisione di eliminazione ritenendo che l'amministratore di una *fanpage* non fosse responsabile del trattamento dei dati e quindi che la società tedesca non potesse essere soggetta ad un tale ordine. Dello stesso avviso era il Tribunale amministrativo superiore del Land (*Oberverwaltungsgericht*) il quale respingeva l'appello dell'autorità competente ritenendo infondata la misura dell'autorità di controllo che poteva essere applicata solo se le finalità del trattamento fossero state determinate dalla società tedesca la quale si limitava a ricevere soltanto statistiche anonime nella sezione "Insight".

Tuttavia, la vicenda non si esauriva con la suddetta decisione ma proseguiva con il successivo ricorso dell'autorità competente dinanzi alla Corte amministrativa federale (*Bundesverwaltungsgericht*). Anche in questo caso, la Corte federale condivideva l'interpretazione del Tribunale amministrativo riguardante la responsabilità del trattamento soltanto in capo al *social network*.

Nondimeno, alcuni dubbi riguardo l'ambito di applicazione della nozione di responsabile del trattamento ai sensi della Direttiva Privacy nonché sull'estensione dei poteri dell'autorità di controllo sulla filiale tedesca di Facebook hanno spinto il giudice nazionale a sollevare alcune questioni interpretative alla CGUE che possono essere così sintetizzate: se sia possibile ritenere l'amministratore di una *fanpage* messa a disposizione da un *social network* quale responsabile del trattamento ai sensi della Direttiva Privacy in caso di violazione delle norme relative alla tutela dei dati personali ²⁰; e se l'autorità di controllo di uno Stato membro possa esercitare autonomamente i poteri riconosciuti dalla Direttiva Privacy ²¹ nei confronti di una filiale situata nel proprio Stato membro ma facente capo a una società con sede in un paese terzo anche qualora tale filiale non sia responsabile del trattamento di dati nell'Unione europea ma svolga soltanto funzioni di *marketing*.

3. TITOLARI DEL TRATTAMENTO SENZA OBBLIGHI (O QUASI)

Nel rispondere alle questioni così delineate, la Corte ha anzitutto focalizzato la sua attenzione sul primo profilo ossia in merito alla possi-

²⁰ Secondo l'art. 2 lett. d) della Direttiva Privacy, per "responsabile del trattamento" si intende: "la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per alla sua designazione possono essere fissati dal diritto nazionale o comunitario".

²¹ L'art. 28, para. 3 della Direttiva Privacy disponeva i poteri dell'autorità di controllo prevedendo la possibilità che le autorità in questione si servano di poteri

investigativi, come il diritto di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio della sua funzione di controllo; di poteri effettivi d'intervento, come quello di formulare pareri prima dell'avvio di trattamenti, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento o quello di adire i Parlamenti o altre istituzioni politiche nazionali; di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della Direttiva ovvero di adire per dette violazioni le autorità giudiziarie.

bilità di ritenere l'amministratore di una *fanpage* quale "responsabile del trattamento" ai sensi della Direttiva Privacy. Giova preliminarmente segnalare che la definizione di "responsabile del trattamento" prevista dalla Direttiva Privacy non deve essere interpretata nel senso previsto dal d. lgs. 196/2003 anche noto come Codice Privacy ²². Al contrario, tale figura corrisponde alla definizione di "titolare del trattamento" (o *data controller*) come anche fatta propria dal GDPR ossia alla "persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali" ²³.

Dapprima, la Corte ha esteso l'ambito interpretativo della nozione di titolare del trattamento attraverso un approccio teleologico ossia mettendo in risalto le finalità della Direttiva Privacy. In particolare, secondo il giudice europeo, lo scopo della Direttiva è garantire un "elevato grado di tutela delle libertà e dei diritti fondamentali delle persone fisiche, in particolare della loro vita privata, riguardo al trattamento dei dati personali" ²⁴ come risulta anche affermato nella sentenza *Google Spain* ²⁵. Inoltre, attraverso un'interpretazione letterale della definizione di titolare del trattamento, si chiarisce il carattere di non obbligatoria esclusività di tale attività potendo questa essere svolta "da sola o insieme ad altri" e, pertanto, aprendo quindi le porte a quella che viene definita contitolarietà del trattamento dei dati personali.

In tale quadro, Facebook è chiaramente titolare del trattamento dei dati dal momento che esso determina le finalità e gli strumenti. Pertanto, la questione ruota attorno al comprendere se la *Wirtschaftsakademie*, in qualità di amministratore della *fanpage*, co-determini i suddetti aspetti svolgendo la funzione di contitolare del trattamento.

Come osservato dalla Corte, occorre distinguere tra l'utilizzatore di un *social network* e l'amministratore di una pagina *web*. Solo in questo secondo caso, la creazione e la gestione di una pagina *web* all'interno del *social network* offre la possibilità a Facebook di trattare attraverso i *cookie* i dati anche di quei visitatori che non possiedono un profilo sul *social network* ²⁶. Inoltre, l'elemento su cui la Corte ha fondato la sua decisione sul punto si basa sul contributo dell'amministratore al trattamento dei dati derivante dalla possibilità di selezionare gli obiettivi e le strategie promozionali servendosi dei parametri e delle opzioni offerte da

²² Il responsabile del trattamento ai sensi del Codice Privacy è definito dall'art. 4 co. 1 lett. g) quale "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali". Tale definizione corrisponde a quella fornita dall'art. 4 n. 8 del Regolamento.

²³ Art. 2 lett. d) della Direttiva Privacy e l'art. 4 n. 7 del Regolamento.

²⁴ Art. 1, para. 1 nonché il considerando 10 della Direttiva Privacy. In giurisprudenza v. Corte di giustizia, sentenza *Ryneš*, C-212/13, ECLI:EU:C:2014:2428.

²⁵ *Google Spain*, cit. punto 66.

²⁶ Secondo la Corte nel caso qui commentato: "Orbene, il mero fatto di utilizzare un *social network* quale Facebook non rende un utilizzatore di Facebook corresponsabile di un trattamento di dati personali effettuato da tale network; occorre, invece, rilevare che l'amministratore di una *fanpage* presente su Facebook, mediante la creazione di una siffatta pagina, offre a Facebook la possibilità di posizionare *cookie* sul computer o su qualsiasi altro dispositivo della persona che ha visitato la sua *fanpage*, indipendentemente dal fatto che tale persona possieda o meno un profilo Facebook" (punto 35).

Facebook²⁷. Di conseguenza, la Corte ha ritenuto, seppur con le dovute differenze²⁸, tale amministratore quale contitolare di tale trattamento insieme a Facebook Ireland, la filiale europea del relativo *social network* che si occupa del trattamento dei dati.

Una volta delineata la scelta della Corte in merito alla qualificazione dell'amministratore di una *fanpage* su Facebook quale contitolare del trattamento dei dati personali riguardanti i suoi visitatori, è necessario un ulteriore approfondimento²⁹. Attraverso un esercizio di astrazione, è possibile ritenere che, seppur la Corte si sia pronunciata su un caso concreto, questa ha ritenuto configurarsi una contitolarità del trattamento ogni qualvolta un soggetto, al fine di pubblicizzare la propria attività e servendosi dei criteri di selezione che contribuiscono a definire il *target* di utenza da raggiungere, utilizzi una pagina *web* messa a disposizione da una piattaforma online che tratta i dati dei visitatori attraverso tecnologie quali ad esempio i *cookie*.

Sebbene possa sembrare una fattispecie piuttosto articolata, tale ricostruzione equivale senz'altro a riconoscere la titolarità del trattamento, e quindi investire di responsabilità, ancorché graduata agli obblighi come ricordato dalla Corte³⁰, non solo la società tedesca in questione ma anche migliaia di soggetti che utilizzano lo strumento della *fanpage* o altri spazi *web* messi a disposizione dalle piattaforme al fine di pubblicizzare il proprio *business* o attività.

La decisione della Corte è chiara sotto questo profilo. Ciò che invece non traspare dalla sentenza riguarda nello specifico gli obblighi ai quali il contitolare in qualità di amministratore di una *fanpage* dovrebbe adeguarsi.

Occorre brevemente richiamare alcuni aspetti basilari riguardanti il funzionamento delle *fanpage*. Tali spazi online costituiscono degli *account* messi a disposizione da Facebook a persone fisiche o imprese al fine

²⁷ Come osservato dalla Corte, l'amministratore della *fanpage* ha la possibilità di: "chiedere di ricevere — e, quindi, chiedere che siano trattati — dati demografici concernenti il suo pubblico destinatario, in particolare tendenze in materia di età, sesso, situazione sentimentale e professionale, informazioni sullo stile di vita e sugli interessi di detto pubblico, nonché informazioni sugli acquisti e il comportamento di acquisto online dei visitatori della sua pagina, le categorie di prodotti o di servizi di loro maggiore interesse, come pure dati territoriali che consentono all'amministratore della *fanpage* di stabilire dove avviare promozioni speciali o organizzare eventi e, in generale, di offrire informazioni maggiormente mirate" (punto 37).

²⁸ La Corte ha condiviso le conclusioni dall'avvocato generale Bot presentate il 24 ottobre 2017 che ai punti 75 e 76, chiarivano che l'esistenza di una corresponsabilità non si traduce necessariamente in una responsabilità equivalente dei diversi operatori nell'ambito di un trattamento di dati

personali. Al contrario, tali operatori 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.

²⁹ Sul tema privacy, responsabilità e *social network*, v., tra gli altri, G. RESTA, *Digital platforms and the law: contested issues*, in *Rivista di diritto dei media* 1, 2018, p. 231 ss.; O. POLLICINO, E. APA, *Modelling the Liability of Internet Service Provider: Google vs. Vivi Down. A Constitutional Perspective*, Milano 2014; E. ROSATI, G. SARTOR, *Social Networks e Responsabilità del Provider*, EU Working Papers Law 5, 2012; S. SICA, G. CODIGLIONE, *Social network sites e il «labirinto» delle responsabilità*, in *Giur. Merito* 12, 2012, p. 2714 ss.; P. GALDIERI, *Il trattamento illecito del dato nei social network*, in *Giur. Merito* 12, 2012, p. 2697 ss.

³⁰ Come già ricordato, la Corte ha aderito all'opinione dell'avvocato generale Bot riguardo la differenziazione nel grado di responsabilità dei contitolari.

di poter pubblicizzare la propria attività o anche più semplicemente per condividere con la propria *community* uno specifico interesse. Giova segnalare, inoltre, che l'utilizzo di una *fanpage* non integra di per sé una finalità lucrativa in quanto la stessa può essere usata anche a fini personali ³¹. Una volta registrato come amministratore della *fanpage*, la persona fisica o l'ente possono utilizzare la pagina potendo, inoltre, usufruire gratuitamente tramite la sezione "Insights" di dati statistici anonimi riguardanti i visitatori di tali pagine ³² raccolti attraverso i *cookie* utilizzati dal *social network*. In altre parole, quando un utente di Facebook o un visitatore esterno visita una *fanpage* i suoi dati vengono trattati dal *social network* al fine di poter fornire le statistiche anonime all'amministratore della pagina.

Da tale breve ricostruzione, risulta chiaro che il trattamento dei dati della *fanpage* è operato da Facebook e, nonostante la Corte ritenga che l'attività dell'amministratore nell'attrarre visitatori pianificando la propria strategia di *marketing* possa costituire un contributo alla selezione delle modalità del trattamento tale da renderlo pari a un titolare del trattamento, non si può escludere che l'amministratore della *fanpage* risulti del tutto estraneo al trattamento di quei dati. Inoltre, sebbene Facebook metta a disposizione delle offerte per pubblicizzare la *fanpage*, l'amministratore non gode di una completa libertà di decidere come valersi di questi servizi essendo vincolato alle opzioni pubblicitarie fornite dal *social network* e, più in generale, alle *Terms and Conditions* ossia al contratto stipulato tra l'amministratore e il *social network* al momento della creazione dell'*account*.

Dal momento che la Corte ha ritenuto che il regime di contitolarità non comporta una necessaria equiparazione tra le responsabilità dei diversi operatori nell'ambito di un trattamento di dati personali, occorre quindi chiedersi quali responsabilità possono essere attribuite all'amministratore della *fanpage* in qualità di titolare del trattamento vista la sua posizione marginale.

Non avendo a disposizione i dati dei visitatori della propria pagina, l'amministratore ad esempio non potrà soddisfare le richieste degli interessati relative all'esercizio dei loro diritti. L'unico obbligo in questo caso sembra essere quella di divenire un mero punto di contatto per gli interessati al fine di raccogliere le richieste di quest'ultimi e trasmetterle a Facebook per la loro concreta esecuzione. Basti pensare al diritto di rettifica ³³ nonché alle istanze di accesso ³⁴ ai dati nei confronti dei quali l'amministratore della *fanpage* sembra essere totalmente estraneo. Simili argomentazioni possono essere svolte per quanto riguarda le misure di sicurezza visto che la piattaforma sulla quale la *fanpage* opera è gestita da Facebook e non certo dall'amministratore.

³¹ Occorre osservare che Facebook mette a disposizione due opzioni: la prima per aziende, la seconda per *community* o personaggi pubblici. Informazioni più dettagliate sono disponibili al seguente link indirizzo: https://www.facebook.com/pages/creation/?ref_type=sitefooter.

³² Ulteriori informazioni in merito agli

Insight sono fornite da Facebook al seguente indirizzo: <https://www.facebook.com/business/a/page/page-insights>.

³³ Art. 12 lett. b) della Direttiva Privacy.

³⁴ Art. 12 lett. a) della Direttiva Privacy.

Riguardo i “nuovi” adempimenti previsti dal Regolamento, ci si potrebbe chiedere ad esempio se tale contitolarità faccia scaturire l’obbligo di tenuta di un registro dei trattamenti ³⁵ per l’amministratore della *fanpage*. Tuttavia, anche in questo caso, il problema di fondo consiste nella possibilità per gli amministratori di conoscere i dati dei visitatori visto che questi vengono poi sottoposti all’amministratore in forma anonima.

Di conseguenza, sebbene tali esempi non possano considerarsi esaustivi, non sembrano essere molte le tipologie di obblighi gravanti sull’amministratore in qualità di contitolare del trattamento. Risulta tuttavia possibile individuare tra gli adempimenti imputabili all’amministratore della *fanpage* l’obbligo di fornire l’informativa ai propri visitatori richiamando sulla propria pagina, *inter alia*, il fatto che i dati degli utenti sono sottoposti a trattamento attraverso i *cookie* di Facebook e che l’amministratore partecipa a determinare alcune modalità del trattamento attraverso la selezione di specifici *target* ³⁶.

Sebbene, la Corte abbia ritenuto che il riconoscimento di una contitolarità costituisca un valore aggiunto al fine di incrementare il livello di tutela dei dati personali degli interessati, non si comprende come tale equiparazione — seppur asimmetrica — possa garantire maggiori tutele all’interessato ³⁷. Anzi, tale scelta che evidentemente è il risultato di un bilanciamento implicito tra esigenze di tutela della *privacy* e altri interessi quali, ad esempio, la libertà di iniziativa economica dell’amministratore della *fanpage*, risulta essere sproporzionata dal momento che tale estensione sembra penalizzare proprio le numerose imprese che si servono di una *fanpage* per pubblicizzare la propria attività senza avere accesso a quei dati che il *social network* tratta attraverso i *cookie*, se non in forma anonima. L’assenza, inoltre, di ulteriori chiarimenti in merito a quali siano gli obblighi dell’amministratore derivanti dalla contitolarità del trattamento rischia di aumentare il livello di incertezza compromettendo ulteriormente la libertà delle imprese che utilizzano le *fanpage* al fine di pubblicizzare la propria attività non conoscendo a quali obblighi dovranno conformarsi. Pertanto, il sacrificio di altri interessi che comunque godono di tutela costituzionale a livello europeo quale ad esempio la libertà di iniziativa economica ³⁸ in nome di una maggiore tutela del diritto fondamentale alla protezione dei dati personali non sembra in questo caso garantire maggiori tutele all’interessato. In altre parole, tale approccio della Corte può essere letto anche come una scelta assiologica dove la

³⁵ Art. 30 del Regolamento.

³⁶ Occorre sottolineare che Facebook spiega come tratta i dati attraverso i *cookie* nella sua *cookie policy* (<https://www.facebook.com/policies/cookies/>) con la conseguenza che l’onere di provvedere all’informativa potrebbe essere ritenuto già ottemperato dal *social network* in virtù del suo ruolo di titolare del trattamento.

³⁷ Sul punto è possibile richiamare le critiche riguardanti la decisione Google Spain di chi ha ritenuto il ragionamento della Corte un’evidente *excusatio non petita* dal momento che l’estensione della definizione

di “responsabile” al fine di assicurare ampia tutela degli interessati sembra trascurare il ruolo del “responsabile del trattamento” e i relativi obblighi che fanno capo in base alla Direttiva, e che rischiano, se applicati in modo sproporzionato di incidere sui modelli di *business* di alcuni operatori. In particolare, v. O. POLLICINO, M. BASSINI, *Bowling for Columbine. La Corte di giustizia sul caso Google Spain: l’obbligo (quasi) prima di tutto?*, Diritto24, 13 maggio 2014.

³⁸ Art. 16 della Carta dei Diritti Fondamentali dell’Unione europea.

tutela della *privacy* che ha come fulcro l'interessato prevale su altri interessi ritenuti nel caso di specie soccombenti.

In tale contesto, alcuni interessanti spunti possono essere ricavati osservando il regime di contitolarità introdotto dal Regolamento. In particolare, l'art. 26 prevede che la contitolarità del trattamento sussista ogni qual volta due o più soggetti contribuiscano a determinare le finalità e i mezzi del trattamento. Dal punto di visto interno, il Regolamento prevede l'obbligo per i contitolari di indicare tramite specifico accordo le rispettive responsabilità riguardo gli obblighi derivanti dal Regolamento come per i diritti degli interessati o l'informativa. Inoltre, il contenuto essenziale dell'accordo deve esser emesso a disposizione all'interessato e indipendentemente dalle disposizioni dell'accordo interne l'interessato può esercitare i propri diritti nei confronti di entrambi i titolari del trattamento.

Riportando tali considerazioni al caso in questione, occorrerebbe un accordo standard sul punto tra Facebook e i vari amministratori delle *fanpage* al fine di regolare gli obblighi rispettivi che tuttavia, come osservato, non sembrano potersi spingere al di là del provvedere a fornire un'informativa o del rappresentare un punto di contatto al fine di costituire un ulteriore centro d'imputazione per l'interessato. Tale previsione potrebbe ridurre il grado di incertezza dovuto all'assenza di chiarimenti da parte della Corte riguardo i rispettivi obblighi dei contitolari contribuendo a ribilanciare la sproporzione derivante dalla qualificazione soggettiva operata dalla decisione qui commentata.

4. STABILIMENTO E GDPR: VERSO UN SUPERAMENTO PARZIALE DELLA DOTTRINA TRADIZIONALE

Una volta definita la posizione di contitolarità dell'amministratore della *fanpage*, la Corte ha risposto all'ulteriore gruppo di quesiti attinenti alla questione dello "stabilimento" di enti non residenti nell'Unione e ai relativi poteri delle autorità di controllo.

Dopo aver ribadito che l'esercizio del potere delle autorità di controllo è limitato al territorio dello Stato membro di appartenenza e che quest'ultimo applica le disposizioni nazionali attuative della Direttiva Privacy alle attività di uno stabilimento del responsabile del trattamento nel proprio territorio, la Corte ha precisato che, al fine di determinare se l'autorità di controllo ha il potere di esercitare le proprie prerogative nel caso di specie, occorre considerare i criteri dello "stabilimento del responsabile del trattamento" e la contestualità delle attività di tale stabilimento³⁹. Richiamando i principi della sentenza *Weltimmo*⁴⁰, la Corte ha osservato che la nozione di stabilimento nell'Unione "implica l'esercizio effettivo e reale di un'attività mediante un'organizzazione stabile e che la forma giuridica di siffatto stabilimento, si tratti di una semplice succursale o di una filiale dotata di personalità giuridica, non è il fattore

³⁹ Art. 4 para. 1 lett. a) nonché il Considerando 19 della Direttiva Privacy.

⁴⁰ Corte di giustizia, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639.

determinante”⁴¹. Nel caso di specie, la Facebook Germany rientra in tale ambito definitorio costituendo quindi uno “stabilimento” nell’Unione. Mentre, con riguardo al secondo requisito, la Corte ha osservato che, sempre tenuto conto delle finalità perseguite dalla Direttiva Privacy, è necessario interpretare tale criterio in modo estensivo. In particolare, sebbene le attività della Facebook Germany siano relative esclusivamente alla promozione di spazi pubblicitari, tale attività, costituendo il nucleo duro dei profitti del *social network*, deve essere ritenuta strettamente collegata al trattamento di dati personali operato dalla Facebook Inc. e dalla Facebook Ireland dal momento che quest’ultimo è funzionale al miglioramento del sistema pubblicitario e di conseguenza a garantire un miglior livello dei servizi offerti. Ne consegue quindi che, essendo anche il secondo criterio soddisfatto⁴², l’attività della Facebook Germany deve essere considerata soggetta al potere dell’autorità di controllo competente.

Con riguardo al grado di autonomia dell’esercizio di tale potere, oltre a quanto già espresso, la Corte ha chiarito che “le autorità di controllo incaricate di sorvegliare l’applicazione, nel territorio degli Stati membri cui appartengono, delle disposizioni adottate da questi ultimi in attuazione della medesima direttiva, sono pienamente indipendenti nell’esercizio delle funzioni loro attribuite”⁴³ come può desumersi non solo dalla Direttiva Privacy ma anche della Carta dei diritti fondamentali dell’Unione europea⁴⁴ e dal Trattato sul funzionamento dell’Unione europea⁴⁵. Sebbene la Direttiva Privacy preveda meccanismi di collaborazione tra le autorità degli Stati membri, non è definita una priorità potendo anche le suddette autorità esprimersi in modo divergente sul medesimo caso. Da tale quadro d’insieme, si desume come l’autorità di controllo tedesca potesse in modo autonomo valutare la liceità del trattamento della filiale tedesca di Facebook.

Ne consegue che l’altra questione rilevante nel caso qui commentato è il riconoscimento da parte della Corte della possibilità per l’autorità di controllo di esercitare i propri poteri nei confronti di una filiale di un’impresa stabilita al di fuori dell’Unione europea che disponga di varie sedi in diversi Stati membri tra cui lo Stato membro dell’autorità di controllo. Ciò anche quando, in base alla ripartizione delle funzioni all’interno del gruppo, la filiale dello Stato membro dell’autorità di controllo in questione è competente solamente per la vendita di spazi pubblicitari e per altre attività di *marketing* sul territorio di detto Stato membro e la responsabilità esclusiva per la raccolta e per il trattamento dei dati personali grava, per l’intero territorio dell’Unione europea, su una filiale situata in un altro Stato membro.

In particolare, secondo la dottrina dello stabilimento applicata dalla Corte, al fine di poter estendere la disciplina nonché i relativi poteri dell’autorità di controllo è necessario poter rinvenire lo stabilimento del

⁴¹ *Ibidem*, punto 54.

⁴² Sulla definizione della contestualità delle attività dello stabilimento v. *Google Spain*, cit., punti 55 e 56.

⁴³ Punto 68.

⁴⁴ Art. 8 della Carta dei Diritti Fondamentali dell’Unione europea.

⁴⁵ Art. 16, para. 2 TFUE nonché, in particolare, la sentenza *Schrems*, cit., punto 40.

titolare⁴⁶. Sul punto, non si può trascurare il fatto che la Corte abbia più volte fornito un'interpretazione estensiva della nozione di stabilimento al fine di includere nel suo ambito di applicazione anche gli *Internet service provider* ossia quegli operatori che sfruttando la natura transnazionale di Internet sfuggivano al controllo delle singole autorità di controllo nazionali⁴⁷. In particolare, le sentenze *Google Spain* e *Weltimmo* possono essere considerate due *landmark decisions* in tema di stabilimento che testimoniano come la dimensione digitale abbia condotto ad un'estensione della nozione di stabilimento e, quindi, di una maggiore tutela del diritto alla protezione dei dati personali.

Nel primo caso, restringendo il campo d'indagine a ciò che concerne l'oggetto d'analisi, occorre osservare come la Corte abbia ritenuto che l'attività di trattamento dei dati fosse eseguita nel contesto delle attività della filiale spagnola di Google. Sebbene il trattamento di dati personali fosse realizzato da un'impresa con sede in uno Stato terzo, lo stabilimento si configura vista "la promozione e la vendita degli spazi pubblicitari proposti dal suddetto motore di ricerca, che servono a rendere redditizio il servizio offerto da quest'ultimo"⁴⁸. Tale riconoscimento che sotto certi aspetti può sembrare una forzatura della definizione di stabilimento si giustifica al fine di assicurare una tutela effettiva (e non solo formale) del diritto alla *privacy* degli interessati che sarebbe frustrato qualora una società che offra servizi su Internet potesse sottrarsi agli obblighi scaturiti dalla Direttiva Privacy solamente in virtù della sua forma giuridica o del suo stabilimento al di fuori del territorio dell'Unione europea.

Nel secondo caso, in particolare, la *Weltimmo*, una società con sede in Slovacchia, gestiva un sito *web* di annunci immobiliari di beni situati in Ungheria trattando i dati degli inserzionisti. Il problema sorse quando molti inserzionisti alla scadenza del periodo gratuito chiesero la cancellazione dei propri annunci nonché dei propri dati ricevendo, tuttavia, come risposta da parte della società slovacca la fatturazione dei servizi forniti e la susseguente azione per il recupero dei crediti non pagati dagli inserzionisti. L'autorità di controllo ungherese ritenne di essere competente nel caso di specie sanzionando la *Weltimmo* per la sua condotta che avverso tale provvedimento lamentava l'assenza di competenza dell'autorità ungherese sulla propria attività. La CGUE investita del quesito sollevato dal giudice ungherese ha sposato una concezione flessibile della nozione di stabilimento discostandosi dall'impostazione formalistica se-

⁴⁶ L'art. 4 della Direttiva Privacy prevede che gli Stati membri applichino le disposizioni nazionali d'implementazione della suddetta Direttiva ai trattamenti effettuati nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro. Il considerando 19 inoltre fornisce ulteriori criteri interpretativi al fine di definire lo stabilimento nel territorio di uno Stato membro riferendosi all'esercizio "effettivo e reale" dell'attività mediante una "organizzazione stabile" non essendo dirimente la forma giuridica di tale stabilimento. Sul principio di territorialità della tutela dei dati personali.

Sulla dottrina dello stabilimento v. A. BARLETTA, *La tutela effettiva della privacy nello spazio (giudiziario) europeo e nel tempo (della "aterritorialità") di Internet*, in *Eur. Dir. Priv.* 4, 2017, p. 1179 ss.; D. J. B. SVANTESSON, *Article 4(1)(a) 'establishment of the controller' in EU data privacy law-time to rein in this expanding concept?*, in *IDPL* 6, 2016, p. 210 ss.; G. Finocchiaro, cit., 121.

⁴⁷ Sul punto occorre osservare che la Corte si sia spinta anche oltre le linee guida fornite dal Working Party 29. Sul punto v. Working Party 29, pareri n. 1 del 2008 e n. 8 del 2010.

⁴⁸ *Google Spain*, cit., punto 55.

condo cui un'impresa sarebbe stabilita esclusivamente nel luogo in cui è registrata. Come osservato dalla Corte, al fine di determinare se una società dispone di uno stabilimento ai sensi della Direttiva Privacy in uno Stato membro diverso dallo Stato membro o dal paese terzo in cui è registrata, bisogna tenere in considerazione “il grado di stabilità dell'organizzazione sia l'esercizio effettivo delle attività in tale altro Stato membro, prendendo in considerazione la natura specifica delle attività economiche e delle prestazioni di servizi in questione. Ciò vale soprattutto per imprese che offrono servizi esclusivamente tramite Internet”⁴⁹.

Dopo aver individuato che la Weltimmo esercita un'attività concreta ed effettiva in Ungheria consistente nella gestione di siti Internet di annunci immobiliari riguardanti beni immobili situati nel territorio di tale Stato membro e redatti nella lingua di quest'ultimo nonché un collegamento stabile attraverso un suo rappresentante ungherese, la Corte ha ritenuto che il trattamento dei dati personali potesse essere ricondotto nell'attività dello stabilimento ungherese dal momento che “l'operazione consistente nel far comparire su una pagina Internet dati personali va considerata come un «trattamento» ai sensi dell'art. 2, lettera b), della direttiva 95/46”⁵⁰. La Corte osserva, inoltre, che la cittadinanza delle persone interessate dal trattamento di dati personali in questione non rileva ai fini di individuare lo stabilimento del titolare del trattamento⁵¹.

Una volta delineato questo breve quadro generale, è possibile osservare come l'impianto del Regolamento non sembra stravolgere la nozione di stabilimento delineata dall'art. 4 della Direttiva Privacy ma, partendo dal punto di arrivo sopra evidenziato, estende tale nozione chiarendo all'art. 3 che il Regolamento si applica “al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione” a patto che i trattamenti riguardino “l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato” o “il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione”⁵². Tale approccio può essere considerato come un parziale superamento della nozione di stabilimento la cui appli-

⁴⁹ Weltimmo, cit., punto 29.

⁵⁰ Ibidem, punto 37. G. CAGGIANO, *L'interpretazione del “contesto delle attività di stabilimento” dei responsabili del trattamento dei dati personali*, in *Diritto inf.* 4-5, 2014, p. 605 ss.

⁵¹ Le stesse considerazioni possono essere stese per altri elementi quali il luogo in cui risiedono i titolari dell'impresa o quello relativo al caricamento dei dati come condiviso al punto 37 delle conclusioni dell'avvocato generale nel caso Weltimmo ma anche come osservato dal WP 29 nel Parere n. 8/2010 che ha ritenuto non decisivi ai fini dell'individuazione del diritto applicabile la

cittadinanza o il luogo di residenza abituale dell'interessato.

⁵² Art. 3, para. 2 del Regolamento. Sul punto già prima dell'entrata in vigore del Regolamento v. G. RESTA, F. BIGNAMI, *Human rights extraterritoriality: Right to Privacy and National Security Surveillance*, in E. BENVENISTI, G. NOLTE (eds.), *Community obligations in Contemporary International Law*, Oxford, 2017; M. G. STANZIONE, *Il Regolamento Europeo Sulla Privacy: Origini E Ambito Di Applicazione*, in *Eur. Dir. Priv.* 4, 2016, p. 1249 ss.; P. DE HERT, M. CZERNIAWSKI, *Expanding the European data protection scope beyond terri-*

cazione sarà limitata ai casi che non rientrano nelle due fattispecie summenzionate.

Per quanto riguarda il ruolo dell'autorità di controllo rispetto ai soggetti stabiliti (e non), il Regolamento ribadisce il principio secondo cui ciascuna autorità di controllo è competente limitatamente al territorio del proprio Stato membro ⁵³ al fine di esercitare i poteri nonché i compiti stabiliti dal Regolamento ⁵⁴. In particolare, il Considerando 122 chiarisce che la competenza delle autorità di controllo si estende a quei trattamenti posti in essere nell'ambito delle attività di uno stabilimento del titolare del trattamento sul proprio territorio. Di conseguenza, il Regolamento ha chiarito che l'attività dell'autorità di controllo, seppur limitata al proprio Stato membro di riferimento, riguarda anche le attività di uno stabilimento del titolare del trattamento. In questo contesto, il Regolamento ha introdotto un ulteriore sistema basato sul concetto di "autorità capofila" ⁵⁵ ossia quell'autorità di controllo legittimata ad esercitare i poteri riconosciuti dal Regolamento per i trattamenti transfrontalieri ⁵⁶ effettuati nel contesto dello stabilimento principale o dello stabilimento unico del titolare e del trattamento ⁵⁷. L'autorità capofila dovrebbe essere

tory, in *IDPL* 6, 2016, p. 230 ss; B. VAN ALSENOY, M. KOEKKOEK, *Internet and Jurisdiction after Google Spain: The Extraterritorial Reach of the "Right to be Delisted"*, in *IDPL* 5, 2015, p. 105 ss.; O. POLLICINO, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in *Dir. Inf.* 4-5, 2014, p. 569 ss.; P. PIRODDI, *Questioni internazionaliprivatistiche sui motori di ricerca*, in *Dir. Inf.* 2014, p. 623 ss; W. KOTSCHY, *The proposal for a new General Data Protection Regulation-problems solved?*, in *IDPL* 4, 2014, p. 274 SS.

⁵³ Art. 55, para. 1 del Regolamento.

⁵⁴ Artt. 57-58 del Regolamento.

⁵⁵ V. le "Linee guida per l'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento" adottate dal WP 29 il 13 dicembre 2016 (e revisionate in data 5 aprile 2017)

⁵⁶ Secondo l'art. 4 n. 23 GDPR per "trattamento transfrontaliero" si intende: "[il] trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure [il] trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del tratta-

mento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessi in più di uno Stato membro".

⁵⁷ Il Regolamento si riferisce allo "stabilimento principale" sia del titolare del trattamento sia del responsabile. Per quanto riguarda il primo, l'art. 4, n. 6, lett. a) prevede che nel caso di stabilimenti in più di uno Stato membro bisogna considerare "stabilimento principale" il luogo della sua amministrazione centrale nell'Unione. Tuttavia, nei casi in cui le decisioni sulle finalità e i mezzi del trattamento di dati personali, ossia quegli elementi che qualificano l'attività del titolare del trattamento, siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni principale, allora quest'ultimo verrà considerato lo stabilimento principale. Similmente alla Direttiva Privacy, il Considerando 36 del Regolamento aggiunge che "lo stabilimento principale deve essere determinato in base a criteri obiettivi e implicare l'effettivo e reale svolgimento di attività di gestione finalizzate alle principali decisioni sulle finalità e sui mezzi del trattamento nel quadro di un'organizzazione stabile. Tale criterio non dovrebbe dipendere dal fatto che i dati personali siano trattati in quella sede. La presenza o l'uso di mezzi tecnici e tecnologie di trattamento di dati personali o di attività di trattamento non costituiscono di per sé lo stabilimento principale né sono quindi criteri determinanti della sua esistenza".

considerata come il soggetto che coopera con le altre autorità interessate ⁵⁸.

In tale scenario, rimane impregiudicato il ruolo dell'autorità di controllo che non agisce in qualità di capofila nei casi in cui il titolare del trattamento o il responsabile del trattamento sia stabilito in più di uno Stato membro, ma l'oggetto dello specifico trattamento riguardi unicamente il trattamento effettuato in un singolo Stato membro e coinvolga soltanto interessati in tale singolo Stato membro ⁵⁹. In tali casi, l'autorità di controllo deve informare la capofila della questione locale. Dopo essere stata informata, l'autorità di controllo capofila dovrebbe decidere se intende trattare il caso a norma della disposizione sulla cooperazione tra l'autorità di controllo capofila e altre autorità di controllo interessate (c.d. meccanismo dello sportello unico) ⁶⁰, ovvero se l'autorità di controllo che l'ha informata debba trattarlo a livello locale ⁶¹ introducendo quindi un principio di sussidiarietà verticale che permette all'autorità capofila di attrarre a sé competenze di autorità di controllo locali.

Nel caso di specie, non si può escludere che la Corte avrebbe ritenuto sussistere la competenza dell'autorità di controllo irlandese in qualità di "autorità capofila" visto che si tratta di un trattamento transfrontaliero operato dallo stabilimento principale di Facebook in Irlanda, l'unico responsabile del trattamento dei dati in Europa.

5. CONCLUSIONI

Alla luce delle considerazioni svolte finora è possibile osservare che il diritto fondamentale alla protezione dei dati personali gode di una particolare tutela nella dimensione digitale. Tale considerazione risulta essere confermata dalla sentenza in commento che porta con sé un'estensione degli obblighi per gli amministratori di pagine *web* messe a disposizione da una piattaforma *online* in virtù della loro posizione di contitolarità del trattamento dovuta alla determinazione delle finalità del trattamento. Resta però da comprendere quali obblighi l'amministratore di tali spazi *online* debba rispettare alla luce della disciplina introdotta dal Regolamento e se, in particolare, occorrerà un accordo tra la piattaforma e l'amministratore al fine di chiarire i rispettivi compiti e adempimenti previsti dal Regolamento. Al di là di tale considerazione tecnica, risulta

⁵⁸ Secondo l'art. 4 n. 22 del Regolamento, l'autorità di controllo è ritenuta "interessata" in quanto "il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure un reclamo è stato proposto a tale autorità di controllo".

⁵⁹ Art. 55, para. 2 del Regolamento.

⁶⁰ Art. 60 del Regolamento.

⁶¹ Secondo il Considerando 127 "[...] Al momento di decidere se intende trattare il caso, l'autorità di controllo capofila do-

vrebbe tenere conto dell'eventuale esistenza, nello Stato membro dell'autorità di controllo che l'ha informata, di uno stabilimento del titolare del trattamento o del responsabile del trattamento, al fine di garantire l'effettiva applicazione di una decisione nei confronti del titolare del trattamento o del responsabile del trattamento. Qualora l'autorità di controllo capofila decida di trattare il caso, l'autorità di controllo che l'ha informata dovrebbe avere la possibilità di presentare un progetto di decisione, che l'autorità di controllo capofila dovrebbe tenere nella massima considerazione nella preparazione del proprio progetto di decisione nell'ambito di tale meccanismo di sportello unico".

cruciale sottolineare l'approccio espansivo della Corte nei confronti della tutela dei dati personali in ambito digitale in linea con il precedente approccio giurisprudenziale.

Nondimeno, è possibile osservare tale orientamento nell'adesione ai precedenti in materia di stabilimento, attraverso quindi il riconoscimento dei poteri dell'autorità di controllo su operatori residenti in paesi terzi ma che offrono servizi *online* nel territorio dell'Unione sottolineando il carattere concreto della tutela del diritto alla *privacy* nella cornice costituzionale europea.

In futuro, il Regolamento avrà un ruolo fondamentale dal momento che la Corte e i giudici nazionali saranno agevolati nell'estendere l'ambito di applicazione della normativa europea in materia di *privacy* anche a soggetti non residenti nell'Unione vista la parziale estensione extraterritoriale riconosciuta dall'art. 3 del Regolamento nei casi analizzati.

Pertanto, la scelta dell'estensione extraterritoriale testimonia un'importante *step* nel processo di costituzionalizzazione del diritto europeo alla tutela dei dati personali che non sembra rivolgersi più esclusivamente all'Unione ma anche alla dimensione transnazionale.

GIOVANNI DE GREGORIO