LUISS

Dipartimento
di Scienze Politiche

Cattedra di Diritto dell'Unione europea

Cooperazione e coerenza: limiti e nuovi orizzonti interpretativi del meccanismo dello sportello unico alla luce della sentenza C-645/19

Francesco Cherubini
RELATORE

Nicolò Rosso Matr. 091212
CANDIDATO

Anno Accademico 2021/2022

INDICE

Introduzione

Nel 2010, il CEO di Facebook, Mark Zuckerberg, destò scalpore quando durante una conferenza stampa, disse che "privacy is no longer a social norm", suscitando l'inquietudine dei presenti[1]. La suggestiva affermazione di Zuckerberg permette di prendere spunto per accennare brevemente allo stato della privacy oggi, sul perché sia assurta a diritto fondamentale e sui motivi che permettono di affermare che, nel contesto odierno, il diritto alla privacy sia messo a dura prova dall'inarrestabile crescita della tecnologia, della rete e del digitale.

Secondo Norberto Bobbio, i diritti umani sono diritti storici, in quanto nascono come riposta a determinate circostanze esterne, le quali, a loro volta, incorniciano fattori storici, politici, sociali ed economici[2]. La dimensione dinamica dei diritti si traduce in una loro periodizzazione segnata dalla continua evoluzione, la quale canonicamente vede il proprio inizio con la prima generazione dei diritti civili e politici nati dalle rivoluzioni nazionali e borghesi della fine del XVIII secolo – ad oggi si parla di quarta generazione[3]. Si deve tenere presente come di generazione in generazione il novero di diritti riconosciuti si sia ampliato, senza tuttavia incorrere in una sostituzione dei diritti più vecchi da quelli più recenti. Infatti, sempre ricorrendo alle parole di Bobbio, "il mondo di diritti vive di accumulazioni, non di sostituzioni"[4], intendendo come il progresso nel campo dei diritti umani non vada inquadrato in un'ottica di superamento, di trionfo, da parte delle generazioni di diritti più recenti su quelle più datate quanto di ampliamento del novero di diritti tutelabili, garantendo una protezione più comprensiva dell'individuo.

L'iter giuridico del diritto alla privacy, prima, e del diritto alla protezione dei dati, poi, segue un percorso analogo, influenzato e modificato dalle condizioni esterne, le quali hanno talvolta finito con l'impedire di trovare una connotazione univoca al concetto di privacy. Per questo motivo, dare una definizione di privacy è compito non facile, in quanto occorre tenere presente da un lato il profilo giuridico e dall'altro le ambiguità terminologiche che spesso accostano, nel linguaggio colloquiale, il termine privacy al termine riservatezza.

La privacy assume per la prima volta consistenza giuridica a partire dall'articolo *The Right of Privacy*, ad opera di Warren e Brandeis (1890), nel quale viene legata al concetto di proprietà privata e dei mezzi di tutela di tale diritto[5]. Il *right to be let alone* riguarda l'aspetto tradizionale del diritto alla riservatezza, ovvero il diritto alla non ingerenza di terzi nella sfera privata personale[6]. Il diritto ad essere lasciati soli nacque come diritto a contenuto negativo, la cui *ratio* è da individuare nel contesto della rivoluzione industriale, in cui la borghesia sentì la necessità di tutelare il proprio spazio vitale da qualsiasi influenza esterna. Nel tempo è emersa un'altra sfaccettatura del diritto alla privacy, vale a dire la sua dimensione sociale, la quale non è più esclusivamente legata all'aspetto più tradizionale della riservatezza e della non ingerenza, quanto alla capacità di autodeterminarsi come individui. Si è quindi passati ad un nuovo tipo di diritto, relativo alla protezione delle informazioni personali e della loro circolazione da parte dei soggetti ai quali quelle informazioni fanno riferimento[7].

---

[1] JHONSON (2010).
[2] BOBBIO (1990: 30 ss.).
[3] HELMONS (2000).
[4] BOBBIO (1990: 15).
[5] WARREN, BRANDEIS (1890: 193-220).
[6] FALLETTI (2009).
[7] MILLER (1971).

Come evidenziato poco più sopra, i diritti umani vanno intesi e compresi all'interno della cornice storica nella quale nascono ed è quindi in quest'ottica che si può meglio comprendere la rivoluzione digitale della privacy. Dall'inizio del XX secolo gli strumenti di informazione di massa sono aumentati in maniera esponenziale, così come sono aumentati gli strumenti attraverso cui si raccolgono dati di ogni cittadino, arrivando ad oggi dove l'alba della rivoluzione digitale ha modificato e facilitato le modalità di fruizione e circolazione delle informazioni. La rivoluzione digitale oltre a modificare gli strumenti di informazione e comunicazione, ha dato vita ad un nuovo modello economico, denominato *data economy*. L'economia dei dati misura l'impatto complessivo del mercato dei dati — vale a dire il mercato in cui i dati digitali sono scambiati in forma di prodotti o servizi derivati dai dati grezzi — sull'economia nel suo insieme[8]. Comprende la produzione, la raccolta, la conservazione, il trattamento, la distribuzione, l'analisi, l'elaborazione, la consegna e l'utilizzo dei dati ottenuti mediante tecnologie digitali[9]. Secondo un recente studio promosso dalla Commissione europea, la *data economy* rappresenterebbe il cuore pulsante dello sviluppo economico, il cui valore nell'Unione europea nel 2019 era di 325 miliardi di euro, ossia il 2,6% del PIL dei Paesi UE27, con una crescita del 42% dal 2015[10]. Tuttavia, va evidenziato come i modelli di business *data-driven* abbiano come principale fonte di *revenue* la monetizzazione dei dati degli utenti. Stando ad uno studio pubblicato da McKinsey & Co, le aziende più performanti e in più rapida crescita hanno adottato la monetizzazione dei dati e l'hanno resa parte integrante della loro strategia[11]. Per chiarezza, la monetizzazione dei dati può essere descritta come quel processo, diretto o indiretto, di vendita delle informazioni di navigazione degli utenti attivi su di una determinata piattaforma verso terze parti. Con la digitalizzazione delle organizzazioni e delle aziende, i dati dei consumatori a cui si ha accesso sono dei più variegati: dettagli di contatto, informazioni demografiche, cronologia delle ricerche, acquisti passati e tempo trascorso su determinati *websites* sono tutti elementi "vendibili" da cui le imprese possono trarre profitto. Shoshana Zuboff è arrivata a definire questa logica di mercato come "capitalismo della sorveglianza", in quanto i profitti delle aziende sono sempre più incentrati su una logica di appropriazione del *behavioural surplus*, ovvero tutte quelle informazioni relative alle *user profile information*, capaci di delineare un profilo informatico degli utenti, rendendo l'*advertising* molto più preciso e in grado di delineare *targets* di riferimento[12]. La profilazione dell'utente è quindi il meccanismo alla base della logica di *marketing* contemporaneo, dove avere più informazioni possibili su di un utente equivale a poter fornire un prodotto su misura, in considerazione degli interessi, delle passioni e dei gusti individuali, oltre ad aver un vantaggio sulla concorrenza. Per farsi un'idea, nel 2016 l'89% dei profitti di Alphabet Inc. derivava dal programma di pubblicità mirata[13].

Sebbene l'economia digitale rappresenti uno dei settori più in crescita nel panorama internazionale, numerosi studi suggeriscono come la compravendita

[8] CARULLO (2017).

[9] IDC, European Data Market study, SMART 2013/0063, 2016.

[10] Report della Commissione europea, dell'8 luglio 2020, *The European Data Market Monitoring Tool: Key facts & figures, first policy conclusions, data landscape and quantified stories: d2.9 final study report*.

[11] MCKINSEY (2017).

[12] ZUBOFF, KARIN (2019).

[13] United States securities and Exchange Commission, *Selected financial data for Alphabet Inc*., Form 10-K, 31 dicembre 2016, reperibile *online.* Stando a quanto riportato dalle dichiarazioni di Alphabet, nel 2016 i suoi profitti furono di oltre $90miliardi. I profitti dovuti alle attività di pubblicità mirata furono di $79miliardi, pari all'88.73% del totale.

delle informazioni personali degli utenti da parte delle diverse piattaforme avvenga in totale contrapposizione con le normative vigenti, circumnavigando la *data privacy* degli utenti, sollevando questioni di natura giuridica prima ancora che morali.[14]

La disciplina che si occupa di *privacy* poggia il proprio fondamento sul diritto all'autodeterminazione informativa, ovvero la libertà dell'individuo di determinare in perfetta autonomia le modalità di costruzione della propria sfera privata, comprese le singole informazioni che andranno a comporla. Negli ultimi anni, la Corte di giustizia dell'Unione europea ha avuto un ruolo pivotale nella definizione di un paradigma giurisprudenziale all'interno della materia della *data privacy*, battendo la strada per prima nel *res nullius* rappresentato dall'innovazione e dall'esigenza di tutela dell'utente. La protezione del diritto alla *privacy* nel contesto normativo dell'Unione europea si è notevolmente ampliata a partire dall'introduzione della Carta dei diritti fondamentali dell'Unione europea e un notevole contributo è stato dato dalla giurisprudenza innovativa della Corte, la quale ne ha notevolmente ampliato la protezione. Fino ad ora, la Corte ha promosso una visione univoca e indiscutibile del diritto alla *privacy*, il quale in casi recenti ha perfino predominato su altrettanti diritti fondamentali finora giudicati intoccabili[15].

L'introduzione fin qui proposta ha lo scopo di delineare gli ambiti di azione del presente elaborato, il quale è nato con l'obiettivo di commentare la sentenza C-645/19, *Facebook Ireland Limited c. Gegevensbeschermingsautoriteit* della Corte di giustizia dell'Unione europea (CGUE), avente ad oggetto le sei domande di pronuncia pregiudiziale proposte alla Corte, ai sensi dell'articolo 267 del Trattato sul funzionamento dell'Unione europea (TFUE), relative in particolare all'interpretazione degli articoli da 56 a 58 e da 60 a 66 del regolamento (UE) 2016/679, comunemente noto come regolamento generale sulla protezione dei dati (RGPD).

Al fine di comprendere meglio le implicazioni di una sentenza di questa portata, il presente elaborato si svilupperà lungo tre assi: in principio, l'indagine si concentrerà sul percorso evolutivo della normativa europea in materia di privacy e protezione dei dati personali. Verrà qui proposta una panoramica sui più recenti sviluppi normativi legati alla materia e sulle più recenti innovazioni in ambito tecnologico. Verrà quindi argomentato come il costante aggiornamento della regolamentazione sul trattamento dei dati personali sia necessario per far fronte e stare al passo con le continue innovazioni della società dell'informazione e della comunicazione.

Nel secondo capitolo sarà oggetto di approfondimento la sentenza C-645/19, dedicando spazio sia alle osservazioni delle parti intervenute, che alle conclusioni dell'Avvocato generale Michal Bobek. Lo studio delle osservazioni delle parti intervenute permetterà di comprendere le diverse posizioni in merito alla necessità o meno di permettere alle autorità di controllo, diverse da quelle c.d. capofila, di avviare o impegnarsi in procedimenti legali nei confronti dei responsabili dei trattamenti dei dati. L'analisi della sentenza verrà condotta prendendo in considerazione due tematiche principali: la ratio del meccanismo del *one-stop-shop* alla luce dell'interpretazione letterale e teleologica del RGPD, ed il diritto dei singoli alla tutela della *privacy*, così come intesa dall'articolo 8 della Carta dei diritti fondamentali dell'Unione europea.

---

[14] MCMILLAN (2014).

[15] Sentenza della Corte di giustizia, del 14 maggio 2014, causa C-131/12, *Google Spain c. Agencia Española de Protección de Datos* (AEPD). Nel giudizio della Corte, il diritto all'oblio prevale anche sul diritto alla libertà di espressione e informazione, così come garantiti dall'articolo 11 della Carta. Si veda in tal senso FRANTZIOU (2014).

Infine, nel terzo capitolo verranno analizzate le conclusioni della Corte, anche alla luce della giurisprudenza passata, e le implicazioni che quest'ultime avranno nell'applicazione del regolamento 2016/679. Infatti, sebbene il ragionamento della Corte possa essere inserito all'interno della giurisprudenza più recente, va fin d'ora notato come la specificità e l'importanza del caso vadano ben oltre una maggiore garanzia per la protezione dei dati. Il caso C-645/19 ha esacerbato le tensioni tra regolatori e il mondo delle compagnie *tech*, con la possibilità per queste ultime di dover affrontare battaglie legali su più fronti nel territorio dell'Unione, vista la possibilità per tutte le autorità di controllo nazionali, nell'ambito di applicazione del RGPD di avviare procedimenti legali pur non essendo le autorità di controllo capofila. Come è evidente, la questione apre nuovamente il dibattito in merito al principio di proporzionalità tra il diritto all'iniziativa economica e il diritto alla *data privacy*.
I diritti umani sono diritti storici, dicevamo, e nascono come reazione alle minacce e alle pressioni esterne. Il diritto alla *privacy*, oggi, inteso come diritto soggettivo alla scelta individuale, alla libertà di scegliere con chi e se condividere le modalità di costruzione della propria sfera privata è la reazione alla minaccia "privacy is no longer a social norm". La giurisprudenza della Corte e l'evoluzione del diritto ci dimostrano che invece, ad oggi, la *privacy* è una delle norme sociali di più alto valore.

Capitolo 1
Il modello europeo della tutela della *privacy*

> "Everything you've heard or seen or experienced will become searchable. Your whole life will be searchable".
> (Larry Page, cofondatore di Google)

La dottrina europea ha ricostruito il diritto alla riservatezza come diritto al controllo sulle informazioni private, nato dall'esigenza di assicurare la sfera di riservatezza del cittadino a partire dalla rivoluzione tecnologica degli ultimi trent'anni. Infatti, la raccolta di dati personali e la trasmissione digitale delle informazioni relative ad un individuo ne può minacciare l'autodeterminazione informativa, concetto che fu espresso per la prima volta in Germania all'inizio degli anni '70 e poi riconcettualizzato nel dicembre 1983 dalla Corte costituzionale tedesca nella celebre sentenza *Volkszählungsurteil*[16].
In questo Capitolo verrà dapprima affrontato il percorso che ha portato all'affermarsi all'interno del panorama comunitario del diritto alla protezione dei dati, per poi proseguire nell'analisi dei due atti normativi che più di tutti hanno segnato il panorama internazionale per il trattamento transfrontaliero dei dati. Nel primo paragrafo, si ripercorrerà l'iter storico che ha portata all'affermarsi della protezione dei dati personali e il suo cammino verso il novero dei diritti fondamentali. Nel secondo paragrafo, verrà evidenziato il carattere inizialmente integralista della direttiva 95/46 e il suo progressivo passaggio a norma a tutela dei diritti fondamentali. Infine, nel terzo paragrafo verranno presentate le principali novità introdotte con il RGPD[17].

1.1 Il lento affermarsi della protezione dati nel panorama europeo

Il lento affermarsi del diritto alla protezione dei dati nel quadro normativo europeo, per poter essere compreso a pieno, deve essere guardato fin dalle sue origini. Come anticipato nell'introduzione, il diritto alla privacy, la cui traduzione italiana può essere resa con riservatezza, viene solitamente confuso e scambiato con il diritto alla protezione dei dati personali. Per quanto entrambi facciano parte del complesso novero di diritti fondamentali di cui l'Unione si fa carico, va tuttavia evidenziato come differiscano tanto in portata quanto in significato, in relazione ad una *ratio* sostanzialmente diversa. Il diritto alla *privacy* è visto come *ius excludendi alios*, ossia come il diritto alla non ingerenza di terzi negli affari privati. In quest'ottica, la già citata opera di Warren e Brandeis va letta contestualmente al periodo storico nella quale viene concepita. Boston, 1890. La stampa in *off-set*, la fotografia e il giornalismo d'impresa, nelle parole di Warren e Brandeis, avevano "invaded the sacred precints of private and domestic life"[18], in quanto permettevano di diffondere migliaia e migliaia di copie di una notizia relativa alla sfera privata di una figura non pubblica, senza il consenso di quest'ultima. Brandeis fu il primo a cogliere questo peculiare aspetto, ovvero il legame della privacy con la tecnologia. Sempre Brandeis, in una nota *dissenting opinion* nella causa *Olmstead v. United States* definì la privacy come "the most comprehensive of rights and the most valued by civilized men"[19]. Per riassumere, il diritto alla privacy va compreso in relazione al diritto alla libertà di espressione e di stampa, come

[16] STEINMULLER, WILHELM (1970).
[17] Regolamento (UE) 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*.
[18] WARREN, BRANDEIS (1899: 50).
[19] Ivi, p. 9.

un limite a quest'ultima, qualora le informazioni non siano relative a figure pubbliche.
Il diritto alla protezione dei dati personali, di contro, nasce in un contesto e con un fine del tutto diverso. Infatti, mentre il diritto alla privacy pone al centro il corretto equilibrio tra libertà di parola e di manifestazione del pensiero con la tutela della riservatezza della persona, il diritto alla protezione dei dati personali, invece, si interfaccia con il ben più complesso problema della difesa dei cittadini da ogni forma di controllo basata sull'acquisizione non consensuale di dati e di informazioni che possono riguardarli. Per comprendere meglio questa differente finalità, occorre inquadrare tale diritto nel contesto europeo del primo e secondo dopo guerra, con una presenza dello Stato sempre più pervasiva e intrusiva, dove regimi totalitari, grazie anche alle innovazioni tecnologiche legate alla archiviazione e al trattamento automatizzato dei dati, controllavano e raccoglievano informazioni sulla vita dei cittadini senza il loro consenso. Un mutamento radicale nella concezione di informazioni e nel modo di controllare: le derive autoritarie di diversi Stati europei hanno come corollario il controllo globale delle idee che i cittadini nutrono dentro di loro, annientando così la dimensione privata con l'obiettivo di ridurre al minimo il dissenso. In un contesto simile, il rapporto con la tecnica e l'innovazione muta all'interno del panorama europeo, non più subordinata all'esigenze dell'uomo, ma strumento capace di condizionare le modalità stesse di esercizio dei diritti[20]. Sebbene, come si è evidenziato fin ora, il percorso storico e politico, addirittura ideologico, che ha portato in Europa all'affermarsi di una particolare forma di tutela per i cittadini sulle proprie informazioni personali, va altresì evidenziato come l'iter normativo che ha portato all'affermarsi di tale diritto inizi solo a partire dall'inizio degli anni Settanta. Se infatti si volesse indicare una prima data nel contesto europeo, di tutela della protezione dei dati personali, ecco che questa apparirebbe solamente nel 1970, quando il Land dell'Assia, parte della Germania Federale, disciplinò e tutelò il trattamento dei dati personali operato attraverso banche dati, introducendo il divieto di schedature di massa a tutela dei lavoratori[21]. Tale data assume una sua rilevanza nella misura in cui viene letta alla luce del contesto storico politico in cui è immersa. La Germania degli anni Settanta vedeva contrapporsi all'interno del proprio territorio due blocchi, due ideologie tra loro agli antipodi, specie in termini di protezione dei dati personali. Mentre l'allora Repubblica Democratica Tedesca, zona d'influenza sovietica, sposava un approccio più orwelliano, schedando di fatto individui sulla base delle loro idee politico-ideologiche, la Repubblica Federale Tedesca, di cui l'Assia era (ed è tutt'ora) un Land, sposava un approccio diametralmente opposto, rifiutando il controllo globale operato dalla DDR e, più in generale, da regimi di carattere autoritario, rifacendosi alla cultura del blocco occidentale. In questo quadro, la legge sulla protezione dei dati rappresenta un punto fermo all'interno del paradigma democratico-liberale, all'interno del quale la libertà *tout court* è tale se e solo se ai cittadini viene lasciato, oltre al diritto alla riservatezza, il diritto alla vita privata nei confronti dell'elaborazione automatizzata dei dati di carattere personale che la riguardano.
Sulla scia del precedente disegnato dal Land tedesco, e la successiva legge federale del 1977, si insinua un altro tassello fondamentale che ha contribuito alla definizione di un quadro della protezione dei dati personali in Europa: la

[20] RODOTÀ (1995: 30).
[21] Hessisches Datenschutzgesetz (HDSG) 1970, del 12 ottobre 1970, Gesetz- und Verordnungsblatt für das Land Hessen, Teil I, 1970, N. 41 (12 ottobre 1970), p. 625 ss., testo originale in tedesco, reperibile *online.*

Convenzione di Strasburgo, o Convenzione n. 108 del 28 gennaio 1981 approvata dal Consiglio d'Europa. Questo trattato fondamentale riguarda esplicitamente la protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale e, ad oggi, rimane l'unico strumento internazionale giuridicamente vincolante per la protezione dei dati personali, in quanto possono aderire, e hanno aderito, Paesi anche esterni al Consiglio d'Europa (ad esempio, nel 2013 aderì l'Uruguay). La Convenzione 108 nasce dall'esigenza di tutela per le persone a seguito del proliferare di tecnologie dell'informazione e comunicazione a partire dagli anni '60[22], considerando i precedenti pericolosi e le minacce sollevate dalle pratiche allora in uso nei regimi non democratici. La Convenzione si applica a tutti i trattamenti di dati personali effettuati sia nel settore privato che pubblico, e quindi anche ai trattamenti effettuati da polizia e autorità giudiziaria. La normativa mira a proteggere gli individui da abusi e regolamentare i flussi transnazionali dei dati, superando e innovando l'articolo 8 della Convenzione europea dei diritti dell'uomo, nel quale viene tutelato il rispetto alla vita privata e al domicilio di ogni persona. L'obiettivo della Convenzione viene evidenziato nell'articolo 1 della stessa, che recita:

> "[s]copo della presente Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano"[23].

Oltre al carattere prettamente legato alla tutela del diritto alla privacy e alla protezione dei dati, la Convenzione 108 aveva anche lo scopo di costruire un *legal framework* comune per gli Stati parte, al fine di poter semplificare il trasferimento transfrontaliero dei dati e ridurre le barriere al commercio internazionale[24].

Il carattere innovativo della Convenzione 108 presenta tuttavia un limite sostanziale, collaterale alla struttura economica che si stava venendo a consolidare in Europa. In quanto trattato internazionale, era privo della forza sufficiente per poter armonizzare le legislazioni nazionali. In altre parole, erano gli Stati a doversi impegnare, attraverso la ratifica della Convenzione, a garantire l'apporto di una legislazione il più simile possibile, evitando cioè legislazioni nazionali tra loro dissimili e favorendo una libera circolazione dei dati garantendo una tutela uniforme del diritto alla protezione dei dati. Il problema relativo ad un'armonizzazione a livello sovranazionale per la tutela delle persone fisiche con riguardo al trattamento automatizzato dei dati fu sollecitato, a livello comunitario, per la prima volta nel 1975, all'interno di una raccomandazione del Parlamento europeo[25]. Tale raccomandazione, prendendo spunto dal precedente dell'Assia, rilevò come l'avanzare della tecnologia e lo svilupparsi di tecniche per il trattamento automatizzato dei dati rendesse necessaria una direttiva sulla libertà dell'individuo e dell'informatica, "per assicurare ai cittadini della Comunità la massima protezione contro gli abusi o i difetti delle tecniche di elaborazione dei dati, ma anche per evitare lo svilupparsi di

[22] SAETTA (2018).

[23] Convenzione del Consiglio d'Europa, *sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, Strasburgo, 28 gennaio 1981.

[24] BAINBRIDGE (2005: 17).

[25] Risoluzione del Parlamento europeo, del 13 marzo 1975, GU C60/48, *sulla tutela dei diritti dei cittadini di fronte al crescente progresso tecnologico nel settore dell'informatica*. Nel documento, il Parlamento sollecita le istituzioni ad adottare atti che abbiamo come obiettivo quello di tutelare i diritti dei cittadini della Comunità a fronte delle crescenti minacce del processo automatizzato dei dati personali.

legislazioni nazionali contraddittorie"[26]. La raccomandazione del Parlamento prevedeva anche l'istituzione di una commissione ad hoc incaricata di prendere in esame il problema per poter studiare proposte da poter presentare alla Commissione europea.
Come visto, sebbene scopo principale della Convenzione 108 fosse quello di costruire un sistema comune di trattamento dei dati, essa, in quanto trattato internazionale, non poteva intervenire direttamente nelle legislazioni nazionali. La Commissione europea[27] sollecitò affinché gli Stati membri della Comunità europea si impegnassero a ratificare la Convenzione 108, in quanto "[l]a reazione e il funzionamento del mercato comune in connessione col trattamento dei dati presuppone un'accentuata standardizzazione delle condizioni di trattamento e della protezione dei dati" e considerava "questa convenzione [la Convenzione 108] appropriata per creare all'interno della Comunità un livello uniforme di protezione nel campo dei dati". Tuttavia, nonostante la raccomandazione della Commissione europea, nel 1989 gli Stati membri ad avere ratificato il documento approvato dal Consiglio d'Europa erano solo sette. Si rese quindi necessario un intervento a livello comunitario per armonizzare le legislazioni nazionali, poiché la profonda frammentazione nel panorama normativo europeo metteva a rischio la stabilità del progetto di mercato unico, in quanto le barriere alla libera circolazione dei dati tra i Paesi membri creavano condizioni di concorrenza ineguali tali da dar luogo a condizioni di partecipazione ineguali al mercato comune.
Il *casus belli* che evidenziò l'esigenza di un sistema comunitario in materia di protezione dei dati, e che rese evidente l'esigenza dell'adozione di un atto giuridico a livello sovranazionale, fu rappresentato dal caso FIAT[28], dove nel contesto del trasferimento dati dei lavoratori dalla sede francese allo stabilimento torinese, venne contestata all'Italia l'assenza di una legge in materia di protezione dati. L'autorità francese di protezione dei dati intervenne in merito alla questione del trasferimento transfrontaliero dei dati, al fine di tutelare i diritti dei lavoratori francesi, i quali, vista l'assenza di una legislazione simile in materia nel vicino d'oltralpe, si ritrovano a non poter usufruire della medesima protezione. In questa prospettiva, quindi, l'assenza di una legislazione comune minacciava anche la stabilità del mercato unico del lavoro, differenziando la tutela dei lavoratori di paese in paese e frammentando la tutela dei diritti a livello comunitario. Nel 1990 la Commissione adottò una proposta per una direttiva del Consiglio con la quale promuoveva l'adozione di un atto giuridico che, fra le altre cose, stabilisse un criterio comune per tutti gli Stati membri in materia di protezione dei dati[29]. Tale direttiva, secondo la Commissione, aveva il fine di armonizzare sia il diritto alla protezione dei dati delle varie legislazioni, sia di garantire il corretto funzionamento del mercato interno. In quest'ottica, un livello coerente ed equivalente di protezione dei dati avrebbe garantito il corretto funzionamento dei mercati interni, in quanto, garantendo un'equa tutela dei dati delle persone fisiche, gli Stati membri non avrebbero più avuto alcuna ragione per imporre limiti al trasferimento transfrontaliero dei dati.

[26] Ivi, 60 ss.
[27] Raccomandazione della Commissione europea, del 29 luglio 1981, 81/679/CEE, *concernente una convenzione del Consiglio d'Europa sulla protezione delle persone per quanto riguarda l'elaborazione automatica dei dati a carattere personale*.
[28] Délibération Commission National de l'Informatique et des Libertés (CNIL), dell'11 luglio 1989, No. 89-7811.
[29] Proposta di direttiva del Consiglio *concernente la protezione delle persone relativamente al trattamento dei dati personali* COM (90) 314 def. (presentata dalla Commissione il 27 luglio 1990).

Possiamo quindi affermare che il processo attraverso il quale si venne a costituire in Europa il diritto alla protezione dei dati ha una natura ibrida, in quanto nasce con l'obiettivo di tutelare il funzionamento del mercato interno, proteggendolo tanto dalle disparità che un trattamento diversificato in materia di dati determina, quanto dalla necessità di assicurare il rispetto della vita privata e dell'autodeterminazione dei cittadini dell'Unione. Occorre adesso andare a specificare le tutele garantite dalla direttiva 95/46/CE e, successivamente, evidenziarne i limiti applicativi, con particolare riferimento a quelli riscontrati dalla Corte.

1.2 La direttiva 95/46: obiettivi, innovazioni, limiti alla luce del caso *Rundfunk*

Come evidenziato nel precedente paragrafo, la genesi della direttiva 95/46 ha una natura ibrida, bifronte: la tutela del diritto alla protezione dei dati in seguito al proliferare del trattamento automatizzato dei dati e il corretto funzionamento del mercato interno. Infatti, come si può leggere nel considerando n. 3 della direttiva 95/46 [30]:

> "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".

Come visto con il caso FIAT, la struttura di mercato che si andava a formare all'interno della Comunità europea rendeva necessaria l'armonizzazione delle legislazioni in materia di trasferimento e trattamento dati, di modo da non arrestare il processo di integrazione economica. La direttiva 95/46 si immette all'interno del quadro legislativo europeo pochi anni dopo la ratifica da parte degli Stati membri del Trattato di Maastricht (Trattato sull'Unione europea, 7 febbraio 1992) che sancì la nascita dell'Unione europea e l'avvio del progetto di mercato unico. Conseguenza di questo processo di integrazione fu la necessità di superare anche le frontiere immateriali quali erano le diverse normative in materia di protezione dei dati personali che altrimenti avrebbero rappresentato un limite sostanziale alla costituzione di un mercato unico, vanificando quanto raggiunto.
Una volta compresa l'esigenza dell'armonizzazione delle legislazioni nazionali, restava da decidere il come. L'articolo 95 del Trattato CE (oggi 114 TFUE) dispone che l'Unione può adottare misure per il riavvicinamento delle disposizioni nazionali "che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno". In altre parole, per poter adottare un atto a livello comunitario è necessario che l'ambito di applicazione, oltre a ricadere nelle competenze dell'Unione, abbia come finalità quella di rafforzare il funzionamento del mercato interno, e non si possano quindi adottare atti che non rientrino nel campo del diritto comunitario, in quanto l'Unione agirebbe *ultra vires*. Inoltre, l'Unione nell'esercizio delle sue competenze deve rispettare il principio di proporzionalità, indicato all'articolo 5 TUE (ex articolo 5 TCE), secondo il quale l'atto adottato a livello dell'Unione deve essere proporzionale al fine e il meno invasivo possibile. L'adozione di una direttiva, invece che di un regolamento, si rese necessaria anche in seguito alle difficoltà ravvedute nel corso dei lavori preparatori in merito ad una normativa comune vincolante, preferendo l'affermarsi del principio del mutuo riconoscimento fra i diversi

[30] Direttiva (CE) del Parlamento europeo e del Consiglio, del 24 ottobre 1995, 95/46, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.*

Paesi membri e con l'attuazione di uno strumento normativo meno invasivo, che lasciava comunque ampi margini alle legislazioni nazionali. Il mutuo riconoscimento consiste nell'applicazione della legge di protezione dei dati del paese in cu ha sede lo stabilimento principale del titolare del trattamento[31] garantendo comunque la libera circolazione dei dati tra i Paesi membri. In sintesi, la direttiva 95/46 si può qualificare come direttiva di armonizzazione, in quanto stabilì una serie di principi e regole non immediatamente vincolanti ma alle quali gli Stati membri dovettero adeguarsi e un riconoscimento diffuso e reciproco dell'adeguatezza delle leggi di attuazione dei principi indicati dalla direttiva. L'obiettivo era quello di evitare il ripetersi di una situazione analoga a quella del caso FIAT, dando a ciascuno Stato la possibilità di adottare la propria legislazione in materia di protezione dati ma con l'obbligo di riconoscere le norme degli altri Paesi membri altrettanto valide, così da poter garantire lungo tutto il territorio dell'Unione il trasferimento dei dati.
Nel capo 1 della direttiva sono indicate le disposizioni generali, in cui vengono individuati l'oggetto della direttiva, le definizioni relative al significato dei termini utilizzati, il campo di applicazione e il diritto nazionale applicabile. L'articolo 1(1), nel definire l'oggetto della direttiva, dispone che gli Stati membri si impegnano a garantire "la tutela dei diritti e della libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata con particolare riguardo al trattamento dei dati personali" per poi proseguire al secondo comma "non possono [gli Stati membri] restringere o vietare la libera circolazione dei dati personali tra gli Stati membri per motivi connessi alla tutela dei dati personali". L'articolo 1, primo e secondo comma, è molto importante in quanto da un lato lega la protezione dei dati alla tutela dei diritti fondamentali e dall'altro lo collega con l'obiettivo di completamento del mercato interno.
Sebbene oggi sembri evidente il nesso tra la protezione dei diritti fondamentali e la normativa in materia di protezione dei dati, l'iniziale giurisprudenza della Corte sembra suggerire il contrario. Va ricordato, infatti, come a discapito delle intenzioni del Parlamento europeo[32] e della Commissione[33], quando la direttiva 95/46 venne introdotta all'interno del panorama normativo dell'Unione, quest'ultima era sprovvista della competenza a poter emanare atti normativi sui diritti fondamentali. Infatti, benché la Corte di giustizia avesse incorporato considerazioni concernenti i diritti fondamentali nella sua giurisprudenza a partire dagli anni '70[34], era assente una base giuridica che consentisse all'Unione di poter adottare disposizioni di carattere positivo per

[31] Direttiva 95/46, articolo 25(1): "[g]li Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva".
[32] Risoluzione del Parlamento europeo, *sulla tutela dei diritti dei cittadini di fronte al crescente progresso tecnologico nel settore dell'informatica*, del 13 marzo 1975. Nel documento, il Parlamento sollecita le istituzioni ad adottare atti che abbiamo come obiettivo quello di tutelare i diritti dei cittadini della Comunità a fronte delle crescenti minacce del processo automatizzato dei dati personali.
[33] Report della Commissione europea, del 15 maggio 2003, COM (2003), 265 final, *First report on the implementation of the Data Protection Directive (95/46/EC)*. Nel Report la Commissione evidenzia come la direttiva custodisca due delle più antiche ambizioni del Progetto di integrazione Europea: il raggiungimento di un mercato interno e la protezione dei diritti e delle libertà degli individui.
[34] Sentenza della Corte di giustizia, del 13 luglio 1989, causa C-5/88 *Hubert Wachauf c. Repubblica federale di Germania*.

la protezione dei diritti fondamentali[35]. Tali motivazioni vengono riprese e chiarite nel parere 2/94 dove la Corte afferma che "nessuna disposizione del Trattato [CE] attribuisce alle istituzioni comunitarie, in termini generali, il potere di dettare norme in materia di diritti dell'uomo"[36]. In quest'ottica è possibile quindi capire le motivazioni che spinsero la Corte a adottare una prospettiva interpretativa integralista della direttiva 95/46, per lo meno nelle prime fasi, sostenendo che l'obiettivo principale di tale atto era proprio quello di garantire la libera circolazione dei dati personali, con l'obiettivo di tutelare il corretto funzionamento del mercato interno[37].
Questa posizione più integralista emerge nella sentenza *Österreichischer Rundfunk e a.*, primo caso relativo alla tutela dei dati personali. Nello specifico, nel caso *Rundfunk*, il giudice nazionale di rinvio ha chiesto alla Corte di esaminare se un requisito della legislazione austriaca, secondo cui le retribuzioni degli alti funzionari pubblici devono essere comunicate all'organo nazionale di controllo, trasmesse al Parlamento nazionale e successivamente rese pubbliche, fosse compatibile con la direttiva 95/46. Inoltre, dinanzi alla Corte fu disputata la stessa applicabilità della direttiva essendoci forti elementi che potevano qualificare la situazione come 'puramente interna'[38], in quanto non erano presenti i requisiti per l'applicazione del diritto comunitario. In altre parole, era necessario individuare un elemento transnazionale per poter applicare la direttiva, e, secondo i ricorrenti, tale elemento era assente nel caso di specie. Infatti, la pubblicazione dei salari non avrebbe in nessun modo minato la possibilità dei lavoratori di poter usufruire delle libertà fondamentali garantite dai Trattati, e come sostenuto dall'Avvocato generale Tizzano, tali possibilità erano sforzate e poco convincenti[39]. Tuttavia, secondo il parere della Corte,

> "l'applicabilità della direttiva 95/46 non può dipendere dalla soluzione del problema se le situazioni concrete di cui trattasi nelle cause principali presentino un nesso sufficiente con l'esercizio delle libertà fondamentali garantite dal Trattato"[40].

Infatti, continua la Corte, un'interpretazione in senso contrario "rischierebbe di rendere particolarmente aleatori i limiti del campo di applicazione della detta direttiva"[41], in quanto non garantirebbe un'armonizzazione in tutte le situazioni in cui vengono utilizzati i dati,

> "il che sarebbe contrario al suo obiettivo essenziale, che è quello di ravvicinare le disposizioni legislative […] degli Stati membri per eliminare gli ostacoli al funzionamento del mercato interno"[42].

---

[35] Vedi sentenza della Corte di giustizia, del 17 dicembre 1970, causa C-11/70, *Internationale Handelsgesellschaft mbH c. Einfuhr- und Vorratsstelle für Getreide und Futtermittel*, e sentenza della Corte di giustizia del 14 maggio 1974, causa C-4/73, *J. Nold, Kohlen- und Baustoffgroßhandlung c. Commissione delle Comunità europee*.
[36] Parere della Corte di giustizia, 28 marzo 1996, 2/94, *Adesione della Comunità alla Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*.
[37] Sentenza della Corte di giustizia del 20 maggio 2003, cause riunite C-465/00, C-138/01 e C-139/0120, *Österreichischer Rundfunk e a.*, par. 70.
[38] Questa è la terminologia usata dalla Corte quando rifiuta di applicare le disposizioni del trattato sulla libera circolazione a situazioni che sono "interamente interne a uno Stato membro"; un elemento interstatale deve essere dimostrato per rientrare nel campo di applicazione materiale delle disposizioni del trattato sul mercato interno.
[39] Conclusioni dell'Avvocato generale Tizzano, del 14 novembre 2002, causa C-465/00 e cause riunite C-138/01 e C-139/01.
[40] Sentenza della Corte di giustizia *Rundfunk*, punto 65.
[41] Ivi, punto 67.
[42] *Ibidem*.

Nello stabilire l'applicabilità della direttiva, la Corte chiarì che non era necessario un nesso diretto con l'esercizio delle libertà fondamentali, in quanto il ricorso alla base giuridica dell'articolo 95 TCE (oggi 114 TFUE) prescindeva dall'esistenza di un nesso effettivo con la libera circolazione in ciascuna delle situazioni previste dall'atto stesso, a condizione che l'atto adottato su tale fondamento avesse effettivamente ad oggetto il miglioramento delle condizioni del mercato interno. Per riassumere, a discapito della natura bifronte della direttiva, dove sembrano convivere gli obiettivi tanto di integrazione economica quando di protezione e tutela dei diritti fondamentali, l'interpretazione che la Corte offre della direttiva suggerisce che a prevalere sia solamente il carattere di funzionamento del mercato interno. Questa iniziale timida giurisprudenza della Corte va compresa alla luce del fatto che la direttiva 95/46 ha dovuto attenersi al diritto primario in vigore al momento della sua adozione, che a seguito della ratifica del Trattato di Maastricht prevedeva l'articolazione in tre pilastri. La base giuridica, come già visto l'articolo 95 TCE, ricadeva nel pilastro comunitario, potendo quindi disciplinare esclusivamente la materia del mercato interno.

Il Trattato di Lisbona ha introdotto cambiamenti significativi all'interno del panorama normativo europeo per la protezione dei dati[43]. Per lo scopo di questo elaborato, è sufficiente evidenziare l'introduzione del diritto alla protezione dei dati personali, benché la portata rivoluzionaria del Trattato si applichi in tutti i settori di competenza dell'Unione. Il diritto alla protezione dei dati personali venne per la prima volta inserito all'interno della Carta di Nizza, all'articolo 8, con il quale venne recepita la crescente esigenza di affermare il carattere sostanziale relativo alla protezione dei dati personali, e dei diritti fondamentali più in generale. Infatti, benché la giurisprudenza della Corte avesse, in via pretoria, accettato come principi generali del diritto dell'Unione i diritti fondamentali[44], quest'ultimi non erano privi di una copertura "costituzionale" a livello normativo, e pertanto, come già sottolineato con il caso *Rundfunk*, l'Unione non aveva alcun potere normativo in tale ambito. L'articolo 6 TUE rende la Carta di Nizza giuridicamente vincolante, e con essa, il suo articolo 8. Inoltre, l'articolo 16 del Trattato sul funzionamento dell'Unione europea, conferisce al Parlamento europeo e al Consiglio il potere di stabilire norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale.

Questo nuovo quadro normativo stabilisce che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano e rafforza i poteri dell'Unione in materia, consentendole di adottare atti aventi come base giuridica l'articolo 16 TFUE. In questo modo, avviene un rovesciamento di prospettiva, dove l'obiettivo di integrazione economica viene subordinato all'obiettivo di tutela delle libertà e dei diritti delle persone fisiche, recependo, dopo oltre trent'anni, i primi moniti del Parlamento europeo[45], rivoluzionando la prospettiva fino ad allora adottata. Ripercussioni evidenti si ebbero anche nella giurisprudenza della Corte, la quale abbandonò la prospettiva più integralista, per sposare un approccio all'interpretazione della direttiva 95/46 più *right-based*: dal 2007 in avanti è possibile rilevare il cambio di tono della Corte, la quale, con sentenze sempre più audaci, si impose alla testa degli sviluppi giuridici sulla tecnologia digitale, promuovendo una visione

[43] Unione europea (UE), Trattato sull'Unione Europea del 13 dicembre 2007.

[44] Ciò è evidente a partire dalla sentenza della Corte di giustizia, del 12 novembre 1969, causa C-29/69, *Stauder*, e dalla sentenza della Corte di giustizia, del 17 dicembre 1970, causa C-11/70, *Internationale Handelsgesellshaft*.

[45] Risoluzione del Parlamento europeo, *sulla tutela dei diritti dei cittadini di fronte al crescente progresso tecnologico nel settore dell'informatica*.

intransigente del diritto alla protezione dei dati[46]. Il ruolo suppletivo della Corte può essere argomentato in base a due questioni, entrambe di una rilevanza centrale per lo scopo del presente elaborato: da un lato, da parte delle istituzioni europee c'era la volontà politica di adottare un nuovo atto, più corposo e che elevasse gli standard di protezione dei dati nel territorio all'interno dell'Unione; dall'altro, la flessibilità della direttiva ne permetteva un'interpretazione che ne svecchiasse i contenuti. Un caso esemplare è la sentenza *Google Spain*[47], la quale fu apripista per l'affermarsi del quadro normativo europeo a livello transatlantico: in sintesi, la Corte affermò l'applicabilità della direttiva anche nel caso in cui i titolari di trattamento dei dati personali fossero non europei e i dati raccolti venissero trattati fuori dall'Unione. L'*iter* argomentativo della sentenza in esame muove dall'interpretazione estensiva che la Corte dà dell'articolo 4 in merito alla nozione di stabilimento[48], ampliandone l'ambito di applicazione territoriale. Infatti, nonostante Google sostenesse che il trattamento dei dati non avvenisse sul territorio dell'Unione, e che lo stabilimento in Spagna si occupasse solo dello spazio di vendita di pubblicità, la Corte constata che Google Spain è una filiale di Google, Inc. sul territorio spagnolo, e quindi uno "stabilimento" ai sensi della direttiva 95/46/CE sulla protezione dei dati. A questo proposito, la Corte afferma che

> "il trattamento di dati personali realizzato per le esigenze di servizio di un motore di ricerca come Google Search, il quale venga gestito da un'impresa con sede in uno Stato terzo ma avente uno stabilimento in uno Stato membro, viene effettuato «nel contesto delle attività» di tale stabilimento qualora quest'ultimo sia destinato a garantire, in tale Stato membro, 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"[49].

E che quindi, "le attività del gestore del motore di ricerca e quelle del suo stabilimento situato nello Stato membro interessato sono inscindibilmente connesse"[50]. Per tali motivi, la Corte constata che:

> "non si può accettare che il trattamento di dati personali effettuato per le esigenze del funzionamento del suddetto motore di ricerca venga sottratto agli obblighi e alle garanzie previsti dalla direttiva 95/46"[51].

Ma oltre ad ampliare la portata e l'applicabilità della direttiva, la Corte arriva ad affermare anche la supremazia valoriale degli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione, i quali costituiscono la base per l'interpretazione della direttiva 95/46/CE. I toni, come si può leggere, sono ben diversi da quelli adottati in *Rundfunk*, e la Corte, oltre ad affermare la superiorità del

---

[46] FABBRINI (2015: 2).
[47] Sentenza della Corte di giustizia, *Google Spain.*
[48] Direttiva 95/46/CE, art. 4, co. 1, stabilisce che: "[c]iascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali: a) effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile; b) il cui responsabile non è stabilito nel territorio dello Stato membro, ma in un luogo in cui si applica la sua legislazione nazionale, a norma del diritto internazionale pubblico; c) il cui responsabile, non stabilito nel territorio della Comunità, ricorre, ai fini del trattamento di dati personali, a strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro, a meno che questi non siano utilizzati ai soli fini di transito nel territorio della Comunità europea".
[49] Sentenza della Corte di giustizia, *Google Spain*, punto 55.
[50] Sentenza della Corte di giustizia, *Google Spain*, punto 56.
[51] Sentenza della Corte di giustizia, *Google Spain*, punto 58.

livello di protezione dei dati in territorio europeo, anticipa l'emanando RGPD evidenziando la ripercussione extra-territoriale della normativa europea, alimentando il fenomeno della c.d. fortezza-Europa.
L'iter giurisprudenziale analizzato in questo paragrafo permette di evidenziare l'evoluzione del *modus iudicandi* della Corte di giustizia, coadiuvato da un'evoluzione nella struttura normativa dell'Unione, il quale per primo ha confermato e ribadito l'importanza, oltre che la centralità, di un approccio normativo alla protezione dei dati. Nel paragrafo successivo verranno approfondite la struttura e le principali disposizioni del RGDP, che, come si vedrà, recepirà in maniera sostanziale le principali innovazioni introdotte in via pretoria dalla Corte di giustizia.

1.3 Il regolamento generale sulla protezione dei dati

Le innovazioni apportate dalla direttiva nel quadro normativo europeo ebbero implicazioni nel panorama globale dei dati personali, ma non furono sufficienti per sventare i rischi associati all'emergere di nuove tecnologie e nuove metodologie di utilizzo dei dati. Come già visto nel precedente paragrafo, l'iniziale assenza di una base giuridica esplicita per il diritto alla protezione dei dati personali lasciò ampio spazio discrezionale alle legislazioni nazionali; inoltre, i confini applicativi della direttiva rimasero a lungo incerti, permettendo alle grandi compagnie del mondo *tech* e alle multinazionali che offrono servizi di rete di approfittare di vuoti normativi[52]. Il carattere costituzionale assunto dal diritto alla protezione dei dati personali ha permesso alla Corte di elaborare una giurisprudenza meno timida e più incisiva[53], che ha condotto ad un *corpus* di pareri, raccomandazioni e decisioni giurisprudenziali in materia, consentendo così una copertura di primo livello alla protezione dei dati personali. La Commissione, con decisione del 25 gennaio 2012, ha proposto al Consiglio e al Parlamento l'adozione di un regolamento relativo alla protezione dei dati personali delle persone fisiche[54], dimostrando quindi l'ambizione di dare al diritto dell'Unione un *framework* normativo in grado di penetrare negli ordinamenti degli Stati membri, per poter assicurare una protezione più adeguata e aggiornata alle esigenze delle nuove minacce digitali. Il regolamento è per definizione un atto giuridico di applicazione generale, vincolante in tutti i suoi elementi e direttamente applicabile in tutti i Paesi dell'Unione. È connaturata alla struttura del regolamento, quindi, una maggior completezza e chiarezza nei suoi contenuti. Fin da una prima lettura, si può evidenziare come il RGPD abbia una struttura molto più densa rispetto alla direttiva: consta di ben 173 considerando e 99 articoli, divisi in 11 capi. L'aspetto che più è evidente fin dalle prime righe del nuovo regolamento è il suo essere molto particolareggiato sul significato delle definizioni e dei principi espressi al suo

[52] Il riferimento qui è in particolar modo all'art. 4, il quale lega l'applicabilità della normativa nazionale al territorio dello Stato dove è situato lo stabilimento del titolare del trattamento con lo scopo di far ricadere nell'ambito del diritto dell'Unione chiunque operi all'interno dei suoi confini. Tuttavia, colossi come Google, Facebook, Apple e Microsoft hanno a lungo sostenuto che a loro non si applicasse la normativa europea in quanto non avevano stabilimenti nel territorio Unione e che quindi non mettevano in atto nessun trattamento di dati all'interno del territorio europeo. Si fa qui ovviamente riferimento alla sentenza della Corte di giustizia *Google Spain*.
[53] Si veda in tal senso sentenza della Corte di giustizia del 6 ottobre 2015, causa C-362/14, *Maximillian Schrems c. Data Protection Commissioner* e anche sentenza della Corte, *Google Spain.*
[54] Proposta della Commissione del 25 gennaio 2012, COM (2012) 11 final 2012/0011 (COD), *di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)*.

interno. Per fare un esempio, mettendo a confronto l'articolo 2 della direttiva, nel quale vengono presi in esame e definiti solo otto termini, l'articolo 4 del regolamento si compone di ventisei paragrafi, articolati in più lettere. Questo aspetto, a tratti maniacale, nella ricerca del dettaglio, va compreso sia alla luce della diversa natura giuridica dell'atto (un regolamento, che per definizione è direttamente applicabile ed obbligatorio in tutti i suoi elementi, deve prevedere norme che siano chiare, precise, incondizionate e non prevede un potere discrezionale da parte degli Stati membri) sia dai precedenti giurisprudenziali, nei quali la flessibilità connaturata alla direttiva ne ha consentito interpretazioni diverse e applicazioni non sempre uniformi negli Stati membri[55]. Al considerando n. 13 vengono espressamente argomentate le motivazioni che hanno spinto all'adozione di un regolamento "che garantisca la certezza del diritto", il quale, nuovamente, concili gli elementi economici e quelli relativi alla tutela delle persone fisiche, in particolare del diritto alla protezione dei dati personali. Il ragionamento sotteso è simile a quello già presente nella direttiva, con la differenza che mentre la seconda aveva il compito di armonizzare le legislazioni nazionali, con l'obiettivo di limare il più possibile le differenze esistenti, il regolamento introduce un *corpus iuris* uniforme per tutti gli Stati membri, per

> "prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno [...] per motivi attinenti alla protezione delle persone fisiche con riferimento ai loro dati personali"[56].

Pertanto, nonostante i tentativi della Corte di giustizia di garantire la certezza del diritto e la sua uniformità, per la natura stessa tanto della direttiva quanto del *topic* – le innumerevoli innovazioni in campo informatico, e la velocità dell'innovazione, rendono difficile per l'attività regolatoria restare al passo – si rese necessaria l'adozione di un atto che garantisse una tutela uniforme in tutti gli Stati membri del diritto alla protezione dei dati. Oltre al cambio di prospettiva operato dal RGPD, occorre per lo scopo e gli obiettivi di quest'elaborato illustrare le principali novità in campo esecutivo, vale a dire studiare le istituzioni e i soggetti incaricati di garantire il rispetto e la conformità, tanto degli operatori economici, quanto dei Paesi membri, al regolamento. A tal fine, sono distinguibili all'interno del regolamento due distinte modalità di controllo: la prima, riguarda maggiormente i doveri dei *controller* e del *processor*, e concerne tutte le misure di sicurezza, imponibili o adottabili in autotutela, che quest'ultimi devono adottare; la seconda, riguarda il rafforzamento e il grande spazio dato all'interno del RGPD all'autorità di controllo e al garante europeo della protezione dei dati[57]. La differenza più rilevante tra il regolamento e la direttiva risiede proprio in quest'approccio diametralmente opposto, ove la prima sembra quasi operare uno *shift* di prospettiva, passando da un approccio più incentrato sui destinatari ad uno più focalizzato sui doveri dei titolari e dei responsabili del trattamento dati[58]. Tale differenza è suffragata dal peso specifico che ricopre l'argomento all'interno dell'architettura dell'atto: quattro delle cinque sezioni in cui è articolato il capitolo IV sono dedicate agli obblighi e ai doveri del responsabile e del titolare del trattamento,

[55] RGDP, considerando 9: "[s]ebbene i suoi principi rimangono tutt'ora validi, la direttiva 95/46 non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica".
[56] RGDP, considerando 13.
[57] Il nuovo regolamento contiene un numero complessivo di articoli che vanno dal 46 al 72, tutti incentrati sulle funzioni, sui poteri e sulla modalità di cooperazione delle Autorità di controllo.
[58] PIZZETTI (2016: 154 ss.).

a discapito della ben più esigua trattazione riservata al tema all'interno della direttiva, la quale dedica alla sicurezza solamente gli articoli 16 e 17. Il regolamento sposta il focus della normativa dalla protezione dell'individuo alla responsabilità del titolare e dei responsabili del trattamento (si parla di responsabilizzazione, anche se la traduzione italiana non rende l'idea, perché "accountability" significa "dover rendere conto delle proprie azioni"), che deve manifestarsi nell'adozione di comportamenti proattivi per dimostrare l'adozione specifica del responsabile del trattamento. Viene affidato ai responsabili e ai titolari il dovere di essere conformi con gli obblighi previsti all'interno del regolamento, decidendo in autonomia gli approcci che più si confacciano alle disposizioni del regolamento. Tale principio va riletto alla luce dei limiti posti al trattamento di dati personali, indicati all'articolo 5 del RGPD[59], in quanto il titolare deve essere in grado di dimostrare la conformità ai vincoli prescritti attraverso l'adozione di comportamenti proattivi volti ad assicurare l'adozione della nuova normativa.

Oltre al profilo esecutivo, completamente riscritto e ampliato, anche il profilo sanzionatorio gode di una particolare trattazione all'interno del RGPD, con ampio spazio dato alla definizione delle responsabilità e dei poteri delle autorità di controllo. Quest'ultime, già presenti anche nel testo della direttiva 95/46 e disciplinate in soli tre articoli (dal 28 al 31), ricevono una notevole trattazione e vedono i loro poteri espansi all'interno del nuovo regolamento.

Nel capitolo successivo, saranno ampiamente discussi i diversi aspetti normativi e i principali compiti di queste nuove figure. Per gli scopi attuali, è sufficiente soffermarsi sulle ragioni giuridiche sottese all'espansione, al rafforzamento e alle norme che disciplinano, in particolare, le autorità di controllo. A differenza della direttiva 95/46, la quale, come più volte visto, è un atto finalizzato all'armonizzazione delle disposizioni nazionali in materia di protezione dei dati personali, il nuovo regolamento è direttamente applicabile in tutti gli Stati membri, rendendo necessaria da parte delle diverse autorità di controllo un'interpretazione uniforme e conforme a quanto disposto. Per questi motivi, e come risulta dalla lettura combinata dei considerando 9 ("la direttiva 95/46 non ha impedito la frammentazione dell'applicazione della protezione dei dati personali") e 13 ("è necessario un regolamento che garantisca la certezza del diritto […] che offra il medesimo livello di diritti azionabili […] e una cooperazione efficace tra le autorità di controllo") risulta evidente che, onde evitare trattamenti differenti e discriminazioni sul territorio

[59] Art. 5, RGPD, dispone che: "1. I dati personali sono: trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) Raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»); f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»). 2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)".

dell'Unione in merito ai diritti concernenti la protezione dei dati personali, era necessario adottare norme stringenti che disciplinassero le modalità di lavoro, di ispezione e di collaborazione da parte delle autorità di controllo[60]. Questi articoli vanno letti anche alla luce della possibilità che – come visto con la sentenza *Google Spain* – un trattamento dati venga eseguito da uno stesso titolare in più di un paese dell'Unione, coinvolgendo più cittadini e più autorità di controllo. Qualora la stessa violazione venisse sollevata dai destinatari di diversi Stati membri presso le rispettive autorità di controllo, ecco che si potrebbe venire a configurare una situazione per la quale diverse autorità di controllo adottano diverse decisioni vincolanti in merito al medesimo trattamento di dati all'interno di una situazione di trasferimento transfrontaliero di dati personali. Paradossalmente, una situazione simile sarebbe contraria agli obiettivi di integrazione del mercato, in quanto rischierebbe di riproporre una situazione analoga a quella riscontrata nel caso FIAT[61] dove una non uniforme tutela del diritto alla protezione dei dati personali tra i Paesi membri comporta l'innalzamento di barriere immateriali al libero scambio, impedendo il completamento del progetto di mercato unico. Come ricordato dal considerando 10 del nuovo regolamento, gli obiettivi di integrazione economica e di fruizione uniforme in tutti i Paesi dell'Unione del diritto alla protezione dei dati personali, rendono necessario un approccio che garantisca coerenza e certezza del diritto. In quest'ottica va letta l'introduzione del meccanismo dello "sportello unico", dove l'autorità di controllo "dello stabilimento principale del titolare del trattamento […] dovrebbe fungere da autorità capofila"[62], ed è competente per l'adozione di decisioni vincolanti, in base ai poteri garantitigli dall'applicazione del RGPD. Il meccanismo dello sportello unico cerca di garantire l'uniformità delle decisioni delle autorità di controllo, quando quest'ultime sono chiamate ad intervenire, vuoi con linee guida vuoi con decisioni vincolanti[63], quando sono chiamate ad intervenire su situazioni il cui carattere sostanzialmente transnazionale potrebbe pregiudicare l'omogeneità del diritto dell'Unione. Nel prossimo capitolo verrà analizzata la sentenza C-645/19: *Facebook Ireland Limited e a. c. Gegevensbescherming-sautoriteit*, attraverso la quale evidenzia come, sebbene il meccanismo dello sportello unico sia stato concepito specialmente in termini economici, in quanto determina una semplificazione delle procedure per le imprese che operano su più territori dell'Unione, l'influenza della recente giurisprudenza della Corte sposta il focus della normativa europea in materia di protezione dati sugli obiettivi di protezione dei diritti fondamentali, rispetto all'iniziale prospettiva integralista[64]. Questo cambio di prospettiva, verrà argomentato, è alla base del ridimensionamento del principio dello sportello unico, a favore di un'estensione della tutela dei diritti alla protezione dei dati per i cittadini dell'Unione.

[60] Al considerando 129, del RGDP, viene affermato che: "[a]l fine di garantire un monitoraggio e un'applicazione coerenti del presente regolamento in tutta l'Unione, le autorità di controllo dovrebbero avere in ciascuno Stato membro gli stessi compiti e poteri effettivi, fra cui poteri di indagine, poteri correttivi e sanzionatori, e poteri autorizzativi e consultivi, segnatamente in caso di reclamo proposto da persone fisiche, e fatti salvi i poteri delle autorità preposte all'esercizio dell'azione penale ai sensi del diritto degli Stati membri, il potere di intentare un'azione e di agire in sede giudiziale o stragiudiziale in caso di violazione del presente regolamento".
[61] Délibération Commission National de l'Informatique et des Libertés (CNIL), dell'11 luglio 1989, No. 89-7811.
[62] RGDP, considerando 124.
[63] RGDP, considerando 125.
[64] FABBRINI (2015).

Capitolo 2
Il caso C-645/19: Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit

> "We have a responsibility to protect your data, and if we can't then we don't deserve to serve you".
> (Mark Zuckerberg, post su Facebook del 21 marzo 2018, a seguito dello scandalo Cambridge Analytica).

2.1 Procedimento principale

Il caso C-645/19 ha ad oggetto la domanda di pronuncia pregiudiziale presentata, nell'ambito della controversia tra Facebook Belgium BVBA, da un lato, e l'autorità per la protezione dei dati belga (APD), dall'altro, in merito ad un'azione inibitoria presentata dal presidente di quest'ultima con l'obiettivo di far cessare per gli utenti residenti in Belgio l'inserimento di *cookies* e la raccolta dati senza il consenso degli utenti. Il giudice del rinvio è la Corte di appello di Bruxelles.
Il procedimento principale origina l'11 settembre 2015, quando il presidente della Commissione per la tutela della vita privata belga (CPVP) intentò un'azione inibitoria a carico di Facebook Ireland, Facebook Inc. e Facebook Belgium dinanzi al Tribunale di primo grado di Bruxelles. L'azione inibitoria si poneva come obiettivo quello di porre fine alle violazioni gravi e su larga scala che, stando a quanto descritto dal CPVP, Facebook stava perpetuando nei confronti degli internauti belgi, non informandoli a sufficienza in merito al trattamento e alla raccolta dei dati personali. Modalità consistenti, tra l'altro, nella raccolta e nell'uso quotidiani con modalità illegali di informazioni sulle abitudini private di navigazione di milioni di utenti di internet in Belgio (sia titolari di profili Facebook che fruitori del servizio di Facebook non registrati), mediante tecnologie come *cookies*, *social plugins* (come, ad esempio, i pulsanti "mi piace" o "condividi") e *pixels*[65]. Il Tribunale di primo grado di Bruxelles si è dichiarato competente, accettando la giurisdizione territoriale sulle tre entità di Facebook. Le motivazioni evidenziate dal Tribunale di primo grado in merito alla sua competenza si rifanno al già citato caso *Google Spain*[66], secondo il quale la legge nazionale sulla protezione dei dati di uno Stato membro dell'UE si applica se le attività di uno Stato membro sono inestricabilmente legate alle attività del responsabile del trattamento dei dati. Infatti, la difesa di Facebook sosteneva che, in virtù dell'articolo 4 della direttiva 95/46[67], fossero da applicare le leggi nazionali in materia di protezione dei dati irlandesi e solamente la Corte irlandese avesse competenza in merito, avendo il responsabile del trattamento (Facebook Ireland Limited) sede legale in Irlanda. Di contro, il Tribunale di primo grado belga rilevò come l'attività di Facebook Belgium fosse inestricabilmente legata alle attività del responsabile del trattamento dei dati (Facebook Ireland), in quanto coinvolta nel marketing e nella vendita di spazi pubblicitari del servizio Facebook Inc. oltre che

[65] Caso C-645/19, sintesi della domanda di pronuncia pregiudiziale ai sensi dell'articolo 98, paragrafo 1, del regolamento di procedura della Corte di giustizia.
[66] Sentenza della Corte di giustizia *Google Spain.*
[67] L'articolo 4 della direttiva 95/46/CE dispone che: "[c]iascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali: a) effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile".

svolgere attività di lobbying per gli interessi del *social network*, e, considerato quanto sopra, dichiarò la sua competenza a giudicare l'applicabilità della legge belga. Il Tribunale di cui sopra si è poi pronunciato nel merito in una sentenza del 16 febbraio 2018, dichiarando che il *social network* in questione "non informava sufficientemente gli internauti belgi relativamente alla raccolta delle informazioni di cui trattasi e all'uso di tali informazioni"[68] e che quindi l'uso dei *cookies* da parte di Facebook fosse in violazione delle leggi belghe sulla *privacy*[69]. Il Tribunale di Bruxelles evidenziò, a sostegno dell'azione inibitoria presentata dal presidente della CPVP, che Facebook collocava *cookies* sui dispositivi di qualsiasi visitatore di siti web di terze parti che utilizzano i *plugins* di Facebook, come i siti di notizie con i pulsanti "mi piace" di Facebook, indipendentemente dal fatto che i destinatari fossero o meno utenti registrati del *social network*. In sua difesa, Facebook ha fatto riferimento all'esistenza sul proprio sito web di un *banner* di *cookies* per quelli collocati su siti *web* di terze parti spiegando come venga poi fatto affidamento ai meccanismi di accettazione dei *cookies* delle stesse terze parti. Nel valutare le informazioni fornite da Facebook attraverso il proprio *banner* dei *cookies*, e la *policy* dei *cookies* a cui questo *banner* fa riferimento, il Tribunale di primo grado ha rilevato che la suddetta *policy* non fosse sufficientemente chiara sulle operazioni di trattamento[70]. Non ci si poteva ragionevolmente aspettare che, in base alle informazioni fornite, gli utenti capissero che il loro comportamento sarebbe stato monitorato e registrato dal *social network*. Peraltro, il Tribunale di Bruxelles ha ritenuto che le informazioni date fossero incomplete in quanto non informavano le persone interessate sui loro diritti di accesso e di rettifica dei loro dati[71] in quanto il meccanismo di raccolta del consenso non garantisce che questo sia "libero, specifico e inequivocabile". Infatti, argomenta il Tribunale di primo grado, gli utenti avevano solo la scelta di accettare tutti i *cookies* o nessuno e, inoltre, gli utenti che avevano scelto di non accettare i *cookies* attraverso le impostazioni del loro browser venivano ancora presi di mira da Facebook[72].
Sulla base di queste osservazioni, il Tribunale di Bruxelles comminò al social una sanzione giornaliera di EUR 250.000, al fine di:

i. smettere di collocare i diversi *cookies* che violano la legge e tecnologie simili;

---

[68] Sentenza della Corte di giustizia, del 15 giugno 2021, causa C-645/19, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 32.
[69] Legge relativa alla tutela della vita privata con riguardo ai trattamenti di dati personali), dell'8 dicembre 1992, come modificata dalla legge dell'11 dicembre 1998, che ha recepito nel diritto belga la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, *relativa alla tutela e alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.*
[70] Art. 7, lettera a), della direttiva 95/46/CE, che recita: "[g]li Stati membri dispongono che il trattamento di dati personali può essere effettuato soltanto quando: a) la persona interessata ha manifestato il proprio consenso in maniera inequivocabile".
[71] Ivi, art. 10, che recita: "[g]li Stati membri dispongono che il responsabile del trattamento, o il suo rappresentante, debba fornire alla persona presso la quale effettua la raccolta dei dati che la riguardano almeno le informazioni elencate qui di seguito, a meno che tale persona ne sia già informata: a) l'identità del responsabile del trattamento ed eventualmente del suo rappresentante; b) le finalità del trattamento cui sono destinati i dati; c) ulteriori informazioni riguardanti quanto segue: - i destinatari o le categorie di destinatari dei dati, - se rispondere alle domande è obbligatorio o volontario, nonché le possibili conseguenze di una mancata risposta, - se esistono diritti di accesso ai dati e di rettifica in merito ai dati che la riguardano nella misura in cui, in considerazione delle specifiche circostanze in cui i dati vengono raccolti, tali informazioni siano necessarie per effettuare un trattamento leale nei confronti della persona interessata".
[72] VAN BAEL, BELLIS (2018: 3 ss.).

ii. smettere di raccogliere informazioni da questi *cookies*;
iii. cessare di fornire qualsiasi informazione "ingannevole" su come la società utilizza i *cookies*[73].

Inoltre, il Tribunale di Bruxelles chiese a Facebook di cancellare tutti i dati personali violati che erano già stati raccolti[74].
Facebook Inc., Facebook Ireland e Facebook Belgium presentarono appello contro la decisione del Tribunale di primo grado presso la Corte di appello di Bruxelles il marzo 2018. Nel periodo che intercorre tra l'azione inibitoria presentata dal CPVP e la sentenza del Tribunale di primo grado di Bruxelles, il quadro normativo viene mutato dall'introduzione del regolamento 2016/679 (RGPD) il quale abroga la direttiva 95/46, e dall'introduzione della legge del 3 dicembre 2017 che abroga la legge di attuazione della direttiva dell'8 dicembre del 1992. In quest'ottica, l'APD agisce in qualità di successore legale del CPVP e del suo presidente che aveva promosso l'azione inibitoria, nel ricorso presentato dinanzi alla Corte di appello dal *social network*. A differenza di quanto statuito dal Tribunale di Bruxelles, la Corte di appello si è dichiarata unicamente competente a intervenire nella sezione riguardante Facebook Belgium. Prima di entrare nel merito, tuttavia, il giudice del rinvio si è trovato dinanzi ad una questione relativa alla legittimazione e all'interesse ad agire da parte dell'APD. Come scritto poco sopra, la Corte di appello si trovava immersa in un nuovo contesto normativo, che, secondo la difesa di Facebook, rendeva l'azione inibitoria irricevibile, poiché priva di base giuridica a seguito dell'abrogazione della legge belga in materia di protezione dei dati personali e l'entrata in vigore del RGDP, e conseguentemente del principio dello sportello unico previsto dalle disposizioni[75] del suddetto atto. Sulle basi di tali disposizioni, argomenta Facebook, spetterebbe solo al *data protection commissioner* (Commissario per la protezione dei dati, Irlanda), in quanto unico ente competente a presentare un'azione inibitoria nei confronti di Facebook Ireland, quest'ultimo l'unico titolare del trattamento dei personali degli utenti presenti nel territorio dell'Unione.
La questione presentata dalla difesa sembra riproporre le osservazioni sollevate nel corso del procedimento principale dinanzi al Tribunale di primo grado, dove venne sostenuto che la legge applicabile fosse quella irlandese, in quanto sede dello stabilimento principale del *social network*. Il ragionamento del Tribunale, che vedeva l'attività di Facebook Belgium inestricabilmente legata a quello di Facebook Ireland, non trova una base giuridica per i fatti successivi al 25 maggio 2018, in quanto all'interno del nuovo regolamento non viene più contemplata l'applicazione delle leggi nazionali di attuazione dei diversi Stati membri, e proprio per evitare pareri discordanti tra le diverse autorità di controllo fu introdotto un meccanismo che potesse garantire coerenza e uniformità al diritto dell'Unione[76]. Ai sensi dell'articolo 56 del RGPD, argomenta il giudice del rinvio, sembrerebbe competente a presentare un'azione inibitoria esclusivamente il Commissario per la protezione dei dati, dinanzi ai giudici irlandesi, in forza del principio dello sportello unico[77]. La Corte di appello ha quindi deciso di sospendere il procedimento, per poter sottoporre i suoi dubbi interpretativi alla Corte di giustizia attraverso un ricorso in via pregiudiziale, così come consentito dall'articolo 267 del TFUE.

[73] *Ibidem.*
[74] Sentenza della Corte di giustizia, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 32.
[75] Art. 55, paragrafo 1, e articoli da 56 a 58 e da 60 a 66 del RGPD.
[76] RGDP, considerando 129.
[77] Sentenza della Corte di giustizia, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 32.

Nel prossimo paragrafo verrà proposta una rapida disamina delle questioni pregiudiziali presentate dal giudice del rinvio, le quali poi saranno lette alla luce tanto del contesto normativo quanto delle conclusioni presentate in fase preliminare dall'Avvocato generale Michael Bubek.

2.2 Questioni pregiudiziali sottoposte alla Corte di giustizia.

Il contenuto delle domande pregiudiziali riporta in auge la tensione che fin dalla nascita della normativa europea in materia di protezione dei dati, in particolare, e protezione dei diritti fondamentali, in generale, circoscrive l'operato dell'Unione. Tale tensione va inquadrata all'interno del contesto teleologico che ha portato alla nascita dell'Unione europea, vale a dire il perseguimento di un'integrazione economica e l'instaurazione del mercato interno, a seguito del quale si è via via affermato – e sancito definitivamente con l'introduzione della Carta di Nizza[78] come atto giuridico vincolante – il compito dell'Unione di tutelare i diritti fondamentali. In quest'ottica va quindi compreso il dubbio relativo all'interpretazione conforme da dare al principio dello sportello unico, e quale aspetto occorre far prevalere tra i due obiettivi (di tutela delle persone fisiche con riguardo al trattamento dei dati personali e la riduzione di barriere al completamento del mercato unico) dell'Unione. La Corte d'appello belga, infatti, nel proporre le questioni pregiudiziali alla Corte di giustizia, ha in fase preliminare evidenziato come quest'ultima, in giudizi recenti, abbia dato un'interpretazione estensiva rispetto alla giurisdizione delle autorità di controllo[79]. Tuttavia, tali giudizi erano relativi alla vecchia normativa – la direttiva 95/46 – e pertanto si è reso necessario un nuovo orientamento giurisprudenziale per la Corte d'appello, che tenesse conto del mutato contesto normativo. Ciò premesso, le sei questioni pregiudiziali riguardano l'interpretazione dell'articolo 55, paragrafo 1, e degli articoli da 56 a 58 e da 60 a 66 del regolamento 2016/679 in merito allo scopo territoriale e ai poteri delle autorità di controllo degli Stati membri. La Corte d'appello belga si chiede se l'APD abbia il potere di agire in sede giudiziale nonostante essa non sia l'autorità di controllo capofila per il trattamento transfrontaliero di cui trattasi, essendo Facebook Ireland, ai sensi dell'articolo 4, paragrafo 16, identificato come stabilimento principale[80] e pertanto, ai sensi dell'articolo 56,

[78] Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, proclamata dal Parlamento europeo, dal Consiglio e dalla Commissione. La Carta divenne vincolante con l'entrata in vigore del TUE, il quale dispone all'articolo 6: "[l]'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adottata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati".

[79] Si veda a tal proposito la sentenza della Corte di giustizia, del 5 giugno 2018, causa C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*. In quest'occasione la Corte dichiarò l'autorità di controllo tedesca competente a pronunciarsi su una controversia in materia di protezione dei dati personali, sebbene il titolare del trattamento dei dati in questione avesse sede in Irlanda e la sua controllata con sede in Germania, ossia la Facebook *Germany GmbH*, si occupasse soltanto della vendita di spazi pubblicitari e di altre attività di marketing nel territorio tedesco. Tuttavia, la domanda di pronuncia pregiudiziale della quale era investita la Corte verteva sulle interpretazioni delle disposizioni contenute nella direttiva 95/46.

[80] Art. 16, paragrafo 16, lettera a: "[p]er quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali 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, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale".

paragrago 1, l'autorità di controllo irlandese (Commissario per la protezione dei dati) ad essere identificata come autorità di controllo capofila[81].
Entrando nel dettaglio, relativamente alla prima questione pregiudiziale, il giudice del rinvio ha chiesto alla Corte di giustizia

> "[s]e gli articoli [55, paragrafo 1], da 56 a 58 e da 60 a 66 del [regolamento 2016/679], in combinato disposto con gli articoli 7, 8 e 47, della [Carta], debbano essere interpretati nel senso che un'autorità di controllo, che, in forza della normativa nazionale adottata in esecuzione dell'articolo [58, paragrafo 5], di tale regolamento, abbia il potere di agire in sede giudiziale dinanzi a un giudice del suo Stato membro contro le violazioni di detto regolamento, non può esercitare tale potere con riguardo a un trattamento transfrontaliero se essa non è l'autorità di controllo capofila per il trattamento transfrontaliero di cui trattasi"[82].

Parafrasando, ciò che preme capire ai fini del giudizio è se l'APD disponga della competenza per quanto riguarda il trattamento dei dati in questione, pur non essendo l'autorità di controllo capofila, la quale ai sensi dell'articolo 4, punto 23, del RGPD è identificabile con l'autorità di controllo dello stabilimento principale. Inoltre, prosegue la Corte d'appello, occorre capire

> "[s]e, a tal riguardo, assuma rilevanza la circostanza che il titolare di detto trattamento transfrontaliero non abbia in tale Stato membro lo stabilimento principale, ma solo un altro stabilimento"[83].

Ai sensi dell'articolo 55, paragrafo 1, del nuovo regolamento, tutte le autorità di controllo posseggono generalmente una *ratione loci* limitata, vale a dire hanno uno scopo territoriale limitato, potendo agire in sede giudiziale per violazioni del regolamento avvenute sul suolo dello Stato membro di appartenenza, presso l'autorità giudiziaria del rispettivo Stato membro. Ciò che però non sembra essere chiaro, alla luce delle domande interpretative presentate dalla Corte d'appello belga, è se la competenza dell'autorità di controllo sia correlata alla presenza di uno stabilimento principale all'interno del territorio in cui dispongono della competenza ad agire, in quanto il regolamento non precisa gli enti nei confronti dei quali le autorità di controllo possano agire in giudizio[84]. Nella seconda domanda pregiudiziale il giudice del rinvio si chiede se la risposta alla prima questione pregiudiziale sarebbe diversa qualora il titolare del trattamento transfrontaliero non avesse lo stabilimento principale, ma solo un altro stabilimento in tale Stato membro. In altre parole, guardando al caso in esame e specificando gli attori coinvolti, il giudice del rinvio vuole sapere se il fatto che Facebook Belgium non sia uno stabilimento principale, e non essendo quindi il titolare del trattamento transfrontaliero dei dati, possa incidere sulla capacità dell'APD di agire in sede giudiziale.
Con la sua terza questione pregiudiziale, il giudice del rinvio chiede

---

[81] Art. 56, paragrafo 1: "[f]atto salvo l'articolo 55, l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare e del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare del trattamento o responsabile del trattamento, secondo la procedura di cui all'articolo 60".
[82] Sentenza della Corte di giustizia, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 4, paragrafo 1.
[83] Ivi, punto 4, paragrafo 2.
[84] Conclusioni dell'Avvocato generale Michal Bobek, del 13 gennaio 2021, causa C-645/19, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 150.

> "[s]e, a tal riguardo, assuma rilevanza la circostanza che l'autorità nazionale di controllo intenti l'azione nei confronti dello stabilimento principale del titolare del trattamento o nei confronti dello stabilimento nel proprio Stato membro"[85].

Parafrasando, ciò che interessa al giudice del rinvio è sapere se le autorità di controllo possano agire anche nei confronti degli stabilimenti situati all'estero, e se quindi abbiano una competenza territoriale limitata o meno. Anche in questo caso, la questione pregiudiziale va calata all'interno degli avvenimenti che hanno dato luogo al procedimento principale, in quanto va chiarito se Facebook Ireland, in qualità di stabilimento principale, debba essere sottoposto alla giurisdizione esclusiva del *data protection commissioner* o se la competenza della autorità di controllo vada interpretata in maniera estensiva. Tuttavia, va chiarito fin d'ora, la competenza dell'autorità di controllo rimane circoscritta alle violazioni avvenute all'interno del suo territorio, e un'eventuale competenza nei confronti di titolari del trattamento o responsabili del trattamento stabiliti fuori dai confini nazionali non implica una competenza per le violazioni non avvenute all'interno del territorio del rispettivo Stato membro. Oltre alla competenza territoriale dell'autorità di controllo e, oltre alla ripartizione di competenze tra autorità di controllo capofila e autorità di controllo degli altri Stati membri, va chiarito, ai fini della risoluzione del caso in esame, se assuma rilevanza il fatto che l'autorità di controllo abbia intentato l'azione legale prima della data di entrata in vigore del RGDP, ossia prima del 25 maggio 2018. Come visto in fase preliminare, il procedimento principale nasce in un contesto normativo incerto, in quanto il giudice di primo grado si trova ad operare all'interno del quadro giuridico della direttiva 95/46, mentre la Corte d'appello belga è chiamata a giudicare sulla base di una mutata cornice normativa. Pertanto, la quarta questione pregiudiziale sollevata dal giudice del rinvio si interroga sulla *ratione temporis* e chiede alla Corte di giustizia

> "[s]e, a tal riguardo, assuma rilevanza la circostanza che l'autorità nazionale di controllo abbia già intentato l'azione prima della data di entrata in vigore (il 25 maggio 2018) del regolamento [2016/679]"[86].

Mentre rimane indiscutibile il principio di irretroattività degli atti giuridici[87], è incerto come porsi dinanzi ai procedimenti giurisdizionali pendenti nati prima dell'entrata in vigore del RGDP, in quanto quest'ultimo è sprovvisto di norme transitorie che "disciplinano lo stato dei procedimenti giurisdizionali in corso"[88] alla data di entrata in vigore del nuovo regolamento.
La difesa di Facebook Ireland, Facebook Inc. e Facebook Belgium sostiene addirittura che l'applicazione del regolamento, la cui data di entrata in vigore è il 25 maggio 2018, comporti l'irricevibilità di un'azione intentata prima di tale data, suggerendo quindi una sorta di amnistia nei confronti delle violazioni effettuate prima del decorrere della stessa. Occorre quindi, ai fini del giudizio della Corte d'appello belga, comprendere come porsi da un lato per i procedimenti precedenti al 25 maggio 2018 e dall'altro per quelli successivi ed in particolare come differisca il potere dell'autorità di controllo a cavallo del cambiamento normativo posto in atto con l'adozione e la successiva entrata in vigore del RGDP.

---

[85] Sentenza della Corte di giustizia, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 4, paragrafo 3.
[86] Ivi, punto 4, paragrafo 4.
[87] Ivi, punto 100.
[88] Conclusioni dell'Avvocato generale Bobek, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 157.

Mentre la seconda, terza e quarta questione cercano di evidenziare la rilevanza o meno di determinati fattori per la risoluzione della prima domanda pregiudiziale al fine dell'esercizio del potere dell'autorità di controllo belga, la quinta questione posta dalla Corte d'appello alla Corte di giustizia chiede se

> "[i]n caso di risposta affermativa alla prima questione, se l'articolo [58, paragrafo 5], del regolamento 2016/679 abbia effetto diretto, cosicché un'autorità nazionale di controllo può invocare detto articolo per intentare o proseguire un'azione nei confronti di privati, anche se l'articolo [58, paragrafo 5], del regolamento 2016/679 non sia stato specificamente trasposto nella normativa degli Stati membri, pur essendo la trasposizione obbligatoria"[89].

Occorre rammentare in questa sede, al fine di facilitare il più possibile la comprensione della questione, come l'articolo 58 paragrafo 5 del RGPD dispone che

> "[o]gni Stato membro dispone per legge che la sua autorità di controllo abbia il potere di intentare un'azione o di agire in sede giudiziale o, ove del caso, stragiudiziale in caso di violazione di tale regolamento per far rispettare le disposizioni dello stesso"[90].

Il regolamento, come già ampiamente discusso, è, ai sensi dell'articolo 288, secondo comma, del TFUE, obbligatorio in tutti i suoi elementi e in quanto regolamento produce effetti immediati negli ordinamenti nazionali, senza che questi adottino alcuna misura applicativa[91]. Tuttavia, Facebook, nelle osservazioni presentate alla Corte, argomenta che l'articolo 58, paragrafo 5, impone chiaramente agli Stati membri di fare qualcosa per la sua attuazione, e pertanto, al fine di poter agire in via giudiziaria e di poter esercitare la propria competenza, sia necessaria tale norma applicativa; quest'ultima, secondo il parere di Facebook, essendo assente nel diritto belga, rende l'azione dell'APD infondata.
Infine, nella sua ultima domanda pregiudiziale, il giudice del rinvio interroga la Corte di giustizia in merito alla possibilità che

> "[i]n caso di risposta affermativa alle questioni che precedono, se l'esito di siffatti procedimenti possa ostare ad una conclusione opposta dell'autorità di controllo capofila nel caso in cui tale autorità capofila esamini le medesime attività di trattamento transfrontaliero o attività analoghe, conformemente al meccanismo previsto agli articoli 56 e 60 del regolamento 2016/679"[92].

In altre parole, il giudice del rinvio si chiede in quale misura si possa derogare al principio di coerenza, stabilito agli articoli 64 e 65[93], qualora venga accertata la competenza di un'autorità di controllo, diversa dall'autorità di controllo capofila, ad intentare un'azione giudiziaria nei confronti di un responsabile o di un titolare del trattamento transfrontaliero di dati personali. Infatti, va rilevato come nell'eventualità in cui più di un'autorità di controllo avesse la competenza ad agire in sede giudiziale, ciò potrebbe comportare un'eventuale

---

[89] Sentenza della Corte di giustizia, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 4, paragrafo 5.
[90] Art. 58, paragrafo 5, RGDP.
[91] Sentenza della Corte di giustizia, del 15 marzo 2017, causa C-528/15, *Policie ČR, Krajské ředitelství policie Ústeckého kraje, odbor cizinecké policie c. Salah Al Chodor e a.*, punto 27.
[92] Sentenza della Corte di giustizia, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 4 paragrafo 6.
[93] Si veda a tal proposito, sentenza della Corte di giustizia, del 24 settembre 2019, causa C-507/17, *Google LLC c.Commission nationale de l'informatique et des libertés (CNIL)*, punto 68.

frammentazione del diritto, trovandosi dinanzi a pareri discordanti di diverse autorità di controllo in merito alle stesse.

2.3 Conclusioni dell'Avvocato generale.

Considerati i fatti del procedimento principale e inquadrato il contesto normativo di riferimento, è opportuno, prima di procedere all'analisi del ragionamento della Corte di giustizia, soffermarsi sulle conclusioni dell'Avvocato generale, Michal Bobek, presentate in data 13 gennaio 2021, e sulle osservazioni formulate dalle parti intervenute per poter meglio comprendere gli argomenti sostenuti dal giudice dell'Unione in fase di giudizio. Il ruolo dell'Avvocato generale viene definito dall'articolo 252, secondo paragrafo, del TFUE, il quale gli assegna la facoltà di presentare pubblicamente, in modo imparziale e indipendente, conclusioni motivate.
Il ragionamento dell'Avvocato generale, il quale si articola a partire da un'analisi dei fatti di cui al procedimento principale, delineerà in modo chiaro quale che sia la corretta interpretazione delle disposizioni in esame da fornire al giudice del rinvio. Bobek argomenta che l'interpretazione del regolamento dovrebbe trovarsi in una posizione intermedia, la quale, benché lontana dalla versione estremista sostenuta dalla APD (secondo la quale ogni autorità di controllo ha la competenza ad agire in sede giudiziale per le violazioni avvenute nel rispettivo stato membro), consente ad un'autorità di controllo diversa dall'autorità di controllo capofila ad agire in sede giudiziale, purché determinate condizioni vengano rispettate. Tale conclusione si avvale di un'esaustiva analisi del RGDP, attraverso un'interpretazione letterale, sistematica, teleologica e storica oltre ad un'interpretazione dello stesso alla luce degli obblighi contenuti nella Carta.
Per prima cosa, l'Avvocato generale riassume in brevi battute il contenuto delle questioni pregiudiziali, enucleando la problematica essenziale, ovvero se

> "[l]'APD possa proseguire un'azione giudiziale nei confronti di Facebook Belgium per quanto riguarda il trattamento transfrontaliero di dati personali che è avvenuto successivamente all'applicabilità del RGPD, dato che l'entità incaricata del trattamento dei dati è Facebook Ireland Ltd"[94].

L'Avvocato generale rileva come la problematica, per essere affrontata, debba essere letta alla luce della portata e del funzionamento del meccanismo dello sportello unico[95], il quale al considerando 127 del RGPD viene descritto come quella serie di norme che, in caso di trattamento transfrontaliero, instaurano un sistema di procedure di cooperazione e coerenza in cui l'autorità di controllo capofila funge da vertice decisionale[96]. Per meglio comprendere il

[94] Conclusioni dell'Avvocato generale Bobek, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 27.
[95] Ivi, punto 28.
[96] RGDP, considerando 127: "[o]gni autorità di controllo che non agisce in qualità di autorità di controllo capofila dovrebbe essere competente a trattare casi locali qualora 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, ad esempio quando l'oggetto riguardi il trattamento di dati personali di dipendenti nell'ambito di specifici rapporti di lavoro in uno Stato membro. In tali casi, l'autorità di controllo dovrebbe informare senza indugio l'autorità di controllo capofila sulla questione. 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 («meccanismo dello sportello unico»), ovvero se l'autorità di controllo che l'ha informata debba

tenore di tale principio, e al fine di illustrare le motivazioni che lo spingono a sostenere una posizione intermedia tra il ricorrente e il resistente, l'Avvocato generale offre un'analisi da un punto di vista letterale e sistematico, prima, e da un punto di vista teleologico e storico, dopo, a sostegno dell'interpretazione che ritiene essere corretta del RGDP.
Sintetizzando il ragionamento contenuto nelle sue conclusioni, a parere dell'Avvocato le disposizioni contenute nel regolamento depongono a favore di un'interpretazione nel senso che l'autorità di controllo capofila detiene una competenza generale in ambito di trattamento transfrontaliero, mentre le autorità di controllo interessate[97] dispongono di un potere più limitato in tal senso. Le motivazioni a sostegno di tale tesi sono *in primis* ravvisate dal tenore letterale e contestuale delle disposizioni del RGDP, dove la competenza generale dell'autorità di controllo capofila viene disposta dall'articolo 56, paragrafo 1, per il quale

> "[l]'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare e del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare del trattamento o responsabile del trattamento, secondo la procedura di cui all'articolo 60".

La competenza generale è rafforzata dalla lettura congiunta del paragrafo 6 dell'articolo ivi menzionata, oltre che dalla lettura del considerando 124; tale competenza a carattere generale può inoltre essere dedotta dall'eccezionalità con la quale vengono descritti i casi, all'interno del RGDP, nei quali la competenza per i trattamenti transfrontalieri viene affidata alle autorità di controllo diverse da quella capofila. Tale carattere di eccezione, incalza l'Avvocato generale, risulta chiaro dalla lettura e dal contenuto degli articoli 55, paragrafo 2, 56, paragrafo 2, e 66, i quali rappresentano deroghe alla regola generale. Per questi motivi, la competenza dell'autorità di controllo capofila è la regola, mentre la competenza delle autorità di controllo diverse dalla capofila, l'eccezione. Tuttavia, le osservazioni presentate dalla APD e dei governi belga, italiano, polacco e portoghese, suggeriscono, invece, che il tenore delle disposizioni ivi citate andrebbe letto in favore di un potere quasi incondizionato di qualsiasi autorità di controllo ad agire in sede giudiziale. Questi, infatti, argomentano che l'articolo 56, paragrafo 1[98], il cui rigo iniziale recita "fatto salvo l'articolo 55", comporterebbe che i poteri delle autorità di controllo capofila non possano in nessun modo limitare quelli attribuiti ad ogni autorità di

---

trattarlo a livello locale. Al momento di decidere se intende trattare il caso, l'autorità di controllo capofila dovrebbe 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".

[97] Al considerando 124 del RGDP: "le autorità di controllo interessate sono coinvolte nel processo decisionale in ambito transfrontaliero in quanto "il titolare del trattamento o il responsabile del trattamento ha uno stabilimento nel territorio dei loro Stati membri, perché il trattamento incide in modo sostanziale sugli interessati residenti nel loro territorio o perché è stato proposto loro un reclamo".

[98] Art. 56, paragrafo 1, RGDP: "[f]atto salvo l'articolo 55, l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare e del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare del trattamento o responsabile del trattamento, secondo la procedura di cui all'articolo 60".

controllo ai sensi dell'articolo 55[99]. Un'interpretazione simile, argomenta Bobek, priverebbe l'articolo 56 di qualsivoglia significato[100], in quanto renderebbe superfluo il ruolo di raccordo affidato all'autorità di controllo capofila all'interno dei meccanismi di cooperazione e coerenza volti a garantire la corretta applicazione del regolamento[101]. Inoltre, e come già sottolineato da un parere del Comitato europeo per la protezione dei dati[102], il rapporto tra l'articolo 56 (competenza dell'autorità di controllo capofila) e l'articolo 55 (competenze delle autorità di controllo) va letto sulla base del criterio *lex specialis derogat lex generali*, per cui la prima derogherebbe alle competenze generali delle autorità di controllo nel caso di un trattamento transfrontaliero di dati. Per questi motivi, aggiunge l'Avvocato generale, l'espressione "fatto salvo l'articolo 55" letta alla luce del contesto in cui viene formulata, assume un significato diametralmente opposto rispetto a quello suggerito dalla APD, la quale isola la lettura dell'articolo 56, paragrafo 1, dal resto del regolamento, offrendone un'interpretazione estensiva e decontestualizzata[103]. I poteri affidati alle autorità di controllo prescindono quindi dalla loro competenza in materia di trattamento transfrontaliero, ma spetta poi all'autorità di controllo capofila adottare le decisioni vincolanti nei confronti del responsabile del trattamento o del titolare del trattamento. Infatti,

> "[c]iascuna autorità di controllo contribuisce all'applicazione corretta e coerente del regolamento. A tal fine, ciascuna autorità di controllo – indipendentemente dal suo ruolo quale ACC o ACI in un caso specifico – deve, ad esempio, esaminare i reclami proposti dinanzi ad essa e farlo con la diligenza richiesta"[104].

E, prosegue l'Avvocato generale,

> "anche nel caso in cui le presunte violazioni riguardino il trattamento transfrontaliero e un'autorità non sia l'ACC, le altre autorità di controllo dovrebbero essere in grado di esaminare la questione al fine di fornire un contributo significativo quando chiamate a farlo nell'ambito dei meccanismi di cooperazione e coerenza"[105].

Pertanto, appare evidente come l'autorità di controllo capofila non sia l'unico organo incaricato dell'applicazione del RGPD in situazioni transfrontaliere ma faccia parte di un modello strutturato che prevede una responsabilità condivisa "per sorvegliare l'applicazione del RGPD e garantirne una coerente applicazione"[106]. Nelle argomentazioni dell'Avvocato generale ciò che viene evidenziato maggiormente sono i motivi sottesi che spinsero in prima battuta all'adozione dello sportello unico e l'introduzione dell'autorità di controllo. Nonostante la APD sostenga che per rispettare gli articoli 7, 8 e 47 della Carta sia necessario un potere incondizionato delle autorità di controllo ad agire in

---

[99] Art. 55, paragrafo 1: "[o]gni autorità di controllo è competente a eseguire i compiti assegnati e a esercitare i poteri a essa conferiti a norma del presente regolamento nel territorio del rispettivo Stato membro".
[100] Conclusioni dell'Avvocato generale Bobek, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 52.
[101] Si veda in particolare l'articolo 60 il quale si intitola "[c]ooperazione tra l'autorità di controllo capofila e le altre autorità di controllo interessate".
[102] Parere del Comitato europeo per la protezione dei dati, del 9 luglio 2019, 8/2019, *sulla competenza di un'autorità di controllo in caso di mutamento delle circostanze relative allo stabilimento principale o unico*, paragrafi 19 e 20.
[103] Conclusioni dell'Avvocato generale Bobek, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 62.
[104] Ivi, punto 69.
[105] *Ibidem.*
[106] Ivi, punto 112.

sede giudiziale, l'introduzione dei meccanismi di cooperazione e coerenza dovrebbe "contribuire a una rafforzata enfasi sulla promozione e salvaguardia dei diritti sanciti, in particolare, agli articoli 7 e 8 della Carta"[107]. Infatti, per i legislatori dell'Unione, la necessità di garantire coerenza rappresenta la questione principale, visti i limiti della precedente direttiva 95/46 e l'assenza di meccanismi di coordinamento lasciava ampio spazio ad incongruenze[108], al fine di sventare il rischio che le varie autorità di controllo adottassero approcci diversi in relazione al trattamento transfrontaliero[109]. Riemerge con forza alla luce delle argomentazioni dell'Avvocato generale, come la complessa architettura del regolamento e il sistema di cooperazione vadano inquadrati sotto il duplice obiettivo di tutela delle persone fisiche e di rimozione degli ostacoli ai flussi di dati personali all'interno dell'Unione. In altre parole, il meccanismo dello sportello unico è stato concepito nell'ottica di garantire certezza del diritto lungo tutto il territorio dell'Unione, al fine di evitare disparità tra i livelli di protezione e salvaguardare il libero scambio di dati nell'area europea[110]. Per questo motivo, e per i motivi sopra citati, l'interpretazione prospettata dall'APD va in senso contrario rispetto a quanto introdotto dal regolamento, ammantando il diritto alla protezione dei dati di un'eterogeneità lontana dai fini e dagli obiettivi di coerenza e uniformità del RGDP. Dare la possibilità a tutte le autorità di controllo di agire in sede giudiziale indistintamente, oltre ad essere contrario ai fini del regolamento[111], farebbe tornare indietro di anni la legislazione europea in materia di protezione dei dati, in quanto eliminerebbe *de facto* alcune parti fondamentali del regolamento ritornando così al sistema introdotto dalla direttiva, il quale, come già più volte visto, voleva esplicitamente essere superato dal legislatore dell'Unione[112]. Il regolamento, proprio al fine di garantire certezza e coerenza del diritto, tutela in modo esplicito e definito da eventuali situazioni di inerzia amministrativa. Infatti, oltre a prevedere meccanismi che consentono di risolvere divergenze tra opinioni e pareri contrastanti espressi dalle autorità di controllo[113], vengono inclusi all'interno del regolamento meccanismi per superare situazioni di inattività da parte dell'amministrazione. Infatti, l'RGPD esige che l'autorità di

[107] Ivi, punto 96.
[108] Ivi, punto 79.
[109] Conclusioni dell'Avvocato generale H. Saugmandsgaard Øe, del 19 dicembre 2019, caso C-311/18, *Data Protection Commissioner c. Facebook Ireland Limited e Maximillian Schrems*, punto 155.
[110] Conclusioni dell'Avvocato generale Bobek, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 111.
[111] Ivi, paragrafo 112.
[112] RGDP, considerando 9, "[s]ebbene i suoi obiettivi e principi rimangono tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche. La compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare la libera circolazione dei dati personali all'interno dell'Unione. Tali differenze possono pertanto costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione. Tale divario creatosi nei livelli di protezione è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE".
[113] Il sistema istituito dal RGPD prevede che in situazioni transfrontaliere l'autorità di controllo capofila può agire solo con il consenso delle altre autorità di controllo interessate e non può ignorarne le opinioni. Qualora dovessero persistere divergenze di opinioni tra le diverse autorità, queste sono regolate da un organo specifico, il comitato europeo per la protezione dei dati. Si veda a tal proposito articolo 60 RGDP.

controllo capofila agisca prontamente[114] e qualora questa non rispetti tale obbligo esistono misure di contrasto alla sua inerzia, come evidenziato dall'Avvocato generale nelle sue conclusioni[115].
Considerato il tenore letterale e valutati tutti gli elementi contenuti nel regolamento, si deve giungere alla conclusione che l'interpretazione data dalla APD non è auspicabile per i motivi sopra elencati, ma ciò non significa che sia *in ogni caso* preclusa la possibilità per un'autorità di controllo, diversa dall'autorità capofila, di agire dinanzi ai giudici nazionali nei confronti di un titolare o di un responsabile del trattamento nel caso di un trattamento transfrontaliero. Esistono, quindi, specifiche circostanze all'interno delle quali è possibile derogare alla competenza generale dell'autorità di controllo capofila e al principio di coerenza.
Tali condizioni particolari sono:

a. La circostanza in cui un'autorità di controllo adisca un giudice nazionale agendo al di fuori dell'ambito materiale del RGDP;
b. Nei casi previsti dall'articolo 55, paragrafo 2, ove il trattamento venga effettuato da autorità pubbliche o organismi privati che agiscono sulla base dell'articolo 6, è competente l'autorità di controllo dello Stato membro interessato;
c. Essendo il meccanismo dello sportello unico applicabile unicamente ai titolari del trattamento con almeno uno stabilimento nell'Unione, non esiste un'autorità di controllo capofila per quanto riguarda un trattamento transfrontaliero da parte di titolari del trattamento che non hanno uno stabilimento nell'Unione europea. In questo caso, i titolari del trattamento deve confrontarsi con ogni autorità di controllo degli Stati membri in cui operano[116];
d. L'articolo 66, paragrafo 1 del RGPD prevede una deroga al meccanismo dello sportello unico per adottare misure urgenti (ad esempio nei casi in cui un'autorità di controllo interessata si trovi di fronte a una persistente inerzia dell'ACC competente) qualora ricorrano le condizioni appropriate. In questa situazione eccezionale, l'intera gamma dei poteri dell'autorità di controllo è esercitabile dalla stessa.
e. Nell'eventualità in cui l'autorità di controllo capofila decida di non trattare il caso, ai sensi dell'articolo 56, paragrafo 5 del RGDP, l'autorità di controllo interessato può conservare il potere di agire in giudizio.

Concludendo, la risposta alla prima questione pregiudiziale da fornire al giudice del rinvio a parere dell'Avvocato generale dovrebbe essere che, alla luce delle disposizioni del RGDP, è consentito ad un'autorità di controllo diversa dall'autorità di controllo capofila di agire in sede giudiziale dinanzi ad un giudice del rispettivo Stato membro, nelle condizioni e secondo le procedure previste dal regolamento[117].

---

[114] Art. 60, paragrafo 3, RGDP, "comunica senza ritardo le informazioni utili sulla questione alle altre autorità di controllo interessate [e trasmette] senza indugio alle altre autorità di controllo interessate un progetto di decisione per ottenere il loro parere e tiene debitamente conto delle loro opinioni".
[115] Conclusioni Avvocato generale Bobek, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 116.
[116] Si veda a tal proposito, linee guida Gruppo di lavoro articolo 29, del 5 aprile 2017, *per la protezione dei dati, per l'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento*.
[117] Conclusioni dell'Avvocato generale Bobek, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 140.

Dalle delucidazioni fornite in merito all'interpretazione del RGPD e alla luce della soluzione proposta per la prima questione pregiudiziale, la risposta da dare per le altre questioni segue lo stesso *fil rouge*, secondo il quale in determinate situazioni, è possibile per un'autorità di controllo diversa da quella capofila agire in sede giudiziale. Di particolare importanza la circostanza per cui non rileva, ai fini dell'esercizio dei poteri dell'autorità di controllo, la presenza o meno di uno stabilimento del titolare del trattamento nello Stato membro di appartenenza[118]. Infatti, a parere dell'Avvocato generale, il criterio discretivo in base al quale vada rilevata la competenza, o meno, dell'autorità di controllo, diversa dall'autorità di controllo capofila, non è tanto la presenza di uno stabilimento del titolare del trattamento, quanto l'esistenza di una delle fattispecie sopraelencata, in deroga al principio di coerenza. Per tale ragione, per rispondere alla seconda questione pregiudiziale[119], conclude l'Avvocato generale, nella misura in cui lo stabilimento principale, così come delineato dall'articolo 4, paragrafo 16, sia situato in un altro Stato membro, non osta all'esercizio dei poteri dell'autorità di controllo ad agire in sede giudiziale per violazioni avvenute sul territorio del rispettivo Stato membro nell'ambito di trattamenti transfrontalieri nei confronti del titolare o del responsabile del trattamento. Addirittura, nell'ambito della terza questione pregiudiziale, l'Avvocato generale afferma che la disposizione relativo all'ambito territoriale delle autorità di controllo, l'articolo 58, paragrafo 5, del RGDP, essendo formulato in modo ampio non precisa le entità nei confronti dei quali le autorità di controllo sarebbero chiamate ad agire. In altre parole, le autorità di controllo – sempre che siano competenti ad agire alla luce di quanto dichiarato in risposta alla prima questione pregiudiziale – non sono obbligate ad agire solo nei confronti dello stabilimento del titolare del trattamento situato nel loro territorio di appartenenza, ma possono agire anche nei confronti degli stabilimenti situati all'estero. L'elemento di territorialità riguarda gli effetti del trattamento, ma non la sede, e pertanto non vi sono limiti alle azioni nei confronti di titolari del trattamento o responsabili del trattamento il cui stabilimento è fuori dai confini nazionali[120]. Nelle parole dell'Avvocato generale,

> "[r]itengo che il nuovo meccanismo dello sportello unico, creando un punto centrale di applicazione delle norme, implichi necessariamente che un'autorità di controllo possa agire anche nei confronti di stabilimenti situati all'estero"[121].

Ciò detto, deve sempre essere tenuto a mente come tale competenza, vuoi in patria vuoi all'estero, sia rilevabile solo a determinate condizioni e non sia rappresentativa della generalità dei casi.
La quarta questione pregiudiziale[122] viene trattata più brevemente, ma non per questo assume minor rilevanza all'interno del quadro generale delle conclusioni. Per rispondere alla quarta questione pregiudiziale, l'Avvocato generale evidenzia in via preliminare come non esistano norme transitorie all'interno del RGPD che disciplinino lo stato dei procedimenti giurisdizionali avviati prima che esso fosse applicabile, ragion per cui la risposta alla questione

[118] Ivi, punto 143.
[119] Con la seconda questione pregiudiziale, il giudice del rinvio chiede se la risposta alla prima questione sarebbe diversa nel caso in cui il titolare di detto trattamento transfrontaliero non abbia lo stabilimento principale in tale Stato membro, ma solo un altro stabilimento.
[120] Conclusioni dell'Avvocato generale Bobek, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 152.
[121] Ivi, punto 155.
[122] Con la quarta questione pregiudiziale, il giudice del rinvio chiede se la risposta alla prima questione sarebbe diversa nel caso in cui l'autorità nazionale di controllo abbia già intentato l'azione legale prima della data di entrata in vigore del RGPD.

dovrebbe dipendere in base alla situazione del caso. In generale, secondo il parere dell'Avvocato generale, possono essere ravvisate due fattispecie generali, per ciascuna delle quali dovrà essere fornita una risposta diversa. Egli distingue tra:

a. Le azioni intentate da un'autorità di controllo per violazioni commesse dai titolari del trattamento delle disposizioni contenute nel regolamento prima della sua entrata in vigore;
b. Le azioni intentate per le violazioni avvenute successivamente all'entrata in vigore del regolamento[123].

Relativamente alla prima fattispecie, l'Avvocato generale ritiene che tali procedimenti possano continuare, in quanto sono azioni che al tempo della loro commissione erano illecite e per le quali erano evidenti le autorità competenti ad agire. Infatti, nel caso di specie, si continuerebbe ad applicare il precedente quadro normativo, con le autorità nazionali competenti ad agire. Per la seconda fattispecie, invece, qualora si dovesse proseguire il procedimento nazionale ciò comporterebbe fattivamente una proroga della direttiva 95/46 in quanto con il nuovo regolamento ha istituito un nuovo sistema di competenze in merito alle violazioni derivanti da un trattamento transfrontaliero[124]. Per questo motivo, l'Avvocato generale ritiene che il regolamento osti alla circostanza per la quale un'autorità nazionale prosegua un'azione in sede giudiziale iniziata prima della data in cui il nuovo regolamento è divenuto applicabile, ma che riguardi una condotta successiva a tale date[125].
Infine, per la quinta questione pregiudiziale, l'Avvocato generale suggerisce come la risposta da fornire al giudice del rinvia vada formulata in senso positivo, in quanto, oltre ad essere contenuta in un regolamento l'articolo 58, paragrafo 5, prescrive in modo chiaro, preciso e incondizionato e pertanto attribuisce ai singoli diritti che possono far valere nei confronti dello Stato.
Prima di muovere l'attenzione verso il giudizio della Corte e il ragionamento sotteso allo stesso, per completezza occorre accennare rapidamente alla sesta questione pregiudiziale, la quale non verrà trattata nel corso del prossimo capitolo in quanto, conformemente alla giurisprudenza costante, non presentando alcuna relazione con la realtà effettiva della causa principale e riguardando un problema ipotetico, viene dichiarata irricevibile dalla Corte[126]. Tuttavia, per gli obiettivi del presente paragrafo, la sesta questione permette nuovamente di mettere in evidenza il ragionamento dell'Avvocato generale, e l'importanza dell'obbligatorietà dei meccanismi di coerenza e cooperazione ai sensi del RGDP. Infatti, con la sesta questione il giudice del rinvio chiede se, nell'eventualità in cui dovesse essere constata la competenza ad agire da parte dell'autorità di controllo nazionale, cosa succederebbe se le medesime attività di trattamento transfrontaliero venissero trattate dall'autorità di controllo capofila e questa giungesse a conclusioni opposte? La problematica qui proposta, benché ipotetica, solleva un quesito importante, in quanto qualora si palesasse una situazione siffatta, la coerenza e la certezza del diritto dell'Unione sarebbero messi a repentaglio, costituendo un precedente

[123] Conclusioni dell'Avvocato generale Bobek, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 159.
[124] Ivi, punto 161.
[125] Ivi, punto 162.
[126] Si veda a tal proposito sentenza della Corte di giustizia, del 28 marzo 2017, causa C-72/15, *PJSC Rosneft Oil Company, c. Her Majesty's Treasury*, punto 194, e giurisprudenza citata; si veda altresì, in tal senso, sentenza della Corte di giustizia, del 16 dicembre 1981, causa C-244/80, *Pasquale Foglia c. Mariella Novello*, punto 18, e sentenza della Corte di giustizia del 12 giugno 2008, causa C-458/06, *Skatteverket c. Gourmet Classic Ltd*, punto 26.

gravissimo. Questo ulteriore esempio, secondo l'Avvocato generale, dimostra come se lo strumento dello sportello unico fosse facoltativo e tutte le autorità di controllo potessero agire unilateralmente, come prospettato dalla APD, andrebbe contro i fini e gli obiettivi del regolamento, il quale, per garantire un livello elevato di protezione delle persone fisiche, ha introdotto "un quadro più solido e coerente in materia di protezione dei dati"[127].

[127] Si veda a tal proposito il considerando 7, 9 e 10 del RGDP.

Capitolo 3
Il giudizio della Corte di giustizia

> "A child born today will grow up with no conception of privacy at all".
> (Edward Joseph Snowden)

La storia del diritto alla protezione dei dati personali è la storia delle difficoltà incontrate nel territorio dell'Unione per l'adozione di una cornice normativa comune, in grado di riuscire in un compito dicotomico: garantire un elevato livello di protezione dei dati personali così come garantire il completamento del mercato unico. L'introduzione del RGPD era stata vista dai più come la sintesi di questa lotta, dove attraverso l'adozione del metodo comunitario per la regolamentazione in materia *data protection* si sarebbe potuto garantire un approccio uniforme da parte di tutti e ventisette gli Stati membri. Nonostante i nobili fini, tuttavia, fin dall'entrata in vigore del nuovo regolamento, numerose sono state le critiche per il meccanismo dello *one-stop-shop*, il quale più che garantire uniformità, incentiverebbe pratiche di *forum shopping* da parte delle corporazioni *tech*. Infatti, il nuovo meccanismo designa il paese sede di ogni impresa come regolatore principale, in quanto l'autorità di controllo di tale Stato assurge ad autorità di controllo capofila. Facebook, Google, Apple, Microsoft e Twitter sono solo alcuni dei giganti i cui stabilimenti principali, così come identificati ai sensi dell'articolo 4, punto 16, del regolamento, hanno sede in Irlanda e sono pertanto sottoposti alla giurisdizione del *data protection commissioner* irlandese, il quale è stato più volte criticato per il suo approccio *corporate friendly*. Inoltre, l'assenza di una completa trasparenza tra le autorità di controllo, oltre che l'adozione di orientamenti non sempre uniformi, rischia di far svanire l'obiettivo posto alla base stessa del nuovo quadro normativo, frammentando il diritto e rendendo meno incisive le disposizioni poste a tutela del diritto alla protezione dei dati personali.
Le critiche al meccanismo dello sportello unico e il clima più generale di avversione nei confronti delle *Big Tech* rendono la sentenza della Corte nel caso *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit* centrale per il futuro della regolamentazione in Europa, in quanto riafferma la necessità, al fine di garantire l'efficacia di un impianto normativo comune, di una leale ed efficace cooperazione tra gli Stati membri per affrontare le nuove sfide digitali.
Nel corso del primo paragrafo verranno analizzate le risposte della Corte ai sei quesiti pregiudiziali posti dal giudice di rinvio nell'ambito del procedimento principale. A seguire, verranno discusse le implicazioni della sentenza da un punto di vista tanto giuridico che sotto il profilo del processo di integrazione europeo.

3.1 Le riposte della Corte alle sei questioni pregiudiziali

In merito alla prima questione pregiudiziale, la pronuncia della Corte di giustizia si mantiene in linea con le considerazioni presentate dall'Avvocato generale, adottando l'approccio mediano tra le posizioni, diametralmente opposte, di Facebook e dell'APD. La Corte rileva in via preliminare come il regolamento abbia come base giuridica l'articolo l16 TFUE[128], il quale pone il diritto alla protezione dei dati personali tra i diritti fondamentali. Tale punto rappresenta le fondamenta del ragionamento della Corte, per la quale è essenziale evidenziare come il regolamento, rispetto alla direttiva 95/46, ne

[128] Sentenza della Corte di giustizia, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 43.

rappresenti un superamento, sia sotto un profilo formale che sostanziale. Infatti, come ricordato dalla Corte e come anticipato nel primo capitolo del presente elaborato, il punto di impasse della direttiva 95/46 era in primis il suo carattere incerto, giano, relativamente alla protezione dei dati personali e all'armonizzazione del mercato interno. Di contro, la Corte ribadisce in via preliminare come il *primum movens* del regolamento sia quello di tutelare il diritto alla protezione dei dati personali e suggerisce come alla luce di questo contesto ne vadano analizzate e comprese le disposizioni. A suffragio della sua tesi, la Corte stabilisce che tale obiettivo vada dedotto alla luce tanto del primo considerando del RGPD, quanto dell'articolo 1, paragrafo 2, di tale regolamento. In particolare, quest'ultimo affida alle istituzioni, organi e organismi dell'Unione, oltre che alle autorità incaricate dei rispettivi Stati membri, il compito di assicurare la tutela dei diritti garantiti dall'articolo 16 TFUE e dall'articolo 8 della Carta[129]. Tutti questi elementi rappresentano lo sfondo sul quale si staglia l'articolo 55, paragrafo 1, del regolamento, il quale affida a ciascuna autorità di controllo la competenza ad esercitare i poteri conferitegli dal regolamento sul territorio del rispettivo Stato membro. Ed è proprio su quest'ultima affermazione che si trovano le difficoltà maggiori per arrivare ad un'intesa comune, in quanto da un lato Facebook suggerisce un'interpretazione più restrittiva delle competenze delle autorità di controllo, suggerendo che solo l'autorità capofila sia competente ad agire in sede giudiziale. Di contro, l'APD sostiene un'interpretazione più estensiva dove tutte le autorità di controllo possano agire in sede giudiziale.
Al fine di poter rispondere in modo esaustivo al primo quesito, la Corte ricostruisce il contesto normativo di riferimento, evidenziando al punto 50 della sentenza in esame come l'interpretazione dell'espressione *fatto salvo* presente all'articolo 56, vada interpretata nel senso che le competenze e i poteri garantiti alle autorità di controllo, così come disposto dall'articolo 55, siano applicabili in tutte quelle situazioni che non rientrino nella fattispecie dei trattamenti transfrontalieri, per i quali l'articolo 56 prevede una struttura e delle modalità specifiche. In altre parole, sebbene l'APD suggerisca che l'incipit dell'articolo 56[130] vada interpretato in modo che quest'ultima disposizione non possa incidere sui poteri attribuiti ad ogni autorità di controllo – tra cui quello di agire in sede giudiziale – a parere della Corte, così come dell'Avvocato generale[131], il trattamento transfrontaliero, rappresentando un caso speciale della competenza di principio[132] delle autorità di controllo, deroga a quanto disposto dall'articolo 55. Tuttavia, il regolamento ammanta di diverse specifiche l'esercizio del potere delle autorità di controllo capofila, in primis "come confermato dal considerando 13 del regolamento 2016/679, una leale ed efficace cooperazione tra l'autorità di controllo capofila e le altre autorità di controllo interessate"[133]. Il meccanismo di coerenza viene precisato agli articoli 64 e 65 del regolamento, ove la finalità della cooperazione può essere dedotta alla luce di quanto disposto in merito all'obbligo di reciproca assistenza tra le autorità di controllo, così come indicato dall'articolo 61,

[129] Ivi, punto 45.
[130] Art. 56, paragrafo 1, RGDP, "[f]atto salvo l'articolo 55, l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare e del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare del trattamento o responsabile del trattamento, secondo la procedura di cui all'articolo 60".
[131] Conclusioni dell'Avvocato generale Bobek, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 51.
[132] Sentenza della Corte di giustizia, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 47.
[133] Ivi, punto 53.

paragrafo 1, al fine di garantire un'applicazione coerente del regolamento in tutta l'Unione.
L'architettura del processo decisionale si avvale così delle garanzie di un confronto continuo tra le diverse autorità di controllo, capofila e interessate, di modo da poter assicurare un impianto normativo basato su di un sistema di responsabilità condivisa. La Corte a tal proposito rileva come l'importanza delle opinioni delle autorità di controllo interessate sia tale da poter bloccare il progetto di decisione dell'autorità di controllo capofila, qualora le prime presentino obiezioni motivate e pertinenti, ai sensi dell'articolo 60, paragrafo 4, del regolamento[134]. Ciò che emerge è un ritratto più delicato circa il ruolo dell'autorità di controllo capofila, dove l'immagine del processo decisionale unidirezionale dipinto dall'ADP lascia spazio ad un meccanismo che vede coinvolti più attori, tutti con l'obiettivo di garantire il rispetto e la tutela dei diritti contenuti nel regolamento attraverso progetti decisionali corali in merito al trattamento transfrontaliero dei dati personali. Infatti, solo una volta approvato il progetto di decisione, l'autorità di controllo capofila, ai sensi dell'articolo 60, paragrafo 7, potrà adottare una decisione riguardo al trattamento transfrontaliero e notificarla al titolare o al responsabile del trattamento[135]. Occorre tuttavia evidenziare come esistano delle eccezioni nell'ambito del principio dello sportello unico in merito alla competenza decisionale dell'autorità di controllo capofila. I punti da 58 a 62 della presente sentenza evidenziano tutte le deroghe previste nel regolamento, le quali sono state già affrontate nel corso della disamina delle conclusioni dell'Avvocato generale. Coerentemente a quanto suggerito da quest'ultimo, la Corte conclude che

> "[i]n materia di trattamento transfrontaliero di dati personali, la competenza dell'autorità di controllo capofila ad adottare una decisione che constati che un siffatto trattamento viola le norme relative alla tutela dei diritti delle persone fisiche con riguardo al trattamento di dati personali contenute nel regolamento 2016/679 costituisce la regola, mentre la competenza delle altre autorità di controllo interessate ad adottare una tale decisione, anche in via provvisoria, costituisce l'eccezione"[136].

Ciò detto, il carattere di eccezionalità rimane tale e non può essere sostenuto che, a proposito di un trattamento transfrontaliero, un'autorità di controllo diversa da quella capofila può esercitare il potere decisionale al di fuori dei casi previsti dal regolamento[137]. Se così fosse, verrebbe pregiudicata l'applicazione coerente ed omogena del regolamento e verrebbe compromesso il meccanismo dello sportello unico, minando sia l'obiettivo di protezione delle libertà e dei diritti fondamentali delle persone fisiche, con riguardo al trattamento dei dati personali in tutta l'Unione, sia la rimozione degli ostacoli ai flussi di dati personali all'interno del mercato unico. Per questi motivi, secondo la Corte, contrariamente a quanto sostenuto dall'APD, la situazione in cui un'autorità di controllo di uno Stato membro che non è un'autorità di controllo capofila può esercitare il potere conferito dall'articolo 58, paragrafo 5, del regolamento 2016/679 solo nel rispetto delle norme che disciplinano la ripartizione dei poteri decisionali, in particolare quelle delineate negli articoli 55 e 56 del regolamento, non è contraria agli articoli 7, 8 e 47 della Carta[138]. In merito al primo argomento presentato dall'APD, la Corte sostiene che non può essere accolta la lettura relativa alla presunta violazione degli articoli 7 e

[134] Ivi, punto 54.
[135] Ivi, punto 56.
[136] Sentenza della Corte di giustizia, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 47.
[137] Ivi, punto 65.
[138] Ivi, punto 66.

8 della Carta in quanto le autorità di controllo capofila hanno il compito di garantire un elevato livello di tutela a prescindere dalle norme relative alla ripartizione delle competenze. Suffragata dal tenore letterale dell'articolo 51 del regolamento, la Corte ricorda come l'obiettivo delle autorità di controllo sia quello di tutelare le persone fisiche, al fine di assicurare un elevato livello di tutela dei diritti garantiti dall'articolo 16 TFUE e che ciascuna autorità di controllo, indipendentemente dal proprio ruolo, deve assicurare tali diritti sul territorio del proprio Stato membro, oltre che del rispetto dei requisiti di cooperazione in caso di un trattamento transfrontaliero. Per questi motivi, in nessun caso si può affermare che le norme sulla ripartizione delle competenze decisionali vadano a deresponsabilizzare le singole autorità di controllo dall'obbligo di garantire un'efficace tutela delle persone fisiche in merito ai diritti fondamentali sopra citati. Lo sportello unico, quindi, non può comportare in nessun caso una deresponsabilizzazione delle autorità di controllo capofila in merito all'efficiente tutela dei diritti delle persone fisiche, pena l'incoraggiamento di pratiche di *forum shopping*[139]. In sintesi, ciò che preme evidenziare è che non è tanto il meccanismo dello sportello unico ad inficiare la protezione delle persone fisiche relativa al trattamento dei dati personali, quanto la corretta applicazione dei meccanismi e degli strumenti previsti dal regolamento. Fermo restando, comunque, il rispetto delle norme sulla ripartizione delle competenze decisionali oltre che i requisiti di cooperazione e di assistenza reciproca. Anche in merito alla presunta violazione dell'articolo 47 della Carta, relativo al diritto a un ricorso effettivo, la Corte non accetta l'interpretazione fornita dalla APD. Viene ribadito come precludere all'autorità di controllo di agire in sede giudiziale nei casi di un trattamento transfrontaliero dei dati, azione la quale poi condurrà ad una decisione vincolante

> "lascia impregiudicato il diritto riconosciuto ad ogni persona, all'articolo 78, paragrafi 1 e 2, di tale regolamento, di proporre un ricorso giurisdizionale effettivo, in particolare, avverso una decisione giuridicamente vincolante di un'autorità di controllo che lo riguarda o contro il mancato trattamento di un reclamo da parte dell'autorità di controllo che dispone della competenza decisionale in forza degli articoli 55 e 56 di detto regolamento"[140].

Affinché l'impianto normativo previsto dal regolamento funzioni, è necessaria una stretta cooperazione tra le parti, senza la quale verrebbe meno il senso di quanto fatto. Ciò che quindi la Corte evidenzia al punto 71 è l'esistenza di un percorso emergenziale qualora il meccanismo dello sportello unico vada in tilt. Infatti, se è vero che l'autorità di controllo capofila può prendere una decisione solo nella misura in cui le autorità di controllo interessate vengano rese partecipi, è altrettanto vero che in caso di atteggiamenti poco cooperativi da parte dell'autorità di controllo capofila, le eventuali violazioni delle norme relative alla tutela dei diritti delle persone fisiche con riguardo al trattamento dei dati personali rischierebbero di essere lasciate impunite, pregiudicando l'esercizio dei diritti previsti dalla Carta. Per questo motivo, la Corte evidenzia come, sebbene non possa essere accettata l'interpretazione dell'APD, va altresì evidenziato come un'autorità di controllo, diversa da quella capofila, possa rivolgersi al giudice del rispettivo Stato di appartenenza "qualora, dopo aver richiesto la reciproca assistenza dell'autorità di controllo capofila, in forza dell'articolo 61 del regolamento 2016/679, quest'ultima non le fornisca le informazioni richieste"[141]. La Corte chiarisce così facendo quali siano le

[139] Ivi, punto 68.
[140] Sentenza della Corte di giustizia, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 69.
[141] Ivi, punto 71.

dinamiche che consentono di utilizzare la misura d'urgenza prevista dall'articolo 61, paragrafo 8, del regolamento, attraverso la quale l'autorità di controllo interessata può adottare una misura provvisoria nel territorio del rispettivo Stato di appartenenza e, qualora dovesse ritenerlo necessario, può chiedere al Comitato europeo per la protezione dei dati un parere d'urgenza o una decisione vincolante d'urgenza, in base a quanto previsto dall'articolo 66, paragrafo 3, del regolamento[142]. Una volta adottato tale parere o decisione vincolante, l'autorità di controllo è competente ad adottare le misure necessarie così da poter

> "garantire il rispetto delle norme relative alla tutela dei diritti delle persone fisiche con riguardo al trattamento di dati personali contenute nel regolamento 2016/679 e, a tale titolo, esercitare il potere conferitole dall'articolo 58, paragrafo 5, del predetto regolamento"[143].

Per questo motivo e nei limiti indicati presenti nel regolamento e delineati dalla Corte, un'autorità di controllo diversa dalla capofila è competente ad accertare che il trattamento transfrontaliero in questione violi le norme del RGPD. La Corte vuole evidenziare come il diritto alla protezione dei dati personali non venga lasciato scoperto e come il regolamento, al fine di evitare situazioni simili, prevede misure straordinarie.
In sintesi, la Corte risponde affermativamente al primo quesito pregiudiziale, fermo restando che tale competenza sia esercitabile esclusivamente in una delle situazioni in cui il regolamento affida tale competenza ad un'autorità di controllo diversa da quella prevista[144]. Nel caso esaminato, spetterà poi al giudice del rinvio verificare se, nonostante l'APD non rappresenti l'autorità di controllo capofila designata in tale causa, e per trattamenti effettuati dal *social network* Facebook, tale situazione rientri nella fattispecie descritta al punto 71[145].
Anche in merito alla seconda questione pregiudiziale la Corte si rifà alle conclusioni proposte dall'Avvocato generale, affermando che, qualora il giudice del rinvio verificasse quanto detto al punto 71, la APD sarebbe competente a presentare un'azione giudiziaria nei confronti di Facebook Belgium e Facebook Ireland, essendo l'articolo 58, paragrafo 5, formulato in termini generali[146]. Ciò che rimane essenziale ai fini dell'esercizio della competenza indicata dal suddetto articolo non va quindi ricercato nella presenza di uno stabilimento principale, così come inteso ai sensi dell'articolo 4, punto 16, del regolamento, né di un altro stabilimento nel territorio di tale Stato membro. Piuttosto, è cruciale dimostrare che tale potere rientri nell'ambito di applicazione territoriale del regolamento. In altre parole, non osta alla verifica della competenza di un'autorità di controllo, diversa dall'autorità di controllo capofila, l'assenza nel territorio del rispettivo Stato di uno stabilimento del titolare o del responsabile del trattamento dei dati personali. Tale affermazione è suffragata dal fatto che l'ambito di applicazione territoriale del regolamento, ai sensi del suo articolo 3, prevede che quest'ultimo sia applicabile a condizione che "il titolare del trattamento o il responsabile del trattamento transfrontaliero disponga di uno stabilimento nel territorio dell'Unione"[147]. Per questi motivi, a parere della Corte, occorre rispondere alla seconda questione pregiudiziale

[142] *Ibidem.*
[143] *Ibidem.*
[144] Sentenza della Corte di giustizia, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 75.
[145] Ivi, punto 73.
[146] Ivi, punto 79.
[147] Ivi, punto 83.

nel senso che, nel caso di una situazione di cui al punto 71 della presente sentenza, per esercitare il potere disposto ai sensi dell'articolo 58, paragrafo 5, non è necessario che

> "il titolare del trattamento o il responsabile per il trattamento transfrontaliero di dati personali, nei cui confronti tale azione viene intentata, disponga di uno stabilimento principale o di un altro stabilimento nel territorio di detto Stato membro"[148].

In merito alla terza questione pregiudiziale, si può intravedere in modo più limpido la conferma di un percorso giurisprudenziale votato ad un'interpretazione estensiva delle tutele garantite dal regolamento. Come precedentemente affermato, il terzo quesito pregiudiziale può essere visto come un caso particolare del secondo quesito, ove si interroga nuovamente sull'ambito di applicazione territoriale del regolamento e sulla *ratione loci* dell'APD. Infatti, sebbene nel rispondere al secondo quesito pregiudiziale la Corte ha evidenziato come l'esercizio del potere di agire in sede giudiziale non sia vincolato alla presenza nel territorio dell'autorità di controllo di uno stabilimento del titolare del trattamento, rimane in dubbio verso quale stabilimento dirigere tale azione qualora nel territorio dell'Unione ve ne sia più di uni. In questo caso, il dubbio era relativo a se l'azione dovesse essere intentata nei confronti di Facebook Ireland (stabilimento principale ai sensi dell'articolo 4, punto 16 del regolamento) o nei confronti di Facebook Belgium, stabilimento situato nel territorio dell'APD. Quest'ultimo stabilimento è adibito a mantenere i rapporti istituzionali con l'Unione Europea e competente a gestire le attività di *advertising* e *marketing* per gli utenti residenti in Belgio[149]. Anche in questo caso, ciò che viene contestato dalla difesa nel procedimento principale è la competenza dell'APD ad agire nei confronti di Facebook Belgium in quanto quest'ultimo, non essendo incaricato del trattamento dei dati personali, non rientrerebbe nell'ambito di applicazione del regolamento. Infatti, il RGPD prevede, ai sensi dell'articolo 3, che quest'ultimo si applichi al trattamento di dati personali "nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento". Nel territorio dell'Unione, il trattamento dati è effettuato solamente dal Facebook Ireland, la quale si occupa di raccogliere informazioni sul comportamento degli utenti e non utenti del *social network* attraverso *social plugin* e *pixel*. Tali tecnologie hanno lo scopo di migliorare l'efficienza del sistema pubblicitario del *social network* in questione, attraverso una comunicazione più mirata basandosi sulle più recenti tecnologie nell'ambito della profilazione. Tuttavia, sebbene la difesa di Facebook neghi la possibilità per l'APD di agire in sede giudiziale tanto nei confronti dello stabilimento belga quando nei confronti dello stabilimento principale, secondo la Corte l'accezione "nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento", di cui all'articolo 3, paragrafo 1, del RGDP, non può essere interpretata in senso restrittivo, visti gli obiettivi del regolamento. Tale visione, sostenuta da precedenti giurisprudenziali[150], vede le attività dei due stabilimenti inscindibilmente connesse, in quanto lo stabilimento del gruppo Facebook situato in Belgio in via principale si occupa fare *lobbying* con le istituzioni dell'Unione, al fine di determinare e influenzare le politiche di trattamento dati, nell'interesse del gruppo Facebook in generale e di Facebook Ireland in

[148] Ivi, punto 84.
[149] Sentenza della Corte di giustizia, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit,* punto 86.
[150] Sentenza della Corte di giustizia, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH.*

particolare[151]. Inoltre, i due stabilimenti, belga e irlandese, sono legati dalle rispettive funzioni in quanto l'attività di Facebook Belgium permette di rendere redditizi i servizi di Facebook attraverso la promozione e vendita di spazi pubblicitari[152] e, come visto, le tecnologie utilizzate per la raccolta dati degli utenti da parte della sede irlandese hanno lo scopo di rendere il sistema pubblicitario di Facebook più redditizio[153]. Alla luce di quanto detto, "le attività dello stabilimento del gruppo Facebook situato in Belgio devono essere considerate inscindibilmente connesse al trattamento dei dati personali di cui trattasi nel procedimento principale"[154] e per tanto tale trattamento deve essere considerato "nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento"[155]. La Corte conclude affermando la possibilità da parte di un'autorità di controllo, diversa dall'autorità di controllo capofila, qualora sia competente a farlo, di agire tanto nei confronti dello stabilimento situato nel territorio dello Stato di appartenenza, quanto nei confronti dello stabilimento principale, a condizioni che l'azione giudiziaria riguardi un trattamento dati effettuato nell'ambito di attività dello stabilimento in questione[156].
Sebbene per gli scopi del presente elaborato sono le prime tre questioni pregiudiziali a rappresentare il nerbo della problematica, prima di passare allo studio delle conseguenze della sentenza per il panorama europeo occorre far un breve cenno nel merito delle ultime tre domande pregiudiziali. Per quanto riguarda il quarto quesito, la risposta fornita dalla Corte non accoglie la critica sollevata da Facebook, secondo il quale il mantenimento di un'azione intentata prima della data di entrata in vigore del regolamento (25 maggio 2018) sia irricevibile. A tale riguardo, la Corte evidenzia l'assenza di norme transitorie all'interno del regolamento, oltre che l'assenza di norme per disciplinare "lo status dei procedimenti giurisdizionali avviati prima che esso fosse applicabile e che erano ancora in corso alla data in cui è divenuto applicabile"[157]. Altrettanto, sono assenti norme che, a differenza di quanto sostenuto dalla difesa di Facebook, obblighino di porre fine a tutti i procedimenti giurisdizionali pendenti alla data di entrata in vigore del RGDP. È necessario per prima cosa distinguere due fattispecie, ossia le azioni intentate per violazioni avvenute prima dell'entrata in vigore del nuovo quadro normativo e le azioni intentate per violazioni avvenute dopo tale data. In merito alla prima fattispecie, secondo la Corte nulla osta affinché possano essere mantenute le disposizioni di cui alla direttiva 95/46, "la quale rimane applicabile per quanto riguarda le violazioni commesse fino alla data della sua abrogazione, ossia il 25 maggio 2018"[158]. Per la seconda fattispecie, la Corte risponde sostenendo che, nell'eventualità in cui venissero verificate dal giudice del rinvio le condizioni descritte al punto 71, nulla osterebbe affinché l'autorità di controllo diversa dall'autorità di controllo capofila intenti un'azione giudiziaria "che accerti che il trattamento di dati di cui trattasi viola le norme contenute in detto regolamento per quanto riguarda la tutela dei diritti delle persone fisiche con riguardo al trattamento di dati personali"[159].

[151] Sentenza della Corte di giustizia, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit,* punto 94.
[152] *Ibidem.*
[153] Ivi, punto 93.
[154] Ivi, punto 95.
[155] *Ibidem.*
[156] Ivi, punto 96.
[157] Sentenza della Corte di giustizia, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit,* punto 101.
[158] Ivi, punto 104.
[159] Ivi, punto 105.

Per quanto riguarda la quinta questione pregiudiziale, la Corte risponde in maniera analoga a quanto suggerito dall'Avvocato generale, evidenziando come benché da un lato l'azione dell'APD si fondi su una disposizione del diritto belga[160] è altrettanto vero che l'articolo 58, paragrafo 5, del RGPD "ha effetto diretto, cosicché un'autorità di controllo nazionale può invocarla per intentare o proseguire un'azione nei confronti di privati"[161]. Così facendo, la Corte conferma un'ormai consolidata giurisprudenza secondo la quale, data la natura stessa dei regolamenti, così che della loro funzione all'interno del sistema del diritto dell'Unione, le disposizioni ivi contenute producono effetti diretti negli ordinamenti nazionali[162].
Infine, come già accennato, la Corte di giustizia non entra nel merito dell'ultimo quesito pregiudiziale, non avendo nessun nesso relazionale con l'oggetto o la realtà della causa principale, e deve per questi motivi essere dichiarato irricevibile[163].
Quanto visto finora permette di affermare che la sentenza presa in esame confermi nuovamente l'interpretazione estensiva fornita dalla Corte in merito alle tutele garantite dal regolamento. Tale attenzione, che verrà argomentata nel prossimo paragrafo, è sintomatica del rischio avvertito dai più che il meccanismo del *one-stop-shop* si trasformi in un collo di bottiglia che, alimentato dalla riluttanza di alcune autorità di controllo ad intervenire, rischia di minare il quadro normativo introdotto con il RGPD mettendo a repentaglio la tutela dei diritti delle persone fisiche con riguardo al trattamento di dati personali.

3.2 Le conseguenze del giudizio della Corte.

Il valore della sentenza fin qui analizzata può essere riassunto mettendo in evidenza il significato delle risposte fornite ai sei quesiti pregiudiziali, ed in particolare alla portata delle prime tre. Volendo sintetizzare, ciò che emerge dall'analisi del giudizio della Corte è la possibilità da parte di un'autorità di controllo diversa dall'autorità di controllo capofila di poter agire in sede giudiziale presso i giudici del proprio Stato di appartenenza verso tutti gli stabilimenti dei titolari del trattamento dei dati personali. Di fatto, quindi, fintanto che il trattamento rientri nell'ambito dell'attività del titolare, l'autorità di controllo si ritrova con una *ratione loci* pressoché limitata esclusivamente dai confini del territorio dell'Unione. Se è pur vero che tale azione da parte di un'autorità di controllo sia limitata e circoscritta a casi specifici e nel rispetto delle procedure di cooperazione e collaborazione, la portata del caso C-645/19 risente inevitabilmente del contesto esterno di sfiducia e diffidenza del meccanismo dello sportello unico. Non poche, infatti, sono le critiche rivolte al *data protection commissioner* irlandese, il quale riveste il ruolo di autorità di controllo capofila per la maggior parte delle compagnie *Big Tech*. Quest'ultime hanno i loro stabilimenti principali, così come definiti ai sensi dell'articolo 4, punto 16, del RGPD, in Irlanda a causa dei vantaggi offerti dal suo regime fiscale[164]. Tuttavia, dati alla mano, è possibile evidenziare come la maggior parte dei casi (il 98%)[165] riguardanti il RGPD trattati dall'autorità irlandese rimangono irrisolti. Infatti, dei 164 casi aventi carattere

[160] Art. 6 della legge del 3 dicembre 2017.
[161] Sentenza della Corte di giustizia, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, punto 113.
[162] Ivi, punto 110.
[163] Ivi, punto 118.
[164] Tuttavia, l'Irlanda ha aderito all'accordo globale su una *corporate tax* minima del 15% per le multinazionali a partire dal 2023, superando così il regime fiscale del 12,5 % che ne ha caratterizzato l'economia.
[165] RYAN, TONER (2021).

transfrontaliero presentati dinnanzi al DPC, sono stati adottati solamente 4 progetti di decisione[166]. Come sottolineato da Geradin ed altri studiosi, il meccanismo del *one-stop-shop* "creates serious bottlenecks which, coupled with the reluctancy of certain [autorità di controllo] to intervene, results in tech giants escaping close monitoring and liability, despite regularly engaging in dubious practices"[167]. Ma tali critiche risultano essere anche interne alle istituzioni, in quanto l'Irlanda è stata accusata dalle altre autorità di protezione dei dati dell'Unione di non prendere abbastanza provvedimenti contro le aziende Big Tech. Le tensioni a lungo covate sulla regolamentazione sono scoppiate in pubblico dopo che i funzionari tedeschi hanno attaccato l'autorità irlandese per non aver fatto rispettare la normativa UE per la protezione dei dati[168]. Ulrich Kelber, a capo dell'autorità di controllo tedesca, ha aspramente criticato il lavoro della sua controparte irlandese, Helen Dixon, ed in particolare l'estrema lentezza con la quale vengono trattati i casi, a fronte del fatto che in Germania, sui 176 casi presentati, 52 ne sono stati chiusi[169]. Per questi motivi, sono numerosi gli Stati i quali ritengono necessario che per fronteggiare l'ingorgo burocratico e le lungaggini di cui sopra sia necessario ripensare il meccanismo dello sportello unico, garantendo quindi la possibilità per più autorità di controllo di far valere il diritto europeo in materia di protezione dati personali.

Le tensioni fin ora rilevate hanno il rischio di minare in modo sostanziale gli obiettivi perseguiti dal regolamento, primo fra tutti il binomio protezione-circolazione dati personali, in quanto fomentano la possibilità di un ritorno a livelli diversi di protezione dati tra i diversi Stati membri. Il 20 maggio 2021 le tensioni evidenziate si sono tradotte in una presa di posizione del Parlamento europeo, il quale ha votato a favore di una risoluzione che chiede alla Commissione europea di aprire una procedura di infrazione contro l'Irlanda per la mancata applicazione del RGPD[170]. Il Parlamento europeo

> "esprime profonda preoccupazione per il fatto che diversi reclami contro le violazioni del GDPR [RGPD] presentati il 25 maggio 2018, il giorno in cui il GDPR è diventato applicabile, e altri reclami di organizzazioni per la privacy e gruppi di consumatori, non sono ancora stati decisi dal DPC, che è l'autorità principale per questi casi"[171].

Ai sensi dei trattati, la Commissione è definita come custode del diritto dell'Unione, e può avviare una procedura formale di infrazione, ossia un procedimento a carattere giurisdizionale disciplinato ai sensi degli articoli 258 e 259 TFUE, qualora uno Stato membro dell'UE non ne attui il diritto. Tuttavia, in merito alla questione sollevata dal Parlamento Europeo, il Commissario alla giustizia, Didier Reynders, ha statuito che è troppo presto per stabilire se il meccanismo di cooperazione alla base del funzionamento del meccanismo dello sportello unico stia funzionando correttamente[172].

Date queste premesse, il giudizio della Corte assume un significato più profondo, in quanto rimette al centro l'importanza del *one-stop-shop* e delle procedure di leale cooperazione tra le autorità degli Stati membri. Essa rileva infatti come alla base stessa della natura del meccanismo dello sportello unico,

---

[166] *Ibidem.*
[167] GERADIN, KARANIKIOTI, KATSIFIS (2020).
[168] ESPINOZA (2021).
[169] *Ibidem.*
[170] Risoluzione del Parlamento europeo, del 20 maggio 2021, *sulla sentenza della Corte di giustizia dell'Unione europea del 16 luglio 2020 — Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems («Schrems II»).*
[171] Ivi, punto 5.
[172] MANACOURT (2022).

e alla base della ripartizione di competenze tra le diverse autorità di controllo, deve essere necessariamente premessa "una cooperazione leale ed efficace"[173] tra le autorità di controllo, così da poter "garantire l'applicazione corretta e coerente del suddetto regolamento [RGPD]"[174]. Vedendo l'enorme arretrato che l'autorità irlandese sta affrontando e la mancanza di decisioni che ha preso finora, questa decisione conferma che altre autorità di controllo possono essere competenti e possono agire in circostanze molto specifiche. Come conclusione, la Corte conferma la formulazione del RGPD senza sorprese: l'autorità di controllo non capofila non può aggirare l'autorità di controllo capofila presentando un'azione giudiziaria in tribunale. Possono farlo solo quando si applica una delle eccezioni al meccanismo dello sportello unico (articolo 55, paragrafo 2, e articolo 56, paragrafo 2, o articolo 66). Nondimeno, la Corte ribadisce nel suo giudizio la conferma che un'autorità di controllo può adottare una decisione urgente ai sensi dell'articolo 66 RGPD quando l'autorità di controllo capofila non riesce a rispondere per fornire assistenza reciproca entro un mese come da articolo 61, paragrafo 8 del suddetto regolamento. Si può quindi concludere affermando che, sebbene il giudizio della Corte non accetti la visione più estrema suggerita dall'APD belga, essa prende atto delle difficoltà rilevate nell'attuazione del regolamento a partire dagli attriti tra le diverse autorità di controllo nazionali e nella riluttanza di alcune ad intervenire. Il giudizio della Corte sembra quindi voler rassicurare, ricordando come lo stesso RGPD presenti delle terze vie attraverso le quali, in caso di inerzia amministrativa da parte dell'autorità di controllo, si possa garantire il rispetto del diritto alla protezione dei dati personali per le persone fisiche.
Pertanto, alla luce di quanto detto e alla luce del contesto esterno, lo spessore del giudizio della Corte nell'ambito della sentenza analizzata si sostanzia principalmente in contrasto all'inerzia che sembra aver caratterizzato l'applicazione del RGPD nei suoi primi anni di attività. Le principali critiche rivolte al regolamento sono relative al meccanismo dello sportello unico e all'inattività dell'autorità di controllo irlandese, i quali sarebbero i responsabili della paralisi del sistema normativo dell'Unione per la protezione dei dati personali. Di contro, per la Corte il meccanismo dello sportello unico, alla luce del considerando 10 del RGPD, riflette tanto gli obiettivi quanto le finalità del regolamento in questione, rendendolo strumento imprescindibile per l'attuazione del nuovo strumento normativo. Qualora, infatti, si dovesse sposare quanto prospettato dall'APD, verrebbero fagocitati comportamenti di *forum shopping*, ove infatti si sostanzierebbe uno squilibrio nei livelli di protezione tra le diverse autorità di controllo, mettendo a repentaglio l'efficacia stessa del regolamento. Un esempio riguarda la multa comminata dalla *Commission nationale de l'informatique et des libertés* (CNIL), l'autorità di controllo francese, in data 31 dicembre 2021, nei confronti sia del motore di ricerca Google che della piattaforma Facebook, per una cifra rispettivamente di 150 milioni di euro e 60 milioni di euro. La sanzione disposta dall'autorità francese nasce a seguito dei numerosi reclami mossi da parte degli utenti in merito al meccanismo più complesso delle modalità di rifiuto dei *cookies* adottato dalle due *Big Tech*. A parere della CNIL, la mancata chiarezza sarebbe una strategia per scoraggiare il rifiuto dei *cookies*, incidendo così sulla libertà di consenso degli utenti e violando l'articolo 82 della legge francese sulla protezione dei dati[175]

[173] Sentenza della Corte di giustizia, *Facebook Ireland Limited e a. c.* Gegevensbeschermingsautoriteit, punto 72.
[174] *Ibidem.*
[175] Legge n. 78-17, del 6 gennaio 1978, *relative à l'informatique, aux fichiers et aux libertés.*

la quale recepisce le disposizioni della direttiva ePrivacy[176] del 2002. Oltre alle sanzioni amministrative, la Commissione ha emesso un'ingiunzione con che ordina alle due imprese di dare agli utenti in Francia un modo semplice per rifiutare i *cookies* entro tre mesi dalla notifica della sentenza, al fine di garantire la loro libertà di consenso. Ciò è possibile in quanto i principi dello sportello unico, e più in generale il quadro normativo introdotto con il RGPD, non si applicano al trattamento dei dati derivanti dall'uso dei *cookies*, il quale è disciplinato ai sensi della direttiva ePrivacy, che viene recepita all'interno dell'ordinamento francese dalla legge del 6 gennaio 1978. In questo caso, l'assenza di un'autorità di controllo capofila, e quindi di decisioni vincolanti per tutto il territorio dell'Unione, favorisce una discriminazione per l'esercizio dei diritti, in quanto utenti situati in paesi dell'Unione diversi dalla Francia non godranno della stessa possibilità dei corrispettivi francesi circa le modalità di rifiuto dei *cookies*. Ciò a riprova del fatto che il meccanismo di coerenza introdotto con il RGPD permette di evitare situazioni analoghe, le quali rallettano il processo di integrazione europeo sabotando la struttura del mercato unico. Il rispetto delle norme della ripartizione delle competenze non vuol dire quindi meno tutela per gli utenti, contrariamente a quanto sostenuto dall'autorità belga, bensì è il tentativo di adottare un quadro europeo uniforme per far fronte alle sfide digitali, garantendo a livello comunitario la tutela del diritto alla protezione dei dati personali.

Per questi motivi, occorre operare una rivoluzione copernicana in merito alle criticità del RGPD, focalizzando l'attenzione non tanto sullo strumento del *one-stop-shop* (il quale, come suggerito dall'esempio precedente, rimane ad oggi centrale al fine di garantire un *enforcement* omogeneo), quanto sulla cooperazione tra le diverse autorità di controllo e sugli strumenti posti a salvaguardia della corretta applicazione del regolamento. Infatti, piuttosto che smantellare il sistema volto a garantire coerenza al diritto dell'Unione, la via mediana adottata dalla Corte suggerisce una risposta, seppur moderata, nei confronti del DPC, in quanto, pur confermando il primato dello sportello unico, ribadisce l'esigenza non solo di cooperazione "efficace" tra l'autorità principale e le altre autorità di controllo interessate, ma richiede anche una cooperazione "sincera", andando così oltre la pura lettera del RGPD[177].

[176] Direttiva (CE) del Parlamento europeo e del Consiglio, del 12 luglio 2002, 2002/58, *relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)*.

[177] Si veda a tal proposito sentenza della Corte di giustizia, *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, paragrafi 53, 60, 63, 72.

Conclusione

> "Crediamo in una transizione digitale antropocentrica. Si tratta di chi vogliamo essere, in quanto europei".
> (Presidente Ursula von der Leyen, Guidare il decennio digitale, Sines, 1º giugno 2021).

La rivoluzione digitale è il fenomeno che più di tutti ha caratterizzato gli ultimi anni, e continuerà ad essere uno dei temi di maggior centralità per gli anni a venire. Ogni elemento della nostra vita è stato trasformato dalla tecnologia, che ci sta fornendo opzioni senza precedenti. Il ritmo accelerato della trasformazione digitale ha portato a scoperte significative, fornendo nuovi strumenti per affrontare le preoccupazioni sociali globali e migliorando l'efficienza dei servizi aziendali e pubblici. Allo stesso tempo, ha reso l'istruzione e la formazione più accessibili, così come le risorse informative, e ha creato nuovi luoghi di dibattito pubblico. Il rapido utilizzo delle tecnologie digitali ha aumentato la libertà, collegando anche le regioni più isolate e fornendo ai cittadini dell'Unione e del mondo nuove opportunità. Tuttavia, la crescente disponibilità di nuove tecnologie digitali e di dati porta con sé minacce indesiderate che possono avere conseguenze di vasta portata per i cittadini, minando i principi democratici, la sicurezza e le basi della società. Le violazioni della privacy e dei dati personali, la diffusione di contenuti illegali e dannosi e di prodotti non sicuri, così come la disinformazione, il crimine informatico e gli attacchi informatici, lo sfruttamento e l'abuso di esseri umani, la sorveglianza di massa, i pregiudizi algoritmici che ostacolano un accesso equo e non discriminatorio alle informazioni e al dibattito democratico, e persino la censura vera e propria sono tutti aumentati in modo significativo. Tali questioni toccano il cuore dei diritti fondamentali, mettendo a repentaglio i progressi faticosamente raggiunti in questo settore sia all'interno dell'Unione europea che a livello globale.

Per questi motivi, al fine di poter conseguire un futuro digitale a misura d'uomo, sostenibile e al riparo dalle vulnerabilità discusse, il 9 marzo 2021 la Commissione ha adottato la comunicazione "Bussola per il digitale 2030: il modello europeo per il decennio digitale"[178] nella quale ha indicato un insieme di principi digitali attraverso cui poter conseguire una trasformazione digitale ispirata ai valori europei. Il piano per il prossimo decennio digitale ruoterà intorno ai quattro punti cardinali *skills*, *government*, *infrastructures*, *business* e per raggiungere i quali sarà necessario adottare un approccio antropocentrico che metta al centro i diritti delle persone. A tal fine, il 26 gennaio 2022, sempre la Commissione ha proposto al Parlamento europeo e al Consiglio di adottare una dichiarazione solenne comune di impegno politico sui diritti e i principi digitali per mettere al centro della transizione digitale "i valori dell'Unione e i diritti e le libertà delle persone tutelati dal diritto dell'Unione"[179] al fine che questi "siano rispettati e rafforzati online così come offline"[180]. L'approccio antropocentrico non può prescindere un'adeguata tutela dei dati personali, il cui sfruttamento è centrale per l'ecosistema digitale sempre più orientato ad un approccio *ad-tech* (ovvero *advertising technology*). Tali tecnologie consentono un notevole vantaggio competitivo, tanto che alcuni operatori di mercato sono in grado di prevedere con notevole precisione la predisposizione dei

[178] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni del 9 marzo 2021, COM(2021) 118 final, *bussola per il digitale 2030: il modello europeo per il decennio digitale*.
[179] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni del 26 gennaio 2022, COM(2022) 27 final, *relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali*.
[180] *Ibidem.*

consumatori verso un bene o un servizio, combinando il tracking con vaste capacità di elaborazione dei dati e componenti di psicologia comportamentale. A questo riguardo, l'evoluzione operata all'interno del contesto normativo europeo, attraverso l'introduzione di una regolamentazione ad *hoc* circa il tema della protezione dei dati personali, sembrava essere la base per garantire, da un lato ai cittadini la possibilità del controllo dei propri dati, e dall'altro di fornire alle imprese un quadro chiaro con il quale conformarsi. Per raggiungere tale scopo, è dapprima necessario garantire nel territorio dell'Unione un approccio uniforme e coerente, capace di garantire un livello adeguato di tutela al diritto per la protezione dei dati personali. Ma, come descritto nel corso del presente elaborato, sebbene l'introduzione del RGPD si ponesse come fine quello di superare la frammentazione delle varie legislazioni nazionali in merito al tema della protezione dei dati personali, sussistono tutt'oggi diversi approcci e concezioni relative all'*enforcement* del citato regolamento. Tali differenze rischiano di annullare la portata rivoluzionaria del nuovo quadro normativo, attenuandone gli effetti attraverso pratiche disomogenee. In più, un'ulteriore sfida è rappresentata dal crescente inasprimento dei rapporti tra le diverse autorità di controllo e dal clima di sfiducia rivolto in particolar modo nei confronti del DPC irlandese. Proprio attraverso l'analisi della sentenza C-645/19, il presente elaborato ha tentato di far luce sullo stato dell'arte attuale relativo alla protezione dei dati personali, fornendo un'analisi tanto della sentenza quanto delle sue implicazioni.

Gli obiettivi futuri, sottesi al modello europeo per il decennio digitale, dovranno tener conto della difficoltà evidenziate dal caso *Facebook Ireland Limited e a. c. Gegevensbeschermingsautoriteit*, il quale esemplifica le fragilità sottese al nuovo regolamento, oltre che lo stato attuale dell'integrazione europea. La realizzazione di un mercato unico digitale è infatti la nuova frontiera dell'integrazione europea, ove il mercato digitale vada intenso come una sottospecie del *genus* mercato interno. È quindi opportuno applicare i risultati e le preoccupazioni per il mercato interno al mercato digitale, sottolineandone i nuovi profili o le innovazioni, pur tenendo presente la necessità di creare un'economia più forte, più equilibrata e più equa, anche in questo contesto. Proprio alla luce di quanto detto va letto il considerando 9 del RGPD, per il quale un livello disomogeneo di tutela può "costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione". Pertanto, nel riaffermare la centralità del *one-stop-shop*, la Corte sancisce l'esigenza di un approccio uniforme per la salvaguardia tanto dei diritti fondamentali quanto del processo di integrazione stesso. La realizzazione di un mercato unico digitale, completo e coerente, rappresenta per l'Unione europea ancora una sfida su cui concentrare maggiori risorse. Testimonianza degli sforzi in tal direzione sono i recenti accordi politici raggiunti su due nuovi strumenti normativi, il *Digital Service Act* (raggiunto il 25 marzo 2022) e il *Digital Market Act* (raggiunto il 23 aprile 2022), i quali formano parte integrante di un pacchetto di riforme proposte dalla Commissione nel 2020, orchestrate dall'obiettivo comune di dettare regole applicabili in tutto lo spazio economico europeo, dando vita ad un unico spazio digitale europeo, secondo l'obiettivo che la stessa Presidente della Commissione ha posto al centro dell'azione politica della Commissione e dell'UE. Tuttavia, per realizzare tale progetto, si dovrà tenere debito conto delle difficoltà e dei limiti applicativi riscontrati per l'adozione di un quadro normativo uniforme e della necessità di garantire un approccio centralizzato in grado di assicurare una tutela omogenea lungo tutto il territorio dell'Unione, nel rispetto di una cooperazione sincera ed efficace tra gli Stati membri.

Bibliografia

BAINBRIDGE (2005), *Data Protection*, in *XPL Law*, p. 132.

BOBBIO (1990), *L'età dei diritti*, Torino.

COLAPS (2020), *Garantire la protezione dei diritti fondamentali nel mercato unico digitale: verso un approccio sinergico tra il diritto della concorrenza e la protezione dei dati*, in DAL POZZO (a cura di), *mercato unico digitale, dati personali e diritti fondamentali*, Palermo, p. 71 ss.

ESPINOZA (2021), *Fight breaks out between Ireland and Germany over Big Tech regulation*, in *Financial Times*, reperibile *online*.

FABBRINI (2015), *The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of justice as a Human Rights Court*, in *Hart Publishing*, Oxford.

FALLETTI (2009), *Comunicazione, corrispondenza e riservatezza online*, in CASSANO et al. (a cura di), *Diritto dell'internet e delle nuove tecnologie telematiche*, Padova, p. 22.

FRANTZIOU (2014), *Further Developments in the right to be forgotten*, in *Human rights law review*.

GERADIN, KARANIKIOTI, KATSIFIS (2020), *GDPR Myopia: How a Well-Intended Regulation endend up Favoring Google in Ad Tech*, in *TILEC Discussion Paper DP*, p. 27.

HELMONS (2000*), La quatrième générations des droits de l'homme*, in *Les droits de l'homme au seuil du troisième millénaire*, Bruxelles.

JOHNSON (2010), *Privacy's no longer a social norm, says Facebook founder*, in *The Guardian*, reperibile *online*.

MANANCOURT (2022), *European Commission defends Ireland tech watchdoamid criticism of privacy record*, in *POLITICO*, reperibile *online*.

MCMILLAN (2014), *Verizon's Perma-Cookie' Is a Privacy-Killing machine*, in *Wired*, reperibile *online*.

MILLER (1971), *The assault of privacy*, in *Arbor University of Michigan Press*, p. 469.

ROSAS (2012), *When is the EU Charter of fundamental rights applicable at national level?*, in *Jurisprudencija*, p. 1269 ss.

VILLANI (2017), *Istituzioni di Diritto dell'Unione europea*, Bari, V ed.

VINOCUR (2019), *We have a huge problem: European tech regulator despairs over lack of enforcement*, in *Politico*, reperibile *online*.

WARREN (1890), *The right of privacy*, in *Harvard Law Review*, p.193.

Summary.

The digital revolution is the phenomenon that has characterized the past few years most of all, and it will continue to be one of the most central themes for years to come. Every element of our lives has been transformed by digital technology, which is providing us with unprecedented options. However, the increasing availability of new digital and data technologies brings with it unintended threats that can have far-reaching consequences for citizens, undermining democratic principles, security, and the foundations of society. Violations of privacy and personal data, dissemination of illegal and harmful content and unsafe products, as well as disinformation, cybercrime and cyberattacks, exploitation and abuse of human beings, including children, mass surveillance, algorithmic biases that hinder fair and non-discriminatory access to democratic information and debate, and even outright censorship have all increased significantly. These issues touch the heart of fundamental rights, undermining the hard-won progress in this area both within the European Union and globally.

The purpose of this paper is to retrace the milestones along the path of the right to personal data protection, first affirmed on a pretrial basis through groundbreaking jurisprudence of the Court of Justice, and then definitively enshrined in both Article 8 of the Charter and Article 16 of the TFEU.

Next, the analysis of judgment C-645/19 will be proposed, which sheds light on the critical issues hovering around the general data protection regulation (GDPR) and the difficulties encountered in the uniform interpretation of the aforementioned regulation, particularly the one-stop-shop mechanism.

The one-stop-shop mechanism was adopted as a key component in harmonizing the EU's legal system on data protection, with the goal of improving regulatory consistency, providing legal certainty, and reducing the administrative burden on data controllers and processors.

Case C-645/19 is concerned with the reference for a preliminary ruling present, in the context of the dispute between Facebook Belgium BVBA, on the one hand, and the Belgian Data Protection Authority (DPA), on the other hand, regarding an injunction action filed by the latter's president with the aim of stopping for users residing in Belgium the insertion of cookies and data collection without the users' consent. The referring court is the Brussels Court of Appeal. The fundamental challenge was whether the GDPR allows a supervisory authority that is not the lead supervisory body to bring crossborder processing cases before the courts of its own country.

The CJUE, in accordance with the conclusion provided by the Advocate general (AG) determines that the principal authority's competence in connection to crossborder processing is the general rule, whereas the competence of other authorities is the exception, after several interpretations of the GDPR wording. As a result, the principal authority is the primary point of contact with the data controller or processor, while also acknowledging that, under Articles 60 et seq., close cooperation and consensus with the other authorities is required to make decisions in this area of the Regulation (GDPR). The CJEU reiterates the need not only for "effective" cooperation between the principal authority and other supervisory authorities concerned, but also requires "sincere" cooperation, thus going beyond the pure letter of the RGPD.

This ruling, although it may seem purely technical, actually offers a broader overview of the European integration process.

In reiterating the one-stop-shop importance, shop's the Court emphasized the importance of a consistent approach to defending both core rights and the

integration process itself. The European Union still has to devote more resources to the creation of a comprehensive and cohesive digital single market.