Oltre le censure della CGUE: il *Data Privacy Framework* e la nuova decisione di adeguatezza per il trasferimento dei dati personali verso gli Stati Uniti*

Beatrice Bessone

Abstract

Il contributo esamina la decisione di adeguatezza della Commissione europea che riconosce l'equivalenza tra il livello di protezione dei dati personali statunitense e quello istituito nell'Unione europea ammettendo, così, la relativa libera circolazione. L'articolo analizza i miglioramenti e le criticità nella protezione dei dati considerando, altresì, le esigenze di coordinamento tra gli ordinamenti.

The paper examines the adequacy decision of the European Commission recognizing the equivalence between the US level of data protection and that one established in the European Union, thus admitting its free movement. The article analyses the improvements and criticalities in data protection, also considering the need for coordination between the legal systems.

Sommario

Keywords

data protection – privacy – circolazione dei dati – decisioni di adeguatezza – trasferimenti di dati personali

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

1. Le decisioni della Commissione europea tra necessità e adeguatezza

Con una recente decisione[1] la Commissione europea, ritenendo adeguato il livello di protezione garantito dagli Stati Uniti verso i dati personali appartenenti a soggetti residenti sul territorio europeo, sembra porre fine all'annosa questione originata dalle pronunce della Corte di giustizia dell'Unione europea (CGUE) sui ricorsi avanzati da Maximillian Schrems, che – come noto – hanno segnato il tramonto del *Safe Harbor* prima, e del *Privacy Shield* transatlantico, poi[2]. Nelle descritte questioni la CGUE ha evidenziato l'assenza nel diritto interno degli Stati Uniti di un livello di protezione adeguato per i dati personali che, raccolti in Europa, siano successivamente trasferiti negli USA.

Il tema della raccolta, utilizzo e trasferimento dei dati personali è tanto complesso quanto imprescindibile. Le nuove tecnologie hanno quale effetto la moltiplicazione della quantità di dati che, quotidianamente, vengono prodotti, raccolti e fatti circolare da imprese, persone ed istituzioni anche verso Paesi Terzi che, perciò solo, non sono tenuti ad applicare il Regolamento Generale sulla Protezione dei Dati Personali, c.d. GDPR (regolamento (UE) 27 aprile 2016, n. 679). Il GDPR stabilisce le condizioni necessarie a rendere legittimo un trasferimento di dati verso un Paese transfrontaliero prevedendo, a tal fine, il ricorrere di due differenti – e alternative – ipotesi, vale a dire l'adozione di una decisione di adeguatezza da parte della Commissione europea oppure la previsione – da parte del Paese extra-UE – di garanzie "adeguate" a tutela dei dati personali appartenenti a soggetti residenti in Europa (art. 45 e 46 GDPR)[3].

Rispetto all'ordinamento statunitense i profili "critici" sono molteplici poiché la disciplina in materia di tutela dei dati personali è frammentata. Per giunta, il c.d *Foreign*

[1] COM (2023) 4745, 10 luglio 2023, decisione di esecuzione della commissione del 10 luglio 2023, ai sensi del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sull'adeguato livello di protezione dei dati personali nell'ambito del Quadro sulla privacy dei dati UE-USA.

[2] CGUE, 6 ottobre 2015, C-362/14, *Maximillian Schrems/Commissario per la protezione dei dati (Schrems*) e CGUE, 16 luglio 2020, C-311/18*, Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems (Schrems II)*. La questione è nota, tuttavia giova ripercorrerne brevemente i fatti. La vicenda nasce nel 2013, quando Maximilian Schrems decise di rivolgersi al *Irish Data Protection Commissioner* per vedere sospeso il trasferimento dei propri dati personali dalla controllata Facebook Ireland a Facebook Inc. La richiesta era sorretta dall'assunto che, contrariamente a quanto accertato dalla Commissione nella sua decisione 2000/520/CE, il livello di protezione dei dati negli USA non potesse essere considerato sufficiente a garantire una adeguata tutela della vita privata da intromissioni generalizzate e indiscriminate da parte delle autorità governative statunitensi. Per dottrina: A. Mantelero, *L'ECJ invalida l'accordo per il trasferimento dei dati personali fra EU ed USA. Quali scenari per cittadini ed imprese?*, in *Contratto e Impresa. Europa*, 2015, 722; O. Pollicino, *Diabolical Persistence: Thoughts on the Schrems II Decision,* in *medialaws.eu,* 2020, 314 ss.; A. Cristofano, *La Sentenza Schrems II e il judicial activism della Corte di Giustizia dell'Unione Europea. Verso un GDPR a vocazione universale?* in *medialaws.eu,* 2021.

[3] Artt. 45 e 46 GDPR. Ai sensi dell'art.45, par. 1: «Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche», mentre, l'art. 46. par. 1, prevede «In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi».

Intelligence Surveillance Act consente l'accesso (ed il relativo utilizzo) ai dati personali provenienti dall'Unione europea per fini di sicurezza nazionale e, sebbene la norma preveda obblighi in capo alle autorità governative federali volti a tutelare la riservatezza (notifica all'interessato, facoltà di modifica), non mancano le eccezioni che rendono le garanzie di protezione di dubbia effettività[4].

Ciononostante, il flusso di dati personali che "migra" negli USA non può essere arginato. Proprio negli Stati Uniti sono insidiati gran parte dei c.d. "servizi di piattaforma di base" tra i quali si annoverano *social network*, motori di ricerca e *marketplaces*. La fruizione di detti servizi implica la raccolta – costante – di una quantità ingente di dati personali che, diventando parte dei *dataset* controllati dai gestori delle piattaforme, rappresentano, per questi ultimi, risorsa e valore economico[5]. A ciò si aggiunge che le grandi potenze aziendali, oltre ad offrire i servizi sopra descritti, mettono a disposizione del mercato anche strumenti di lavoro che vengono utilizzati tanto da soggetti privati quanto dalle amministrazioni pubbliche[6] (si pensi a Google LLC).

La centralità assunta dai dati personali nei rapporti commerciali tra UE e USA ha perciò comportato una serie di negoziazioni tra la Commissione europea e il *Department of commerce* statunitense, rivelandosi necessario un bilanciamento tra la protezione e il trasferimento dei dati sin dall'entrata in vigore della Direttiva 95/46/CE. Il primo accordo, c.d. *Safe Harbor,* consisteva in una decisione di adeguatezza adottata dalla Commissione europea contenente una serie di principi cui, necessariamente, dovevano attenersi i *partners* americani, dunque le imprese "registrate" al *Safe Harbor*[7]. La previsione di una decisione di adeguatezza ha consentito il libero trasferimento di dati; sennonchè la Corte di giustizia, con la prima sentenza *Schrems*, ha invalidato la citata decisione dopo aver valutato la mancanza – nell'ordinamento statunitense – di norme idonee a limitare l'ingerenza delle autorità statunitensi nei dati personali dei soggetti europei, assenza che, di fatto, avrebbe potuto comportare un indiscriminato accesso da parte di queste ultime. Inoltre, il *Safe Harbor* vincolava soltanto le imprese aderenti all'accordo, condizione che è stata censurata dalla Corte di giustizia europea[8].

Nuove negoziazioni hanno poi condotto, nel 2016, alla stipula del *Privacy Shield*, accordo incrementato di garanzie ulteriori, tali da definire puntualmente gli obblighi di protezione in capo alle aziende statunitensi ed altresì gli strumenti da adottare per implementare la tutela dei dati personali. Rispetto alla raccolta "indiscriminata" di dati non ostacolata dal *Safe Harbor,* sono state definite forti limitazioni superabili solo in

---

[4] E. Terolli, *Privacy e protezione dei dati personali, UE vs. USA. Evoluzioni di diritto comparato e il trasferimento di dati personali dopo la sentenza "Schrems II",* in *Diritto dell'informazione e dell'informatica*, 2021, 49.

[5] F. Ferrari, *Le concentrazioni nei mercati data driven: la privacy rinnegata,* in *Diritto del commercio Internazionale,* 2021, 2029 ss.

[6] F. Ferrari, *Le concentrazioni nei mercati data driven: la privacy rinnegata,* cit., 2030 ss.

[7] COM (2000), 1250, 25 agosto 2000.

[8] Per dottrina sul punto si rimanda a S. Sica-V. D'Antonio, *I Safe Harbour Principles: genesi, contenuti, criticità, in Diritto dell'informazione e dell'informatica*, 2015, 808; R. Bifulco, *La sentenza Schrems e la costruzione del diritto europeo della privacy, in Giurisprudenza costituzionale*, 2016, 289 ss. Da ultimo si rimanda a C. Bertoldi, *Tutela dei diritti e accesso ai dati personali da parte delle autorità governative: l'equilibrio precario della decisione di adeguatezza e delle clausole contrattuali standard,* in *Federalismi*, 2022, 5 ss.

ragione di "casi limite" o estremi, a garanzia della pubblica sicurezza[9]. Pur ripercorrendo il GDPR solo parzialmente, le garanzie previste dallo "Scudo" sono state ritenute sufficienti, tanto da spingere la Commissione europea all'adozione di una nuova decisione di adeguatezza[10]. Quanto contenuto nell'accordo obbligava l'importatore ma non le autorità governative statunitensi, fatto che – sull'impulso del secondo ricorso presentato da Schrems alla CGUE – ne ha causato la caducazione[11].
La questione centrale, cui attengono le descritte vicende, riguarda la mancata sussistenza – nel territorio statunitense – di un livello di protezione equivalente a quello previsto dal Regolamento generale per la protezione dei dati personali europeo; equivalenza che differisce da uguaglianza, ben potendo il Paese Terzo assicurare la protezione dei dati personali in modo anche molto diverso rispetto al GDPR[12]. Ad assumere rilevanza, dunque, è che il Paese extra-Ue abbia previsto in relazione al trattamento dei dati personali una normativa capace di tutelare i diritti e gli interessi dei soggetti interessati tanto quanto il Regolamento europeo[13]. Negli Stati Uniti, si è detto, la disciplina è lacunosa; i dati personali non sono tutelati a livello costituzionale ma, per lo più, da atti regolamentari o di autoregolamentazione e da norme settoriali, fatto che rende poco sicura la libera circolazione dei dati personali.

2. Verso nuovi, deboli equilibri - le clausole contrattuali standard

Come dimostrato, negli anni sono "caduti" entrambi i tentativi di rendere libero il trasferimento di dati verso gli importatori ubicati negli Stati Uniti. L'essenzialità degli scambi commerciali tra Stati Uniti ed Unione europea ha tuttavia richiesto, dopo il secondo arresto dovuto dalla pronuncia della CGUE c.d. *Schrems II*, l'adozione di garanzie puntuali, tra le quali si annoverano le clausole contrattuali standard (art. 46 GDPR). Queste ultime hanno costituito – nell'assenza di una decisione di adeguatezza – lo strumento per legittimare il flusso di dati verso gli Stati Uniti; rappresentando un "sostegno" per le imprese che costruiscono il proprio valore sullo scambio di dati personali, sono state impiegate su larga scala. Non si tratta, tuttavia, di una novità. Con le "clausole contrattuali tipo" (o standard, SSC) la Commissione europea tenta di

[9] COM (2016), 1250, 12 luglio 2016, considerando 69.

[10] COM (2016), 1250, 12 luglio 2016.

[11] B. Carotti, *Il trattamento dei dati personali dinanzi alla Corte di Giustizia: un anno difficile,* in *Giornale Giornale di Diritto Amministrativo,* 2021, 473 ss.

[12] Per un'analisi sull'applicazione del principio dell'equivalenza, anche negli ordinamenti giuridici degli Stati membri: B. Ponti, *Attività amministrativa e trattamento dei dati personali: gli standard di legalità tra tutela e funzionalità,* Milano, 2022; M. Midiri-S. Piva, *L'interesse pubblico come base giuridica e come finalità del trattamento dei dati personali*, in *Il "nuovo" codice in materia di protezione dei dati personali. La normativa italiana dopo il d.lgs. n. 101/2018*, a cura di S. Scagliarini, Torino, 2018, 21 ss.

[13] Secondo quanto previsto dalla sentenza CGUE, 16 luglio 2020, C-311/18, *Schrems II,* § 12, la Commissione dovrebbe valutare se il quadro giuridico del paese terzo preveda norme volte a limitare le interferenze con i diritti fondamentali dei soggetti i cui dati siano trasferiti dall'Unione, che gli enti statali di tale paese sarebbero autorizzati a intraprendere quando perseguono obiettivi legittimi, come la sicurezza nazionale, e fornisca un'efficace protezione giuridica contro interferenze di questo tipo.

garantire un livello adeguato di protezione nel trasferimento dei dati da un Titolare o Responsabile del trattamento stabilito nell'Unione ad un Titolare o Responsabile del trattamento stabilito in un Paese terzo[14]. Imponendo l'adozione di strumenti definiti, le clausole contrattuali si propongono di garantire un trasferimento sicuro[15]. Se i Titolari del trattamento interni agli Stati Membri hanno riposto sulle medesime grande fiducia, la CGUE si è dimostrata – sin dalla pronuncia che ha comportato l'eclissi del *Privacy Shield* – più dubbiosa[16].

Il monito della Corte di giustizia dato, con la sentenza c.d. *Schrems II*, ai Titolari dei trattamenti che contemplino un trasferimento di dati verso paesi Terzi non è di poco conto. Quest'ultima è intervenuta nella vigenza del GDPR e, pertanto, pone obblighi di protezione più restrittivi rispetto alla sua precedente (*Schrems I*). In particolare, in capo ai Titolari del trattamento vi è l'obbligo di valutare le caratteristiche del Paese di destinazione nonché il livello di tutela dal medesimo garantito, che deve essere quantomeno omogeneo agli standard europei[17]. In altri termini la CGUE richiede che sia assicurato – avuto riguardo alla legislazione nazionale – un livello di protezione delle libertà e dei diritti fondamentali equivalente, anche quando il trattamento avvenga sulla base delle c.d. clausole standard. Tale incombenza, quanto agli Stati Uniti, può risultare ardua, se si considera che la "sensibilità" sul tema della protezione dei dati personali che caratterizza i sistemi USA e UE è molto diversa[18].

Le clausole citate debbono inserirsi all'interno dei contratti stipulati tra soggetti importatori ed esportatori, dunque in un rapporto contrattuale che, in quanto tale, produce effetti *inter partes*[19]. Con le clausole contrattuali l'importatore e l'esportatore si impegnano ad assicurare, indipendentemente dal Paese cui i dati vengano "trasmessi", uno standard di protezione adeguato, equivalente, dunque, alla tutela assicurata dal Regolamento europeo. Per mezzo delle clausole, dunque, le imprese – ma anche le pubbliche amministrazioni – hanno tentato di compensare l'assenza di una decisione di adeguatezza che consentisse, in via generale, il trasferimento dei dati negli USA.

Resta tuttavia da chiarire se lo strumento sopra descritto sia idoneo ad assicurare una protezione sufficiente, tale da superare il "*gap*" di tutela che differenzia la normativa USA e UE in materia tanto di protezione, quanto di tutela per la riservatezza. Poiché, come detto, le clausole contrattuali sono elemento di un contratto instaurato tra due o più parti specificamente individuate, né lo Stato di afferenza dell'importatore né, tantomeno, le pubbliche autorità sono tenute alla loro osservanza. Più precisamente – avendo riguardo agli USA – i servizi di *intelligence* (NSA, FBI) e le autorità governative,

[14] C. Bertoldi, *Tutela dei diritti e accesso ai dati personali da parte delle autorità governative: l'equilibrio precario della decisione di adeguatezza e delle clausole contrattuali standard,* cit., 5 ss.

[15] Da ultimo, (COM) 2021, 914, 4 giugno 2021. Si precisa che le decisioni della Commissione europea sono obbligatorie in tutti i loro elementi (art. 288; par. 4, TFUE).

[16] C. Bertoldi, *Tutela dei diritti e accesso ai dati personali da parte delle autorità governative: l'equilibrio precario della decisione di adeguatezza e delle clausole contrattuali standard,* cit., 5 ss.

[17] R. Bifulco, *Il trasferimento dei dati personali nella sentenza Schrems: dal contenuto essenziale al principio di proporzionalità e ritorno,*in *Diritto pubblico europeo*, 2020.

[18] F. Rossi Dal Pozzo, *La tutela dei dati personali UE a seguito della sentenza Schrems,* in *Eurojus,* 2015.

[19] CGUE, 16 luglio 2020, C-311/18, *Schrems II,* par.104. R. Bifulco, *Il trasferimento dei dati personali nella sentenza Schrems: dal contenuto essenziale al principio di proporzionalità e ritorno,*cit.

non essendo parte degli accordi che si instaurano tra l'importatore (USA) e l'esportatore (UE), operano secondo il proprio assetto normativo[20]. Per le citate ragioni, lo strumento in esame non ha ottenuto il "benestare" della CGUE. Il "crollo" delle decisioni di adeguatezza e la dubbia tutela concessa dalle SSC ha spinto Stati Uniti ed Unione europea a nuove negoziazioni per individuare un punto di equilibrio tra le esigenze, imprescindibili, di protezione e circolazione dei dati personali provenienti dall'Europa.

Tuttavia le SSC hanno rappresentato (e rappresentano!) un *escamotage* di particolare rilievo. Le clausole contrattuali sono individuate, come accennato, dalla Commissione europea tramite l'assunzione di decisioni. Per ovviare alle ingerenze dell'*intelligence* e delle Autorità governative, l'Unione europea ha previsto, nell'adozione della decisione di esecuzione più recente ((COM) 2021, 914, 4 giugno 2021), alcune disposizioni, più o meno specifiche, che vincolano il Titolare del trattamento – e soprattutto il soggetto importatore – che intenda effettuare un trasferimento di dati personali verso un Paese Terzo (è sufficiente utilizzare, nell'attività o organizzazione, strumenti quali Google LLC, Microsoft, Outlook ecc.). Tra queste assumono particolare importanza gli obblighi previsti in capo all'importatore, allorquando una autorità pubblica faccia richiesta di accesso ai dati personali di soggetti residenti in UE (clausola 15)[21]. Debbono, inoltre, essere garantiti i diritti dell'interessato secondo la declinazione propria del GDPR[22] e, dunque, il diritto all'informazione, cancellazione, rettifica e opposizione (clausola 10).

Sul punto è intervenuto anche l'*European data protection board* (EPDB)[23]che, avuto riguardo a quanto statuito dalla CGUE, ha suggerito, ai Titolari del trattamento che si accingono a trasferire i dati raccolti presso gli USA, l'applicazione di misure di sicurezza supplementari. Queste ultime sono individuate dal gruppo consultivo e – anche se

[20] Di tale aspetto, peraltro, tiene conto la stessa decisione di adeguatezza ove, all'art. 15, prevede una serie di obblighi in capo all'importatore allorquando una autorità pubblica faccia richiesta di accesso ai dati personali di soggetti residenti in UE. Per dottrina: R. Bifulco, *Il trasferimento dei dati personali nella sentenza Schrems: dal contenuto essenziale al principio di proporzionalità e ritorno,* cit.; G. Formici, *Schrems colpisce ancora? Il trasferimento dei dati personali dall'Unione europea a Stati terzi, le Conclusioni dell'Avvocato generale nel caso Data Protection Commissioner v. Facebook Ireland Limited e Maximillian Schrems e una storia che rischia di ripetersi,* in questa *Rivista,* 1, 2020, 310 ss.

[21] (COM) 2021, 914, 4 giugno 2021, clausola 15, a mente della quale è previsto che l'importatore informi prontamente l'esportatore e, ove possibile, l'interessato (se necessario con l'aiuto dell'esportatore) se: riceve una richiesta giuridicamente vincolante di un'autorità pubblica, comprese le autorità giudiziarie, a norma della legislazione del paese di destinazione, di comunicare dati personali trasferiti in conformità delle presenti clausole; tale notifica comprende informazioni sui dati personali richiesti, dall'autorità richiedente, sulla base giuridica della richiesta e sulla risposta fornita; o viene a conoscenza di qualunque accesso diretto effettuato, conformemente alla legislazione del paese terzo di destinazione, da autorità pubbliche ai dati personali trasferiti in conformità delle presenti clausole; tale notifica comprende tutte le informazioni disponibili all'importatore. Inoltre, se la legislazione del paese di destinazione vieta all'importatore di informare l'esportatore e/o l'interessato, l'importatore accetta di fare tutto il possibile per ottenere un'esenzione dal divieto.

[22] Artt. 15, 16 e 17 GDPR.

[23] European Data Protection Board, Opinion 18/2021 on the draft Standard Contractual Clauses submitted by the LT SA (Article 28(8) GDPR). L'EDPB è un organismo indipendente che ha sostituito il gruppo ex art. 29 della direttiva 95/46/CE che deve assicurare l'applicazione coerente, in tutti gli Stati membri, del GDPR. Tra le sue funzioni vi è, altresì, l'attività consultiva a favore della Commissione europea sulle questioni riguardanti i dati personali.

l'elencazione proposta non può ritenersi esaustiva – tra le più efficaci vi sono le note misure di cifratura, anonimizzazione e pseudonimizzazione. Cionondimeno, quanto prospettato comporta diverse problematiche dal punto di vista applicativo. Si pensi alle caselle di posta elettronica (gmail); le citate misure comporterebbero la ricezione di e-mail ove il destinatario sarebbe "identificato" a mezzo di numeri o codici, fatto che renderebbe pressoché inutile l'utilizzo dello strumento stesso.

3. Il *Data Privacy Framework*

Nel marzo 2022, Unione europea e Stati Uniti hanno siglato un nuovo accordo, il *Data privacy Framework* (DPF), che rappresenta l'ennesimo tentativo di rendere libera la circolazione di dati personali negli USA. Alla stipula dell'accordo è seguita la nuova decisione di adeguatezza della Commissione europea, nella quale è stabilito che gli Stati Uniti assicurano un livello di protezione equivalente a quello dell'UE. In forza della nuova decisione di adeguatezza, i dati personali possono circolare dall'UE alle società statunitensi che aderiscono al *Framework*, senza la necessità di adottare ulteriori garanzie e misure di protezione[24].

Poiché il quadro normativo degli Stati Uniti, di fatto, è rimasto immutato, occorre comprendere come i vertici USA e UE abbiano inteso porre "rimedio" alle già descritte carenze di tutela per i flussi transatlantici di dati personali. I negoziati hanno preso avvio a seguito dell'invalidazione del *Privacy Shield* sull'impulso del ricorso di Maximilian Schrems. L'obiettivo del nuovo quadro è porre rimedio alle criticità e lacune evidenziate dalla Corte di giustizia europea nella sentenza Schrems II.

Assume particolare rilevanza nel descritto contesto l'*Executive order 14086* (EO), firmato dal Presidente Biden per rafforzare le garanzie "contro" le attività di *intelligence* delle autorità governative statunitensi, talvolta ingiustificate. L'impegno degli Stati Uniti è senza precedenti: nell'ambito del nuovo accordo è stata attuata una serie di riforme volte a rafforzare la tutela della riservatezza. Sono state così previste misure di salvaguardia volte a garantire la proporzionalità delle operazioni dei servizi di *intelligence*. Con particolare riferimento al principio di proporzionalità, l'*Executive order 14086* elenca dei casi specifici nei quali è ammessa l'ingerenza delle autorità governative, evidenziando in questo modo il primato delle necessità di sicurezza nazionale. Si tratta quindi di ipotesi definite, ove l'accesso ai dati personali di soggetti residenti in Europa è giustificato perché necessario a garantire la pubblica sicurezza e, dunque, proporzionato[25]. È parimenti proposta, sempre dall'ordine esecutivo, una serie di ipotesi in cui, di contro, l'intrusione nella sfera privata dei soggetti interessati da un trattamento

[24] La protezione offerta dal DPF UE-USA si applica a tutti i dati personali trasferiti dall'Unione alle organizzazioni negli Stati Uniti che hanno certificato la loro adesione ai principi con il *Department of Commerce*. L'elenco delle organizzazioni statunitensi aderenti è pubblico. Il DoC, inoltre, ha compiti di monitoraggio ai fini di rilevare eventuali false dichiarazioni di partecipazione al DPF UE-USA o l'uso improprio del marchio di certificazione DPF UE-USA, sia d'ufficio che sulla base di reclami. Quanto descritto si evince anche dalla decisione COM (2023),4745, cit., considerando 56.

[25] M. Giacalone, *Verso Shrems III? Analisi del nuovo EU-US Data Privacy Framework*, in *European papers,*1, 2023, 147 ss.

dati è esclusa[26]. Quanto prospettato limita fortemente l'intromissione ingiustificata delle autorità pubbliche statunitensi. Ciononostante, la formulazione delle ipotesi che legittimano l'ingerenza nei dati personali dei servizi di *intelligence* statunitensi, lascia spazio ad ampie aperture "interpretative" poiché l'*Executive Order* non ne delimita precisamente i confini.

Non stupisce poi che gli Stati Uniti, con l'emanazione del citato ordine esecutivo, non abbiano inteso intervenire sulla normativa vigente, lasciando così invariato il *Foreign Intelligence Surveillance Act*. Si tratta dell'assetto normativo più criticato dalla Corte di giustizia europea; ivi è infatti riconosciuta la facoltà per le agenzie federali statunitensi di raccogliere informazioni personali sui soggetti esteri, sospettati di attività di terrorismo[27].

Altro aspetto di rilievo è l'introduzione di un sistema di ricorso a due livelli che sostituisce la c.d. figura del mediatore, prevista dal *Privacy Shield* e censurata dalla Corte di giustizia europea[28]. Al mediatore, infatti, non era concessa la facoltà di adottare rimedi effettivi e neppure decisioni vincolanti. Quest'ultimo, al più, poteva dettare raccomandazioni volte ad incentivare l'adozione di misure correttive. Critiche sono state mosse anche verso l'indipendenza e l'imparzialità del mediatore. L'organo, secondo la Corte di giustizia, non poteva considerarsi impermeabile rispetto ad eventuali influenze esterne e, soprattutto, verso la possibile influenza del potere esecutivo, cui era incardinato[29]. Il nuovo meccanismo di ricorso, di contro, consente ai cittadini europei di avanzare reclamo avanti al *Civil Liberties Protection Officer* (CLPO), per segnalare eventuali violazioni commesse dai servizi di *intelligence* ai danni della riservatezza e in contrasto con quanto previsto dalla legge statunitense. La decisione del CLPO – che può prevedere anche un "risarcimento" (c.d. riparazione) per il soggetto leso – può essere appellata innanzi e alla *Data Protection Review Court* (DPRC) e ha carattere vincolante, per espressa previsione dell'*Executive order*[30].

La formulazione dell'ordine esecutivo, pur non rispettando pienamente gli standard europei[31], è sintomatica di una maggiore apertura verso la protezione effettiva dei dati appartenenti ai soggetti interessati da un trattamento con flusso transatlantico di dati. Gli Stati Uniti, nonostante l'immutato assetto normativo del *Foreign Intelligence Surveillance Act,* hanno mosso passi importanti verso le richieste di tutela avanzate dall'Unione europea. L'approccio degli Stati Uniti riguardo alla protezione dei dati personali è

[26] Presidente degli Stati Uniti, Executive Order 14086, 7 cit., vol. 87, n. 198, 2022, Sec. 2, 62283.

[27] M. Giacalone, *Verso Shrems III? Analisi del nuovo EU-US Data Privacy Framework*, cit., 147 ss.

[28] CGUE, 16 luglio 2020, C-311/18, *Schrems II,* §§ 168, 190.

[29] CGUE, 16 luglio 2020, C-311/18, *Schrems II,* §§ 150-162. M. Giacalone, *Verso Shrems III? Analisi del nuovo EU-US Data Privacy Framework*, cit., 147 ss.

[30] Il nuovo sistema di ricorso tenta di ottemperare a quanto previsto dall'art. 47 della Carta dei diritti Fondamentali dell'Unione europea. Tramite la previsione della figura del CLPO e della Protection Court review, gli Stati Uniti tentano di garantire una tutela effettiva ed imparziale a chi abbia subito interferenze ingiustificate nella propria sfera personale.

[31] La Carta dei diritti fondamentali dell'Unione europea richiede – perché sia legittima la limitazione di diritti e libertà ivi contenuti – che vi sia specifica previsione di legge (art. 52) e, soprattutto, che detta limitazione avvenga nel rispetto del principio di proporzionalità rispetto all'esigenza di proteggere i diritti e le libertà altrui.

da sempre caratterizzato da una sorta di utilitarismo. Nel sistema USA, infatti, i dati personali delle persone fisiche paiono rappresentare, più che un diritto della persona umana, un valore economico che deve essere protetto anche (e soprattutto) in ragione della rilevanza degli scambi commerciali[32].

4. La nuova decisione della Commissione europea.

In virtù di quanto sopra prospettato, la Commissione europea ha emanato una nuova decisione di adeguatezza. Dal luglio 2023 è perciò consentito il libero scambio di dati personali con gli Stati Uniti, senza obbligo – in capo ai Titolari del trattamento – di adottare ulteriori garanzie. In particolare la Commissione, dopo aver esaminato e valutato quanto previsto dal *Data Privacy Framework*, ha concluso che «gli Stati Uniti garantiscono un livello adeguato di protezione dei dati personali trasferiti ai sensi del DPF UE-USA da un Titolare del trattamento nell'Unione a organizzazioni certificate negli Stati Uniti». Il livello di protezione garantito dagli USA, pertanto, deve ritenersi sostanzialmente equivalente.

La decisione di adeguatezza, a seguito di una disamina dei principi applicabili al trattamento transfrontaliero di dati che, in larga misura, ripropongono quanto stabilito dal regolamento europeo (limitazione delle finalità, correttezza, minimizzazione del dato, trasparenza, diritti del soggetto interessato)[33], analizza nel dettaglio i punti del DPF che si propongono di porre rimedio alle carenze perpetrate dagli accordi precedenti (*Safe Harbor* e *Privacy Shield*) e valutate dalla Corte di giustizia europea quali gravi lacune nelle esigenze di protezione. Nella decisione in esame la Commissione dedica, perciò, particolare attenzione ai profili del *Framework* che riguardano i limiti all'accesso delle autorità governative statunitensi ai dati personali dei cittadini europei e il nuovo meccanismo di ricorso innanzi al CLPO. Nello specifico, è dato atto delle garanzie previste dagli Stati Uniti a protezione dei dati personali pensate per colmare il vuoto di tutela rispetto all'intromissione – un tempo incontrollata – dei servizi di *intelligence*. La decisione ripercorre i punti salienti dell'ordine esecutivo che, si è detto, pare ridurre la legittima intrusione nella sfera privata dei cittadini europei ad ipotesi residuale.

Più precisamente, la Commissione, nel valutare se le condizioni che rendono lecito l'accesso governativo ai dati trasferiti agli USA rispettino il già descritto requisito dell'equivalenza (art. 45 GDPR)[34], ha tenuto conto di diversi criteri. Nello specifico, sono legittime le limitazioni del diritto alla protezione dei dati personali fondate su una legge che definisca, altresì, la portata dell'"intrusione". Inoltre, l'affievolimento della protezione è consentito solo nella misura strettamente necessaria a conseguire obiettivi precisi, nell'interesse generale e speculari a quelli riconosciuti dall'UE[35]. Le dispo-

[32] Decisione di adeguatezza, allegato I, par.1. M. Giacalone, *Verso Schrems III? Analisi del nuovo EU-US Data Privacy Framework*, cit., 147 ss.

[33] Art. 5 GDPR.

[34] Art. 45, par. 1, GDPR, come interpretato dalla Corte di giustizia alla luce della Carta dei diritti fondamentali.

[35] Art. 23 GDPR e considerando 104.

sizioni previste dalla legge debbono essere, oltreché vincolanti, chiare e precise nella definizione delle misure intrusive e nella previsione di garanzie idonee a proteggere i dati personali dal rischio di abusi. Nondimeno, occorre che sia garantita ai soggetti interessati la possibilità di adire un tribunale indipendente e imparziale, per avere accesso alle proprie informazioni personali e ottenerne, eventualmente, la cancellazione o la rettifica[36]. La decisione in esame ha ritenuto le condizioni cui la legislazione degli Stati Uniti subordina l'accesso in linea con i requisiti richiesti, stante la previsione di limitazioni e garanzie nonché la definizione di meccanismi di controllo e di ricorso[37].
Rispetto ai mezzi di ricorso, la Commissione considera gli strumenti proposti dagli Stati Uniti, così come sopra declinati (CLPO e DPRC), capaci di offrire ai soggetti interessati una tutela effettiva. In capo a questi ultimi vi è, infatti, la possibilità di adire un Tribunale indipendente, imparziale e con poteri vincolanti[38]. L'indipendenza del processo decisionale è data dal divieto per la componente esecutiva (Procuratore generale e Agenzie di *intelligence*) di interferire o influenzare, in qualsiasi modo, l'eventuale revisione data dalla DPRC[39]. Il cittadino europeo che voglia presentare un reclamo deve rivolgersi all'Autorità di controllo dello Stato membro di appartenenza, che provvederà a trasmetterlo al segretariato del Comitato europeo per la protezione dei dati. Perché il reclamo sia accolto è necessario rendere noti i dati personali che si ritengono violati, ma non è richiesto di provare l'intrusione – nella sfera privata e personale – da parte delle autorità governative USA[40]. Si tratta, dunque, di un meccanismo di ricorso facilmente accessibile sia dal punto di vista dell'onere probatorio, sia perché i soggetti "lesi" possono avanzare il proprio reclamo "vicino a casa", senza che si interpongano barriere linguistiche.
D'altro canto, anche l'*European data protection board* ha accolto con favore le nuove misure di tutela introdotte dagli USA a protezione dei dati personali, nonostante alcune "resistenze" iniziali[41]. Di recente, il Comitato europeo per la protezione dei dati ha adottato una nota informativa[42] rivolta tanto alle persone fisiche quanto alle organiz-

[36] COM (2023),4745, cit., considerando 83.

[37] COM (2023), 4745, cit., considerando 86,119. Per la legislazione USA: Presidente degli Stati Uniti, Executive Order 14086, 7, cit., vol. 87, n. 198, 2022, Sec. 2 (ii), 14086.

[38] COM (2023), 4745, cit., considerando 86,119.

[39] COM (2023), 4745, cit., considerando 185 descrive le funzioni e la composizione della DPRC. Si tratta di un tribunale indipendente istituito dal Procuratore generale sulla base dell'EO 14086. È composto da almeno sei giudici, nominati dal Procuratore generale in consultazione con il PCLOB, il Segretario al Commercio e il Direttore dell'Intelligence nazionale per mandati rinnovabili di quattro anni. La nomina dei giudici da parte del Procuratore generale si basa sui criteri utilizzati dalla componente esecutiva per valutare i candidati alla magistratura federale, dando peso a qualsiasi esperienza giudiziaria precedente. Inoltre, i giudici devono essere professionisti del diritto (cioè membri attivi e in regola dell'ordine degli avvocati e debitamente abilitati all'esercizio della professione) e avere un'adeguata esperienza in materia di privacy e sicurezza nazionale. Il Procuratore generale deve cercare di garantire che almeno la metà dei giudici in qualsiasi momento abbia una precedente esperienza giudiziaria e tutti i giudici devono essere in possesso di nulla osta di sicurezza per poter accedere a informazioni classificate sulla sicurezza nazionale.

[40] COM (2023) ,4745, cit., considerando 117.

[41] Per un approfondimento si veda: EPDB, Opinion 5/2023 *on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework,* 28 febbraio 2023.

[42] EPDB, *Information note on data transfers under the GDPR to the United States after the adoption of the adequacy*

zazioni che, nelle proprie attività, trasferiscono dati negli Stati Uniti. Il documento, tramite alcune indicazioni sintetiche, intende chiarire l'impatto della decisione di adeguatezza della Commissione UE, nonché le implicazioni del DPF e del meccanismo di ricorso sopra descritto. L'EPDB, in particolare, evidenzia che i trasferimenti "coperti" da decisioni di adeguatezza non necessitano dell'integrazione di misure supplementari, le quali debbono invece applicarsi ogni qualvolta il trasferimento transfrontaliero avvenga a favore di organizzazioni non comprese nell'elencazione del DPF. Il Comitato sottolinea, ancora, che le garanzie messe in atto dagli Stati Uniti rispetto all'ambito della sicurezza nazionale – ivi compreso il nuovo meccanismo di ricorso – hanno da applicarsi a tutti i dati che siano trasferiti negli USA, sia il trasferimento giustificato, o meno, dalla nuova decisione della Commissione europea.

In virtù di quanto sin ora rappresentato, può concludersi che gli Stati Uniti abbiano tentato, tramite l'emanazione del DPF, di proteggere i dati personali conformemente a quanto richiesto dal GDPR, in ossequio al principio di equivalenza (art. 45 GDPR). Restano, ciononostante, talune perplessità. Si è detto, ma giova ribadirlo, che l'*Executive Order* stabilisce le ipotesi legittimanti l'ingerenza delle attività di *intelligence* nei dati personali dei cittadini europei. Tuttavia la formulazione delle medesime – che non definisce le fattispecie – lascia aperti ampi margini interpretativi. Sebbene l'intento dell'ordine esecutivo sia quello di circoscrivere la violazione della riservatezza a quei casi concreti che, in un bilanciamento tra interessi, risultino proporzionati a esigenze di sicurezza nazionale, il rischio è che tali ipotesi-limite si tramutino in un "lasciapassare" a ingerenze ultronee rispetto ai fini previsti dall'EO. La normativa degli USA è, forse, incompatibile con la protezione dei dati personali richiesta dall'Unione europea, poiché il "peso" e la configurazione attribuiti al dato personale, rispettivamente da USA e UE, sono divergenti. Se, per l'UE, la riservatezza e la protezione dei dati personali (quali proiezioni della persona fisica) sono diritti fondamentali – tanto da trovare tutela nella Carta dei diritti fondamentali dell'Unione europea (artt. 8, 48, 52 CDFUE) – per gli Stati Uniti i dati delle persone fisiche trovano protezione in quanto "beni"[43], un valore economico di cui servirsi. D'altra parte, pretendere che gli Stati Uniti cambino il proprio assetto normativo è utopico. L'approdo cui si è giunti a seguito dei nuovi negoziati – dunque la decisione di adeguatezza esaminata– è senz'altro una soluzione di compromesso. Il flusso di dati e lo scambio transfrontaliero di questi ultimi è fenomeno prorompente e incontenibile, cui occorre, perciò, dare regolazione.

decision on 10 July 2023, 18 luglio 2023.

[43] Ricostruzione che, peraltro, trova spazio anche nel nostro ordinamento giuridico. La dottrina sul punto è ampia. In particolare, sul dato personale quale controprestazione contrattuale: F. Agnino, *Fino a che punto è possibile disporre contrattualmente dei propri diritti? (Vedi contratto FB)*, in *Giurisprudenza di merito*, 2012, 2559 ss.; G. Giannone Codiglione, *I dati personali come corrispettivo della fruizione di un servizio di comunicazione elettronica e la "consumerizzazione della privacy",* in *Diritto dell'informazione e dell'informatica*, 2017; S. Thobani, *il mercato dei dati personali tra tutela dell' interessato e tutela dell' utente,* in questa *Rivista,* 3, 2019, 131 ss.; Id., *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018; G. D'Ippolito, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale,* in *Il diritto dell'informazione e dell' informatica,* 2020; A. Caravita di Toritto, *La proporzionalità multilivello in un mercato presidiato dai dati personali,* in questa *Rivista,* 3, 2021, 57 ss. In generale, sulla natura giuridica del dato S. Foà e M. Renna, *Dati e riservatezza ai tempi del predominio della tecnica. Una riflessione sulla natura giuridica dei dati,* relazione al II Tavolo di Generazioni Future, Roma, 2022, in *generazionifuture.org/video.*

Il DPF e la conseguente decisione di adeguatezza della Commissione UE tentano di rendere "adeguato" ciò che, di fatto, è inadeguato *ab origine,* poiché le "lacune" sono dovute alla legislazione degli Stati Uniti. Rispetto al passato è indubbio che la tutela concessa dagli Stati Uniti ai dati personali sia rafforzata, e anche di molto. Si tratta di un compromesso dal quale non può prescindersi posto che la regolazione dei flussi transfrontalieri deriva da una necessità oggettiva.

5. La regolazione della società digitale tra USA e UE

Lo sviluppo delle nuove tecnologie ha ridefinito profondamente il ruolo delle grandi piattaforme digitali che, più che attori economici in senso stretto, si configurano quali poteri privati in competizione tra loro e, talvolta, con il potere pubblico[44]. Non si tratta soltanto di potenze economiche: la loro natura è assai più pervasiva, arrivando a toccare persino i diritti fondamentali, la cui tutela rischia di essere compromessa[45]. Tutela che deve essere assicurata dall'apparato statale, spesso caratterizzato da un potere legislativo poco dinamico rispetto alle accelerazioni spasmodiche della tecnologia e che subisce, perciò, il cambiamento senza porvi adeguata regolazione.

In questo, la visione di Stati Uniti e Unione europea – come si accennava – è radicalmente differente: caratterizzata per un lato da apertura e liberalismo, per altro verso da resistenza e prevalenza per la protezione dei dati personali.

Gli USA, sin da subito, hanno mostrato un'ampia apertura verso i servizi della società dell'informazione, eliminando gli ostacoli che avrebbero potuto limitare la circolazione dei dati – e, conseguentemente, lo sviluppo del mercato elettronico – al punto da prevedere la totale deresponsabilizzazione degli *internet provider* per i contenuti caricati in rete da soggetti terzi[46]. Le prime dieci società nel mondo afferenti al comparto tecnologico sono statunitensi, di talché può facilmente comprendersi l'interesse degli Stati Uniti nel difendere la posizione di supremazia tecnologica. Se un tempo gli USA rappresentavano una potenza senza rivali in campo tecnologico, oggi debbono fare i conti con la concorrenza – sempre più incisiva – di Cina, Giappone e Taiwan. La Cina, peraltro, è antagonista ideologico, oltreché commerciale[47]. L'innovazione si realizza mediante lo sfruttamento dei dati. Ed è proprio sui dati – personali e non – che soggetti economici privati e Stati fondano le loro strategie. Emerge, allora, quella che per gli USA è la priorità: assumere e mantenere un ruolo di spicco non solo nel mercato,

[44] O. Pollicino, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quaderni costituzionali*, 3, 2023, 569 ss.

[45] *Ibidem.*

[46] *Communication Decency Act*, Title 476, Sec. 230, 1996 ove si prevedeva la completa deresponsabilizzazione degli internet provider, ripresa, poi, dal *Digital Millenium Copyright Act* del 1996. Per dottrina si veda, da ultimo, L. Fabiano, *Il liberal protezionismo digitale statunitense fra difesa della* leadership *nel mercato tecnologico e sicurezza nazionale,* in *DPCE online*, 2023, 233 ss.

[47] Sul punto si vedano O. Pollicino, *Di cosa parliamo quando parliamo di costituzionalismo digitale?,* in *Quaderni costituzionali,* cit. 570 ss., L. Fabiano, *Il liberal protezionismo digitale statunitense fra difesa della* leadership *nel mercato tecnologico e sicurezza nazionale,* cit., 233 ss. Per un ulteriore approfondimento sulla questione: E. Chiti-B. Marchetti, *Divergenti? Le strategie di Unione Europea e Stati Uniti in materia di intelligenza artificiale,* in *Regolazione e mercati,* 2, 2020, 29 ss.

ma anche dal punto di vista geopolitico, pure se occorre sacrificare la sicurezza dei privati cittadini (e non). L'approccio liberista degli Stati Uniti si fonda sull'interpretazione del I emendamento della Costituzione, caposaldo della libertà di espressione[48]. Il decisore politico, così come la giurisprudenza[49], vedono la libertà di espressione come strumento per lo sviluppo del mercato digitale che, a sua volta, rappresenta il mezzo di diffusione e esportazione della cultura americana nel mondo. Tuttavia, a fare da contraltare, è l'esigenza di proteggere la dignità umana, anche online, e la sicurezza nazionale. L'approccio nordamericano, come si è tentato di dimostrare, è più coerente con l'obiettivo di massimizzare il mercato tecnologico[50]. Nel bilanciamento tra gli interessi rappresentati, infatti, gli USA hanno optato per una maggior tutela delle piattaforme, viste quali "fori pubblici", e dunque ricomprese in un'interpretazione estensiva della disposizione di cui al I emendamento. Coerentemente con tale impostazione, quanto a idee e contenuti nelle piattaforme digitali[51] sorge in capo al potere pubblico l'esigenza di conformare la propria attività a neutralità.

L'Unione europea, d'altro canto, ha adottato un'impostazione radicalmente differente – come si è tentato di delineare nei precedenti paragrafi – poiché riconosce alla riservatezza e alla protezione dei dati personali la natura di diritti fondamentali della persona umana[52]. La *ratio* principale del GDPR è di contemperare le esigenze di circolazione – provenienti dal mercato – e quelle di protezione – afferenti alla sfera individuale. Sebbene il Regolamento, sin dai primi articoli, precisi che la circolazione dei dati – almeno nel territorio unionale – non possa subire limitazioni per motivi attinenti alla protezione dei dati medesimi, le esigenze di protezione cui si è fatto cenno, spesso, divengono ostacolo allo sviluppo del mercato digitale[53]. È forse questa la ragione che, da ultimo, ha spinto l'Unione a un cambio di prospettiva.

Il fenomeno attuale, che può definirsi *datification,* si compone di tre fattori: l'aumento esponenziale del flusso di dati prodotti nel mondo, la capacità di analisi ed estrazione di informazioni dai dati e, infine, la capacità di prendere decisioni fondate sulle informazioni estratte, anche attraverso algoritmi decisionali[54]. Perché un Paese possa oggi definirsi competitivo nel mercato e nello scenario globale occorre che sia in grado di

---

[48] Sul punto, per giurisprudenza *Reno v. American Civil Liberties Union,* 521 US 844 (1997). Per dottrina si veda R.H. Barrage, *Reno v. American Civil Liberties Union: First Amendment Free Speech Guarantee Extended to the internet,* in *Mercer Law Review,* 1998, 389 ss.

[49] *Miami Herald publishing v. Tornillo,* 418 US 241 (1974) e, di nuovo, *Reno v. American Civil Liberties Union,* cit.

[50] L. Fabiano, *Il liberal protezionismo digitale statunitense fra difesa della* leadership *nel mercato tecnologico e sicurezza nazionale,* cit., 233 ss.

[51] Cfr. *Packingham v. North Carolina*, 582 U.S. __ (2017) Per dottrina: M. Bassini, *Libertà di espressione e social network, tra nuovi spazi pubblici e poteri privati,* in *Rivista italiana di informatica e diritto*, 2, 2021, 43 ss. D. Scopelliti, *Poteri privati e responsabilità pubbliche dei social network al tempo della democrazia digitale*, in *Federalismi.it,* 2024.

[52] Come si evince dall'articolo 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea nonchè dall'articolo 16, par. 1, del Trattato sul Funzionamento dell'Unione europea (TFUE).

[53] Art. 1 GDPR. O. Pollicino, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in questa *Rivista*, 3, 2018, 138 ss.

[54] S. Calzolaio, *Introduzione. Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati,* in *Rivista italiana di informatica e diritto,* 1. 2021.

gestire l'insieme di tali fattori, spie del contesto *data driven* in cui la società si trova, ormai, inserita[55].

Quanto rappresentato evidenzia *ictu oculi* l'inadeguatezza del GDPR che, in ragione della celerità con cui la tecnologia si sviluppa, risulta obsoleto rispetto alla realtà attuale. Il flusso dei dati scorre e sfugge alle categorie del diritto, tanto che emergono dubbi circa i quesiti più basilari: si pensi, ad esempio, agli interrogativi relativi all'effettiva "appartenenza" dei dati[56]. L'impianto normativo europeo qualifica il dato personale quale diritto della persona umana e perciò appartenente al soggetto cui si riferisce. La realtà fattuale, d'altro canto, ne dimostra tutto il valore economico e l'appetibilità commerciale, al punto che è sempre più complesso "difendere" i propri dati[57]. La protezione richiede che sia il soggetto interessato ad attivarsi per richiedere tutela senza che costui sia, tuttavia, posto nelle condizioni di conoscere dove circolano, chi li detiene (o possiede?) e come li utilizza in modo costante e continuativo. Le persone fisiche, attraverso l'utilizzo dell'*Internet of things*, si rendono produttrici di dati e generano dei flussi di informazioni che si mescolano ad altri dati non personali o anonimi. Il risultato è un insieme complesso di reticoli che sfugge al controllo dell'interessato (*data subject*)[58]. Di talché, anche il consenso perde la sua efficacia[59]. Sui siti internet l'informativa è spesso contenuta in *policies* complesse e predisposte unilateralmente dal gestore, senza che vi sia la possibilità – per l'interessato – di negoziare il trattamento. Di frequente, i dati vengono trasmessi dal primo titolare ad altri operatori, e perciò si "perdono" e sfuggono al diretto controllo del *data subject*[60]. Le scelte di protezione operate dall'UE mirano, oltrechè, si ribadisce, alla tutela dei diritti fondamentali dei singoli[61], anche a difendere il proprio patrimonio informativo. Dunque, all'obiettivo del legislatore europeo di implementare l'economia *data driven* si lega la necessità di realizzare una

---

[55] D. Poletti, *Il controllo dell'interessato e la strategia europea sui dati,* in *Osservatorio sulle fonti,* 2, 2023,368. In generale, sullo Stato digitale, si veda L. Torchia, *Lo Stato digitale. Una introduzione,* Bologna, 2023.

[56] S. Calzolaio, *Introduzione. Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati,* cit.

[57] Sul ruolo attivo del soggetto interessato per veder garantita la tutela dei propri dati personali: F. Piraino, *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato,* in *Nuove leggi civ. comm.,* 2017, 2777 ss.; F. Calisai, *I diritti dell'interessato,* in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo,* Torino, 2019, 327 ss. In generale sul bilanciamento tra protezione dei dati personali, evoluzione della società digitale e scambi commerciali si vedano L. Califano, F. Galli, V. Fiorillo, *la protezione dei dati personali: natura, garanzie e bilanciamento di un diritto fondamentale,* Torino, 2023; L. Califano, *I diritti e le garanzie degli interessati nel Regolamento europeo 2016/679*, in *Cultura giuridica e diritto vivente,* 2022, 1 ss.; G. Finocchiaro, *Il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, in *Il trattamento dei dati personali in ambito giudiziario*, Roma, Scuola Superiore della Magistratura, 2021, 19 ss.

[58] D. Poletti, *Il controllo dell'interessato e la strategia europea sui dati,* cit., 368.

[59] *Ibidem.* Sulla base giuridica del consenso, vista quale controprestazione contrattuale si veda: C. Irti, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, 74 ss.; F. Bravo, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e impresa*, 2019, 34 ss. G. Resta, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva 2019/770 e il Regolamento 2016/679*, in *Annuario del contratto*, 2018, 127 ss.

[60] G. Resta, *I dati personali oggetto del contratto,* cit., 127 ss.

[61] Non a caso l'Unione europea ha adottato la Dichiarazione europea sui diritti e principi digitali, presentata dalla Commissione nel gennaio 2022. Per dottrina: P. De Pasquale, *Verso una carta dei diritti digitali (fondamentali) dell'Unione Europea?* in *Il diritto dell'Unione Europea,* 22, 1 ss.

governance capace di contrastare i modelli mercantili di Stati Uniti e Cina[62].
L'UE per disciplinare la tecnologia si avvale dello strumento regolamentare, scelta non casuale, che vuole infatti essere espressione di una sovranità politica condivisa in tutti i settori e, soprattutto, in quelli caratterizzanti la società digitale[63]. Se il modello statunitense lascia spazi liberi da interventi normativi, quello europeo, all'opposto, tende a regolare ogni elemento della società digitale (dati, piattaforme, intelligenza artificiale)[64]. Nondimeno, se la mole normativa risponde alla complessità della materia, da un lato, dall'altro evidenzia una discrasia della relativa regolazione: dall'analisi del paradigma europeo sembrerebbe emergere un'ipotesi di eterogenesi dei fini, dovuta alla necessità, avvertita in ambito unionale, di disciplinare il settore del digitale nell'ottica della competitività. Senonché le riscontrate criticità connesse ad una crescente complessità del fenomeno, corrono il rischio di restituire un *framework* di disciplina sfavorevole alla competizione tra gli ordinamenti.
Da altro angolo di visuale, l'Unione europea intende realizzare uno spazio comune di dati, che consenta di concretizzare un mercato unico, aperto ad accogliere dati provenienti da tutto il mondo, dati che possono essere, altresì, personali. Il mercato unico consentirà ai dati di circolare liberamente sul territorio europeo, a vantaggio di imprese, ricerca e amministrazioni pubbliche[65]. Questo l'obiettivo della strategia europea per i dati[66]. Il quadro regolatorio deve, pertanto, conciliare il riuso, la condivisione e la libera fruizione dei dati con i diritti fondamentali e la tutela dei consumatori nel mercato. Mercato che, s'intende, dovrebbe tendere alla protezione della persona fisica (o, almeno, la sua proiezione) quale produttrice della "materia" oggetto di scambio[67].
Diversi i regolamenti che si propongono di disciplinare la materia digitale, ognuno con il proprio ambito di azione. Il rischio è di incorrere in una sovrabbondanza normativa, come è stato peraltro evidenziato tanto dall'EDPB, quanto dall'*European Data Protection Supervisor* (EDPS)[68]*,* nell'ambito della proposta del *Data Governance Act* (DGA)*[69]*. Il ti-

[62] In generale, sul modello cinese, anche rispetto al trasferimento di dati si veda Y. Li, *Cross Border Data Transfer Regulation in China*, in *Rivista italiana di informatica e diritto,* 2021, 67 ss.

[63] D. Poletti, *Il controllo dell'interessato e la strategia europea sui dati,* cit., 368 ss.

[64] A. Iannuzzi, *Le fonti del diritto per la disciplina della società digitale*, in F. Pizzetti (dir.), *La regolazione europea della società digitale,* Torino, 2023, 19 ss. L'A. definisce il fenomeno quale "rischio di un'ipertrofia legislativa in tema di regolazione dati, che si porrebbe esattamente all'opposto al modello statunitense maggiormente teso a lasciare ampi spazi liberi da interventi normativi".

[65] In generale, sul mercato unico digitale: F. Rossi dal Pozzo, *Il mercato unico digitale europeo e il regolamento Ue sulla privacy,* in R. Cavallo Perin-D.U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020, 43 ss. e Id. *Qualche considerazione d'insieme sul mercato unico dei dati e la loro tutela nell'Unione europea,* in *Eurojus,* 2020, 7; B. Nascimbene, *Il Mercato Unico Digitale quale nuova frontiera dell'integrazione europea considerazioni introduttive,* in *Eurojus,* 2020, 11 ss.; A. Sajia, *Protezione dei dati personali, tutela del consumatore e concorrenza: un rapporto in evoluzione*, in *Eurojus*, 2020, 103 ss.

[66] Strategia annunciata dalla commissione il 19 febbraio 2020 e che si fonda oggi sul c.d. "pacchetto digitale", che comprende i seguenti regolamenti: regolamento (UE), 30 maggio 2022, n. 868; regolamento (UE), 19 ottobre 2022, n. 2065; regolamento (UE), 13 dicembre 2023, n. 2854.

[67] D. Poletti, *Il controllo dell'interessato e la strategia europea sui dati,* cit., 368 ss.

[68] EDPB-EDPS Opinion 3/2021 on the proposal for a regulation of the European Parliament and of the
Council on European data governance (Data Governance Act)

[69] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on

more degli organi consultivi è che si manifestino antinomie tra le diverse discipline[70]. Il DGA, infatti, mira a regolamentare il riutilizzo dei dati pubblici e protetti, potenziandone la condivisione anche attraverso la regolamentazione dei c.d. "intermediari di dati", cui è attribuito – tra gli altri – il compito di supportare gli interessati nell'esercizio dei loro diritti in relazione ai dati personali. Di contro, il Garante europeo per la protezione dei dati ha affermato, invece, la complementarietà tra le informazioni che le piattaforme digitali sono chiamate a fornire sulla base *Digital Service Act* (DSA)[71] e l'informativa resa ai soggetti interessati dal Titolare del Trattamento[72]. Il DSA disciplina i servizi digitali ed è stato approvato dal Parlamento europeo congiuntamente al *Digital Markets Act.* Il provvedimento promuove il corretto funzionamento del mercato digitale interno per creare un ambiente sicuro, affidabile e che tuteli, in concreto, i diritti dei singoli. È a questo proposito che il DSA velocizza le procedure per la rimozione dei contenuti illegali e di migliora il controllo pubblico sulle piattaforme online. Pioniere dell'innovazione digitale è, tuttavia, il *Data Act*[73]*,* ultimo tassello della strategia europea, che si propone di disciplinare l'accesso ai dati ed il loro utilizzo, con l'obiettivo di concedere un potere maggiore a imprese e consumatori.

Nonostante i regolamenti citati ribadiscano l'intangibilità della disciplina del GDPR, pare che al modello di *data protection* l'Unione europea abbia, ormai, affiancato una politica di *data sharing*. Il contrasto tra controllo e condivisione non è, tuttavia, di agevole soluzione, anche a voler considerare che l'armonizzazione raggiunta per mezzo dello strumento regolamentare potrebbe subire, ancorché *in melius*, differenziazioni in virtù del "margine di manovra" riconosciuto agli Stati Membri al momento della relativa attuazione.

European data governance and amending Regulation (EU) 2018/1724. Per dottrina: D. Poletti, *Il controllo dell'interessato e la strategia europea sui dati,* cit., 368 ss.; O. Pollicino, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, cit., 570 ss.

[70] A. Iannuzzi, *Le fonti del diritto per la disciplina della società digitale*, in *La regolazione europea della società digitale,* cit., 19.

[71] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

[72] Il contenuto dell'informativa è disciplinato dagli artt. 13 e 14 GDPR.

[73] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).