SULLE RECENTI EVOLUZIONI NORMATIVE E GIURISPRUDENZIALI EUROPEE IN MATERIA DI DATI PERSONALI

Alessandro Tomaselli

Docente a contratto di diritto dell'Unione Europea presso l'Università degli studi di Catania

Abstract: the recent provisions adopted by the European Union regarding the protection of personal data, although on the one hand, provide for greater guarantees in favor of the citizen, on the other hand seem to actually constitute instruments aimed at protecting the data market of the European citizen: both the Adequacy Decision on the US-EU Framework that the judgment of the General Court of the EU on data anonymization and pseudonymization that the Regulation 868 2022 (Data Governance Act) seem directed in the opposite direction to the GDPR by transforming personal data into common goods to be shared and to be profited from rather than unconditionally protected.

Key words: personal data, GDPR, European Union, Charter of Fundamental Rights of the European Union

1. La Decisione di adeguatezza della Commissione Europea sul Quadro UE-USA per la protezione dei dati personali

Il 10 luglio di quest'anno la Commissione europea ha adottato la Decisione di adeguatezza sul Quadro UE-USA[1] per la protezione dei dati personali trasferiti dall'UE alle

[1] Consultabile su *Adequacy decision for the EU-US Data Privacy Framework* | Commissione europea (europa.eu). È da specificare che il requisito dell'adeguatezza fu introdotto dalla Direttiva CE 95/46 come meccanismo per permettere il trasferimento di dati personali verso Paesi extra UE che forniscono un livello adeguato di protezione. Il criterio è stato ripreso dal Regolamento 2016/679 che abroga la suddetta Direttiva. Tuttavia, a seguito soprattutto delle rivelazioni di *Edward Snowden* circa la sorveglianza di massa attuata dagli Stati Uniti, la Corte di Giustizia dell'Unione Europea nella sentenza *Schrems I* ha interpretato il requisito di adeguatezza in modo maggiormente rigoroso sostenendo che "la nozione di 'livello di protezione adeguato' deve essere intesa nel senso che essa

imprese statunitensi, nel rispetto, precipuamente, dell'art. 45, pp. 1 e 3 del GDPR (Regolamento (UE) 2016/679) che conferisce all'esecutivo di Bruxelles il potere di decidere, mediante un atto di esecuzione, che un Paese extra UE garantisca un livello di protezione dei dati personali sostanzialmente equivalente a quello riconosciuto all'interno dei confini europei[2].

In particolare, tale Decisione sancisce che gli Stati Uniti d'America assicurano, almeno in astratto, un livello adeguato di protezione per i dati personali dei cittadini europei trasferiti dall'UE alle imprese statunitensi che partecipano al suddetto Quadro, al riguardo prevedendo limitazioni nell'accesso da parte dell'intelligence statunitense solo a quanto necessario e proporzionato in materia penale e per proteggere la sicurezza nazionale, nonché l'istituzione di un meccanismo di ricorso indipendente e imparziale, compendiato da un Tribunale di Revisione della Protezione dei Dati (*Data Protection Review Court - DPRC*) a cui ci si potrà rivolgere nel caso di violazione delle disposizioni previste dal provvedimento in questione.

Le imprese d'oltreoceano potranno (non dovranno, si noti) aderire al Quadro UE-USA sulla privacy dei dati impegnandosi a rispettare una serie dettagliata di obblighi, come, ad esempio, la cancellazione dei dati personali qualora non più necessari per lo scopo per il quale

---

richiede che il Paese terzo assicura, effettivamente, in forza del suo diritto interno o dei suoi impegni internazionali, un livello di tutela dei diritti e delle libertà fondamentali 'sostanzialmente equivalente' a quello garantito all'interno dell'UE in forza della direttiva 95/46, letta alla luce della Carta di Nizza": Causa C-362/14 *Maximillian Schrems c Data Protection Commissioner* ECLI:EU:C:2015:650 (di seguito *Schrems I*) par. 73. L'interpretazione restrittiva è stata confermata in *Schrems II* – v. oltre.

[2] "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. 3. La Commissione, previa valutazione dell'adeguatezza del livello di protezione, può decidere, mediante atti di esecuzione, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo. L'atto di esecuzione prevede un meccanismo di riesame periodico, almeno ogni quattro anni, che tenga conto di tutti gli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale. L'atto di esecuzione specifica il proprio ambito di applicazione geografico e settoriale e, ove applicabile, identifica la o le autorità di controllo di cui al paragrafo 2, lettera b), del presente articolo. L'atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 93, paragrafo 2". Inoltre, sembra il caso di specificare che in mancanza di una decisione di adeguatezza siffatta, un trasferimento del genere può essere effettuato solo se l'esportatore dei dati personali, stabilito nell'Unione Europea, prevede garanzie adeguate, le quali possono risultare, in particolare, da clausole tipo di protezione dei dati adottate dalla Commissione, e se gli interessati dispongono di diritti azionabili e di mezzi di ricorso effettivi (art.46, paragrafo 1 e paragrafo 2, lettera c, del GDPR). Il GDPR stabilisce precisamente, inoltre, a quali condizioni può avvenire un trasferimento dati in mancanza di una decisione di adeguatezza o di garanzie adeguate (art. 49 del GDPR).

sono stati raccolti e la garanzia della continuità della protezione nell'ipotesi di dati personali condivisi con terzi.

Inoltre, è da rimarcare che l'adesione al nuovo *Framework* si basa su un meccanismo di autocertificazione gestito dal *Department of Commerce* americano e attraverso il quale le imprese statunitensi richiedenti si impegnano al rispetto dei principi fondanti la materia della protezione dei dati personali in ambito europeo; conseguentemente, azione propedeutica al trasferimento di dati personali di un cittadino UE verso gli Stati Uniti dovrà necessariamente essere rappresentata dalla verifica relativa alla presenza del destinatario tra le *certified organizations* inserite all'interno del corrispondente elenco (c.d. "*Data Privacy Framework List*")[3].

Certamente, *g*li oneri previsti dal provvedimento in esame a carico degli Stati Uniti faciliteranno in generale i flussi di dati transatlantici, poiché si applicheranno anche quando i dati verranno trasferiti utilizzando altri strumenti, come le clausole contrattuali standard[4] e le regole aziendali vincolanti; oltretutto, ad ulteriore garanzia della privacy dei cittadini europei, è sancito come l'effettivo funzionamento del quadro UE-USA per la protezione dei dati sarà soggetto a revisioni periodiche da parte della Commissione Europea, in collaborazione con i rappresentanti delle competenti autorità europee e statunitensi.

Il provvedimento in esame ha rappresentato l'esito di una serie di colloqui e trattative intervenuti tra l'amministrazione nord-americana guidata da *Joe Biden* e i rappresentanti dell'Unione Europea a far data dall'agosto 2020[5] in seguito alla sentenza *Schrems II*

[3] Considerate le conseguenze e gli oneri che derivano dall'inclusione nel *Framework* (*e.g.*, soggezione ai poteri della *Federal Trade Commission* del *Department of Transportation*, etc.), risulterà certamente probabile, tuttavia, che alcuni trasferimenti di dati personali verso gli Stati Uniti possano non rientrare nell'ambito di applicazione della Decisione, in ragione, ad esempio, della mancata adesione da parte di determinate aziende americane. Sulla base volontaria dell'adesione in questione e sulle possibili conseguenze in termini di depotenziamento, in concreto, delle tutele previste dal Quadro in oggetto a favore dei cittadini europei, si rimanda al punto 4.

[4] V. nota 5.

[5] Nel marzo 2022, la presidente della Commissione europea *Von der Leyen* e il presidente USA *Biden* hanno annunciato di aver raggiunto un accordo di principio su un nuovo quadro per i flussi di dati transatlantici, a seguito dei negoziati tra il commissario Reynders e il segretario al commercio degli Stati Uniti Raimondo. Nell'ottobre 2022, il presidente *Biden* ha firmato un ordine esecutivo sul rafforzamento delle salvaguardie statunitensi per le attività di intelligence dei segnali statunitensi, che è stato integrato dalle regole adottate dal procuratore generale degli Stati Uniti Garland. Insieme, questi due strumenti hanno consentito l'attuazione degli impegni assunti dagli Stati Uniti nel quadro dell'accordo di principio nel diritto statunitense e hanno integrato gli obblighi delle imprese statunitensi nell'ambito del quadro UE-USA in materia di protezione dei dati.

pronunciata dalla Corte di Giustizia dell'Unione Europea (di seguito, anche CGUE) il 16 luglio dello stesso anno[6] e che sancisce l'invalidità, in nome dell'inadeguatezza della legislazione americana nella tutela dei dati personali dei cittadini europei trasferiti ad aziende operanti sotto la sua egida, della precedente Decisione 2016/1250 della Commissione europea sull'adeguatezza della protezione offerta dal regime dello Scudo UE-USA per la privacy (*Privacy Shield*).

Segnatamente, tale pronuncia statuisce l'incompatibilità di tale Scudo con l'art. 45 GDPR, letto alla luce degli art. 7, 8 e 47 della Carta dei Diritti Fondamentali dell'Unione Europea (di seguito, anche Carta di Nizza) e si articola in due profili: 1) il mancato rispetto del principio di proporzionalità *ex* art. 52 di tale ultimo documento richiamato, in quanto i programmi di intelligence statunitensi permettevano una sorveglianza governativa ingiustificatamente ampia, ritenuta, dunque, dalla Corte di Giustizia UE causa di violazione dei diritti fondamentali di cui agli art. 7 e 8 della Carta di Nizza in quanto non necessaria né proporzionata rispetto alle esigenze di sicurezza nazionale; 2) la violazione dell'art. 47 della Carta medesima poiché, in relazione a tale sorveglianza statunitense, gli interessati europei non disponevano del diritto a un ricorso effettivo dinnanzi a un giudice indipendente e imparziale.

Il Quadro testé accennato, dunque, sembra introdurre nuove garanzie vincolanti per rispondere a tutte le preoccupazioni sollevate dalla CGUE in occasione della sentenza *Schrems II*, così ponendosi, almeno in astratto, alla stregua di rinnovato baluardo ad effettiva protezione della privacy del cittadino europeo, financo in forza di un'originale (quanto controversa – v. oltre) applicazione extraterritoriale del GDPR: la Corte, infatti, rimarca che il diritto dell'Unione (e segnatamente il GDPR, appunto) si applica ad un trasferimento di dati personali effettuato a fini commerciali da un operatore economico stabilito in uno Stato membro verso un operatore economico stabilito in un Paese terzo anche se, durante o dopo detto trasferimento, tali dati possono essere soggetti a trattamento a fini di sicurezza pubblica, di difesa e di sicurezza dello Stato ad opera delle autorità del Paese terzo considerato.

[6] Causa C-311/18 *Data Protection Commissioner c Facebook Ireland Limited e Maximillian Schrems*. Si ricorda che in tale occasione la CGUE ha comunque giudicato valida la Decisione n. 2010/87 relativa alle Clausole Contrattuali Tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi.

2. La sentenza del Tribunale dell'Unione Europea T-557-20 sull'anonimizzazione e pseudonimizzazione dei dati

Il concetto di identificabilità dell'interessato, da intendersi come "qualsiasi informazione riguardante una persona fisica identificata o identificabile" (art. 4, n.1 del GDPR e art. 3 del Regolamento (UE) 2018/1725[7]), è determinante ai fini dell'applicabilità o meno della disciplina sulla protezione dei dati personali.

La disciplina precisa, inoltre, che "si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente" ed in relazione a tale concetto vengono in rilievo due ulteriori temi di primario rilievo, e cioè l'anonimizzazione e la pseudonimizzazione dei dati.

Dal primo punto di vista, i dati potranno considerarsi anonimi soltanto qualora non sia possibile re-identificare l'interessato in maniera irreversibile; in tal caso, questi non saranno più qualificabili come dati personali e, pertanto, risulteranno sottratti alla disciplina dettata dal GDPR[8].

Al contrario, la pseudonimizzazione, pur essendo riconosciuta come una misura utile a garantire la sicurezza nel trattamento dei dati personali e che i relativi titolari dovrebbero adottare in ossequio agli obblighi derivanti dall'art. 32 GDPR, non fa venir meno la natura di dato personale, né preclude, dunque, l'applicazione della relativa disciplina: ai sensi dell'art. 4, n. 5 del GDPR, infatti, si ha pseudonimizzazione laddove il trattamento sia effettuato in modo tale che "i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive", e che tali informazioni aggiuntive siano soggette a specifiche misure tecniche volte a garantire che tali dati non possano essere attribuiti a una persona fisica identificata o identificabile.

[7] Consultabile su L_2018295IT.01003901.xml (europa.eu).

[8] Al riguardo è da specificare che l'efficacia delle tecniche di anonimizzazione, intesa come la possibilità di garantire che l'irreversibilità del processo di identificazione o re-identificazione sia effettiva, è da sempre al centro di un ampio dibattito, legato al crescente rischio di obsolescenza delle tecniche utilizzate a fronte dell'incessante evoluzione tecnologica.

A ciò si aggiunga che il Considerando n. 26 del GDPR, nell'affermare in via generale che i dati personali pseudonimizzati dovrebbero essere considerati dati personali, precisa che per accertare l'identificabilità di una persona a partire dal dato, è opportuno considerare anche tutti i mezzi che sono ragionevolmente utilizzabili dal titolare del trattamento per re-identificare l'interessato a partire da un dato non direttamente identificativo (lasciando così spazio ad un inevitabile e piuttosto rilevante margine d'incertezza nell'interpretazione all'interno di tale contesto – v. oltre).

In materia, lo scorso 26 aprile il Tribunale dell'Unione europea ha pronunciato una controversa sentenza relativamente alla causa T-557/20, Comitato di Risoluzione Unico (*Single Resolution Board - SRB)* contro Garante Europeo per la Protezione dei Dati (*European Data Protection Supervisor - EDPS)*[9].

Nell'ambito di una procedura di risoluzione, di cui al Regolamento (UE) 806/2014[10], cui è stato sottoposto il *Banco Popular Espanol*, con relativa vendita dell'attività di impresa, il *Single Resolution Board* , al fine di definire la necessità di riconoscere in capo agli azionisti un indennizzo, ha invitato questi a manifestare il loro interesse ad esercitare il diritto di essere ascoltati ai sensi dell'articolo 41, paragrafo 2, lettera a), della Carta dei Diritti Fondamentali dell'Unione Europea e che al riguardo prevede un procedimento composto da due fasi: la prima di iscrizione e la seconda di consultazione. In tale seconda fase, gli azionisti e i creditori interessati hanno presentato osservazioni sulla decisione preliminare, nonché sulla versione non riservata della "valutazione 3".

In tale contesto, il *SRB* ha chiesto a una società terza (la *Deloitte*, nota azienda di revisione e consulenza finanziaria), nella sua qualità di valutatore indipendente, "*di valutare le osservazioni pertinenti relative alla valutazione 3, di fornirgli un documento contenente la sua valutazione e di esaminare se la valutazione 3 restasse valida alla luce di tali osservazioni*"; di conseguenza, il *SRB* ha trasmesso a *Deloitte* le osservazioni ricevute nella fase di consultazione

[9] Consultabile su EUR-Lex - 62020TJ0557 - EN - EUR-Lex (europa.eu).

[10] Provvedimento normativo che fissa norme e una procedura uniformi per la risoluzione degli enti creditizi e di talune imprese di investimento nel quadro del meccanismo di risoluzione unico e del Fondo di risoluzione unico e che modifica il regolamento (UE) n. 1093/2010 e che al riguardo, tra l'altro, istituisce ai sensi del proprio art. 42 il richiamato Comitato di Risoluzione Unico.

recanti un codice alfanumerico tramite il quale solo lo stesso Comitato avrebbe potuto collegare le osservazioni ai dati ricevuti durante la fase di iscrizione.

A seguito di una serie di reclami, il Garante Europeo della Protezione dei Dati ha contestato al *SRB* la violazione dell'art. 15 del Regolamento 2018/1725[11] per mancata informazione a favore dei reclamanti in merito alla possibilità del trasferimento di questi ultimi a *Deloitte*, nella convinzione che i dati trasferiti non andassero considerati personali, vista l'impossibilità per il destinatario di risalire all'identità dei corrispondenti soggetti interessati.

In particolare, a parere del suddetto Garante le osservazioni e il codice alfanumerico trasmessi ai terzi andrebbero, in realtà, considerarsi alla stregua di dati pseudonimi, e dunque come dati personali, sulla base della considerazione che gli azionisti che avevano espresso le osservazioni potevano essere identificati utilizzando i dati ulteriori in possesso del *SRB*.

Nel sostenere la propria tesi, l'EDPS ha sottolineato che:

[11] "1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni: a) l'identità e i dati di contatto del titolare del trattamento; b) i dati di contatto del responsabile della protezione dei dati; c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; d) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; e) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 48, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili. 2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente: a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o, ove applicabile, del diritto di opporsi al trattamento o del diritto alla portabilità dei dati; c) qualora il trattamento sia basato sull'articolo 5, paragrafo 1, lettera d), oppure sull'articolo 10, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; d) il diritto di proporre reclamo al Garante europeo della protezione dei dati; e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati; f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 24, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. 3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2. 4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni".

- l'art. 3, n. 1 del Regolamento (UE) 2018/1725 (in maniera simile a quanto fatto dal GDPR) nel definire i dati personali fa riferimento anche alla possibilità di identificare una persona fisica "indirettamente", non dovendo dunque tenersi conto del fatto che la singola informazione sia o meno idonea a identificare l'interessato;
- ai fini dell'identificazione, occorre fare riferimento sia ai mezzi ragionevolmente utilizzabili dal titolare, che da qualsiasi altro soggetto, non avendo alcuna rilevanza la circostanza che le informazioni ulteriori siano in possesso di una o più persone;
- il codice alfanumerico, secondo quanto previsto dall'art. 3, n. 6 del Regolamento (UE) 2018/1725 in relazione alla pseudonimizzazione, anche in assenza di dati ulteriori, poteva essere qualificato come "informazione aggiuntiva", che consentiva di ricondurre le osservazioni agli interessati.

Nel formulare la propria decisione, il Tribunale UE ha in primo luogo fatto riferimento ai principi espressi dalla Corte di Giustizia dell'Unione Europea ("CGUE") nella sentenza Breyer (C-582/14), riguardo l'ipotesi in cui non tutte le informazioni idonee a consentire l'identificazione sono detenute da una sola persona, bensì da più parti.

Nella sentenza appena citata, infatti, la CGUE aveva stabilito che la semplice disponibilità da parte di più soggetti di informazioni aggiuntive che consentono l'identificazione dell'interessato non sia sufficiente ad escludere la possibilità di re-identificazione.

A parere del Tribunale, tuttavia, tale ultima evenienza non comporta necessariamente la qualifica dei dati come personali, dovendo comunque tenere conto della possibilità che tale identificazione avvenga in concreto, alla luce delle circostanze del caso di specie.

Applicando questo principio al caso in esame, il Tribunale è giunto alla conclusione che, dal momento che il terzo destinatario non disponeva, né avrebbe potuto in alcun modo avere accesso alle informazioni aggiuntive idonee ad identificare gli interessati, i dati trasmessi (ossia, le osservazioni e i codici alfanumerici) dovessero essere qualificati come dati anonimi, e non come dati pseudonimi.

In altre parole, a parere del Tribunale, la valutazione in merito alla concreta identificabilità dell'interessato andrebbe effettuata tenendo conto della posizione in concreto ricoperta dal terzo, dunque in tal senso prescindendo dal richiamo a criteri di natura astrattamente assoluti.

3. Il Regolamento (UE) 868 del 2022 (*Data Governance Act*)

Il 24 settembre 2023, a seguito di un periodo di tolleranza di 15 mesi, troverà applicazione all'interno del territorio europeo il Regolamento (UE) 2022/868 del 30 maggio 2022 (*Data Governance Act - DGA*)[12] che modifica il Regolamento (UE) 2018/1724 e che, in materia di protezione dei dati personali, integra quanto già previsto a livello europeo aggiungendosi al GDPR, alla Direttiva 2002/58/CE (Direttiva e-Privacy), al Regolamento (UE) 2018/1807 in materia di libera circolazione dei dati non personali all'interno dell'Unione Europea, nonché alla Direttiva 2019/1024/UE (Direttiva *open data*) relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.

Il *DGA*, in forza della considerazione dei dati personali alla stregua di autentico patrimonio da mettere a servizio di un bene o obiettivo comune ed espressamente ispirato allo scopo di "creare fiducia tra gli individui e le imprese per quanto riguarda l'accesso ai dati, la loro condivisione e il loro controllo, utilizzo e riutilizzo, in particolare stabilendo adeguati meccanismi per gli interessati affinché conoscano ed esercitino fattivamente i propri diritti" (considerando n. 5), prevede l'istituzione di un punto unico di accesso europeo, che farà capo alla Commissione UE e da cui accedere ad un registro elettronico a disposizione degli sportelli unici nazionali; inoltre, similmente al suddetto Quadro USA-UE, è introdotto un sistema di certificazione volontaria basato su un logo e un codice QR a favore dei fornitori dei servizi di intermediazione dei dati che decideranno di accedervi.

[12] Pubblicato in GUUE del 3.6.2022, L 152/1 e destinato, a sua volta, ad essere integrato dal Data Act (proposta di Regolamento del 23 febbraio 2022) che detta regole armonizzate per il corretto accesso e uso dei dati - sia personali sia non personali - generati dall'uso dei prodotti connessi e dei servizi correlati, al fine di garantire un'equità dei contratti di condivisione dei dati, con tutto ciò che ne deriverà in termini di coordinamento e complementarietà. Sembra il caso di precisare fin d'ora come tale provvedimento normativo si inserisca all'interno della più generale Strategia Europea sui Dati avviata dalle Istituzioni europee per il periodo 2019-2024 al fine specifico di "creare uno spazio unico europeo di dati – un autentico mercato unico di dati, aperto ai dati provenienti da tutto il mondo – nel quale sia i dati personali sia quelli non personali, compresi i dati commerciali sensibili, siano sicuri e le imprese abbiano facilmente accesso a una quantità pressoché infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore, riducendo nel contempo al minimo la nostra impronta di carbonio e ambientale". Così Commissione Europea, Una strategia europea per i dati, Bruxelles, 19 febbraio 2020, COM (2020) 66 final, p. 5. In tema, v., tra gli altri, POLETTI, *Gli intermediari dei dati*, in European Journal of Privacy Law & Technologies, 1, 2022, p. 48; TRANQUILLI, *Il nuovo citoyen européen nell'epoca del Data Governance Act,* in Rivista di Digital Politics, 1-2, 2022, p. 183 ss..

Più specificamente, il Regolamento *de quo*, ulteriore essenziale tassello nel cammino di progressivo rafforzamento della c.d. economia dei dati, si sviluppa lungo quattro linee direttrici: 1. il riutilizzo di determinati dati detenuti da soggetti pubblici (Capo II), 2. l'attività di intermediazione dei dati (Capo III), 3. la messa a disposizione dei dati per fini altruistici (Capo IV), 4. l'istituzione di un nuovo sistema di governance dei dati e di sanzioni (Capo V e Capo VI).

1. Dal primo punto di vista, è da dire che il *DGA* non introduce un obbligo generalizzato di riutilizzo dei dati, ma solo una facoltà: ogni soggetto pubblico sarà infatti libero di decidere se consentire o meno l'accesso a determinati dati al fine del loro riutilizzo. E solo in caso di valutazione positiva, l'accesso dovrà avvenire nel rispetto delle specifiche condizioni di cui all'articolo 5: ad esempio, se si tratta di dati personali, questi dovranno essere resi in forma anonima; se invece l'accesso ha ad oggetto informazioni commerciali riservate (compresi i segreti commerciali o i contenuti protetti da diritti di proprietà intellettuale), queste andranno modificate, aggregate o trattate per salvaguardarne la confidenzialità.

2. Con riguardo all'attività di intermediazione dei dati, definita dall'articolo 2, n. 11 come "un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali a fini di condivisione dei dati tra un numero indeterminato di interessati e di titolari di dati, da un lato, e gli utenti dei dati dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali", viene delineato un nuovo modello di impiego dei dati che separa la fase di fornitura dalla fase di utilizzo, interponendo tra le due il servizio di intermediazione. E sulla base delle definizioni all'uopo rinvenibili all'interno del GDPR (le persone fisiche alle quali i dati si riferiscono come soggetti interessati, il titolare dei dati coincidente con la persona giuridica, comprese le pubbliche amministrazioni, o con la persona fisica diversa dall'interessato che ha il diritto di concedere l'accesso a determinati dati o di condividerli, gli utenti di dati come coloro (persone fisiche o giuridiche) che hanno l'accesso legittimo a determinati dati e che hanno diritto, ai sensi del GDPR, di utilizzarli per fini commerciali o non commerciali) l'articolo 10 al riguardo specifica tre tipologie di servizi di intermediazione: a) la prima finalizzata a mettere in contatto titolari e utenti dei dati, al fine di instaurare rapporti commerciali aventi ad oggetto lo scambio dei dati. In tal caso, l'azione dell'intermediario è facilitata grazie la creazione di piattaforme o banche dati che consentono

anche l'utilizzo congiunto dei dati, oppure attraverso l'istituzione di una infrastruttura specifica per l'interconnessione di titolari dei dati con gli utenti dei dati[13]; b) la seconda intesa a mettere in contatto gli interessati a rendere accessibili i propri dati (personali e non) con potenziali utenti di dati, agevolando l'esercizio dei diritti riconosciuti dal GDPR. In ipotesi del genere, l'attività dell'intermediario sarà volta a rafforzare la posizione dell'interessato, assicurandogli un maggior controllo dei dati che lo riguardano, in sostanza dunque assistendo quest'ultimo nell'esercizio dei diritti a norma del GDPR, quali, ad esempio, la concessione o la revoca del consenso al trattamento dei dati, la rettifica dei dati personali inesatti, la cancellazione, il diritto all'oblio o alla portabilità. Dall'altro lato, l'intermediario è gravato dall'onere di assicurare che l'utente tratti i dati dell'interessato con la dovuta diligenza, vigilando in merito ad un eventuale utilizzo diffferente o addirittura illecito[14]; c) un'ulteriore tipologia di servizio di intermediazione comprende, infine, i servizi di cooperative di dati con l'obiettivo di rendere informato l'interessato (o qualsiasi membro del gruppo) riguardo ai suoi diritti in relazione a determinati dati, in particolare per quanto riguarda i dati personali o altri dati che godono di una specifica tutela[15].

3. In riferimento alla circolazione dei dati per fini altruistici, è intanto da specificare che tale attività riguarda dati personali messi a disposizione dagli interessati su base volontaria (e comunque previo il rilascio del consenso al trattamento) oppure di dati non personali messi a

[13] L'utilizzo di questi sistemi è auspicato dal DGA in quanto funzionale ad un risparmio dei costi di transazione.

[14] Al fine di ottimizzare la protezione dei dati, all'interno del Regolamento in questione viene espressamente auspicata, ad opera del soggetto intermediario, la creazione di uno spazio dove possa essere svolto il trattamento, in modo da evitare che i dati personali siano trasmessi a terzi. Tali spazi di dati personali potrebbero contenere il nome, l'indirizzo, la data di nascita dell'interessato, nonché dati generati dall'utilizzo di un servizio on line o da un oggetto connesso all'internet of things. Potrebbero essere utilizzati anche per conservare informazioni verificate sull'identità dell'interessato, quali numeri di passaporto o conti bancari (considerando 30).

[15] Anche in questo caso il servizio di intermediazione ha l'obiettivo di assistere l'interessato nell'effettuare una scelta consapevole sull'utilizzo dei propri dati. L'intermediario potrebbe essere utile anche per trovare soluzioni comuni sulle modalità di utilizzo, laddove vi siano posizioni contrastanti all'interno di uno stesso gruppo. Il controllo sull'attività degli intermediari è esercitato tramite un sistema di notifica obbligatoria all'autorità nazionale competente (articolo 11) e una serie di obblighi e requisiti posti in capo agli intermediari volti a scongiurare un uso improprio dei dati (articolo 12). In particolare, l'intermediario deve: assicurare che la procedura di accesso al servizio sia equa, trasparente e non discriminatoria (anche per quanto riguarda i prezzi e le condizioni di servizio); garantire un adeguato livello di sicurezza per la conservazione dei dati e per prevenire pratiche fraudolente o abusive da parte dei soggetti che richiedono l'accesso; agevolare lo scambio dei dati nel formato in cui li riceve e convertirli in formati specifici solo allo scopo di migliorarne l'interoperabilità, intrasettoriale e intersettoriale. Il DGA delinea una figura di intermediario neutrale rispetto ai soggetti coinvolti nello scambio che deve svolgere il ruolo di facilitatore della condivisione dei dati.

disposizione dai titolari degli stessi. I dati così messi a disposizione dovranno essere utilizzati esclusivamente per scopi di interesse generale (tutela della sanità pubblica, il miglioramento della mobilità e della fornitura dei servizi pubblici, la lotta al cambiamento climatico, il sostegno alla ricerca scientifica) e, a tal fine, è rimessa agli Stati l'adozione di politiche nazionali per incentivare la raccolta dei dati da utilizzare per fini altruistici. Al riguardo, l'articolo 18 delinea poi le condizioni necessarie per aumentare la fiducia degli interessati nel mettere a disposizione i loro dati: conseguentemente, i soggetti che gestiranno i dati per fini altruistici dovranno dimostrare di possedere specifici requisiti a garanzia della loro indipendenza in armonia con quanto a proposito previsto dagli artt. 19 e 20.

4. Con riguardo alle sanzioni, gli Stati membri dovranno adottare misure necessarie a garantire l'applicazione delle disposizioni del Regolamento, compresa la definizione di norme sanzionatorie nel caso di violazione (articolo 34). Le sanzioni devono essere effettive, proporzionate e dissuasive e, poiché eventuali differenze tra regimi sanzionatori rischiano di generare distorsioni della concorrenza all'interno del mercato unico digitale, gli Stati membri nell'adottare le norme sanzionatorie dovranno tener contro delle raccomandazioni del European Data Innovation Board.

Infine, affinchè lo scambio dei dati avvenga nel rispetto della normativa, il *DGA* prevede l'istituzione di un'autorità competente per i servizi di intermediazione dei dati (articolo 13) e un'autorità competente per la registrazione delle organizzazioni per l'altruismo dei dati (articolo 23); le due funzioni potranno essere svolte anche dalla stessa autorità, purchè distinta e indipendente da qualsiasi fornitore di servizi di intermediazione o organizzazione per l'altruismo dei dati ed entro il 24 settembre 2023 ogni Stato membro UE dovrà comunicarne alla Commissione Europea l'identità. Su tali soggetti graveranno compiti relativi alla procedura di notifica dei soggetti che intendono offrire servizi di scambio di dati, bilaterali o multilaterali ed alla corrispondente comunicazione alla Commissione Europea, al monitoraggio e controllo del rispetto da parte dell'intermediario delle condizioni per la fornitura dei servizi, nonché all'irrogazione di sanzioni pecuniarie o perfino di cessazione della fornitura del servizio in caso di loro violazione.

4. Riflessioni conclusive

Il quadro testè sommariamente delineato in materia dei più recenti, ulteriori e differenti per natura ed origine strumenti adottati a tutela dei dati personali da parte dell'ordinamento europeo sembrano recare conforto in merito al costante innalzamento della soglia di protezione della privacy del singolo, anche e soprattutto all'interno dell'infinita galassia di internet: pare, infatti, fuor di dubbio il rafforzamento, nonché l'incremento dei diritti del soggetto di cui gli ultimi sviluppi normativi e giurisprudenziali cui si è fatto cenno si fanno latori in riferimento all'ambiente virtuale che ormai permea ogni aspetto della nostra esistenza: decisioni quali la sentenza *Schrems II*, con la quale la Corte di Giustizia, lungi dal palesare forma di riverenza alcuna nei confronti di un Paese estraneo all'UE ma di fatto assoluto dominante sulla scena politico-economica internazionale, ha di fatto costretto gli USA a rinegoziare le condizioni disicplinanti il flusso transoceanico dei dati sensibili dei cittadini europei, rappresenta senza dubbio una tappa fondante nel percorso di tutela di questi ultimi; del pari, la Strategia Europea sui Dati, cui ricondurre anche la normativa prossima ventura di cui al *DGA*, certamente concorre ad attribuire maggiore pregnanza giuridica ad un contesto cui, a causa dell'estremo grado di aleatoria mutevolezza cartterizzante soprattutto l'ambiente *online*, non bastava più quanto statuito solo (o quasi) dal GDPR.

Tuttavia, a ben riflettere, sembra posssibile individuare più di un *vulnus* in riferimento ai richiamati provvedimenti, nonché alla sentenza del Tribunale dell'Unione Europea T-557-20 sull'anonimizzazione e pseudonimizzazione dei dati, astrattamente in grado, nell'opinione di chi scrive, di depotenziare il concreto impatto di tali iniziative in riferimento ad un contesto sì "scivoloso" come quello della protezione della *privacy* latamente intesa.

Più in particolare, ciò che lascia innanzitutto perplessi riguarda il contenuto della Decisione di adeguatezza della Commissione UE sul Quadro UE-USA per la protezione dei dati personali laddove la relativa adesione da parte delle imprese statunitensi interessate è lasciata alla mera discrezionalità di queste ultime anziché formare oggetto di un obbligo specifico. E a ciò si aggiunga che, qualora le stesse dovessero in tal senso decidersi, il corrispondente meccanismo di partecipazione al *Framework* in questione è contraddistinto da

una natura auto-certificativa, così dunque ulteriormente ampliando la libertà in capo a quegli enti (pubblici o privati) residenti nel territorio nordamericano riguardo alla gestione dei dati dei cittadini europei in loro possesso.

Oltretutto, si ricordi che gli Stati Uniti non dispongono ancora di una legge federale sulla protezione dei dati e che, quindi, il loro modello di regolazione in tema è circoscritto all'aspetto economico e di sicurezza nazionale, in particolare in forza della vigenza del *Patriot Act* emanato subito dopo l'attentato dell'11 settembre 2001 al World Trade Center di New York e alla sede del Pentagono ed a dispetto delle modifiche cui è stato oggetto nel corso del tempo (anche per le numerose critiche mosse all'interno degli stessi USA) nei confronti della sua disciplina estremamente invasiva.

In sostanza, al di là dei contenuti del richiamato Quadro, occorre verificare la reale volontà da parte degli *States* in merito ad una svolta di diritto interno con oggetto la tutela dei dati personali (nonché, in caso affermativo, quali tempistiche aspettarsi al riguardo), stante che non può ancora considerarsi nei fatti rispettato il requisito della sostanziale equivalenza alla normativa europea in materia, letta alla luce degli art. 7, 8 e 47 della Carta di Nizza; né a ciò pare potere sopperire l'applicazione extraterritoriale del diritto dell'UE (nella specie, del GDPR) sancita dalla CGUE in occasione della sentenza *Schrems II* e ribadita all'interno della Decisione di adeguatezza *de quo*: in assenza di un substrato normativo preventivamente *ad hoc* predisposto da parte del Paese extra UE in merito alla piena equiparazione di disciplina della protezione di dati sensibili rispetto a quanto al riguardo statuito dal diritto europeo, la diretta e piena applicazione di quest'ultimo all'interno di un territorio posto al di fuori dei confini del Vecchio Continente non pare, infatti, opzione pienamente attuabile se solo si ponga a mente che un vuoto normativo di tal fatta non può certamente colmarsi o comunque aggirarsi per il tramite della conclusione di un'intesa dalla valenza legislativa non certamente paragonabile ad una legge (e per quanto certificata da un provvedimento della Commissione UE).

A ciò si aggiunga la necessità altresì di verificare in concreto il reale grado d'imparzialità e indipendenza del Tribunale di Revisione della Protezione dei Dati istituito *ad hoc* dal richiamato provvedimento e oltretutto non ad esso preesistente, nonché e soprattutto, i criteri da quest'ultimo adottati in sede di risoluzione di controversie proprio in considerazione di

quanto testè evidenziato a proposito del sostanziale mancato allineamento normativo tra USA e UE in merito alla tutela dei dati.

E tali criticità sembrano paradossalmente trarre ulteriore vigore se calate all'interno del calco normativo all'uopo predisposto dallo stesso GDPR: ai sensi del già richiamato art. 45, p. 2 del Regolamento europeo per la Protezione dei Dati, infatti, nel valutare l'adeguatezza del livello di protezione, la Commissione prende in considerazione, tra gli atri, elementi quali "la pertinente legislazione generale e settoriale", tuttavia allo stato inesistente nell'ordinamento nord-americano, insiema al "l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo (…) con competenza per garantire e controllare il rispetto delle norme in materia di protezione dei dati, comprensiva di adeguati poteri di esecuzione, per assistere e fornire consulenza agli interessati in merito all'esercizio dei loro diritti e cooperare con le autorità di controllo degli Stati membri", del pari previamente insussistente e infatti istituita proprio dalla richiamata Decisione di adeguatezza.

In altri termini, un'inaccettabile doppia violazione del GDPR cui non si vede, almeno a breve, come porre rimedio.

Differenti rilievi, ma parimenti rilevanti nell'ottica di una reale protezione dei diritti dei singoli, pare potersi avanzare nei confronti della sentenza pronunciata di recente dal Tribunale dell'UE in materia di pseudonimizzzazione e anomizzazione dei dati laddove tale istanza giurisdizionale, in luogo di un approccio di matrice assolutistica, al contrario opta per l'applicazione di criteri basantesi sull'analisi del caso concreto, riflesso di un flessibile relativismo di tutela foriero più di dubbi che certezze.

Segnatamente, considerato l'estremo tasso in termini di varietà e, dunque, imprevidibilità con riguardo alle implicazionni dirette ed indirette riconducibili alla materia del trattamento dei dati personali all'interno del tendenzialmente illimitato ambiente virtuale, risulta piuttosto arduo concludere in merito alla capacità del singolo interprete di individuare la corretta soluzione per ogni singolo caso sottoposto alla sua attenzione ed in assenza di precisi riferirmenti cui attingere per la relativa soluzione: il mondo di internet, cioè, è già abbastanza variegato e complessso per sopportare un ulteriore elemento di sostanziale incertezza per il tramite di una valutazione in ultima analisi basantesi, almeno per ciò che riguarda il tema della pseudonimizzazione e anomizzazione, sulla sensibilità personale dell'organo giudicante, fattore

vieppiù da aggiungersi alle carenze di matrice tecnica che lo stesso inevitabilmente sconta (e per quanto in tal direzione coadiuvato da apposita consulenza).

Conseguentemente, per quanto la scelta in merito a strumenti di tutela tradizionalmente legati alla regolamentazione di fattispecie astratte sulla base di presunzioni e rigidi paletti ermeneutico-concettuali certamente rechi con sé il rischio di un giudizio avulso dalla realtà circostante, il ricorso a tale impostazione di giudizio sembra comunque da preferirsi rispetto alla maggiore alea che, nell'opinione di chi scrive, inevitabilmente caratterizza una valutazione lasciata alla discrezionalità dell'interprete e che, all'interno del tema che in tale sede ci compete, potrebbe rivelarsi un *boomerang* dagli effetti nefasti: se il reale oggetto di tutela dell'intera disciplina sulla protezione dei dati personali è costituito dal singolo individuo, in un'ottica di bilanciamento tra vantaggi e svantaggi si ritiene, infatti, dovere comunque propendere per l'opzione che, in quanto ispirata ad una *ratio* di natura incondizionata, almeno in astratto sembra garantire una difesa più stringente delle ragioni del cittadino.

A ciò si agggiunga che con riferimento al concetto di re-identificazione e riconducibilità di un codice pseudonimo al novero dei dati personali la pronuncia in questione torna di fatto indietro nel tempo, in particolare sia in forza del quanto mai vago accenno a non meglio precisati "mezzi legali" utili alla de-identificazione che in merito alla giurisprudenza della CGUE all'uopo richiamata: a tal ultimo proposito, infatti, viene citata la sentenza del 19 ottobre 2016 *Breyer*[16] che concerne ambiti di trattamenti di dati personali, ovvero mole e tipologia di dati profondamente diversi.

Il punto è che, come correttamente osservato, "*De-identification can reduce the privacy risk associated with collecting, processing, archiving, distributing or publishing information. De-identification thus attempts to balance the contradictory goals of using and sharing personal information while protecting privacy*"[17] e, quindi, il rischio di violazione della *privacy* non viene eliminato solo tramite l'applicazione di tecniche anonimizzzazione e de-identificazione[18].

[16] C-582/14, EU:C:2016:779.
[17] GARFINKEL, *De-identication of Personal Information,* NIST IR 8053, 2015.
[18] Concetti, questi ultimi, che comunque non andrebberoo considerati sinomini: come specificato ancora dal NIST (ISO/TS 25237:2008(E), infatti, "*Anonymization is another subcategory of de-identification. Unlike pseudonymization, it does not provide a means by which the information may be linked to the same person across*

Ancora, è da dire, e non senza un certo allarmismo, che nonostante le difficoltà nell'assicurare l'irreversibilità assoluta del processo di anonimizzazione e l'effettività del risultato, a livello europeo l'utilizzo di tecniche di anonimizzazione e pseudonimizzazione a presidio della sicurezza dei dati è spesso incoraggiato soprattutto nel caso di trattamenti che riguardano particolari categorie di *personal data* (art. 9 GDPR), come ad esempio in ambito sanitario e nel settore della ricerca medico-scientifica ove la generale ispirazione di matrice protezionistica in materia sembra degradare ad un ruolo subordinato rispetto alla circolazione e dunque all'utilizzo (nonché ri-utilizzo o uso secondario) di tali elementi identificativi di un determinato soggetto.

E proprio in relazione al contesto medico-sanitario (con ciò anticipando in parte quanto si evidenzierà nel prosieguo del presente lavoro con riguardo al Regolamento 868 del 2022) è piuttosto inquietante analizzare la direzione verso cui muovono le nuove proposte di regolamentazione adottate dalla Commissione Europea nell'ambito della richiamata Strategia europea in materia di dati: si fa particolare riferimento alla proposta di Regolamento del Parlamento Europeo e del Consiglio sullo spazio europeo dei dati sanitari del 3 maggio 2022 (di seguito "*European Health Data Space*" o "*EHDS*") istitutiva dello Spazio Europeo dei Dati Sanitari contraddistinto da disposizioni, norme e prassi comuni, infrastrutture e un quadro di governance per l'uso primario e secondario dei dati sanitari elettronici.

---

multiple data records or information systems. Hence reidentification of anonymized data is not possible". Oltretutto, è da dire che con riguardo al ruolo del terzo intermediario protagonista nella causa su cui si è pronucniato il Tribunale dell'UE, e cioè la società *Deloitte*, emerge un'ulteriore problematica, riflesso diretto, in più ampia prospettiva, di uno dei più rilevanti quanto sottovalutato ostacolo al compimento del processo d'integrazione europeo, in particolare rappresentato dalla mancanza di una lingua comune, lacuna che non sembra certamente trovare nel ricorso alla lingua inglese una soluzione definitiva (anche considerato che in forza della *Brexit*, almeno in teoria tale idioma non dovrebbe più rappresentare una lingua ufficiale dell'UE…): nella versione in lingua italiana della sentenza succitata è facilmente riscontrabile un errore di traduzione: al punto 32 n. 2 della stessa sentenza la versione in lingua inglese riporta che "*The fact that Deloitte was not mentioned in SRB's [privacy statement] as a potential recipient of the personal data collected and processed by the SRB as the controller in the context of the [right to be heard] process constitutes an infringement of the information obligations laid down in Article 15(1)(d) [of Regulation 2018/1725]*.". Ovvero viene rappresentato dai Giudici che Deloitte assume il ruolo di titolare del trattamento, mentre nella versione in lingua italiana del pronunciamento è riportato che "*Il fatto che Deloitte non sia stata menzionata nella informativa sulla protezione dei dati personali del CRU quale potenziale destinatario dei dati personali raccolti e trattati dal CRU, nella sua qualità di responsabile del trattamento nell'ambito della procedura relativa al diritto di essere ascoltato, costituisce una violazione dell'obbligo di informazione previsto all'articolo 15, paragrafo 1, lettera d), [del regolamento 2018/1725*".

Tale provvedimento fornirebbe dunque una base giuridica per l'uso secondario dei dati, tanto ai sensi dell'art. 6 par. 1 del GDPR (in particolare, ai sensi della lett. c), ovvero l'obbligo legale al quale è soggetto il titolare del trattamento) quanto ai sensi dell'articolo 9, par. 2, del GDPR (in particolare, ai sensi della lett. j), per motivi di ricerca scientifica, sulla base del diritto dell'Unione).

Inoltre, la versione proposta dalla Commissione Europea sembrerebbe consentire, in nome dell'armonizzazione di disciplina nell'UE, perfino il superamento del "sacro" totem del consenso (nei Paesi ove tale restrizione è stata introdotta dalla legislazione, quali ad esempio l'Italia) in quanto, all'art. 33, comma 5 prevede che "qualora il diritto nazionale prescriva il consenso della persona fisica, gli organismi responsabili dell'accesso ai dati sanitari si basano sugli obblighi di cui al presente capo per fornire l'accesso ai dati sanitari elettronici".

In sostanza, una prospettiva non certo particolarmente incoraggiante in ottica di tutela dei dati personali come obiettivo primario dell'intera disciplina normativa europea in tema.

Tali ultime considerazioni consentono, come anticipato, di rimarcare alcune delle principali criticità ascrivibili, nell'opinione di chi scrive, al *Data Governance Act* del 2022, espressamente ispirato, al pari del Regolamento (UE) 2018/1807, nonché alla Direttiva 2019/1024/UE, ad una finalità sostanzialmente antitetica, a ben ragionare, a quella basantesi sulla protezione dei dati personali, e cioè relativa alla condivisione, utilizzo e accesssibilità agli stessi: in pratica, così proseguendo sul percorso di una palese deriva a-protezionistica rispetto al GDPR e di cui gli ultimi provvedimenti normativi citati sembrano caratterizzati.

Laddove, in particolare, il *DGA* individua come propri paradigmi teorico-operativi principi la condivisione e il riutilizzo dei dati, tutt'uno con il *naif* valore dell'altruismo, il tutto in nome di una chiara, quanto improvvisa riscoperta di un insospettabile oriente solidaristico pervasivo dell'intera disciplina normativa europea sul trattamento (e non più sulla sostanziale protezione) della *privacy* dei propri cittadini, sembra infatti potersi insinuare il sospetto in merito alla reale valenza in termini di oggetto di tutela e di obiettivi primari all'interno del contesto che in tale sede ci riguarda e che, a quanto pare, non sembra davvero rappresentato dall'individuo nell'esplicazione della propria personalità anche e soprattutto nell'ambiente virtuale, ma, al contrario, dal neonato mercato dei dati, novello contesto economico

decisamente appetibile per le sue infinite possibilità e rispetto al quale, dunque, la protezione del singolo assume per il diritto europeo il ruolo di mera funzione.

E ad avallo di tale conclusione, sembra deporre, oltretutto in termini piuttosto espliciti, proprio quanto espressamente indicato dalle Istituzioni facenti capo a Bruxelles (Commissione in testa) a proposito della più volte citata Strategia Europea dei Dati e del proprio reale genetico *humus*, e quindi primario obiettivo di matrice sfacciatamente economica: "L'UE sta creando un mercato unico per i dati all'interno del quale: i dati potranno circolare all'interno dell'UE e in maniera transsettoriale, a beneficio di tutti; le norme europee, in particolare sulla tutela della vita privata e sulla protezione dei dati, e il diritto della concorrenza saranno pienamente rispettati; le norme relative all'accesso ai dati e al loro utilizzo saranno eque, pratiche e chiare. L'UE diventerà un'economia basata sui dati attraente, sicura e dinamica grazie: alla definizione di norme chiare ed eque sull'accesso ai dati e sul loro riutilizzo, all'investimento in strumenti e infrastrutture di prossima generazione per l'archiviazione e l'elaborazione dei dati, a uno sforzo congiunto per creare una capacità di cloud a livello europeo, alla condivisione dei dati europei in settori chiave, con spazi di dati interoperabili e comuni, a diritti, strumenti e competenze offerti agli utenti per consentire loro di mantenere il pieno controllo dei propri dati. Per garantire ulteriormente la leadership dell'UE nell'economia globale dei dati, la strategia europea per i dati intende: adottare misure legislative in materia di governance, accesso e riutilizzo dei dati. Ad esempio, per la condivisione dei dati tra imprese e amministrazioni a fini di interesse pubblico; rendere i dati più ampiamente disponibili mediante l'apertura di serie di dati di alto valore pubblico in tutta l'UE e consentendone il riutilizzo gratuitamente"[19].

Insomma, una macrospcopica riproposizione, a ben vedere, nei confronti della c.d. economia dei dati (appunto) dei medesimi criteri, meccanismi e logiche alla base della circolazione dei quattro fattori produttivi (merci, persone, servizi e capitali) strumentale nel corso del tempo alla creazione e al costante rafforzamento del mercato "tradizionale", adesso dunque rispolverati alla bisogna da parte di un'UE solo capace, a quanto pare, di ritradurre in termini economico-mercantili qualsivoglia materia, ambito o contesto si pone alla sua attenzione, financo per tal via giungendo ad una sostanziale negazione di sé stessa in nome del

[19] Strategia europea in materia di dati (europa.eu).

pedissequo ossequio nei confronti della sovranità dell'economicamente rilevante: piuttosto stridente, si ripete, il deciso cambio di rotta cui gli ultimi provvedimenti normativi richiamati sembrano indirizzati rispetto al GDPR, gradualmente nei fattti radicalmente smantellato in nome del rinnovato ossimoro in pratica costituito dalla condivisione della *privacy*.

E in questo senso, pare potersi individuare un sottile filo rosso che lega quanto in tale sede citato, e dunque il *DGA* (insieme alle più recenti disposizioni legislative UE sui dati), la Decisione di Adeguatezza sul Quadro USA –UE e la sentenza del Tribunale UE T-557-20, così contribuendo a svelarne le autentiche fonti ispiratrici e relative finalità.

Segnatamente, se posti all'interno della suggerita prospettiva d'analisi, i tre richiamati provvedimenti sembrano acquisire rinnovato nitore anche e soprattutto avuto riguardo agli accennati limiti: assumendo, cioè, una visuale mercato-centrica, ecco motivati sia l'individuazione dei caratteri della condivisione e dell'altruismo dei dati, sia la mancata prescrizione di un onere a carico delle imprese statunitensi aderenti al suddetto *Framework*, tutt'uno con la pacifica accettazione palesata dalla Commissione di fronte alla duplice infrazione del GDPR da parte del Quadro medesimo, che la relatività di valutazione posta alla base della decisione del Tribunale dell'UE sulla pseudonimizzzazione e anomizzazione dei dati, nuovo petrolio al cospetto del quale l'Unione (Economica) Europea ha scelto di genuflettersi.