ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

18 DICEMBRE 2024

Trasferimento dei dati personali UE-USA novità e criticità del *data privacy framework*

di Angela Busacca
Ricercatore di Diritto privato
Università degli Studi Mediterranea di Reggio Calabria

Trasferimento dei dati personali UE-USA novità e criticità del *data privacy framework*[*]

di Angela Busacca
Ricercatore di Diritto privato
Università degli Studi Mediterranea di Reggio Calabria

Abstract [It]: Il trasferimento dei dati personali verso paesi gli USA costituisce uno dei temi di discussione più attuali dell'ultimo decennio, soprattutto in considerazione delle vicende giudiziarie che, su impulso dell'attivista austriaco Max Scherms, hanno portato per ben due volte alla invalidazione delle decisioni di adeguatezza relative agli accordi EU-USA noti come "Safe Harbor" (CGUE 6 Ottobre 2015) e "Privacy Shield" (CGUE, 16 luglio 2020). L'assenza di una base giuridica generale per il trasferimento dei dati, quale appunto una dichiarazione di adeguatezza da parte della Commissione Europea, secondo il disposto dell'art.45 GDPR, determina una serie di problemi, soprattutto per le imprese e gli operatori economici. Nel marzo 2022 è stato annunciato un terzo accordo, lo EU-US Data Privacy Framework (DPF) e nel luglio 2023 la Commissione Europea ha, infine, rilasciato una nuova dichiarazione, riconoscendo l'adeguatezza delle tutele garantite dalla legislazione statunitense e corrispondente al livello di protezione offerto dal Regolamento generale sulla protezione dei dati dell'UE (GDPR). Con tale nuova dichiarazione di adeguatezza, sembra chiuso il contenzioso che ha posto non pochi problemi alle imprese europee e ha messo in luce, ancora una volta, i diversi approcci al tema della protezione dei dati da parte di UE e USA: i primi sono più orientati verso una prospettiva centrata sulla persona, quest'ultima più orientata verso una prospettiva centrata sul mercato. Il presente contributo, riprendendo le fila di un precedente lavoro che si era concluso proprio in modo interrogativo, sollevando dubbi sul ruolo del DPF come elemento di soluzione o come prologo al caso Scherms III, propone una breve analisi delle innovazioni del DPF, evidenziando tuttavia la presenza di alcune criticità ed elementi di rischio tuttora esistenti per i diritti e la protezione dei dati personali dei cittadini europei, anche in considerazione di nuove prospettive di utilizzo dei dati personali per la creazione dei training dataset per finalità di addestramento dei sistemi di intelligenza artificiale

Title: EU-US personal data transfer news and critical issues in the data privacy framework
Abstract [En]: Lawfulness and admissibility of licit transfer of personal data from the European Union (EU) to the United States of America (US) is one of the most debated topics of the last ten years, and has seen many rulings pertaining to the matter. Twice the Court of Justice of the European Union (CJEU) has invalidated the adequacy decision relating EU-US data transfer agreements: first with the ruling of 6 October 2015 (so-called Scherms I ruling, related to "Safe Harbor" agreement) and then with the ruling of of 16 July 2020 (so-called Scherms II ruling, related to "Privacy Shield" agreement). In March 2022 a third agreement, the EU-US Data Privacy Framework (DPF) was announced and in July 2023 the European Commission has, lastly, issued a new declaration of adequacy, recognizing the appropriateness of the protections granted by US legislation and corresponding to the level of protection offered by the EU General Data Protection Regulation (GDPR). With the new declaration of adequacy, the dispute that has posed many problems to European companies and has highlighted, once again, the different approaches to the issue of data protection by the EU and the USA seems to be over: the former is more oriented towards a person-centric perspective, the latter more oriented towards a market-centric perspective. Picking up the threads of a previous work that ended precisely in a questioning way, raising doubts about the role of the DPF as an element of solution or as a prologue to the Scherms III case, this work aims to analyse the characteristics and innovations of the DPF that are at the basis of the declaration of adequacy, also highlighting the presence of some ongoing critical issues and elements of risk for the rights and protection of personal data of European citizens, also considering the new critical perspectives of using personal data to improve AI training dataset.

[*] Articolo sottoposto a referaggio.

Parole chiave: Protezione dei dati personali, GDPR, Trasferimento dati EU-US, Data Privacy Framework, Decisione di Adeguatezza
Keywords: Personal data protection, GDPR, EU-US data transfer, Data Privacy Framework-EU Commission Implementing Decision

1. Introduzione

La questione della liceità ed ammissibilità del trasferimento di dati personali dall'Unione Europea (EU) agli Stati Uniti d'America (USA) costituisce uno dei temi più dibattuti degli ultimi dieci anni, da quando la Corte di Giustizia dell'Unione Europea (CGUE), con la sentenza 6 ottobre 2015 (cd. Sentenza Scherms I[1]), invalidò la decisione di adeguatezza relativa al cd. "Safe Harbor", evidenziando le lacune della disciplina statunitense in materia di protezione dei dati personali e l'insufficienza delle garanzie offerte per la tutela dei dati dei cittadini europei che venivano trasferiti oltreoceano[2].

Nel corso di quasi un decennio, infatti, si sono succeduti dapprima un nuovo accordo (il cd. "Privacy Shield"[3] del 2016) con relativa decisione di adeguatezza (adottata il 12 luglio 2016[4]), anche quest'ultima poi invalidata dalla CGUE con la sentenza 16 luglio 2020 (cd. Sentenza Scherms II[5]), e, da ultimo, un

[1] Sentenza della Corte (Grande Sezione) del 6 ottobre 2015 – M. Schrems contro Data Protection Commissioner ; il testo completo della decisione può leggersi sul sito Eur-Lex. In argomento, nell'ambito di una vasta bibliografia, cfr. G. RESTA, V. ZENO ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, RomaTrE-Press, Roma, 2016 (disponibile sul sito romatre-press); A. MANTELERO, *L'ECJ invalida l'accordo per il trasferimento dei dati personali tra EU ed USA. Quali scenari per cittadini ed imprese?* in *Contratto e Impresa. Europa*, 2015, p. 719; P. PIRODDI, *I trasferimenti di dati personali verso apesi terzi dopo la sentenza "Scherms" e nel nuovo Regolamento generale sulla protezione dei dati,* in *Il diritto dell'informazione e dell'informatica*, 2015, p. 827.

[2] Sin dalla prima pronuncia della CGUE è stato evidenziato come la carenza di una normativa generale in tema di *data protection* renda decisamente inferiore lo standard di tutela garantito negli USA rispetto a quello garantito nella UE ed esponga i cittadini europei a trattamenti illeciti od ad abusi sui dati personali; a ciò si deve altresì aggiungere la diversità di fondo che caratterizza le strategie data protection negli USA ed in Europa, evidenziando come quest'ultima ponga al centro la persona/cittadino mentre i primi guardino maggiormente alla persona/consumatore parametrando trattamenti e tutele secondo logiche decisamente mercato-centriche.

[3] Sin dalla sua presentazione, il Privacy Shield è stato investito da una serie di dubbi sulla reale possibilità di superare le criticità che già avevano investito il "Safe Harbor"; in argomento, cfr. R. FERRARIO, Lo "EU-U.S. Privacy Shield". Una risposta insufficiente alle richieste della Corte di giustizia dell'Unione europea nella sentenza "Safe Harbour"? in *Il Diritto del commercio internazionale*, 2017, p. 635.

[4] Decisione di esecuzione UE 2016/1250 della Commissione del 12.07.2016, consultabile sul sito Eur-Lex.

[5] Sentenza della Corte (Grande Sezione) del 16 luglio 2020 - Data Protection Commissioner contro Facebook Ireland Limited e M. Schrems; il testo completo della decisione può leggersi sul sito Eur-Lex; anche con riferimento alla sentenza Scherms II la bibliografia di commento si presenta molto vasta, senza alcuna pretesa di esaustività, cfr. E. TEROLLI, Privacy e protezione dei dati personali UE vs USA. Evoluzioni di diritto comparato e il trasferimento dei dati dopo la sentenza "Schrems II", in Il diritto dell'informazione e dell'informatica, 2021, p. 49; R. BIFULCO, Il trasferimento dei dati personali nella sentenza Schrems II: dal contenuto essenziale al principio di proporzionalità e ritorno, in *Diritto pubblico europeo – rassegna on line*, 2020.

terzo accordo, lo EU-US Data Privacy Framework (DPF)[6] annunciato nel marzo del 2022 ed oggetto dell'Executive Order del Presidente Usa n.14086 del 07 ottobre 2022[7].

In relazione al Data Privacy Framework, la Commissione Europea ha, da ultimo, emanato una nuova dichiarazione di adeguatezza in data 10 luglio 2023[8], riconoscendo congruità delle tutele accordate dalla normativa statunitense e corrispondenza al livello di tutela offerto dal Regolamento Generale EU sulla Protezione dei Dati (GDPR).

Con la nuova dichiarazione di adeguatezza sembra chiudersi la *querelle* che ha posto non pochi problemi alle imprese europee ed ha evidenziato, ancora una volta, le diversità di approccio alla tematica della *data protection* da parte della EU e degli USA: più rivolta ad un'ottica persona-centrica la prima, più rivolti ad un'ottica mercato-centrica i secondi.

Nonostante, sulla carta, il Data Privacy Framework sembri offrire maggiori garanzie in relazione alle criticità emerse in sede giudiziale, tuttavia non sono mancate le perplessità già in ambito istituzionale, dal momento che la prima bozza della decisione di adeguatezza aveva incassato parere negativo sia dal Comitato dei Garanti Europei (European Data Protection Board, EDPB)[9] che dalla Commissione per le libertà civili, la giustizia e gli affari interni del Parlamento Europeo; successivamente, alla pubblicazione della decisione di adeguatezza, diversi operatori tra i quali la stessa ONG Nyob non hanno mancato di manifestare un aperto dissenso, evidenziando come in realtà il nuovo accordo Data Privacy Framework sia solo apparentemente risolutivo dei problemi e delle criticità già presenti nel Safe Harbor e nel Privacy Shield, ed anzi sottenda le medesime possibilità di sorveglianza, accesso ai dati e profilazione massiva dei dati dei cittadini europei da parte delle agenzie di *intelligence* statunitensi.

Riprendendo le fila di un precedente studio[10] che si concludeva proprio in modo interrogativo, ponendo il dubbio sul ruolo del Data Privacy Framework (nel prosieguo indicato con l'acronimo DPF), come

---

[6] EU-US Data Privacy Framework – una scheda informative può leggersi sul sito della Commissione Europea; per un commento a prima lettura, cfr. A. TERRASI, *EU-US Data privacy Framework: much ado about nothing?* in *Diritti umani e Diritto Internazionale*, 2023, p. 778; G. PROIETTI, *Il trasferimento dei dati personali all'estero: proporzionalità, poteri delle agenzie di intelligence ed effetto Bruxelles*, in *Il diritto dell'informazione e dell'informatica*, 2023, p. 691; A. ORTEGA GIMENEZ, *¿Y a la tercera va la vencida?... El nuevo marco transatlántico de privacidad de datos UE-EE.UU*, in *Cuadernos de Derecho Transnacional*, 2024, p. 483 (specialmente sez. V, p. 500).

[7] Executive Order n.14086 - Enhancing Safeguards For United States Signals Intelligence Activities. Il testo complete può leggersi sul sito ufficiale The White House.

[8] Decisione di esecuzione UE 2023/1795 del 10.07.2023; il testo è consultabile sul sito della Commissione Europea.

[9] Il Comitato Europeo per la Protezione dei dati *(European Data Protection Board*) è stato istituto dall'art.68 GDPR quale organismo del Unione con carattere di indipendenza (art.69) e funzioni di controllo e monitoraggio del rispetto e della conformità al Regolamento nonché di consultazione ed elaborazione di linee-guida, raccomandazioni e buone pratiche (artt.70-71). L'EDPB è un ente pubblico europeo con personalità giuridica, è composto dal Garante Europeo per la Protezione dei dati personali (*European Data Protection Supervisor*) e dalle figure di vertice delle autorità di controllo nazionali (o da loro rappresentanti) e, dal 2018, ha sostituito il Gruppo di Lavoro art.29 (WP29).

[10] Il riferimento è al contributo *Web Analytic Tools e trasferimento di dati personali verso gli USA: il monito delle NDPA Europee e le prospettive del "Trans-Atlantic Data Privacy Framework*", pubblicato in D. CANANZI (a cura di) *Annali del Dipartimento di Giurisprudenza, Economia e Scienze Umane - 2022*, ESI, Napoli, 2024, p. 55; il contributo riprende ed amplia il testo della

elemento di soluzione o come prologo di un eventuale caso Scherms III[11], il presente lavoro si indirizza ad analizzare i caratteri e le innovazioni del DPF che sono alla base della decisione di adeguatezza, evidenziando altresì la presenza di eventuali perduranti criticità ed elementi di rischio per i diritti e la tutela dei dati personali dei cittadini europei.

2. Il quadro giuridico di riferimento e gli interventi della Corte Europea di Giustizia

Preliminare all'analisi dei profili più rilevanti del DPF e della nuova decisione di adeguatezza, appaiono opportune alcune puntualizzazioni sul quadro giuridico di riferimento e sulle motivazioni che avevano condotto alle sentenze della CGEU nei confronti delle dichiarazioni di adeguatezza del Safe Harbor e soprattutto del Privacy Shield.

Come previsto dall'art.45 GDPR ("*Trasferimento sulla base di una dichiarazione di adeguatezza*") la dichiarazione di adeguatezza rappresenta il primo e più importante strumento per il trasferimento dei dati personali "*oggetto di un trattamento o destinati ad essere oggetto di un trattamento dopo il trasferimento*" verso paesi terzi secondo canoni di sicurezza e con la garanzia che il livello di protezione delle persone fisiche offerto dal GDPR "*non sia pregiudicato*"[12]. In presenza di una dichiarazione di adeguatezza, infatti, non sarà necessario avvalersi di ulteriori basi giuridiche per la liceità del trasferimento verso un paese terzo o una organizzazione internazionale, indipendentemente dalla natura dell'attività nell'ambito della quale il trasferimento viene effettuato[13]. Proprio la nozione di "adeguatezza" del livello di protezione assume,

relazione «*Data transfer to the US: Italian Data Protection Authority (IDPA) «stops» Google Analytics*», presentata in occasione della Conferenza Internazionale «Cyberspace 2022» presso l'Università Mysarykova di Brno (Repubblica Ceca) nei giorni 24/25 novembre 2022, sessione «Law: Privacy and Personal Data» (25 novembre, chair: Jakub Misek – Bettina Bacher).

[11] L'espressione è utilizzata anche da M. GIACALONE, *Verso Scherms III? Analisi del nuovo EU-US Data Privacy Framework*, in *www.europeanpapers.it*, 2023, p.149; ed altresì da M. CONNELLY, *Will the EU-US Data Privacy Framework survive Scherms III?* in *Trinity College Law Review*, 2024, vol 27, p. 89.

[12] Le espressioni all'interno delle virgolette sono riportate dall'art.44 GDPR che enuncia il "Principio generale per il trasferimento" dei dati verso i paesi terzi o le organizzazioni internazionali. L'indicazione specifica, che riconduce all'ambito di operatività sia i dati già oggetto di trattamento sia i dati che saranno oggetto di trattamento dopo il trasferimento, permette di prendere in considerazione sia i flussi continui di dati che le mere comunicazioni una tantum tra titolari, purché abbiano natura transfrontaliera; sul punto, cfr. G. M. RICCIO, *Art.44 – Principio generale per il trasferimento*, in G. M. RICCIO, G. SCORZA, E. BELISARIO (a cura di*) GDPR e normativa privacy*, II edizione, WKI, Milano, 2022, p. 495.

[13] In assenza di una dichiarazione di adeguatezza, il trasferimento sarà lecito solo in presenza degli elementi indicati dagli artt. 46 (garanzie adeguate offerte dal titolare e presenza di diritti azionabili e mezzi di ricorso effettivi per gli interessati) e 47 (norme vincolanti di impresa approvate dall'autorità di controllo competente in conformità del meccanismo di coerenza previsto dall'art.63 GDPR) od ancora in presenza di una delle ipotesi di deroga in specifiche situazioni come previsto dall'art.49, che elenca una serie di ipotesi ed assume valore di norma di chiusura, dal momento che interviene solo in carenza sia della dichiarazione di adeguatezza che in carenza degli elementi degli artt.46 e 47; tra le ipotesi previste si ritrovano il consenso dell'interessato, l'esecuzione di un contratto in favore dell'interessato, l'esercizio o la difesa di un diritto in sede giudiziaria, l'interesse vitale dell'interessato o di altre persone, importanti motivi di interesse pubblico, il trasferimento di dati da un registro pubblico, il legittimo interesse del titolare. In relazione alle specifiche deroghe ex art.49 è importante ribadire, come affermato in dottrina, che esse "hanno carattere di eccezione alla regola generale" dal momento che "non forniscono garanzie adeguate per i dati trasferiti e considerato che tali trasferimenti non sono soggetti ad alcuna autorizzazione da parte delle autorità di controllo, per cui il ricorso a tali deroghe comporta di per sé

dunque, valore centrale in relazione alla libera circolazione transfrontaliera dei dati personali al fine di assicurare che, una volta trasferiti nel paese terzo di destinazione, i dati personali dei cittadini europei non possano subire violazioni o arbitrarie compressione delle tutele assicurate dal GDPR. La decisione sull'adeguatezza del livello di protezione garantito dal paese terzo o dall'organizzazione internazionale verso la quale avviene il trasferimento è rimessa alla Commissione EU la quale agisce poi mediante un atto di esecuzione, una volta effettuata la valutazione sugli standard di *data protection* riguardo agli elementi indicati dal comma 2 dell'art.45 (condizioni giuridiche con riferimento allo stato di diritto, al rispetto dei diritti umani e delle libertà fondamentali nonché alla legislazione vigente, esistenza ed attivo funzionamento di una o più autorità di controllo indipendenti, impegni internazionali assunti oppure partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali[14]). L'atto di esecuzione, come richiesto dallo stesso art.45, deve inoltre contenere specifiche indicazioni riferite all'area geografica e settoriale di applicazione e, ove possibile, l'indicazione delle autorità indipendenti di controllo alle quali è rimessa l'opera di monitoraggio sul rispetto della tutela dei dati personali e l'assistenza agli interessati che lamentino (eventuali) trattamenti illeciti. La dichiarazione di adeguatezza è un provvedimento chiaramente collegato alla (perdurante) attualità del livello di tutela assicurato; pertanto, è un provvedimento che deve essere sottoposto a revisione periodica e, in caso di modifiche che pongano il paese terzo o l'organizzazione internazionale in condizione di non poter garantire il livello di tutela richiesto, essa potrà essere modificata, sospesa o revocata.

Come già anticipato, nel corso dell'ultimo decennio la *vexata quaestio* del trasferimento dei dati personali verso gli USA ha costituito oggetto di ben due interventi della CGUE che ha invalidato altrettante decisioni di adeguatezza, evidenziando una serie di elementi che non permettono di ritenere il livello di *personal data protection* degli USA equivalente a quello accordato ai cittadini europei dal GDPR, soprattutto in considerazione della possibilità di ingerenza da parte delle autorità federali USA e della mancanza di

maggiori rischi per i diritti e le libertà degli interessati" (L. M. SALVATI, *Art. 49 – Deroghe in specifiche situazioni*, in G. M. RICCIO, G. SCORZA, E. BELISARIO (a cura di) *GDPR e normativa privacy*, *cit.*, p. 517.

[14] Le disposizioni sul trasferimento verso paesi terzi riprendono quanto già previsto dalla direttiva 95/46/CE agli artt.25 e ss. evidenziando tuttavia una significativa innovazione proprio nella specificazione degli indici di riferimento sui quali la Commissione deve parametrare la propria decisione: nella precedente disciplina, infatti, era contenuto solo un riferimento, generico, alla legislazione nazionale del paese di destinazione ed agli impegni internazionali da quest'ultimo assunti. Guardando alla formulazione attuale dell'art. 45 GDPR appare chiaro come la pluralità di indici di riferimento sia funzionale ad una più completa valutazione della situazione del paese terzo di destinazione che potrà essere definito "sicuro" solo in base ad una più attenta e completa valutazione; in argomento, cfr. A. TERRASI, *EU-US Data privacy Framework: much ado about nothing?, cit.*, p. 780: in particolare, l'autore evidenzia come il concetto di adeguatezza basato sulla pluralità di criteri e preso a modello dalla CGEU nel caso Scherms non solo assume valore in riferimento alla protezione dei dati ma altresì "in connessione con questo" in riferimento al "livello di protezione dei diritti fondamentali (rectius, di quei diritti che possono subire una limitazione in ragione di un trattamento illecito di dati personali)" sicché un flusso di dati transfrontaliero potrà dirsi sicuro "in quanto lo Stato di destinazione garantisca una tutela dei diritti e delle libertà fondamentali che sia, nella sostanza, comparabile a quella garantita dall'ordinamento UE".

una autorità amministrativa indipendente con funzioni di controllo e (eventuale) giudizio, alla quale i cittadini europei possano fare ricorso in caso di violazioni dei dati o di utilizzo illecito.

Sebbene il primo degli interventi della CGUE sia relativo ad una dichiarazione di adeguatezza resa in riferimento alle norme della direttiva 95/46/CE (decisione di esecuzione 2000/520/CE del 26 luglio 2000 sull'adeguatezza dell'accordo cd. "Safe Harbor") ed il secondo sia invece relativo ad una dichiarazione di adeguatezza resa in riferimento alle norme del GDPR (decisione di esecuzione UE 2016/1250 del 12 luglio 2016 sull'adeguatezza dell'accordo cd. "Privacy Shield"), entrambi si basano sugli stessi ordini di criticità: l'esposizione dei dati trasferiti ad attività di monitoraggio e controllo potenzialmente illimitate (e non controllabili) da parte da parte delle autorità federali e delle agenzie di intelligence USA per finalità di sicurezza (genericamente intesa) ed al contempo assenza di strumenti in grado di garantire il ricorso effettivo ad un giudice imparziale per contestare le violazioni di dati subiti e/o i trattamenti illeciti sugli stessi. L'assenza di criteri e/o limiti per temperare le capacità di ingerenza delle autorità federali USA e l'assenza di strumenti di ricorso verso autorità indipendenti in grado di rendere giustizia alle istanze dei cittadini europei integrano una doppia lacuna in relazione ai criteri indicati dall'art.45 GDPR e si traducono, nella lettura della CGUE, in violazioni dei diritti fondamentali della persona e precisamente in violazione dei diritti previsti agli artt. 7 (rispetto della vita privata e della vita familiare), 8 (protezione dei dati di carattere personale) e 47 (diritto ad un ricorso effettivo ed ad un giudice imparziale) della Carta di Nizza, interpretati nel prisma dell'art. 52 (portata e interpretazione dei principi) della stessa Carta in base al quale la potenziale ingerenza degli agenti USA appare del tutto priva di proporzionalità in relazione agli interessi tutelati. Su quest'ultima norma, peraltro, appaiono opportune alcune precisazioni: l'art.52 della Carta di Nizza, infatti, prevede che le limitazioni all'esercizio dei diritti ed alle libertà riconosciute dalla Carta stessa devono trovare fondamento esplicito nella legge, devono rispettare il contenuto essenziale dei diritti e delle libertà e devono apparire necessarie e finalizzate alla tutela di un interesse generale riconosciuto dall'UE o all'esigenza di proteggere diritti e libertà altrui: con questa previsione devono confrontarsi le esigenze di sicurezza nazionale poste a fondamento degli *executive orders* presidenziali e delle altre normative USA che legittimano facoltà di accesso pressoché illimitate per finalità di intelligence alle autorità federali ed alle agenzie di intelligence preposte ad attività di controllo con finalità di sicurezza nazionale; a titolo esemplificativo si considerino due degli atti più

rilevanti: l'Executive Order 12333[15] ed il Foreign Intelligence Surveillance Act (FISA)[16], in forza dei quali sono state realizzate attività di sorveglianza e raccolta massiva di dati personali con successive attività di trattamento senza che siano stati resi conoscibili (e valutabili) le reali esigenze di sicurezza o le modalità di trattamento o ancora i tempi di ritenzione e successivo trattamento dei dati[17]. La generale finalità di sicurezza nazionale sottesa alle disposizioni indicate, infatti, non può essere riconosciuta come valida base giuridica proprio per la mancanza di un criterio che permetta di delimitarne il perimetro di liceità, e, per contro, permetta di individuare le ipotesi di trattamento illecito e di violazione dei dati.

Sul portato delle censure emesse dalla CGUE, si sono consolidate le due direttrici di intervento funzionali ad una risoluzione delle criticità più rilevanti in tema di circolazione dei dati personali dagli Stati UE verso gli USA: per un verso limitare le facoltà di ingerenza delle agenzie di intelligence e delle autorità federali, individuando un perimetro di necessità e proporzionalità, e per altro verso garantire uno strumento di tutela dei diritti dei cittadini UE che lamentino una violazione o un trattamento illecito dei propri dati ed assicurare che tale strumento sia rimesso ad un organismo in grado di agire con modalità efficienti e tempestive.

---

[15] L'executive Order n.12333 (United States Intelligence Activities) fu firmato nel 1981 dal presidente Reagan per estendere i poteri di monitoraggio ed accesso alle informazioni delle agenzie di intelligence e porre obblighi di collaborazione con la CIA per le agenzie federali USA. Il testo dell'Executive Order fu successivamente modificato ed implementato nel 2004, con l'Executive Order n. 13355 ed ancora nel 2008 con l'Executive Order n. 13470, entrambi firmati dal Presidente G. Bush.

[16] Il Foreign Intelligence Surveillance Act (FISA), emanato negli anni '70 e successivamente rafforzato dopo gli attentati terroristici del 2001, detta norma in materia di sorveglianza, sia in dimensione fisica che in dimensione elettronica e digitale, e rafforza le possibilità di accesso ai dati ed alle informazioni per finalità di sorveglianza per motivi di sicurezza nazionale. Negli ultimi anni si sono succedute una serie di disposizioni, ultima delle quali il National Defence Authorization Act (NDAA) del novembre 2023 che hanno progressivamente ampliato, sia in senso quantitativo che in senso qualitativo, l'ambito di applicazione del FISA ed in particolare l'ambito di operatività della sezione 702, in forza della quale possono essere autorizzate attività di controllo e raccolta dati su cittadini stranieri che siano sospettati di avere collegamenti con attività terroristiche e, più in generale, di pericolo per la sicurezza nazionale senza un provvedimento autorizzatorio di natura giudiziario, ma unicamente sulla base di un provvedimento della Foreign Intelligence Surveillance Court (FISC). La possibilità di disporre attività di controllo per raccolta dati su ogni forma di comunicazione, fisica ed elettronica, riferibile ai soggetti "sorvegliati" in forza della decisione di un organismo autonomo, che opera al di fuori del sistema giudizio e che potrebbe agire senza garantire i diritti individuali e senza dover rispettare criteri di necessità e proporzionalità, rende la sezione 702 potenzialmente molto rischiosa per i diritti e le libertà individuali dei cittadini europei che potrebbero ritrovarsi oggetto delle attività di intelligence e non avere modalità per far valere i propri diritti e ricorrere ad un organismo indipendente anche solo per far cessare le attività di trattamento illecite. Sia la sezione 702 del FISA che l'Executive Order n.12333 sono stati più volte indicati come violazioni dello standard di sicurezza dei dati garantito dal GDPR e sono stati considerati elementi che concorrono ad evidenziare la mancanza del livello di tutela equivalente. Proprio per superare il gap esistente tra standard di tutela garantito dal GDPR e standard di tutela attuato negli USA il nuovo Executive Order n.14086 ha posto una serie di limitazioni alle facoltà di monitoraggio e controllo da parte delle agenzie di intelligence e delle autorità federali, anche se permangono diversi dubbi sulla reale attuazione di tali nuove garanzie.

[17] In argomento, G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Il Diritto dell'Informazione e dell'Informatica*, 2015, p. 679. Le cronache di questi anni sono state caratterizzate dall'emersione di vicende che hanno evidenziato la labilità e l'incertezza del confine di liceità delle attività di sorveglianza, seppur indicate come finalizzate ad esigenze di sicurezza nazionale: a titolo esemplificativo, basti considerare il caso Snowden e le rivelazioni sul cd. progetto PRISM e sulle attività di sorveglianza massiva sulle comunicazioni elettroniche.

La risoluzione delle suddette criticità al fine di poter realizzare un nuovo accordo per il trasferimento transfrontaliero dei dati ed ottenere una nuova dichiarazione di adeguatezza con decisione di esecuzione da parte della Commissione UE si è posta, già all'indomani della sentenza Scherms II come una esigenza primaria per permettere alle imprese europee e statunitensi di utilizzare lo strumento ex art.45 GDPR come (generale) base giuridica di trasferimento; la carenza di una decisione di adeguatezza ha determinato, infatti, in più occasioni delle vere e proprie situazioni di stallo con interventi delle Autorità Garanti che si traducevano in divieti e/o limitazioni ai flussi di dati, con ripercussioni negative sugli stessi equilibri di mercato e con la possibilità che le imprese finissero per operare in situazioni ibride, facendo ricorso anche a strumenti che potevano sottendere attività di raccolta e trasferimento illecite[18]. I negoziati intrapresi al fine di raggiungere un nuovo accordo si sono svolti seguendo come direttrici proprio le indicazioni della CGUE per individuare modalità e termini in grado di rispondere al meglio alle diverse esigenze degli operatori presenti sul mercato, delle istituzioni ma soprattutto degli interessati che risultano essere i più esposti ai rischi della circolazione transfrontaliera dei flussi di dati.

3. Principi ed innovazioni dello EU-US Data Privacy Framework, adozione della decisione di adeguatezza UE 2023/1795 e perplessità dell'EDPB

Il primo annuncio sul raggiungimento di un nuovo "accordo di principio" in tema di trasferimento transfrontaliero dei dati EU-USA fu dato dalla Presidente della Commissione EU Von Der Leyen nel marzo del 2022, in occasione della visita del Presidente Biden in Europa. Dopo più di un anno di intensi lavori e di negoziati, basati sulle criticità evidenziate delle pronunce della CGUE e proiettati alla realizzazione di un accordo in grado di supportare una "*economia digitale inclusiva*", lo US-EU Privacy Data Framework venne presentato come il segno tangibile di "*un impegno senza precedenti da parte degli Stati Uniti per attuare riforme che rafforzeranno la tutela della privacy e delle libertà civili*"[19] non soltanto in relazione alle attività

[18] In argomento appare significativa la vicenda relativa ai provvedimenti dell'Autorità Garante Italiana sull'utilizzo dei Web Analytic tools di Google nel 2022: ravvisando un trasferimento privo di base giuridica valida, l'Autorità impose ad una società operante sul web l'interruzione dell'utilizzo di tali strumenti di Web Analysis, dal momento che tale utilizzo comportava il trasferimento dei dati personali degli utenti verso gli USA e che gli stessi utenti non erano adeguatamente informati sul trasferimento stesso, nonché sulle implicazioni e sui potenziali rischi. A fronte delle condivisibili affermazioni di principio sulla opportunità della tutela degli interessati e sul rispetto delle norme del GDPR in tema di informazione e trasferimento transfrontaliero, appare opportuno evidenziare come l'utilizzo degli strumenti di Web Analysis appaia fondamentale per ogni operatore presente sul web ed al contempo come proprio i tools offerti dalle Big Tech extra EU appaiano i più efficienti e completi: le esigenze di un mercato sempre più interconnesso e nell'ambito del quale la dimensione temporale si è ridotta al minimo comportano necessariamente l'individuazione di un punto di equilibrio tra i diversi interessi. Per una panoramica sulla citata vicenda che ha coinvolto l'Autorità Garante italiana, sia consentito il rinvio a A. BUSACCA *Web Analytic Tools e trasferimento di dati personali verso gli USA, cit.,* p. 55.

[19] Le frasi riportate sono tratte dalla dichiarazione rilasciata dalla Commissione UE alla stampa in occasione della presentazione dell'accordo di principio; il testo completo della dichiarazione "European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework", può leggersi, in lingua inglese, sul sito della Commissione Europea.

di trattamento dei dati personali realizzate dagli operatori economici, ma soprattutto in relazione alle possibili ingerenze delle autorità federali USA. Come già evidenziato, infatti, tra i punti di maggiore criticità, che avevano portato alle decisioni della CGUE nel 2016 e soprattutto nel 2020, si ritrovavano proprio le possibili attività di intelligence che le autorità federali potevano svolgere, in modo pressoché illimitato, sui dati raccolti ed allocati sui server delle corporate USA. La limitazione dell'accesso delle autorità federali USA ai dati, tuttavia, rappresenta solo uno dei punti sui quali si basa l'impianto generale del Privacy Data Framework, che appare indubbiamente orientato a colmare le differenze di sicurezza e tutela dei flussi di dati personali tra USA ed EU, rispondendo più alle esigenze (pratiche) degli operatori del mercato che non a quelle, sistemiche, legate alla mancanza di una disciplina generale in tema di *data protection*. Ulteriore riprova di quanto detto può rinvenirsi avendo riguardo alle attività che caratterizzano l'intervallo di tempo di quasi 18 mesi che intercorre tra l'annuncio del marzo del 2022 e l'adozione della dichiarazione di adeguatezza della Commissione UE del luglio del 2023.

Negli USA vengono emanati l'Executive Order n. 14086 ("*Enhancing Safeguards for United States Signals Intelligence Activities*", firmato dal Presidente Biden nel mese di ottobre del 2022) ed una serie di dichiarazioni, rilasciate da diverse amministrazioni federali, riconducibili principalmente al Dipartimento per il Commercio, al Dipartimento per dei Trasporti ed al Dipartimento per la Giustizia, indirizzate tutte al consolidamento di un più completo livello di tutela per i dati personali trasferiti oltre oceano, sia sotto il profilo delle limitazioni all'accesso che sotto il profilo della possibilità di agire per la tutela giudiziale ed amministrativa in caso di trattamento illecito. Tali dichiarazioni, può già anticiparsi, saranno poi allegate alla decisione di adeguatezza, pur senza che ne sia ben chiaro, come evidenziato in dottrina, quale ne sia la reale natura e rilevanza in relazione a quest'ultima[20]. Un primo sguardo d'insieme permette di evidenziare un generale intento propositivo, indirizzato a realizzare, almeno sulla carta, un livello di *personal data protection* molto simile a quello del GDPR pur non rinnegando la matrice *profit-oriented* delle attività di raccolta e trattamento dei dati: sebbene sembri accogliere diverse indicazioni dal GDPR, la normativa USA sui dati continua a muoversi seguendo una duplice direttrice: la sicurezza nazionale ed il mercato; e tra i due poli, la persona in sé, né cittadino né consumatore, stenta a trovare il giusto posto al sole.

Per altro verso, sempre nel medesimo intervallo di tempo (marzo 2022-luglio 2023) in Europa sono state realizzate una serie di consultazioni, anche in ambito istituzionale, per analizzare se ed in quale misura il nuovo accordo potesse realmente risultare risolutivo delle criticità emerse in sede giudiziaria o se, diversamente, sia il nuovo accordo che diverse comunicazioni/dichiarazioni delle amministrazioni

[20] In argomento, cfr. A. TERRASI, *EU-US Data privacy Framework: much ado about nothing?, cit*., p. 784; ma altresì S. GERKE, D. REZAEIKHONAKDAR, *Privacy Shield 2.0 - A New Trans-Atlantic Data Privacy Framework between the European Union and the United States* in *Cardozo Law Review* 45, 2023, p. 351ss.

federali potessero rappresentare un cambiamento ed un enforcement solo apparente, senza aver realmente risolto le criticità riscontrate dalle due pronunce della CGUE. In particolare, una prima bozza della decisione di adeguatezza è stata resa pubblica in data 13.12.2022 e subito sottoposta all'EDPB che, in data 28.02.2023 ha reso il parere n. 5/2023, ponendo in risalto una serie di criticità; nelle stesse settimane, anche la "Commissione per le libertà civili, la giustizia e gli affari interni" del Parlamento Europeo aveva espresso un parere negativo, individuando come ancora attuali i rischi di interferente illecite e di controllo massivo per finalità di intelligence. In relazione alle principali questioni controverse, quali appunto il livello di sicurezza della circolazione dei dati e la protezione contro le ingerenze nella sfera privata personale e, per altro profilo, il riconoscimento di un diritto di azione contro le eventuali situazioni di abuso o trattamento illecito dei dati, l'EDPB non ha mancato di evidenziare come, sebbene in presenza di alcune innovazioni, tuttavia permangono una serie di lacune che impediscono di ritenere equivalente il livello di tutela garantito dal GDPR in raffronto a quello offerto dal DPF.

A seguito delle valutazioni dell'EDPB, la dichiarazione di adeguatezza è stata adottata con un testo che si presenta complesso ed articolato nella prima parte, con oltre 60 considerando, e molto più semplice nella seconda parte, che consta di sole 4 disposizioni.

Una delle principali innovazioni introdotte riguarda la qualificazione soggettiva delle organizzazioni USA che possono aderire al PDF ed a tal fine devono dotarsi di una certificazione ottenibile all'esito di una specifica procedura[21]; la certificazione sottende la soggezione ai poteri investigativi ed esecutivi della Federal Trade Commission e del Department of Transportation ed ha valore annuale; con riferimento alla tutela dei diritti degli interessati, viene altresì previsto che le organizzazioni certificate si dotino di sistemi di reclamo esperibili dagli interessati che assumano di aver subito una violazione dei dati o un trattamento illecito; tali sistemi interni devono essere gratuiti e prevedere procedure improntate a criteri di efficienza e celerità.

Con riferimento alle due principali criticità evidenziate dalla CGUE, pur senza entrare nel dettaglio delle indicazioni del DPF, possono riportarsi le principali linee di intervento adottate.

Con riferimento alla facoltà di monitoraggio e controllo ed all'ingerenza delle agenzie di intelligence e delle autorità federali, viene evidenziato come esse debbano avere quale base legittimante la legge o un ordine esecutivo presidenziale e debbano altresì essere giustificati da ragioni di sicurezza nazionale secondo parametri di necessità e proporzionalità degli interventi previsti. L'accesso ai dati trasferiti alle organizzazioni certificate ed allocati sui server di queste ultime sarà possibile solo in presenza di comprovati motivi ed autorizzazioni specifiche, volendo così rimuovere il rischio di attività di

[21] Sulle caratteristiche della certificazione e sulle implicazioni della stessa cfr. C. CICCIA ROMITO, *Trasferimento dei dati UE-USA: cosa prevede il Data Privacy Framework*, in QG 19 luglio 2023 (banca dati OneLegal)

sorveglianza massiva. L'Executive Order n.14086 non elide del tutto le perplessità ingenerate dall'applicazione del FISA e dall'Executive Order n.12333, tuttavia pone, almeno sulla carta, dei significativi temperamenti che dovrebbero evitare il prodursi di nuove situazioni di abuso: ogni attività di intelligence dovrebbe, infatti, essere svolta a seguito di una valutazione preventiva che consideri tutti i fattori rilevanti nonché gli interessi ed i diritti individuali potenzialmente esposti a rischi e parametri gli stessi secondo il principio di proporzionalità.

Ancora, vengono individuate e delimitate anche due categorie di obiettivi distinti in obiettivi perseguibili ed obiettivi non perseguibili; in relazione a questi ultimi sono indicate le attività che possono ostacolare la libera manifestazione del pensiero e la circolazione delle idee nonché sottendere e/o promuovere idee e programmi discriminatori e di incitamento all'odio ed alla discriminazione).

Con riferimento alla predisposizione di strumenti di ricorso (effettivo) per violazioni o trattamenti illeciti dei dati personali, per rispondere al meglio alle doglianze basate sul mancato rispetto del diritto sancito dalla Carta di Nizza all'art. 47 (diritto ad un ricorso effettivo e ad un giudice imparziale), il DPF e l'Executive Order n.14086 prevedono la possibilità di ricorrere ad un organismo nuovo ed indipendente: la *Data Protection Review Court* con competenza per tutti i trasferimenti transfrontalieri, indipendentemente dalla base giuridica utilizzata[22]. Il reclamo può essere presentato dal soggetto che assuma di aver subito un trattamento illecito e subito un danno, con riferimento ai dati personali, da parte di una impresa statunitense certificata. Come previsto dal Principio 7 lett a, n.1 del Dipartimento del Commercio, l'interessato europeo, diversamente che in passato, può quindi utilizzare una serie di strumenti che gli permettano di risolvere in tempi rapidi e con efficienza ogni controversia insorta: viene previsto un doppio binario di tutela anche se, ed è una delle principali critiche in argomento, non appare del tutto chiaro quali siano le modalità più efficienti per gli interessati in caso di violazioni non riferibili alle organizzazioni private od alle corporate ma piuttosto alle agenzie ed alle stesse istituzioni.

A margine delle linee di intervento riportate emerge un primo ordine di considerazioni: sebbene l'attenzione sia stata concentrata sulle questioni inerenti la tutela contro gli accessi potenzialmente illimitati ed indiscriminati da parte delle agenzie di intelligence e delle autorità federali, resta "sul campo" l'ulteriore questione dei limiti di circolazione dei flussi di dati per finalità economiche e commerciali delle corporate che, assumendo di volta in volta il ruolo di titolare o co-titolare, potrebbero porre in essere

[22] La circostanza che il ricorso alla *Data Protection Review Court* sia riconosciuto a tutti i soggetti che lamentano un profilo di illiceità in attività di trattamento dei propri dati personali e particolarmente per trattamenti indicati come finalizzati alla sicurezza nazionale deve interpretarsi come una declinazione del generale principio di accesso alla giustizia ed agli strumenti di tutela dei diritti e di composizione dei conflitti. In particolare, il ricorso viene riconosciuto non soltanto per i trasferimenti realizzati sulla base della decisione sulla dichiarazione di adeguatezza, ma altresì per quelli basati sugli strumenti ex artt.46 e 47 GDPR; un esempio, in argomento, può essere quello del trasferimento effettuato verso una società che non ha rinnovato od anche non ha mai presentato l'autocertificazione e che, quindi, può operare sulla base delle Clausole contrattuali standard o dei codici di condotta.

attività di cessione e vendita dei dati trasferiti, ingenerando, dopo l'arrivo dei dati nel paese terzo di destinazione, ulteriori movimenti di circolazione del tutto sconosciuti agli interessati e, con buona probabilità, anche agli stessi titolari dai quali ha avuto origine il trasferimento. Quest'ultima circostanza acquista inedito valore in considerazione di una specifica (e nuova) attività di trattamento collegata allo sviluppo ed alla diffusone dei sistemi di intelligenza artificiale.

4. Prospettive e criticità…con uno sguardo all'utilizzo dei dati personali per l'addestramento dei sistemi di intelligenza artificiale

L'ottica mercato-centrica che informa il DPF e la progressiva monetizzazione dei dati personali, con la quale anche il legislatore europeo si è recentemente trovato a confrontarsi, pongono nuovi interrogativi in relazione ad una categoria di (possibili) trattamenti ai quali i dati personali possono essere sottoposti una volta giunti nel paese terzo di destinazione: quelli relativi alla composizione dei pattern per l'addestramento dei sistemi di intelligenza artificiale. Si tratta, con tutta evidenza, di una questione nuova che solo parzialmente risponde alle logiche consolidate del trasferimento con ammissibilità dei trattamenti successivi basate sulle diverse ricostruzioni dottrinali della cd. ultrattività del consenso o del cd. utilizzo non antagonista. L'utilizzo per finalità di addestramento dei sistemi e degli strumenti AI sottende una serie di attività che comportano non soltanto quelle riferibili al *data mining*, e quindi alla estrazione della conoscenza dalla strutturazione dei dati grezzi secondo logiche e modalità prevalentemente lineari, ma altresì quelle relative alla strutturazione dei cd. BIG DATA, quindi ingenti quantitativi di dati che necessitano infrastrutture informatiche in grado di reggerne volume, varietà e velocità, ed ulteriormente quelle attività relative alla formazione dei *training dataset*, ossia i blocchi di dati per realizzare modalità di addestramento supervisionato/non supervisionato o per rinforzo od ancora "nutrire" il sistema e poi testarne le capacità di restituire output attraverso sistemi di Machine Learning (ML)[23]. Nell'ultimo anno, le questioni relative alla raccolta massiva di dati, particolarmente di dati personali, per finalità di addestramento dei sistemi e degli strumenti AI hanno richiamato l'attenzione delle Autorità Garanti per la protezione dei dati personali di diversi Stati UE, tra i quali anche l'Italia, determinando l'apertura di una serie di istruttorie per la verifica della liceità dei trattamenti e della presenza di valide basi giuridiche

[23] L'attività di addestramento dei sistemi e degli strumenti AI mediante machine learning (ML) può riassumersi, in estrema sintesi, con un percorso in cinque momenti successivi, che dalla raccolta/selezione/pulizia dei dati (creazione dei diversi dataset) porta alla creazione del modello, all'addestramento del modello (mediante i training dataset, che mediamente rappresentano il 60% dei dati raccolti), alla successiva validazione del modello (attraverso i validation set, che mediamente rappresentano il 20% dei dati raccolti e sono funzionali a verificare che il modello non incorra in situazioni di overfitting) ed alla verifica di accuratezza dello stesso (attraverso i testing set, che mediamente rappresentano l'ultimo 20% dei dati raccolti e sono funzionali a verificare che il modello restituisca output accurati anche in relazione ai nuovi dati); in caso di esito positivo della validazione e della verifica, il modello sarà poi implementato in un ambiente di produzione.

di trattamento. In particolare, il Garante Italiano, nel 2023, è stato protagonista di una controversia con Open AI, la corporate USA che ha rilasciato sul mercato le diverse versioni di ChatGPT e, più recentemente, il software AI chiamato "SORA" in grado di creare video e contenuti audiovisivi sulla base di un prompt testuale; proprio con riferimento a quest'ultimo prodotto, peraltro, dopo l'apertura di una prima istruttoria nel mese di marzo del 2024, è di pochi giorni fa la notizia di un "formale avvertimento" rivolto dalla stessa Autorità Garante ad un gruppo editoriale che avrebbe concluso un accordo per permettere l'accesso[24] alle banche dati delle proprie testate giornalistiche alla corporate USA proprio per l'addestramento di sistemi AI.

Poter disporre di sempre nuove e sempre più affidabili quantità di dati per costituire i training dataset per l'AI rappresenta un vantaggio competitivo sul mercato digitale, soprattutto guardando al rapido e, per certi versi, convulso progresso che sta accompagnando lo sviluppo dei sistemi AI e la loro diffusione sul mercato. Se a tali considerazioni correliamo quelle sulla distribuzione geografica delle Big Tech operanti nel settore dell'AI, appare chiaro come la questione del trasferimento dati, particolarmente qualora si tratti di dati personali, acquisti un rilievo del tutto nuovo e ponga dei (legittimi) dubbi sulla validità delle normative esistenti in funzione di tutela dell'interessato e dei suoi diritti. Restando nell'ambito (geografico) del presente contributo, il trasferimento transfrontaliero dei dati verso gli USA determina la concreta possibilità che i dati personali dei cittadini UE possano essere, una volta allocati sui server in territorio USA, ceduti ed utilizzati per finalità di AI, senza essere anonimizzati o sintetizzati: in questo modo essi potrebbero essere utilizzati per nutrire sistemi di Machine Learning senza che l'interessato, peraltro rimasto sull'altra sponda dell'Oceano, ne abbia cognizione e possa, eventualmente, far valere i (nuovi) rimedi in tema di violazione dei dati. Ulteriormente dovrebbe poi individuarsi entro quale limite si sia ancora in presenza di un dato sul quale insistono i diritti dell'interessato e quando, invece, si sia in presenza di un pattern o di un dataset sul quale insistono dei diritti dello sviluppatore e/o del titolare od ancora del soggetto che ha richiesto ed assume su di sé i rischi dell'attività di addestramento AI.

Su tutte queste considerazioni, emerge il dubbio sulla opportunità di individuare una normativa diversa, con tutele dei diritti degli interessati che siano rafforzate in caso di trasferimenti finalizzati, o che possano comportare, tramite successivi trasferimenti, l'impiego per addestramento AI; parimenti, emerge una rafforzata esigenza di chiarezza e trasparenza da parte dei titolari che raccolgono i dati e da parte di quelli, successivi, che li ricevono in trasferimento o cessione.

[24] Dalle notizie di stampa non emerge con chiarezza la natura del rapporto tra il gruppo editoriale e Open AI: se i titoli più espliciti parlano di "vendita di dati", il comunicato del Gruppo editoriale parla in modo più generico di "permettere l'accesso agli utenti di ChatGPT ai contenuti in lingua italiana degli archivi di un prestigioso gruppo editoriale", senza specificare se tale accesso e la correlata possibilità di utilizzare i dati contenuti negli archivi digitali siano oggetto di un rapporto a titolo oneroso e/o siano previste altre e diverse modalità di controprestazioni (sul punto possono consultarsi le notizie presenti sul sito del quotidiano Ilsole24ore .ultimo accesso in data 02.12.2024)

Ravvisando una finalità di addestramento dei sistemi AI, diventa ancora più forte la necessità di tutela dei cittadini europei nei confronti di un sistema normativo, quale quello statunitense, che offre ancora standard non ottimali e che, sebbene sembri aver inaugurato un nuovo corso, individuando il perimetro delle attività e degli obiettivi consentiti con riferimento alle attività di intelligence ed ai rischi connessi alla sorveglianza massiva, rischia tuttavia di lasciare privi di tutele adeguate gli interessati/cittadini europei con riferimento ad altri utilizzi determinati da logiche di mercato.

Accanto alle possibili ipotesi di un nuovo intervento della CGUE per l'eventuale (e da più parti preconizzato) caso Scherms III, pertanto, sarebbe opportuno avviare un dialogo finalizzato all'implementazione delle tutele per le attività a rilevanza economica e collegate alle creazione dei training dataset per l'addestramento dei sistemi di intelligenza artificiale, ad esempio chiedendo delle espresse indicazioni alle imprese che intendono certificarsi e che hanno tra le proprie attività o finalità di trattamento l'addestramento AI; l'evoluzione del mercato e della tecnologia rendono necessarie nuove forme di tutele e rinnovata attenzione per evitare che il rafforzamento delle tutele contro le ingerenze provenienti dalle organizzazioni e dalle agenzie di intelligence non faccia dimenticare la necessità di tutela contro le ingerenze e i possibili abusi provenienti dal mercato. La tutela degli interessati/cittadini europei deve necessariamente indirizzarsi in entrambe le direzioni, anche per scongiurare l'eventualità di una carenza di tutela nel caso, non auspicabile ma non imprevedibile, di commistioni e situazioni ibride tra istituzioni e mercato, che potrebbero esporre a rischi ben più significativi le dimensioni individuali della data protection ma altresì la stessa libera circolazione dei flussi di dati.