



## La Dichiarazione europea sui diritti e principi digitali, il Trans-Atlantic Data Privacy Framework e l'Unione Federale dei consumatori tedeschi contro Meta Platforms Ireland\*

di Flavia Zorzi Giustiniani\*\*

Il **26 gennaio** scorso la Commissione europea ha proposto al Parlamento europeo e al Consiglio l'adozione di una dichiarazione solenne congiunta sui diritti e principi digitali<sup>1</sup>. La dichiarazione, come enfatizzato nella scheda informativa che accompagna il progetto, “è la prima al mondo nel suo genere”<sup>2</sup>. Essa intende fissare dei parametri che guidino l'Unione nella trasformazione digitale al fine di realizzare una società inclusiva, prospera e sostenibile<sup>3</sup> secondo un modello imperniato non soltanto sui valori dell'Unione europea ma anche sulle persone<sup>4</sup>. Il *draft* è stato pubblicato in esito ad una consultazione pubblica volta a raccogliere le opinioni di tutte le parti interessate quali in particolare gli Stati membri, le autorità regionali e locali, le organizzazioni non governative e della società civile, le associazioni di imprese e le imprese, i cittadini.

Questa iniziativa, che ha subito una forte accelerazione a seguito della crisi pandemica e del ritmo impresso da quest'ultima alla digitalizzazione, è il compimento di un processo inteso a facilitare i cittadini dell'Unione nel trarre il massimo vantaggio dalla trasformazione digitale. Più specificatamente, l'iniziativa recepisce anzitutto le richieste del Parlamento europeo di modellare il futuro digitale nel rispetto di diritti fondamentali quali la protezione dei dati o la non discriminazione, nonché di principi quali la neutralità tecnologica e della rete e l'inclusività<sup>5</sup>. In secondo luogo, essa dà seguito a iniziative precedenti del Consiglio, come da ultimo la dichiarazione di Lisbona del giugno 2021 concernente un modello di trasformazione digitale che

\*Contributo sottoposto a *peer review*.

\*\* Professoressa associata di Diritto dell'Unione europea presso l'Università degli Studi “Link Campus University” di Roma.

<sup>1</sup> Commissione europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali, COM(2022) 27 final, 26.01.2022.

<sup>2</sup> Commissione europea, Diritti e principi digitali, gennaio 2022, p. 1.

<sup>3</sup> Cfr. Commissione europea, Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, COM(2022) 28 final, Bruxelles, 26.1.2022.

<sup>4</sup> Per un'analisi puntuale del progetto di dichiarazione si rinvia a P. De Pasquale, Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?, 17 marzo 2022, disponibile al link [http://www.dirittounioneeuropea.eu/Tool/Evidenza/Single/view\\_html?pid\\_evidenza=1355](http://www.dirittounioneeuropea.eu/Tool/Evidenza/Single/view_html?pid_evidenza=1355).

<sup>5</sup> Cfr. Parlamento europeo, Il futuro digitale dell'Europa: mercato unico digitale e uso dell'IA per i consumatori europei. Risoluzione del Parlamento europeo del 20 maggio 2021 sul tema «Plasmare il futuro digitale dell'Europa: eliminare gli ostacoli al funzionamento del mercato unico digitale e migliorare l'uso dell'IA per i consumatori europei» (2020/2216(INI)).

rafforzi la dimensione umana dell'ecosistema digitale e sia imperniato sul mercato unico digitale<sup>6</sup>.

Il progetto di dichiarazione è suddiviso in sei capitoli, che corrispondono agli obiettivi da perseguire *in subiecta materia* secondo la Commissione, ovvero: mettere le persone al centro della trasformazione digitale; solidarietà e inclusione; libertà di scelta; partecipazione allo spazio pubblico digitale; sicurezza, protezione e conferimento di maggiore autonomia e responsabilità; sostenibilità<sup>7</sup>.

Il documento è stato concepito nel duplice intento di essere, per tutti, un chiaro punto di riferimento sul tipo di trasformazione digitale che l'Europa promuove e di fornire, ai responsabili politici e alle aziende, delle linee guida nell'utilizzo delle nuove tecnologie. Non stupisce pertanto che esso, come precisato dallo stesso progetto di dichiarazione e dalla relativa comunicazione della Commissione, abbia un valore “meramente” politico e non giuridico.

Quanto al suo contenuto, il progetto di dichiarazione compendia in un unico testo i principi e i valori della UE rilevanti nel campo digitale, a partire da quelli affermati dalla Corte di Giustizia nella sua giurisprudenza recente. Il documento si basa segnatamente sul diritto primario della UE, di cui riafferma vari principi, quali *in primis* la solidarietà, che vengono adattati al contesto digitale. Tra i nuovi principi digitali figurano invece, tra gli altri, quelli relativi all'interazione con gli algoritmi e l'intelligenza artificiale. Al riguardo viene anzitutto garantita la trasparenza e l'uguaglianza nell'uso degli algoritmi e dell'intelligenza artificiale; è altresì impedita la predeterminazione delle scelte. Conseguentemente, si afferma che “ogni persona dovrebbe essere messa nelle condizioni di godere dei benefici offerti dall'intelligenza artificiale facendo le proprie scelte informate nell'ambiente digitale, e rimanendo al contempo protetta dai rischi e dai danni alla salute, alla sicurezza e ai diritti fondamentali”<sup>8</sup>.

Il documento dovrebbe essere discusso e approvato dal Parlamento europeo e dal Consiglio entro l'estate prossima. La Commissione effettuerà poi, con cadenza annuale, una valutazione dell'attuazione dei principi digitali nella relazione sullo “stato del decennio digitale” e un'indagine Eurobarometro al fine di monitorare le misure di *follow-up* adottate dagli Stati membri.

Il **25 marzo** la Commissione europea e gli Stati Uniti d'America hanno annunciato la conclusione del *Trans-Atlantic Data Privacy Framework*, un accordo “di principio” che, giunto dopo più di un anno di trattative, intende stabilire nuove basi per il trasferimento dei dati personali dei residenti dell'Unione oltre Atlantico. L'accordo, nelle parole della Presidente della Commissione Ursula Von Der Leyen, consentirà “predictable and trustworthy data flows” tra l'Unione e gli Stati Uniti sulla base di un nuovo bilanciamento tra sicurezza e diritti alla privacy e alla protezione dei dati personali<sup>9</sup>.

Com'è noto, la Grande Sezione della Corte di Giustizia europea (di seguito CGE) il 16 luglio 2020, nel caso Schrems II, aveva dichiarato invalida la decisione della Commissione 2016/1250<sup>10</sup>.

<sup>6</sup> Cfr. Lisbon Declaration – Digital Democracy with a Purpose, 1° giugno 2021, disponibile al link <https://futurium.ec.europa.eu/en/digital-compass/digital-principles/library-video/lisbon-declaration-digital-democracy-purpose?language=it>.

<sup>7</sup> A ciascun obiettivo corrisponde uno specifico capitolo del progetto di dichiarazione.

<sup>8</sup> Commissione europea, Dichiarazione cit., p. 3.

<sup>9</sup> Cfr. Commissione europea, Statement by President von der Leyen with US President Biden, Bruxelles, 25 marzo 2022, p. 1.

<sup>10</sup> Cfr. Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy.

Mediante tale atto la Commissione aveva stabilito l'adeguatezza del sistema di trasferimento dei dati tra UE e USA detto *Privacy Shield* per violazione dell'art. 45.1 del regolamento 2016/679 (cd. GDPR)<sup>11</sup> alla luce dei diritti al rispetto della vita privata e familiare, alla protezione dei dati personali e a un ricorso effettivo come affermati dagli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea. Secondo la CGE infatti tale sistema, come il precedente *Safe Harbor* (ritenuto adeguato dalla Commissione con la decisione 2000/520<sup>12</sup>), ratificava il primato delle esigenze di sicurezza nazionale rispetto ai diritti fondamentali delle persone i cui dati personali erano trasferiti senza prevedere alcun limite né garanzie di tutela per gli interessati. A seguito di tale sentenza il flusso di dati trasferiti dall'Unione agli USA non si era interrotto ma, in assenza di una valida e stabile base giuridica, l'iter da seguire per gli esportatori di dati è divenuto, ed è tuttora, più lungo e difficoltoso. I *data exporters* si sono visti costretti, volta volta, ad adottare misure supplementari ex art. 46 GDPR per garantire quantomeno un livello *minimo* di protezione che sia equivalente a quello richiesto dalla normativa europea secondo i dettami dei giudici di Lussemburgo<sup>13</sup>.

Il *Trans-Atlantic Data Privacy Framework* prevede che i dati potranno fluire liberamente e in sicurezza tra le aziende partecipanti dell'Unione europea e degli Stati Uniti, sulla base di nuove regole che limiteranno l'accesso ai dati da parte dell'intelligence statunitense ai soli casi in cui l'accesso si riveli necessario e proporzionato al fine di proteggere la sicurezza nazionale<sup>14</sup>. Le agenzie di intelligence saranno chiamate ad adottare procedure per garantire un controllo efficace della privacy e il rispetto delle norme sulle libertà civili. Le aziende americane che trattano dati personali provenienti dalla UE dovranno invece autocertificare la propria adesione ai principi del *Privacy Shield* attraverso il Dipartimento del Commercio statunitense<sup>15</sup>. È poi prevista la creazione, da parte statunitense, di un meccanismo di ricorso multi-livello che includa un tribunale di revisione della protezione dei dati indipendente al quale potranno rivolgersi i residenti della UE.

L'accordo di principio non è ancora operativo e per divenire tale dovrà essere traslato in atti giuridici ufficiali. Da parte statunitense ciò avverrà allorché gli impegni assunti prenderanno la forma di un atto interno, ovvero più specificamente, come annunciato dalla Casa Bianca, di un decreto esecutivo (*executive order*). Successivamente, e in base al contenuto di tale atto statunitense, la Commissione europea adotterà poi una nuova decisione di adeguatezza che diventerà la base

<sup>11</sup> L'art. 45 GDPR, recante «Trasferimento sulla base di una decisione di adeguatezza», così dispone: «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».

<sup>12</sup> Decisione della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti.

<sup>13</sup> Al riguardo il Comitato europeo per la protezione dei dati personali ha adottato la Raccomandazione n. 2/2020 sulle misure supplementari per i trasferimenti di dati e, in data 22 febbraio 2022, le Linee Guida n. 4/2021 sui codici di condotta come strumenti per i trasferimenti verso paesi terzi o organizzazioni internazionali.

<sup>14</sup> I principi cardine dell'accordo di principio sono stati resi pubblici sia dalla Commissione europea (si veda [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_22\\_2087](https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087)) sia, in modo invero più dettagliato, dalla Casa Bianca (<https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/>).

<sup>15</sup> Va sottolineato che la Corte di Giustizia non ha invalidato il *Privacy Shield* bensì la relativa decisione di adeguatezza della Commissione. Ne consegue che, nella misura in cui non saranno modificati dalla normativa di attuazione del nuovo *Privacy Framework*, i principi affermati nel *Privacy Shield* rimangono validi.

giuridica per il trasferimento dei dati verso gli USA. Solo al termine di tale processo, che probabilmente richiederà diversi mesi, sarà possibile valutare appieno la portata delle modifiche introdotte al *Privacy Shield*. Si deve tuttavia rimarcare che, al fine di colmare le patenti inadeguatezze del quadro normativo statunitense in materia di tutela della vita privata, recentemente evidenziate dalla sentenza della Corte Suprema nel caso *FBI v. Fazaga*<sup>16</sup>, che ha confermato lo *state secrets privilege*, l'*executive order* non appare uno strumento idoneo. Per evitare l'ennesima bocciatura della Corte di Lussemburgo sarebbe invero necessario che il Congresso procedesse per via legislativa ad una più ampia riforma del settore.

Un ultimo sviluppo degno di nota si deve infine alla CGE, che il **28 aprile** si è pronunciata nella causa C-319/20, relativa a un rinvio pregiudiziale presentato dalla Corte federale tedesca (Bundesgerichtshof) nella controversia intentata dall'associazione dei consumatori "Unione federale delle centrali e delle associazioni di consumatori" (di seguito "Unione federale") contro Meta Platforms Ireland Limited, già Facebook Ireland Limited. Il giudice del rinvio aveva chiesto alla CGE se il capo VIII del GDPR, e in particolare l'art. 80, par. 1 e 2, nonché l'art. 84, par. 1 di tale regolamento, ostino a norme nazionali, le quali conferiscano, da un lato, ai concorrenti e, dall'altro, ad associazioni, organismi ed organi camerali legittimati in base alla normativa nazionale il potere di agire, in caso di violazioni del GDPR, contro l'autore della violazione, indipendentemente dalla lesione di diritti specifici di singoli interessati e in assenza di un mandato dell'interessato, proponendo un ricorso dinanzi ai giudici civili fondato sul divieto di pratiche commerciali sleali, o sulla violazione di una legge di tutela dei consumatori, o sul divieto di applicare condizioni generali di contratto nulle.

Il rinvio ha origine nell'azione inibitoria intentata dall'Unione Federale contro la *Meta Platforms Ireland* per aver asseritamente violato, nell'ambito della messa a disposizione degli utenti di giochi gratuiti forniti da terzi, delle norme relative alla protezione dei dati personali, alla lotta contro la concorrenza sleale e alla tutela dei consumatori. La Bundesgerichtshof si interrogava sulla ricevibilità di tale azione a seguito dell'entrata in vigore del GDPR. Rimarcava poi come il testo del GDPR sembri implicare che la verifica dell'applicazione dello stesso spetta principalmente alle autorità di controllo.

Nella sua pronuncia la CGE, conformandosi all'opinione dell'Avvocato Generale de la Tour<sup>17</sup>, ha risposto in modo pienamente affermativo alla questione pregiudiziale posta dal giudice del rinvio. Ha pertanto constatato che il GDPR non osta ad una normativa nazionale, la quale permetta ad un'associazione di tutela degli interessi dei consumatori di agire in giudizio, in assenza di un mandato che le sia stato conferito a questo scopo e indipendentemente dalla violazione di specifici diritti degli interessati, contro il presunto autore di un atto pregiudizievole per la protezione dei dati personali, facendo valere la violazione del divieto delle pratiche commerciali sleali, la violazione di una legge in materia di tutela dei consumatori o la violazione del divieto di utilizzazione di condizioni generali di contratto nulle, qualora il trattamento dei dati in questione

<sup>16</sup> Cfr. Corte Suprema degli Stati Uniti d'America, *Federal Bureau of Investigation et al. v. Fazaga et al. Certiorari to the United States Court of Appeals for the Ninth Circuit*, 4 marzo 2022.

<sup>17</sup> Cfr. le Conclusioni dell'Avvocato Generale Jean Richard de la Tour presentate il 2 dicembre 2021 nella causa C-319/20.

sia idoneo a pregiudicare i diritti che delle persone fisiche identificate o identificabili si vedono riconosciuti dal GDPR.

Preliminarmente, la Corte ha osservato che il GDPR intende garantire un'armonizzazione in linea di principio completa delle normative nazionali in materia di protezione dei dati personali. Tuttavia, alcune disposizioni dello stesso offrono agli Stati membri la possibilità di prevedere norme nazionali supplementari che lascino a questi ultimi un margine di discrezionalità circa il modo in cui tali disposizioni possono essere attuate, a condizione che tali norme non pregiudichino il contenuto e gli obiettivi del regolamento summenzionato. In proposito, gli Stati membri hanno in particolare la possibilità di prevedere un meccanismo di azione rappresentativa contro il presunto autore di un atto pregiudizievole per la protezione dei dati personali, fissando al contempo un certo numero di requisiti che devono essere rispettati<sup>18</sup>.

Quanto al campo di applicazione *ratione personae* di un tale meccanismo, la Corte ha sottolineato anzitutto che un'associazione per la tutela degli interessi dei consumatori, come l'Unione federale, rientra nella nozione di "organismo legittimato ad agire" ai sensi del GDPR giacché persegue un obiettivo di interesse pubblico consistente nell'assicurare i diritti dei consumatori<sup>19</sup>. La violazione di norme relative alla tutela dei consumatori o alle pratiche commerciali sleali può infatti essere correlata alla violazione di una norma relativa alla protezione dei dati personali<sup>20</sup>. Nel senso che l'art. 80 GDPR non impedisce l'esercizio di azioni rappresentative complementari nel settore della tutela dei consumatori depongono anche, secondo la CGE, vari elementi della direttiva 2020/1828 in materia di azioni rappresentative<sup>21</sup>, che pure non è applicabile alla controversia di cui al procedimento principale e il cui termine di trasposizione non è ancora scaduto.

La CGE ha evidenziato, poi, che l'instaurazione di un'azione rappresentativa presuppone soltanto che un ente rispondente ai requisiti menzionati all'art. 80.1 GDPR, indipendentemente da qualsiasi mandato che gli sia stato conferito, *ritenga* che i diritti di un interessato previsti dal Regolamento siano stati violati a seguito del trattamento dei suoi dati personali, senza che sia necessario identificare, individualmente e preliminarmente, la persona specificamente interessata dal suddetto trattamento di dati ed allegare l'esistenza di una specifica violazione dei diritti riconosciuti dalle norme in materia di protezione dei dati<sup>22</sup>. L'art. 80.2 GDPR lascia invero un certo margine di discrezionalità agli Stati membri al riguardo, a patto che una tale azione senza mandato sia prevista dalla normativa nazionale. Un'interpretazione siffatta è inoltre conforme all'obiettivo perseguito dal GDPR, che consiste nell'assicurare un elevato livello di protezione dei dati personali<sup>23</sup>.

La sentenza in oggetto è stata da più parti definita rivoluzionaria per le sue implicazioni in materia di protezione dei dati e avrà con tutta probabilità un impatto significativo sul *modus operandi* delle aziende interessate: tra queste ultime, quelle che non l'hanno ancora fatto saranno

<sup>18</sup> Cfr. il par. 63 della sentenza.

<sup>19</sup> Cfr. il par. 65 della sentenza.

<sup>20</sup> Cfr. il par. 66 della sentenza.

<sup>21</sup> Cfr. direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, del 25 novembre 2020, relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE.

<sup>22</sup> Cfr. il par. 72 della sentenza.

<sup>23</sup> Cfr. i par. 73-74, 76 della sentenza.

infine indotte a rispettare le prescrizioni del GDPR. Nondimeno, la pronuncia evidenzia, senza risolverle, le problematiche derivanti da un'attuazione parallela sul piano nazionale del GDPR e della direttiva 1828/2020<sup>24</sup>. Quest'ultima, il cui termine di trasposizione è fissato per il 25 dicembre 2022, si limita a prevedere degli standard minimi per gli enti qualificati ad instaurare azioni transfrontaliere, con il rischio che la diversità delle normative nazionali applicabili renda più difficoltoso, se non in alcuni casi impossibile, per gli enti non profit avviare un'azione; ciò soprattutto allorché la legislazione nazionale pone dei requisiti più stringenti di quelli richiesti dal GDPR o dalla stessa direttiva 1828.

---

<sup>24</sup> Sul punto si vedano in particolare le osservazioni critiche di: A. Pato, *GDPR Collective Litigation Against Facebook*, 18 maggio 2022, disponibile al link <https://verfassungsblog.de/gdpr-collective-litigation-against-facebook/>; P. Jain, *Standing of Non-Profit Associations or Consumer Associations to File Collective Actions without a Data-Subjects Mandate: Case C-319/20 Meta Platforms*, 16 maggio 2022, disponibile al link <https://europeanlawblog.eu/2022/05/16/standing-of-non-profit-associations-or-consumer-associations-to-file-collective-actions-without-a-data-subjects-mandate-case-c-319-20-meta-platforms/>.