https://doi.org/10.6092/issn.1825-1927/22301 ISSN 1825-1927

Bindl vs Commissione Europea (T-354/22)

Un crocevia per la cittadinanza digitale europea?

Guido Gorgoni [1]

[1] University of Padova, Italy

Nella prima sentenza del 2025 il Tribunale dell'UE si è pronunciato (in composizione ampliata) sul caso *Bindl* v. *Commissione Europea* (T-354/22)[1], la cui rilevanza emergerà certamente solo col passare del tempo, ma che può già segnalarsi quale importante crocevia per la costruzione della cittadinanza digitale europea, non solo per il suo statuto inaugurale – trattandosi della prima decisione del 2025, proclamato dal Consiglio d'Europa anno europeo dell'educazione alla cittadinanza digitale[2].

Si tratta della prima pronuncia relativa alle condizioni per l'esercizio dei ricorsi diretti nell'ambito del regolamento (UE) 2018/1725 (EUDPR), sulla protezione dei dati personali per le istituzioni dell'Unione, fonte per le istituzioni europee omologa del regolamento generale sulla protezione dei dati 2016/679 (GDPR). Nella pronuncia il Tribunale ha ravvisato che la Commissione non ha rispettato le condizioni poste dal diritto dell'Unione per il trasferimento, da parte di un'istituzione, di un organismo o di un organismo dell'Unione, di dati personali verso un paese terzo, condannandola a un risarcimento dei danni di modestissima entità economica, respingendo le altre domande, ma che potrebbe avere risvolti positivi possono avere ben più grande valore simbolico e pratico.

Vorremmo commentare la la decisione non tanto sotto il profilo della configurabilità della responsabilità delle istituzioni europee per il rispetto delle norme riguardanti il trasferimento dei dati personali all'infuori dell'UE, che rappresentano la vicenda al centro della decisione, bensì sotto il profilo dello sviluppo dello status di cittadinanza digitale Europea, quale sarebbe emergere dalla giurisprudenza della Corte di Giustizia[3], sulla scia delle decisioni nei casi *Schrems I* e *Schrems II*[4], alle quali è direttamente legata – almeno sotto il profilo in esame.

Le due note pronunce si inseriscono infatti nella più ampia giurisprudenza della Corte relativa alla protezione dei dati, nella quale sembra possibile leggere lo sviluppo del nucleo fondamentale della cittadinanza digitale europea[5], nella quale la figura del *data subject*, sembra assurgere allo status di cittadino digitale grazie a una lettura "costituzionale" dei suoi diritti alla luce del diritto fondamentale alla protezione dei dati personali, in

guido.gorgoni@unipd.it (Guido Gorgoni);
(Guido Gorgoni);

1. Case C-311/22, *Thomas Bindl* v. *European Commission*, EU:T:2025:4.
2. https://www.coe.int/en/web/education/european-year-of-digital-citizenship-education-2025.
3. A. Iliopoulou-Penot, *The construction of a European digital citizenship in the case law of the Court of Justice of the EU*, «Common Market Law Review» 59/4 (2022) 969-1006.
4. Case C-362/14, *Maximillian Schrems* v. *Data Protection Commissioner*, EU:C:2015: 650 (*Schrems I*); Case C-311/18, *Data Protection Commissioner* v. *Facebook Ireland Ltd, Maximillian Schrems*, EU:C:2020:559 (*Schrems II*).
5. A. Iliopoulou-Penot, *The construction of a European digital citizenship in the case law of the Court of Justice of the EU*

particolare sulla scorta dei principi affermati nella storica decisione *Digital Rights Ireland*[6] e nella giurisprudenza successiva (casi *Tele2*[7] e *La Quadrature du Net*[8]) nelle quali la Corte si schierava a favore dei diritti fondamentali del cittadino europeo, tramite un'interpretazione delle norme sulla *data retention* alla luce dei diritti fondamentali del cittadino europeo.

Le due decisioni nei casi *Schrems* – come noto – hanno riaffermato con forza il diritto alla protezione dei dati personali nel caso di trasferimenti di dati personali extra UE, portando all'annullamento delle norme che regolavano il trasferimento dei dati con gli Stati Uniti d'America, il *Safe Harbour Framework*[9] e il *Privacy Shield Framework*[10], invalidando le relative decisioni di adeguatezza della Commissione Europea in quanto prive di adeguate garanzie per i diritti legati alla protezione dei dati personali del cittadino europeo. In particolare, nei due casi la Corte ha interpretato le norme rispettivamente della Direttiva 95/46 (nel caso *Schrems I*) e del GDPR (nel caso *Schrems II*) alla luce degli articoli 7 (diritto alla privacy) e 8 (diritto alla protezione dei dati personali) della Carta dei diritti fondamentali dell'Unione Europea, rilevando inoltre la violazione dell'articolo 47 della stessa Carta (Diritto a un ricorso effettivo e a un giudice imparziale).

Si tratta di profili che sono egualmente implicati dalla decisione in esame. Mentre però in quei casi ad essere censurata era la valutazione di adeguatezza degli standard di protezione dei dati operata dalla Commissione nei confronti degli USA, nel caso in esame si trattava di analizzare l'adeguatezza della protezione rispetto a trasferimenti di dati negli USA resi possibili dalla stessa Commissione. A essere sottoposte a giudizio erano dunque non soltanto le regole che presiedevano, nel caso di specie, a tali trasferimenti ma anche gli atti della Commissione di cui veniva contestata la legittimità.

L'interesse della vicenda sta proprio nel suo essere in continuità con quella giurisprudenza; come è dato leggere nella sintesi ufficiale fornita dall'ufficio stampa della Corte di Giustizia: *"*il Tribunale si pronuncia, in maniera inedita, sull'interpretazione delle disposizioni del regolamento 2018/1725 *e trae, per la prima volta, le conseguenze della giurisprudenza cosiddetta «Schrems II»"* nell'ambito dell'applicazione di tale regolamento nonché del «principio» di interpretazione omogenea delle disposizioni analoghe dei regolamenti 2016/679 e 2018/1725*,* anche se in realtà i commenti sin qui apparsi sottolineano gli aspetti critici, indubbiamente presenti, della decisione[11].

La pronuncia nasce dal ricorso di Thomas Bindl, cittadino tedesco, il quale nel 2021 e nel 2022 aveva visitato a più riprese il sito web della Commissione europea relativo alla "Conferenza sul futuro dell'Europa" (https://futureu.europa.eu); successivamente, il 30 marzo 2022, egli si è registrato all'evento "GoGreen" utilizzando il proprio account Facebook, visitando nuovamente il sito web l'8 giugno 2022. Durante la navigazione, il richiedente ha osservato connessioni a fornitori terzi, in particolare Amazon Web Services (AWS) con sede negli Stati Uniti. Il 9 novembre 2021, il richiedente ha inviato un'e-mail al Responsabile della Protezione dei Dati della Commissione, chiedendo informazioni sul trattamento e sul potenziale trasferimento dei suoi dati personali verso paesi terzi. La Commissione ha risposto il 3 dicembre 2021, affermando che i suoi dati erano trattati da AWS EMEA SARL, con sede in Lussemburgo, e che non erano avvenuti trasferimenti di dati al di fuori dell'UE. Non soddisfatto della risposta, il richiedente ha inviato un'ulteriore richiesta il 1° aprile 2022, chiedendo informazioni dettagliate sul trattamento e sui trasferimenti dei dati, inclusa la copia dei propri dati conservati da terze parti come Facebook. La Commissione ha risposto il 30 giugno 2022, indicando che la sua

6. Joined Cases C-293 & 594/12, *Digital Rights Ireland and Seitlinger and others*, EU:C:2014:238.

7. Joined Cases C-203 & 698/15, *Tele2 Sverige AB* v. *Post-och telestyrelsen and Secretary of State for the Home Department* v. *Tom Watson, Peter Brice and Geoffrey Lewis*, EU:C:2016:970.

8. Joined Cases C-511, 512 & 520/18, *La Quadrature du Net* v. *Premier ministre and others*, EU:C:2020:791,

9. Commission Decision 2000/520 of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, O.J. 2000, L 215/7.

10. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield, O.J. 2016, L 207/1.

11. A. Miglio, *Op-Ed: "If you sign in to an EU Website using a Social Media Account, the Commission owes you Damages (Case T- 354/22, Bindl)"*,; A. Fiorentini, *L'illusorietà del diritto a un ricorso effettivo nell'ambito del regolamento (UE) 2018/1725: note a margine della sentenza Bindl c. Commissione*, «Rivista del Contenzioso Europeo» 1 (2025) 1-10; A. Lucchini, *Privacy violata, l'Ue sanziona sé stessa: impatti della sentenza Bindl*, 17 febbraio 2025

richiesta di aprile 2022 era pressoché identica a quella precedente del novembre 2021, alla quale era già stato risposto.

Di conseguenza, il 9 giugno 2022, il sig. Bindl ha introdotto un ricorso dinanzi al Tribunale, avanzando tre richieste:

1. l'annullamento dei trasferimenti dei suoi dati personali verso paesi terzi privi di adeguata protezione.

2. La dichiarazione dell'illecita omissione da parte della la Commissione di rispondere in merito alla sua richiesta di informazioni del 1° aprile 2022.

3. Infine ha presentato tre domande di risarcimento danni relativi a: a) la violazione del diritto di accesso; b) il trasferimento di dati personali all'infuori dell'UE; c) i trasferimenti verificatisi in occasione dell'iscrizione all'evento "GoGreen" tramite Facebook.

Poiché all'epoca dei fatti non esisteva una decisione di adeguatezza ai sensi dell'art. 45, par. 3, GDPR, il trasferimento di dati personali verso un paese terzo poteva avvenire solo se la Commissione, in qualità di titolare del trattamento, avesse fornito garanzie adeguate ai sensi dell'art. 48 EUDPR. Il Tribunale ha dichiarato irricevibili sia il ricorso di annullamento, ovvero la prima delle richieste, sia il ricorso in carenza per l'omissione della Commissione, ritenuti entrambi privi di oggetto. Solo la domanda di risarcimento danni per il trasferimento illecito di dati personali all'infuori UE è stata parzialmente accolta, mentre l'azione di annullamento e il ricorso in carenza sono stati dichiarati irricevibili. Come è stato osservato, in sostanza il ricorrente si è visto negare ogni possibilità di contestare in modo effettivo la condotta della Commissione[12].

Infatti, i trasferimenti di dati asseritamente avvenuti in occasione della consultazione del sito sono stati qualificati dai giudici come "atti materiali e non giuridici" (paragrafo 33), cui l'istituzione non ha voluto conferire effetti giuridici vincolanti e, pertanto, non rientranti nella categoria degli atti impugnabili: "i trasferimenti controversi non sono atti della Commissione produttivi di effetti giuridici vincolanti, vale a dire non sono destinati a disciplinare una situazione giuridica e, come risulta dalla loro stessa natura, la Commissione non ha affatto avuto l'intenzione di conferire ad essi tali effetti" (paragrafo 33). La conclusione, giustamente criticata per il suo formalismo[13], è che "i trasferimenti controversi non sono idonei a produrre effetti giuridici vincolanti idonei ad incidere sugli interessi del ricorrente, modificando in misura rilevante la sua situazione giuridica, conformemente alla giurisprudenza richiamata" (paragrafo 34).

Riguardo al ricorso relativo al presunto comportamento omissivo da parte della commissione, i giudici ritengono che con la risposta del 30 giugno 2022 si sia posto fine alla carenza, essendo irrilevante e la circostanza che tale presa di posizione dell'istituzione non dia soddisfazione alla parte ricorrente, in quanto l'articolo 265 TFUE riguarda la carenza per astensione dal pronunciarsi o dal prendere posizione e non l'adozione di un atto diverso da quello che tale parte avrebbe desiderato o ritenuto necessario" (paragrafi 41-42), confermando così l'interpretazione estensiva di tale nozione adottata nella giurisprudenza del giudice europeo, che ritiene che rientrino nella nozione di "presa di posizione" anche le risposte delle istituzioni che non soddisfano il richiedente.

Per ciò che riguarda le richieste di risarcimento dei danni, il Tribunale si richiama al principio di effettività del danno, che dev'essere reale e certo, circostanza che dev'essere provata dalla parte ricorrente, mentre un danno puramente ipotetico e indeterminato non dà diritto a risarcimento (paragrafi 53-54). La prima di tali richieste è stata respinta sulla base di considerazioni puramente formali in quanto essa era "fondata sulla violazione del diritto di accesso alle informazioni e non su quella delle disposizioni relative al trasferimento di dati personali verso paesi terzi" (paragrafo 71).

Constatando che "alla data dei trasferimenti controversi, non esisteva alcuna decisione di adeguatezza, ai sensi dell'articolo 47 del regolamento 2018/1725, per quanto riguarda gli Stati Uniti" né altra clausola standard di protezione dei dati o altra clausola contrattuale (paragrafo 100), ne risultava un vuoto normativo così che la disciplina del collegamento ipertestuale «connettersi con Facebook» proposta sul sito Internet di EU Login

12. A. Fiorentini, *L'illusorietà del diritto a un ricorso effettivo nell'ambito del regolamento (UE) 2018/1725: note a margine della sentenza Bindl c. Commissione*

13. *Ivi*

risultava essere regolata unicamente dalle condizioni generali di Facebook. Il vuoto normativo si sostanziava in un vuoto di diritto o meglio nella violazione dei diritti fondamentali del cittadino digitale europeo, così come definiti dalla Carta dei Diritti fondamentali, dal GDPR e dalla giurisprudenza comunitaria.

Interessante appare quanto i giudici scrivono a proposito degli articoli 7 e 8 della Carta dei Diritti Fondamentali dell'UE: "[le] disposizioni del regolamento 2018/1725 concretizzano diritti fondamentali, come quelli stabiliti agli articoli 7 e 8 della Carta, e mirano nel loro insieme a garantire la continuità del livello elevato di protezione dei dati personali in caso di trasferimento di tali dati verso paesi terzi o organizzazioni internazionali" e che tali disposizioni "mirano a tutelare l'interesse *individuale* delle persone interessate e costituiscono quindi norme giuridiche preordinate a conferire diritti ai singoli, ai sensi della giurisprudenza richiamata al precedente punto 50." (paragrafi 106-107).

Ci pare di poter dire che i diritti sanciti agli artt. 7 e 8 della Carta si collocano oltre il solo interesse individuale, nella misura in cui la protezione dei dati personali tutela non solo i singoli presi isolatamente, ma i singoli anche – e forse soprattutto – in quanto membri di una collettività, che si tratti di un gruppo[14] o che si tratti della cittadinanza nel suo insieme. Questo dà ragione del perché la pronuncia in esame trascende il caso da cui origina: non solo contribuisce – in attesa del prevedibile appello – a definire i contenuti di diritti e doveri nel caso di specie, bensì nel decidere sul caso singolo dice qualcosa sulla cittadinanza digitale più in generale.

Appare in questo senso criticabile[15] l'opinione secondo cui "è il comportamento del ricorrente che deve essere considerato come la causa diretta e immediata del danno morale lamentato e non l'illecito asseritamente commesso dalla Commissione utilizzando il servizio Amazon CloudFront. Pertanto, è il ricorrente che ha posto in essere le condizioni necessarie per provocare connessioni a server situati negli Stati Uniti" ed è sempre "il comportamento del ricorrente che ha causato il rinvio mediante il meccanismo di instradamento del servizio Amazon CloudFront delle sue richieste di consultazione del sito Internet della CAE verso server ubicati negli Stati Uniti" (paragrafi 160-161).

Infatti i giudici qui non solo addossano un onere della prova piuttosto consistente all'utente di internet senza tener conto dell'asimmetria informativa esistente; il comportamento volontario del ricorrente viene infatti ritenuto la causa diretta del danno, mentre il comportamento della Commissione consistente nel mettere a disposizione il link al login tramite Facebook è considerato condizione necessaria ma non sufficiente perché il trasferimento dei dati extra UE si verifichi (paragrafo 161).

Tale interpretazione restrittiva non solo appare poco comprensibile dal punto di vista dell'utente, salvo forse nell'ottica di proteggere l'operato delle istituzioni europee rispetto a possibili ricorsi in massa, specie a seguito del riconoscimento di *noyb*, l'ONG fondata da Maximilian Schrems, quale *Qualified Entity* abilitata a introdurre ricorsi collettivi ai sensi della Direttiva 2020/1828[16]. La decisione finisce per indebolire notevolmente le tutele giurisdizionali a disposizione del *data subject*, in quanto "rischia di rendere illusorio il diritto degli interessati a un ricorso giurisdizionale effettivo" ma soprattutto in quanto "sul piano fattuale, tale esclusione ignora che le istituzioni dell'Unione esercitano il loro potere anche attraverso condotte di fatto, che non sempre si traducono in atti formali, ma che possono incidere direttamente sulla sfera giuridica degli individui"[17].

Questo approccio formalistico riguardo l'interpretazione della nozione di "effetti giuridici vincolanti" sulla base delle intenzioni dell'istituzione (punto 33), si pone in contrasto con l'approccio sostanzialistico adottato dalla giurisprudenza comunitaria tanto rispetto alla qualificazione degli atti impugnabili[18], bensì anche – e soprattutto – rispetto alla postura interpretativa adottata nei confronti dei diritti fondamentali del cittadino digitale sopra richiamata, del tutto analoga a quella che ha presieduto allo sviluppo dei diritti del cittadino

14. U. Pagallo, *The Group, the Private, and the Individual: A New Level of Data Protection?*, in L. Taylor – L. Floridi – B. van der Sloot (ed.), *Group Privacy: New Challenges of Data Technologies*, Springer International Publishing, Cham 2017, 159-173

15. A. Lucchini, *Privacy violata, l'Ue sanziona sé stessa*

16. noyb, *noyb is now qualified to bring collective redress actions*, *noyb.eu*, , in https://noyb.eu/en/noyb-now-qualified-bring-collective-redress-actions (Consultato: 25 aprile 2025)

17. A. Fiorentini, *L'illusorietà del diritto a un ricorso effettivo nell'ambito del regolamento (UE) 2018/1725: note a margine della sentenza Bindl c. Commissione*, 5

18. Case C-60/81, *IBM* c. *Commissione*, ECLI:EU:C:1981:264.

europeo[19], mettendo in questione lo sviluppo della cittadinanza digitale europea in senso coerente con lo spirito "costituzionale" delle pronunce sopra richiamate.

Proprio tale spirito costituzionale è però presente nel ricorso del *data subject*, il sig. Bindl nella circostanza, che ha intrapreso un'azione legale chiedendo un risarcimento dei danni – peraltro come visto largamente negato – non tanto in nome del suo modestissimo valore monetario, quanto per il suo valore simbolico, che ci sembra poter essere quello di alimentare l'immaginario della cittadinanza digitale prima ancora che quello di ottenere un ristoro economico degno di tale nome.

Il ricorso in esame è esemplare nella misura in cui il *data subject* qui si pone come cittadino digitale, rivendicando diritti per sé e per altri, in linea con una concezione performativa della cittadinanza digitale lontana dall'idea dell'educazione al buon cittadino digitale, e incentrata invece sull'atto di porsi in quanto cittadini rivendicando diritti nel cyberspazio[20]. Secondo questa idea, la figura del cittadino digitale non coincide con quella del *data subject*, bensì è più ampia in quanto il cittadino digitale non è colui che ha già dei diritti bensì anche colui che li rivendica, e anzi è proprio in questo modo che lo diviene. Si tratta, come evidente, di una prospettiva che sta a cavallo tra una concezione giuridica e una concezione politica della cittadinanza digitale e che potrebbe sembrare lontana dalle preoccupazioni tipiche del giurista. Eppure riteniamo che proporio questa figura potrà essere ancora foriera – come lo è in fondo stata con le sentenze *Schrems* – di sviluppi fondamentali dello status giuridico del cittadino digitale europeo, auspicabilmente anche tramite l'intervento della Corte di Giustizia o dello European Data Protection Supervisor.

La figura del cittadino digitale europeo non coincide dunque con quella del *data subject* contemplato dal GDPR (figura che nella versione italiana viene denominata "l'interessato", perdendo parte della propria pregnanza semantica), cui spesso la riconduce anche la retorica della Commissione: la vigilanza critica e attiva del cittadino digitale è più che mai necessaria affinché il *data subject* resti anzitutto un soggetto di diritti in carne e ossa da tutelare, più che un "soggetto di dati" da analizzare[21]; questo è ancor più vero in relazione all'entrata in vigore del Regolamento 2025/327 del Parlamento europeo e del Consiglio, dell'11 febbraio 2025, sullo spazio europeo dei dati sanitari, nella misura in cui i dati di salute dei cittadini europei – dati sensibili – una volta anonimizzati, e dunque sottratti alla disciplina del GDPR, saranno disponibili per l'uso secondario[22], ossia per finalità ulteriori rispetto a quelle connesse alla loro raccolta.

Nel corso del *Data Protection Day* tenutosi il 28 gennaio presso la Commissione Europea è stato affermato che la disciplina contenuta nel regolamento sullo Spazio Europeo dei Dati Sanitari (EHDS - *European Health Data Space*) realizza un buon contemperamento tra la protezione dei dati personali e la promozione della ricerca e dell'innovazione, in particolare riguardo il contemperamento ottimale tra i diritti dei cittadini rispetto all'uso primario dei dati e gli interessi del settore ricerca e innovazione connessi al loro uso secondario. Tuttavia, già dalla prima proposta di Regolamento del maggio 2022 la disciplina ha sollevato più di qualche critica, che permane anche rispetto alla versione definitiva del testo entrato in vigore lo scorso 25 marzo. In particolare il Regolamento presenta alcuni nodi problematici in merito alla tutela dei diritti fondamentali dei cittadini europei proprio rispetto all'uso secondario dei dati sanitari[23], un aspetto in cui i diritti di cittadinanza digitale e di cittadinanza *tout court* sono strettamente intrecciati e dai quali, crediamo, potranno scaturire vicende analoghe a quella in oggetto, nelle quali cioè sono le istituzioni europee a essere chiamate in causa per le scelte operate nella gestione dei dati personali sanitari, se pure anonimi.

Oltre all'esercizio dei diritti propri del *data subject,* la vigilanza e l'impegno dei cittadini europei e in particolare la loro propensione a dare battaglia (legale e politica) rivendicando diritti nel cyberspace, anche e soprattutto nei confronti delle istituzioni che per prime dovrebbero garantirli, saranno probabilmente i più pilastri

19. C. Margiotta, *Cittadinanza europea: istruzioni per l'uso*, Gius. Laterza & Figli Spa 2014

20. E. Isin – E. Ruppert, *Being Digital Citizens*, Rowman & Littlefield International, London 2020[2]; N. Couldry et al., *Digital citizenship? Narrative exchange and the changing terms of civic culture*, «Citizenship Studies» 18/6-7 (2014) 615-629

21. M. Hildebrandt, *Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, «Theoretical Inquiries in Law» 20/1 (2019) 83-121

22. M. Catanzariti, *Verso una nuova epistemologia dei dati sanitari: le promesse mancate del secondary use*,

23. E.S. Dove, *The European Health Data Space as a Case Study*, «Ethics & Human Research» 46/6 (2024) 29-35

dello sviluppo – auspicabile – dello status di cittadinanza digitale europea in linea con i diritti fondamentali sanciti dalla Carta.