

L'ILLUSORIETÀ DEL DIRITTO A UN RICORSO EFFETTIVO NELL'AMBITO DEL REGOLAMENTO (UE) 2018/1725: NOTE A MARGINE DELLA SENTENZA *BINDL C. COMMISSIONE*

*Le caractère illusoire du droit à un recours effectif dans le cadre du règlement (UE)
2018/1725: remarques sur l'arrêt Bindl c. Commission*

*The illusory nature of the right to an effective remedy under Regulation (EU)
2018/1725: remarks on the Bindl v. Commission judgment*

ANNA FIORENTINI

(Dottoranda in Diritto dell'Unione europea, Università di Bologna)

Introduzione

Con la sentenza *Bindl c. Commissione* dell'8 gennaio 2025¹, il Tribunale si è pronunciato per la prima volta sulle condizioni per l'esercizio dei ricorsi diretti nell'ambito del regolamento (UE) 2018/1725 ("EUDPR")², omologo del regolamento (UE) 2016/679 ("GDPR")³, sulla protezione dei dati personali per le istituzioni dell'Unione. Dei tre ricorsi presentati, solo la domanda di risarcimento danni per il trasferimento illecito di dati personali extra-UE è stata parzialmente accolta, mentre l'azione di annullamento e il ricorso in carenza sono stati dichiarati irricevibili. Il risultato è una sostanziale *débâcle* per il ricorrente, che si è visto negare ogni possibilità di contestare in modo effettivo la condotta della Commissione.

¹ Trib., 8 gennaio 2025, causa T-354/22, *Bindl c. Commissione*, ECLI:EU:T:2025:4.

² Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE, in GUUE L 295, 21 novembre 2018, p. 39 ss.

³ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, in GUUE L 119, 4 maggio 2016, p. 1 ss.

Dopo una breve ricostruzione dei fatti, questa segnalazione si concentrerà su tre aspetti chiave della decisione: i) l'interpretazione della nozione di “atto impugnabile” ai sensi dell' art. 263 TFUE; ii) l'efficacia preclusiva della “presa di posizione” nel ricorso in carenza ex art. 265 TFUE; iii) l'onere probatorio richiesto per accertare la responsabilità extra-contrattuale dell'Unione. La tesi sostenuta è che l'orientamento adottato dal Tribunale possa incidere profondamente sull'accesso ai ricorsi diretti e, più in generale, sul pieno esercizio del diritto a un ricorso giurisdizionale effettivo⁴ in caso di violazioni delle norme europee sulla protezione dei dati personali.

I fatti e le richieste al Tribunale

Tra il 2021 e il 2022, un cittadino tedesco ha visitato più volte il sito web della Commissione europea dedicato alla Conferenza sul futuro dell'Europa. Il 30 marzo 2022 si è registrato all'evento “GoGreen” utilizzando il proprio account Facebook per autenticarsi. Durante la navigazione, ha rilevato connessioni a fornitori terzi, in particolare Amazon Web Services (AWS), con sede negli Stati Uniti.

Preoccupato per un possibile trasferimento dei suoi dati a AWS e Facebook, il 9 novembre 2021 il ricorrente ha chiesto chiarimenti alla Commissione, che ha risposto il 3 dicembre 2021, precisando che i dati erano trattati da AWS EMEA – gestore della rete di distribuzione di contenuti Amazon CloudFront, con sede in Lussemburgo –, e che non vi erano stati trasferimenti di dati personali al di fuori dell'Unione. Il 1° aprile 2022, il ricorrente ha inviato una nuova richiesta alla Commissione domandando maggiori dettagli e una copia dei dati memorizzati da terze parti. La Commissione ha risposto il 30 giugno 2022, dopo due solleciti e a causa già incardinata davanti al Tribunale, sostenendo che la richiesta fosse sostanzialmente identica a quella precedente.

Il ricorrente ha quindi chiesto al Tribunale l'annullamento dei trasferimenti dei suoi dati personali effettuati senza adeguate garanzie, nonché la dichiarazione dell'omissione illecita da parte della Commissione nel rispondere alla sua richiesta di informazioni del 1° aprile 2022. Inoltre, ha presentato tre domande di risarcimento danni relative a: i) la violazione del diritto di accesso alle informazioni; ii) i trasferimenti di dati personali extra-UE avvenuti durante le consultazioni del sito tramite Amazon CloudFront; iii) i trasferimenti verificatisi in occasione dell'iscrizione all'evento “GoGreen” tramite Facebook.

⁴ Art. 47 CdFUE.

La decisione del Tribunale

Prima di esaminare i punti chiave della decisione del Tribunale, occorre ricordare che, all'epoca dei fatti, non esisteva una decisione di adeguatezza ai sensi dell'art. 45, par. 3, GDPR⁵. Nel 2020, infatti, la Corte aveva dichiarato invalida la decisione di esecuzione (UE) 2016/1250⁶, così come aveva fatto in precedenza con la decisione 2000/520/CE⁷. Di conseguenza, il trasferimento di dati personali verso un paese terzo poteva avvenire solo se il titolare del trattamento – in questo caso la Commissione – avesse fornito garanzie adeguate, ai sensi dell'art. 48 EUDPR.

Inoltre, in caso di trasferimenti di dati extra-UE, l'EUDPR riconosce agli interessati il diritto di ottenere informazioni sui destinatari situati in paesi terzi e sulle garanzie adeguate per i relativi trasferimenti⁸. I tempi di risposta da parte delle istituzioni sono disciplinati dall'art. 14, parr. 3-4 dello stesso regolamento: l'istituzione ha un mese di tempo per rispondere alla richiesta dell'interessato e, qualora decida di non ottemperare, deve fornire una motivazione entro un mese.

Fatte queste premesse, il Tribunale ha dichiarato irricevibili sia il ricorso di annullamento sia il ricorso in carenza, ritenendoli privi di oggetto. Da un lato, i trasferimenti di dati contestati, derivanti dall'interazione del ricorrente con i sistemi della Commissione (ad es. la consultazione del sito), sono stati qualificati come meri atti materiali, a cui l'istituzione non ha voluto conferire effetti giuridici vincolanti e, pertanto, non rientranti nella categoria di "atti impugnabili" ex art. 263 TFUE (punti 33-34). Dall'altro, la risposta della Commissione del 30 giugno 2022 è stata considerata una "presa di posizione" ai sensi dell'art. 265 TFUE, conformemente alla giurisprudenza consolidata della Corte, che ha adottato un'interpretazione estensiva di tale nozione, includendo anche le risposte delle istituzioni che non soddisfano il richiedente (punto 42).

Per quanto riguarda poi il ricorso per danni, il Tribunale ha respinto le prime due richieste di risarcimento relative ai danni morali derivanti rispettivamente: i) dalla violazione del diritto a ottenere informazioni ex art. 17, par. 1 e 14, parr. 3-4, EUDPR, e ii) dai trasferimenti illeciti di dati extra-UE avvenuti durante le consultazioni del sito. Il motivo principale del rigetto è l'incapacità del ricorrente di dimostrare la sussistenza delle condizioni cumulative necessarie per accertare la responsabilità extracontrattuale dell'Unione. In particolare, il Tribunale ha rilevato che il ricorrente

⁵ Com'è noto, attualmente i flussi di dati personali UE-USA sono regolati dalla decisione di esecuzione (UE) 2023/1795.

⁶ Corte giust., 16 luglio 2020, causa C-311/18, *Schrems II*, ECLI:EU:C:2020:559.

⁷ Corte giust., 6 ottobre 2015, causa C-362/14, *Schrems I*, ECLI:EU:C:2015:650.

⁸ Art. 17 EUDPR.

non ha fornito prove dell'effettivo trasferimento di dati personali tramite Amazon CloudFront a server situati al di fuori dell'Unione, impedendo così di configurare una violazione sufficientemente qualificata dell'EUDPR.

In relazione al diritto di accesso alle informazioni, il Tribunale ha stabilito che la Commissione non era obbligata, ai sensi dell'art. 17 EUDPR, a fornire informazioni sui destinatari situati in paesi terzi o sulle garanzie richieste dell'art. 48 dello stesso regolamento, in assenza di prove che dimostrassero un effettivo trasferimento di dati extra-UE (punti 71-72). La Commissione ha pertanto adempiuto ai suoi obblighi fornendo le informazioni disponibili sul trattamento dei dati in questione nelle risposte del 3 dicembre 2021 e del 30 giugno 2022. Inoltre, sebbene la seconda risposta sia stata pervenuta oltre il termine previsto dall'art. 14, par. 4, EUDR, il ricorrente non ha dimostrato l'esistenza di un danno morale "reale e certo" derivante da tale ritardo, limitandosi ad affermare che il comportamento della Commissione gli avrebbe impedito di monitorare il trattamento dei suoi dati personali (punti 79-82).

Con riferimento invece alle violazioni delle norme sul capo V dell'EUDPR per i trasferimenti di dati extra-UE avvenuti durante le consultazioni del sito, i giudici hanno chiarito che il mero rischio di un trasferimento di dati non imponeva alla Commissione l'adozione di garanzie adeguate ai sensi dell'art. 48 EUDPR. A questo proposito, è stata ritenuta irrilevante la circostanza, fatta valere dal ricorrente, che AWS EMEA, in quanto controllata da un'impresa americana, potesse teoricamente essere soggetta a richieste di accesso ai dati da parte delle autorità statunitensi, anche quando i dati erano conservati all'interno dell'Unione (punti 133-134). Il Tribunale ha affermato che il solo rischio di accesso da parte di paesi terzi non equivale a una violazione diretta delle disposizioni del capo V dell'EUDPR e, quindi, non è sufficiente a configurare un comportamento illecito da parte della Commissione (punti 135-137).

Il Tribunale ha respinto tale richiesta di risarcimento anche per insufficienza di prove riguardo al nesso causale. Rifacendosi alla giurisprudenza della Corte secondo cui un semplice rapporto di condizionalità non basta a dimostrare un nesso causale diretto, i giudici hanno stabilito che le connessioni ai server statunitensi non erano dovute al normale funzionamento del servizio Amazon CloudFront, come sostenuto dal ricorrente, ma piuttosto al fatto che lo stesso ricorrente aveva deliberatamente modificato la sua posizione apparente del dominio digitale, simulando spostamenti in più località per interagire con server situati in diversi paesi, tra cui gli Stati Uniti (punto 157). In sintesi, mentre l'uso del servizio Amazon

CloudFront da parte della Commissione costituisce una condizione necessaria ma non sufficiente per il presunto trasferimento dei dati, è il comportamento del ricorrente a rappresentarne la causa diretta (punto 161).

L'unica richiesta di risarcimento accolta dal Tribunale riguarda i trasferimenti di dati avvenuti in occasione dell'iscrizione all'evento "Go-Green" tramite Facebook. Il Tribunale ha ritenuto che il collegamento ipertestuale "connettersi a Facebook", predisposto dalla Commissione, avesse creato le condizioni per la trasmissione dei dati personali dell'utente a Facebook, configurando così un effettivo trasferimento di dati extra-UE (punti 187-188). Di conseguenza, la Commissione è stata ritenuta responsabile di una violazione sufficientemente qualificata dell'art. 46 EUDPR, avendo appunto consentito il trasferimento di dati personali verso un paese terzo senza prevedere le necessarie garanzie (punto 192). Il Tribunale ha quindi riconosciuto il danno morale subito dal ricorrente, derivante dalla situazione di incertezza relativa al trattamento dei suoi dati, e ha confermato, seppur *en passant*, la sussistenza del nesso di causalità (punti 197-198).

I limiti ai ricorsi di annullamento e in carenza...

Se confermato dalla Corte – e dal Tribunale stesso in future pronunce – l'orientamento espresso nella decisione in esame rischia di rendere illusorio il diritto degli interessati a un ricorso giurisdizionale effettivo⁹. Innanzitutto, l'interessato non può esercitare un'azione di annullamento qualora un'istituzione dell'Unione tratti illecitamente i suoi dati. L'esclusione delle operazioni di trattamento, incluso il trasferimento di dati, dall'ambito di applicazione dell'art. 263 TFUE risulta problematica sotto due profili principali. 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 individui¹⁰. Sul piano giuridico, l'interpretazione formalista del Tribunale riguardo alla nozione di "effetti giuridici vincolanti" sulla base delle intenzioni dell'istituzione (punto 33), sembra superare il criterio sostanzialistico adoperato dal giudice dell'Unione nella qualificazione degli atti impugnabili¹¹.

⁹ Diritto che, nell'ambito dell'EUDPR, è espressamente garantito dall'art. 64, par. 1, EUDPR.

¹⁰ F. COMAN-KUND, *Legal Protection against Fundamental Rights Breaches through Factual Conduct by the European Union*, in M. FINK (eds), *Redressing Fundamental Rights Violations by the EU. The Promise of the 'Complete System of Remedies'*, Cambridge, 2024, p. 311.

¹¹ Si veda, *inter alia*, Corte giust., 11 novembre 1981, causa C-60/81, *IBM c. Commissione*, ECLI:EU:C:1981:264, punto 9.

In base a questa giurisprudenza, il Tribunale avrebbe dovuto preliminarmente accertare se i trasferimenti di dati controversi fossero avvenuti in violazione dell'EUDPR, invece di limitarsi a esaminarne tali aspetti solo nell'ambito delle richieste di risarcimento del danno. Se fosse stata riconosciuta l'assenza delle garanzie previste dall'EUDPR per i trasferimenti extra-UE, si sarebbe potuto sostenere che questi trasferimenti avessero prodotto effetti vincolanti per il ricorrente, ledendo il suo diritto fondamentale alla protezione dei dati personali¹². Infatti, come sottolineato da Rademacher nel commento alla sentenza *Akzo*¹³, «any act capable of violating an applicant's right or legally protected interest was considered to be— for this very reason— binding on him or her or it»¹⁴. Seguendo questa logica, il trasferimento illecito di dati personali verso gli Stati Uniti avrebbe dovuto essere considerato un atto produttivo di conseguenze giuridiche e, quindi, impugnabile.

Inoltre, la possibilità di ottenere una declaratoria di carenza risulta limitata dall'interpretazione estensiva che il Tribunale fornisce della “presa di posizione” dell'istituzione in risposta a una richiesta di accesso alle informazioni. I giudici arrivano infatti a ritenere che anche la semplice esposizione dei motivi per cui si ritiene opportuno non adottare una risposta sia sufficiente a porre fine all'omissione (punti 41-42). Sebbene tale approccio sia in linea con l'orientamento prevalente della giurisprudenza della Corte e della dottrina sul punto – fatte salve rare eccezioni¹⁵ – esso comporta il rischio che l'interessato venga privato sia dell'azione in carenza (per via dell'intervenuta reazione) sia del ricorso di annullamento (in ragione della natura generica della presa di posizione).

... e il ricorso per risarcimento dei danni

Esclusa la possibilità di ricorrere ex art. 263 TFUE e di far valere la carenza ex art. 265 TFUE, anche l'azione di risarcimento danni ex artt. 268 e 340, par. 2, TFUE si rivela una via impervia per contestare l'operato delle istituzioni in materia di protezione dei dati personali. Fatta eccezione per la richiesta di risarcimento relativa all'iscrizione all'evento “GoGreen”,

¹² Art. 8 CdFUE.

¹³ Cause riunite T-125/03 e T-253/03, *Akzo c. Commissione*, ECLI:EU:T:2007:287, punto 45.

¹⁴ T. RADEMACHER, *Factual Administrative Conduct and Judicial Review in EU Law*, in *European Review of Public Law*, 2017, n. 29, p. 407.

¹⁵ L. CECCHETTI, *On Time Limits, Position Definition and “Discretionary Shall”: the Grand Chamber Rules on the Action for Failure to Act Conditions in an Interinstitutional Context*, in *Rivista del Contenzioso Europeo*, 2024.

il Tribunale ha infatti adottato un'interpretazione restrittiva delle condizioni cumulative per la responsabilità extracontrattuale dell'Unione,¹⁶ imponendo un onere della prova particolarmente gravoso per l'interessato.

In primo luogo, il Tribunale ha stabilito che, affinché si configuri una violazione sufficientemente qualificata dell'EUDPR, l'interessato deve dimostrare che i suoi dati siano stati *effettivamente* trasferiti extra-UE senza le dovute garanzie (punti 71 e 135). Questa interpretazione non tiene conto della profonda asimmetria informativa tra gli interessati e le istituzioni (o i fornitori di servizi digitali). Nel caso di specie, ad esempio, non era realisticamente esigibile che il sig. Bindl potesse provare un trasferimento illecito di dati che, sebbene conservati in server situati nell'Unione, potevano essere soggetti a richieste specifiche della casa madre statunitense ad AWS EMEA. Un approccio più equilibrato avrebbe dovuto considerare non tanto l'effettiva prova di trasferimento, quanto piuttosto la sussistenza di un *rischio* concreto di violazione, capace di compromettere la conformità alle norme sulla protezione dei dati personali¹⁷.

In secondo luogo, per quanto concerne il danno morale subito a causa del diniego di accesso alle informazioni, il Tribunale ha escluso che l'interessato possa ritenere soddisfatto tale requisito adducendo come ragione la perdita di controllo sul trattamento dei propri dati derivante dalla condotta della Commissione (punti 79-82). Tale approccio si discosta dalla giurisprudenza della Corte – citata dallo stesso Tribunale in relazione ai trasferimenti di dati tramite Facebook – che ha riconosciuto il diritto al risarcimento del danno morale anche in assenza di una soglia di gravità particolarmente elevata¹⁸.

In terzo luogo, relativamente al nesso causale, il Tribunale ha imposto all'interessato l'onere di provare che il danno sia direttamente imputabile alla condotta del titolare – ovvero sia la Commissione – e che eventuali sue azioni non abbiano interrotto il rapporto di causa-effetto (punto 161). Tuttavia, questa impostazione manca di considerare la complessità del funzionamento delle infrastrutture digitali, come Amazon CloudFront, che operano su scala globale e comportano un rischio intrinseco di trasferimenti extra-UE, indipendentemente dall'interazione individuale dell'utente (ad esempio, accedendo da diverse località).

Come anticipato, mentre le richieste di risarcimento per il diniego di accesso alle informazioni e per le semplici consultazioni del sito sono state

¹⁶ Cfr., *ex multis*, Corte giust., 28 aprile 1971, causa C-4/69, *Lütticke c. Commissione*, ECLI:EU:C:1971:40, punto 10.

¹⁷ Corte giust., 6 ottobre 2015, causa C-362/14, *Schrems I*, cit., punto 91.

¹⁸ Corte giust., 4 maggio 2023, causa C-300/21, *Österreichische Post*, ECLI:EU:C:2023:370, punti 45 e 51.

respinte, il Tribunale ha adottato un criterio meno restrittivo per il trasferimento di dati tramite Facebook. Questa divergenza potrebbe essere giustificata dal fatto che, in quest'ultimo caso, il trasferimento non era solo potenziale, ma effettivo, poiché l'integrazione di Facebook come metodo di autenticazione ha reso inevitabile l'accesso ai dati da parte di un soggetto stabilito extra-UE. Di conseguenza, il Tribunale ha riconosciuto l'esistenza di un danno morale sulla base della sola incertezza relativa al trattamento dei dati personali, senza richiedere il superamento di una soglia *de minimis* di gravità (punti 196-197), come invece imposto per la richiesta di accesso alle informazioni. I giudici hanno altresì ritenuto soddisfatto il nesso causale (punto 198), sebbene – come argomentato in relazione ai trasferimenti di dati durante le consultazioni del sito – anche in questo caso la scelta dell'interessato di autenticarsi tramite Facebook avrebbe potuto essere considerata una condotta interruttiva del rapporto causa-effetto.

Infine, sebbene il Tribunale abbia accolto l'ultima richiesta di risarcimento, la somma accordata – 400 euro rispetto ai 1200 richiesti – ha un valore più simbolico che realmente compensativo. È quindi plausibile che entrambe le parti decidano di impugnare la decisione. In tal caso, la Corte potrebbe adottare un approccio più severo nei confronti della Commissione, in linea con il suo orientamento generalmente favorevole alla tutela degli interessati, soprattutto in contesti in cui la protezione dei diritti fondamentali appare incerta. La Corte, infatti, si è mostrata meno incline rispetto al Tribunale¹⁹ a minimizzare le violazioni in materia di protezione dei dati personali da parte di organismi e istituzioni dell'Unione²⁰, ampliando così le possibilità per gli interessati di ottenere un risarcimento²¹, anche eventualmente mediante il conferimento di mandato a un'organizzazione senza scopo di lucro²².

Alcune riflessioni conclusive: l'opportunità della via amministrativa

L'interpretazione adottata dal Tribunale riguardo alle condizioni per l'esercizio dei ricorsi diretti rischia di mettere in discussione, nell'ambito dell'EUDPR, il paradigma della completezza del sistema rimediale, pilastro dell'assetto giurisdizionale dell'Unione²³. A questo proposito, sebbene la

¹⁹ Trib., 4 maggio 2022, causa T-384/20, *OC c. Commissione*, ECLI:EU:T:2022:273.

²⁰ Corte giust., 7 marzo 2024, causa C-479/22 P, *OC c. Commissione*, ECLI:EU:C:2024:215.

²¹ Art. 65 EUDPR.

²² Art. 67 EUDPR.

²³ Corte giust., 23 aprile 1986, causa C-294/83, *Les Verts*, ECLI:EU:C:1986:166, punto 23; 25 luglio 2002, C-50/00 P, *Unión de Pequeños Agricultores*, punti 38 e 40; 3 settembre 2008, C-402/05 P, *Kadi*, punto 281; 3 ottobre 2013, C-583/11 P, *Inuit*, punto 92.

Corte abbia chiarito che l'art. 47 della Carta non può «modificare il sistema di controllo giurisdizionale previsto dai Trattati, ed in particolare le norme relative alla ricevibilità dei ricorsi proposti direttamente dinanzi al giudice dell'Unione europea»²⁴, sarebbe stato auspicabile che il Tribunale avesse adottato un'interpretazione “costituzionalmente” orientata delle vie di ricorso esistenti, valorizzando il diritto a una tutela giurisdizionale effettiva.

In un contesto profondamente mutato rispetto a quello in cui sono stati originariamente concepiti i requisiti per l'accesso alla giustizia, se non altro per le trasformazioni tecnologiche che incidono (anche) sul funzionamento delle istituzioni dell'Unione, un simile approccio avrebbe consentito di includere nella nozione di “atto impugnabile” anche atti materiali, come i trasferimenti di dati, qualora fosse stato dimostrato che essi producono effetti giuridici vincolanti nei confronti di terzi, indipendentemente dalla volontarietà dell'istituzione. Inoltre, le condizioni cumulative per l'accertamento della responsabilità extracontrattuale dell'Unione avrebbero dovuto essere interpretate in modo da non rendere eccessivamente gravoso l'onere della prova per il ricorrente, specialmente in situazioni di marcata asimmetria informativa tra il titolare del trattamento e l'interessato.

I detrattori di questa impostazione potrebbero richiamare il timore espresso dalla Corte secondo cui l'invocazione dei diritti fondamentali comporti un'erosione dei requisiti procedurali previsti dai Trattati, finendo per riconoscere agli individui un diritto incondizionato a contestare qualsiasi comportamento delle istituzioni²⁵. Se questa posizione dovesse prevalere, il ricorso al Garante per la protezione dei dati personali (EDPS) potrebbe rappresentare la strada più efficace per gli interessati che intendono far valere una violazione dell'EUDPR²⁶. L'EDPS dispone, infatti, di ampi poteri, tra cui l'accesso a tutti i dati personali e le informazioni necessarie per l'esecuzione dei suoi compiti, la facoltà di ingiungere al titolare di soddisfare le richieste dell'interessato, l'ordine di sospensione di trasferimenti illeciti verso paesi terzi, e l'irrogazione di sanzioni amministrative fino a 500 000 euro all'anno per violazioni relative ai diritti degli interessati e ai trasferimenti di dati extra-UE²⁷. Inoltre, l'ottenimento di una decisione di condanna da parte dell'EDPS agevolerebbe significativamente l'azione di risarcimento – soggetta a un termine di prescrizione quinquennale²⁸ –

²⁴ Corte giust., 3 ottobre 2013, causa C-583/11 P, *Inuit*, cit., punto 97.

²⁵ Corte giust., 25 marzo 2021, causa C-565/19 P, *Carvalho e a. c. Parlamento e Consiglio*, punti 77-78.

²⁶ Art. 63, par. 1, EUDPR.

²⁷ Artt. 58, par. 1 e 66, par. 3 EUDPR.

²⁸ Art. 46 dello statuto della Corte di giustizia.

per chi ritenga violati i propri diritti, semplificando al contempo l'analisi del Tribunale.

In passato, l'EDPS ha adottato decisioni di rilievo in materia, come quella con cui ha accertato la violazione dell'EUDPR da parte della Commissione nell'utilizzo di Microsoft 365²⁹. Considerata l'impugnazione di tale decisione³⁰, sarà interessante vedere se il Tribunale confermerà l'approccio adottato nella sentenza in commento o se, al contrario, adotterà un'interpretazione più favorevole alla tutela dei diritti fondamentali, anche a costo di limitare la capacità operativa della Commissione.

²⁹ https://www.edps.europa.eu/data-protection/our-work/publications/investigations/2024-03-08-edps-investigation-european-commissions-use-microsoft-365_en.

³⁰ Causa T-262/24, *Commissione c. EDPS* e causa T-265/24, *Microsoft c. EPDS*.