Raccolta della giurisprudenza

SENTENZA DEL TRIBUNALE (Sesta Sezione ampliata)

8 gennaio 2025 *

[Testo rettificato con ordinanza del 3 giugno 2025]

«Trattamento dei dati personali – Tutela delle persone fisiche rispetto al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione – Regolamento (UE) 2018/1725 – Nozione di "trasferimento di dati personali verso un paese terzo" – Trasferimento di dati in occasione della consultazione di un sito Internet – Eu Login – Ricorso di annullamento – Atto non impugnabile – Irricevibilità – Ricorso per carenza – Presa di posizione che pone fine alla carenza – Non luogo a statuire – Ricorso per risarcimento danni – Violazione sufficientemente qualificata di una norma giuridica che conferisce diritti ai singoli – Nesso causale – Danno morale»

Nella causa T-354/22,

Thomas Bindl, residente in Monaco di Baviera (Germania), rappresentato da T. Herbrich, avvocato,

ricorrente,

contro

Commissione europea, rappresentata da A. Bouchagiar, B. Hofstötter e H. Kranenborg, in qualità di agenti,

convenuta,

IL TRIBUNALE (Sesta Sezione ampliata),

composto da M.J. Costeira (relatrice), presidente, M. Kancheva, U. Öberg, P. Zilgalvis e E. Tichy-Fisslberger, giudici,

cancelliere: S. Jund, amministratrice

vista la fase scritta del procedimento,

vista la misura di organizzazione del procedimento del 21 luglio 2023 e le risposte della Commissione e del ricorrente depositate presso la cancelleria del Tribunale, rispettivamente, il 7 e l'8 settembre 2023,

* Lingua processuale: il tedesco.

in seguito all'udienza del 17 ottobre 2023,

vista la misura di organizzazione del procedimento del 9 febbraio 2024 e le risposte della Commissione e del ricorrente depositate presso la cancelleria del Tribunale, rispettivamente, il 12 e il 13 marzo 2024,

ha pronunciato la seguente

Sentenza

1 Con il suo ricorso fondato sugli articoli 263, 265 e 268 TFUE, il sig. Thomas Bindl, ricorrente, chiede al Tribunale, in primo luogo, di annullare trasferimenti dei suoi dati personali verso paesi terzi che non dispongono di un livello di protezione adeguato, in secondo luogo, di constatare che la Commissione europea si è illegittimamente astenuta dal prendere posizione sulla sua domanda di informazioni del 1º aprile 2022 e, in terzo luogo, di risarcire il danno morale che egli avrebbe subito a seguito, da un lato, di una violazione del suo diritto di accesso alle informazioni e, dall'altro, dei trasferimenti dei suoi dati personali.

Fatti all'origine della controversia e fatti successivi alla presentazione del ricorso

2 Il ricorrente è un cittadino tedesco che si interessa a questioni nei settori dell'informatica e della protezione dei dati personali.

3 La direzione generale della Comunicazione della Commissione è responsabile del trattamento dei dati personali ai fini del sito Internet della Conferenza sul futuro dell'Europa all'indirizzo «https://futureu.europa.eu (in prosieguo: il «sito Internet della CAE»).

4 Il ricorrente ha consultato il sito Internet della CAE a più riprese durante gli anni 2021 e 2022. In particolare, egli ha consultato tale sito Internet il 30 marzo 2022 e si è iscritto all'evento «GoGreen» ivi contenuto, utilizzando il suo account Facebook e, l'8 giugno 2022, ha nuovamente consultato detto sito Internet.

5 Con messaggio di posta elettronica del 9 novembre 2021 (in prosieguo: la «richiesta di informazioni del 9 novembre 2021»), il ricorrente ha chiesto al responsabile della protezione dei dati della Commissione di fornirgli informazioni ai sensi del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, relativo alla protezione delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché alla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU 2018, L 295, pag. 39).

6 In detto messaggio, in primo luogo, il ricorrente ha indicato di aver rilevato che, quando si è collegato sul sito Internet della CAE, era stata attivata una connessione con fornitori terzi, quali l'impresa americana Amazon Web Services; in secondo luogo, ha chiesto che gli fosse indicato quali dati personali che lo riguardavano fossero stati trattati o conservati e quali, se del caso, fossero stati trasferiti a terzi; in terzo luogo, esso ha chiesto informazioni sulla base giuridica di un siffatto trasferimento nonché sull'esistenza di eventuali garanzie riguardanti il trasferimento verso paesi terzi che non dispongono di un livello di protezione adeguato.

7 Con messaggio di posta elettronica del 3 dicembre 2021, la direzione generale della comunicazione della Commissione ha trasmesso al ricorrente un collegamento elettronico e lo ha informato che tale collegamento gli consentiva di generare direttamente un elenco dei dati personali che erano stati trattati in occasione della consultazione del sito Internet della CAE. Inoltre, essa ha indicato al ricorrente, da un lato, che i suoi dati personali non erano stati trasferiti a destinatari situati al di fuori dell'Unione europea e, dall'altro, che essi erano memorizzati e trattati dal sito Internet della CAE, il quale utilizzava una rete di diffusione di contenuti gestita dalla Amazon Web Services EMEA SARL (in prosieguo: la «AWS EMEA»), con sede in Lussemburgo (Lussemburgo). Inoltre, essa ha precisato che, nell'ambito degli accordi contrattuali conclusi tra la Commissione e la AWS EMEA, il responsabile del trattamento dei dati non si serviva di servizi che richiedessero un trasferimento di dati verso i partner della AWS EMEA situati negli Stati Uniti e che il trasferimento di dati al di fuori del territorio dell'Unione non era, in linea di principio, autorizzato.

8 [Come rettificato con ordinanza del 3 giugno 2025] Con messaggio di posta elettronica del 1º aprile 2022, il ricorrente ha chiesto alla Commissione, ai sensi del regolamento 2018/1725, informazioni sul trattamento dei suoi dati (in prosieguo: la «richiesta di informazioni del 1º aprile 2022»). In primo luogo, esso ha indicato di aver rilevato che, quando si è collegato sul sito Internet della CAE, si era stabilita una connessione con fornitori terzi quali la AWS EMEA e sarebbe stata dimostrata una connessione all'impresa Meta Platform quando ha utilizzato i suoi dati di connessione Facebook per registrarsi su tale sito Internet. In secondo luogo, egli ha chiesto che gli fosse indicato quali dati personali che lo riguardavano fossero stati trattati o conservati e quali, se del caso, fossero stati trasferiti a terzi. In terzo luogo, esso ha chiesto informazioni sulla base giuridica di un siffatto trasferimento nonché sull'esistenza di eventuali garanzie riguardanti il trasferimento verso paesi terzi che non dispongono di un livello di protezione adeguato. In quarto luogo, egli ha chiesto una copia dei suoi dati, compresi quelli conservati o trattati da terzi come Facebook.

9 Con messaggi di posta elettronica del 22 aprile e del 2 maggio 2022, il ricorrente ha insistito presso la Commissione affinché gli fornisse una risposta alla richiesta di informazioni del 1º aprile 2022.

10 Con atto introduttivo depositato presso la cancelleria del Tribunale il 29 ottobre 2008, il ricorrente ha proposto il presente ricorso.

11 Con messaggio di posta elettronica del 30 giugno 2022, la Commissione ha informato il ricorrente che essa riteneva che la richiesta di informazioni del 1º aprile 2022 fosse quasi identica alla richiesta di informazioni del 9 novembre 2021 e che essa avesse già risposto a quest'ultima con il suo messaggio di posta elettronica del 3 dicembre 2021.

12 La Amazon Web Services è un'impresa con sede negli Stati Uniti e la AWS EMEA è un'impresa con sede in Lussemburgo. Queste due imprese sono controllate dall'impresa di diritto americano Amazon.com, Inc.

Conclusioni delle parti

13 La ricorrente chiede che il Tribunale voglia:

– annullare i trasferimenti dei suoi dati personali verso paesi terzi che non dispongono di un livello di protezione adeguato che hanno avuto luogo il 30 marzo e l'8 giugno 2022;

– dichiarare che la Commissione si è illegittimamente astenuta dal prendere posizione sulla richiesta di informazioni del 1º aprile 2022;

– condannare la Commissione a versargli la somma di EUR 1 200, maggiorata degli interessi, corrispondenti, da un lato, all'importo di EUR 800, a titolo di risarcimento del danno morale subito a seguito di una violazione del suo diritto di accesso alle informazioni e, dall'altro, all'importo di EUR 400, a titolo di risarcimento del danno morale subito a seguito di detti trasferimenti dei suoi dati;

– condannare la Commissione alle spese.

14 La Commissione chiede che il Tribunale voglia:

– respingere la domanda di annullamento e la domanda di declaratoria di carenza in quanto irricevibili;

– in subordine, dichiarare che non vi è più luogo a statuire sulla domanda di declaratoria di carenza;

– respingere il ricorso per risarcimento danni in quanto infondato;

– condannare il ricorrente alle spese.

In diritto

Considerazioni preliminari sulla protezione dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione

15 L'articolo 16, paragrafo 1, TFUE e l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta») dispongono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

16 Il 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 (regolamento generale sulla protezione dei dati) (GU 2016, L 119, pag. 1) stabilisce norme generali volte a tutelare le persone fisiche con riguardo al trattamento dei dati personali e a garantire la libera circolazione di tali dati (articolo 1, paragrafo 1, del regolamento 2016/679).

17 Il regolamento 2018/1725 stabilisce norme relative alla protezione delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organi dell'Unione, nonché norme relative alla libera circolazione dei dati personali tra tali istituzioni e organi o verso altri destinatari stabiliti nell'Unione (articolo 1, paragrafo 1, del regolamento 2018/1725). Detto regolamento tutela i diritti e le libertà fondamentali delle persone fisiche, e in particolare il loro diritto alla protezione dei dati personali (articolo 1, paragrafo 2, del regolamento 2018/1725). Esso si applica al trattamento di dati personali da parte di tutte le istituzioni e di tutti gli organismi dell'Unione (articolo 2, paragrafo 1, del regolamento 2018/1725).

18 Il considerando 5 del regolamento 2018/1725 ricorda che, conformemente alla giurisprudenza della Corte, ogni volta che le disposizioni del regolamento 2018/1725 seguono gli stessi principi delle disposizioni del regolamento 2016/679, questi due insiemi di disposizioni devono essere interpretati in modo omogeneo, in particolare per il fatto che il regime del regolamento 2018/1725 dovrebbe essere inteso come equivalente a quello del regolamento 2016/679. A tal riguardo, da una lettura congiunta delle disposizioni dell'articolo 2, paragrafo 3, del regolamento 2016/679 e dell'articolo 99 del regolamento 2018/1725 risulta inoltre che quest'ultimo regolamento è adeguato ai principi e alle norme del regolamento 2016/679.

Sulla ricevibilità

Ricevibilità della domanda di annullamento

19 Con il primo capo delle sue conclusioni, il ricorrente chiede l'annullamento dei trasferimenti dei suoi dati personali verso paesi terzi che non dispongono di un livello di protezione adeguato, che avrebbero avuto luogo il 30 marzo e l'8 giugno 2022 (in prosieguo: i «trasferimenti controversi»).

20 Nel suo controricorso, la Commissione eccepisce l'irricevibilità di tale domanda di annullamento per il motivo che essa non è diretta contro un atto impugnabile, ai sensi dell'articolo 263 TFUE, ma è diretta a ottenere un'ingiunzione nei suoi confronti.

21 Il ricorrente sostiene la ricevibilità della domanda di annullamento, facendo valere che i trasferimenti controversi sono atti che producono effetti giuridici vincolanti e che incidono sulla sua situazione giuridica, pregiudicando il suo diritto fondamentale alla protezione dei dati personali, garantito dall'articolo 8 della Carta. Qualsiasi altra interpretazione sarebbe incompatibile con il diritto fondamentale a una tutela giurisdizionale effettiva, mentre l'articolo 64, paragrafo 1, del regolamento 2018/1725 riconosce esplicitamente tale diritto.

22 Come ricordato dall'articolo 64, paragrafo 1, e dal considerando 79 del regolamento 2018/1725, ogni persona ha diritto a un ricorso giurisdizionale effettivo dinanzi alla Corte di giustizia dell'Unione europea, conformemente ai trattati, se ritiene che i diritti conferitile da detto regolamento siano violati.

23 Ne consegue che, nell'ambito del regolamento 2018/1725, ogni persona interessata ha il diritto, in particolare, di proporre un ricorso di annullamento alle condizioni previste all'articolo 263 TFUE.

24 Secondo una giurisprudenza costante, il ricorso di annullamento previsto all'articolo 263 TFUE deve potersi esperire nei confronti di qualsiasi atto delle istituzioni, indipendentemente dalla sua forma, che miri a produrre effetti giuridici vincolanti idonei ad incidere sugli interessi del ricorrente, modificando in misura rilevante la sua situazione giuridica (v. sentenze del 19 gennaio 2017, Commissione/Total e Elf Aquitaine, C-351/15 P, EU:C:2017:27, punti 35 e 36 e giurisprudenza ivi citata, e del 16 luglio 2020, Inclusion Alliance for Europe/Commissione, C-378/16 P, EU:C:2020:575, punto 71 e giurisprudenza ivi citata).

25 Per stabilire se un atto produca effetti giuridici vincolanti, occorre, conformemente a una giurisprudenza costante della Corte, riferirsi alla sua sostanza e valutarne gli effetti in funzione di criteri obiettivi, quali il contenuto dell'atto stesso, tenendo conto, eventualmente, del contesto in

cui esso è stato adottato nonché dei poteri dell'istituzione, dell'organo o dell'organismo dell'Unione da cui esso promana (v. sentenza del 15 luglio 2021, FBF, C-911/19, EU:C:2021:599, punto 38 e giurisprudenza ivi citata).

26 Nel caso di specie, il ricorrente chiede l'annullamento dei trasferimenti controversi, che, a suo avviso, hanno avuto luogo in tre occasioni. In primo luogo, in occasione della sua consultazione del sito Internet della CAE del 30 marzo 2022 (in prosieguo: il «trasferimento controverso in occasione della consultazione del sito Internet della CAE del 30 marzo 2022»), alcuni dati personali ad esso appartenenti, in particolare il suo indirizzo IP nonché informazioni sul suo browser e sul suo terminale, sarebbero stati trasferiti all'impresa americana Amazon Web Services, nella sua qualità di operatore della rete di diffusione di contenuti denominata Amazon CloudFront, che sarebbe utilizzata da detto sito Internet.

27 In secondo luogo, al momento della connessione stabilita dal ricorrente, il 30 marzo 2022, al servizio di autenticazione utente della Commissione EU Login, utilizzando il suo account Facebook, al fine di iscriversi all'evento «GoGreen» sul sito Internet della CAE (in prosieguo: il «trasferimento controverso al momento della connessione all'EU Login del 30 marzo 2022»), alcuni dati personali ad esso appartenenti, in particolare il suo indirizzo IP nonché informazioni sul suo browser e sul suo terminale, sarebbero stati trasferiti all'impresa americana Meta Platforms, Inc.

28 In terzo luogo, in occasione delle consultazioni, da parte del ricorrente, del sito Internet della CAE dell'8 giugno 2022 (in prosieguo: il «trasferimento controverso in occasione delle consultazioni del sito Internet della CAE dell'8 giugno 2022»), alcuni dati personali ad esso appartenenti sarebbero stati trasferiti verso un server di Amazon CloudFront situato a Newark (New Jersey, Stati Uniti).

29 Peraltro, il ricorrente menziona nel suo ricorso di aver avuto accesso al sito Internet della CAE il 9 novembre 2021 e di essersi iscritto sul sito Internet della CAE in tale data avvalendosi del suo account Facebook. Tuttavia, esso non deduce alcun elemento concreto che consenta di concludere che tali circostanze sono oggetto della sua domanda di annullamento dei trasferimenti controversi. Occorre quindi prendere in considerazione unicamente i trasferimenti controversi menzionati ai precedenti punti da 26 a 28.

30 Occorre rilevare che i trasferimenti controversi di cui il ricorrente chiede l'annullamento, menzionati ai precedenti punti da 26 a 28, corrispondono, secondo lo stesso ricorrente, ad operazioni informatiche di migrazione di dati che sarebbero state lanciate da sistemi o servizi informatici della Commissione, in particolare il sito Internet della CAE, verso server appartenenti a imprese terze stabilite al di fuori del territorio dell'Unione.

31 È certamente vero che l'operazione consistente nel trasferire dati personali da un'istituzione o da un organismo dell'Unione verso un paese terzo costituisce, in quanto tale, un trattamento di dati personali, ai sensi dell'articolo 3, punto 3, del regolamento 2018/1725, effettuato nel territorio dell'Unione, trattamento al quale tale regolamento si applica in forza del suo articolo 2, paragrafo 5 (v., per analogia, sentenza del 16 luglio 2020, Facebook Ireland e Schrems, C-311/18, in prosieguo: la «sentenza Schrems II», EU:C:2020:559, punto 83).

32 Tuttavia, non tutte le operazioni che possono comportare un trasferimento di dati personali, ai sensi dell'articolo 3, punto 3, del regolamento 2018/1725, costituiscono atti impugnabili, ai sensi dell'articolo 263 TFUE, come interpretato dalla giurisprudenza richiamata al precedente punto 24.

33 Nel caso di specie, anche supponendo che i trasferimenti controversi siano dimostrati, è giocoforza constatare che essi costituiscono atti materiali e non atti giuridici. Infatti, i trasferimenti controversi, come descritti nel ricorso, sono operazioni informatiche di migrazione di dati da un terminale o da un server ad un altro, che risultano dalle interazioni tra il ricorrente e sistemi o servizi informatici della Commissione, durante le consultazioni del sito Internet della CAE o del servizio EU Login. Per contro, 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.

34 Pertanto, 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 al precedente punto 24. Essi non possono quindi essere considerati atti impugnabili ai sensi dell'articolo 263 TFUE.

35 Ne consegue che la domanda di annullamento del ricorrente deve essere respinta in quanto irricevibile.

Ricevibilità della domanda di declaratoria di carenza

36 Con il secondo capo della sua domanda, il ricorrente chiede al Tribunale di dichiarare che la Commissione si è illegittimamente astenuta dal prendere posizione sulla richiesta di informazioni del 1º aprile 2022.

37 Nel suo controricorso, la Commissione eccepisce l'irricevibilità di tale domanda di declaratoria di carenza, a causa dell'assenza di una richiesta di agire ai sensi dell'articolo 265, secondo comma, TFUE. In subordine, la Commissione fa valere che non vi è più luogo a statuire sulla domanda di declaratoria di carenza, tenuto conto della sua risposta al ricorrente con messaggio di posta elettronica del 30 giugno 2022.

38 Il ricorrente sostiene, in sostanza, che la Commissione è sempre obbligata a rispondere alla richiesta di informazioni del 1º aprile 2022, dato che le informazioni da essa fornite con il suo messaggio di posta elettronica del 30 giugno 2022 sono insufficienti e inesatte.

39 Secondo una costante giurisprudenza, alla base del ricorso previsto dall'articolo 265 TFUE vi è l'idea secondo cui l'inerzia illegittima dell'istituzione chiamata in causa consente di adire il giudice dell'Unione affinché egli dichiari che il fatto di astenersi dall'agire è contrario al Trattato, qualora l'istituzione interessata non abbia posto rimedio a tale astensione (sentenza del 12 luglio 1988, Parlamento/Consiglio, 377/87, EU:C:1988:387, punto 9; v., altresì, sentenza del 16 dicembre 2015, Svezia/Commissione, T-521/14, non pubblicata, EU:T:2015:976, punto 33 e la giurisprudenza ivi citata).

40 In un caso nel quale l'atto la cui omissione costituisce l'oggetto della controversia è stato adottato dopo la proposizione del ricorso, ma prima che sia pronunciata la sentenza, la declaratoria del giudice dell'Unione dell'illegittimità dell'iniziale astensione non può più produrre gli effetti contemplati dall'articolo 266 del Trattato. Ne risulta che, in un caso del genere, l'oggetto del ricorso viene meno, sicché non vi è più luogo a statuire (sentenza del 12 luglio 1988, Parlamento/Consiglio, 377/87, EU:C:1988:387, punti 10 e 11; v., altresì, ordinanza del 13 dicembre 2000, Sodima/Commissione, C-44/00 P, non pubblicata, EU:T:2000:686, punto 83 e giurisprudenza ivi citata).

41 Nel caso di specie, occorre constatare che la Commissione ha risposto alla richiesta di informazioni del 1º aprile 2022, con il suo messaggio di posta elettronica del 30 giugno 2022 (v. punto 11 *supra*). La Commissione ha quindi posto fine alla carenza lamentata dal ricorrente nell'ambito del presente ricorso, dopo la proposizione di tale ricorso. Il secondo capo della domanda diretto a far dichiarare, sulla base dell'articolo 265 TFUE, una carenza della Commissione in assenza di risposta alla richiesta di informazioni del 1º aprile 2022 è quindi divenuto privo di oggetto.

42 Il fatto che il contenuto del messaggio di posta elettronica della Commissione del 30 giugno 2022 non corrisponda alla risposta auspicata dal ricorrente è irrilevante al riguardo. Infatti, la circostanza che tale presa di posizione dell'istituzione non dia soddisfazione alla parte ricorrente è al riguardo irrilevante, 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 (v. ordinanza del 6 aprile 2017, Brancheforeningen for Regulerkraft i Danmark/Commissione, T-203/16, non pubblicata, EU:T:2017:279, punto 22 e giurisprudenza ivi citata).

43 Ne consegue che non vi è più luogo a statuire sulla domanda di declaratoria di carenza del ricorrente e che non occorre pronunciarsi sull'irricevibilità di tale domanda sollevata dalla Commissione.

Sulla richiesta di risarcimento danni

44 Con il suo terzo capo della domanda, il ricorrente formula due domande di risarcimento danni. In primo luogo, egli chiede il versamento di EUR 800 a titolo di risarcimento del danno morale che avrebbe subito a causa del mancato rispetto, da parte della Commissione, del suo diritto di accesso alle informazioni, in violazione dell'articolo 14, paragrafi 3 e 4, e dell'articolo 17, paragrafi 1 e 2, del regolamento 2018/1725 nonché del principio di trasparenza previsto all'articolo 4, paragrafo 1, lettera a), di detto regolamento. In secondo luogo, egli chiede il versamento di EUR 400 a titolo di risarcimento del danno morale che avrebbe subito a causa dei trasferimenti controversi, avvenuti in violazione dell'articolo 46 e dell'articolo 48, paragrafo 1, e paragrafo 2, lettera b), del regolamento 2018/1725.

45 La Commissione conclude per il rigetto della domanda di risarcimento danni.

Considerazioni preliminari sulle condizioni per il sorgere della responsabilità extracontrattuale dell'Unione nell'ambito del regolamento 2018/1725

46 L'articolo 65 del regolamento 2018/1725 prevede che chiunque subisca un danno materiale o immateriale causato da una violazione di detto regolamento ha il diritto di ottenere il risarcimento del danno dall'istituzione o dall'organo dell'Unione, fatte salve le «condizioni previste dai trattati».

47 Occorre interpretare tale articolo 65 del regolamento 2018/1725 nel senso che esso prevede che il diritto di ottenere dall'istituzione o dall'organo dell'Unione il risarcimento del danno subito a causa di una violazione di tale regolamento è subordinato alle condizioni di cui all'articolo 340, secondo comma, TFUE, in forza del quale l'Unione deve risarcire, conformemente ai principi generali comuni ai diritti degli Stati membri, i danni cagionati dalle sue istituzioni o dai suoi agenti nell'esercizio delle loro funzioni.

48 Secondo una giurisprudenza costante, il sorgere della responsabilità extracontrattuale dell'Unione presuppone il ricorrere di tre condizioni cumulative, vale a dire l'illiceità del comportamento contestato alle istituzioni, l'effettività del danno e l'esistenza di un nesso di causalità fra tale comportamento e il danno lamentato (v., in tal senso, sentenze del 4 luglio 2000, Bergaderm e Goupil/Commissione, C-352/98 P, EU:C:2000:361, punti da 39 a 42, e del 28 ottobre 2021, Vialto Consulting/Commissione, C-650/19 P, EU:C:2021:879, punto 138).

49 Il carattere cumulativo di tali condizioni implica che, qualora una di esse non sia soddisfatta, il ricorso per risarcimento danni deve essere respinto integralmente, senza che sia necessario esaminare le altre condizioni (sentenza del 9 settembre 1999, Lucaccioni/Commissione, C-257/98 P, EU:C:1999:402, punti 14 e 63; v., altresì, sentenza del 25 febbraio 2021, Dalli/Commissione, C-615/19 P, EU:C:2021:133, punto 42 e giurisprudenza ivi citata).

50 Con riferimento alla prima delle condizioni, la giurisprudenza richiede che sia accertata una violazione sufficientemente qualificata di una norma di diritto preordinata a conferire diritti ai singoli (v. sentenza del 4 luglio 2000, Bergaderm e Goupil/Commissione, C-352/98 P, EU:C:2000:361, punto 42 e giurisprudenza ivi citata).

51 Tale presupposto di una violazione sufficientemente qualificata del diritto dell'Unione è diretto, indipendentemente dalla natura dell'atto illecito in questione, ad evitare che il rischio di dover risarcire i danni addotti dai soggetti interessati ostacoli la capacità dell'istituzione di cui trattasi di esercitare pienamente le sue funzioni nell'interesse generale, tanto nell'ambito della sua attività normativa o implicante scelte di politica economica che nell'ambito della propria competenza amministrativa, senza per questo lasciare a carico dei singoli l'onere delle conseguenze di violazioni flagranti e inescusabili (v., in tal senso, sentenza del 14 dicembre 2018, East West Consulting/Commissione, T-298/16, EU:T:2018:967, punto 124 e giurisprudenza ivi citata).

52 Il criterio decisivo per considerare una violazione sufficientemente qualificata è quello della violazione manifesta e grave, commessa dall'istituzione o dall'organo dell'Unione in questione, dei limiti posti al suo potere discrezionale. Qualora l'istituzione o l'organo in questione disponga solamente di un margine di discrezionalità considerevolmente ridotto, se non addirittura inesistente, la semplice trasgressione del diritto dell'Unione può essere sufficiente per constatare l'esistenza di una violazione sufficientemente qualificata (v. sentenza del 10 dicembre 2002, Commissione/Camar e Tico, C-312/00 P, EU:C:2002:736, punto 54 e giurisprudenza ivi citata). Tuttavia, tale giurisprudenza non stabilisce alcun nesso automatico tra la mancanza di potere discrezionale dell'istituzione interessata, per un verso, e la qualificazione dell'infrazione come violazione sufficientemente qualificata del diritto dell'Unione, per altro verso (sentenza del 3 marzo 2010, Artegodan/Commissione, T-429/05, EU:T:2010:60, punto 59). Infatti, la portata del potere discrezionale dell'istituzione interessata – quantunque presenti un carattere determinante – non costituisce un criterio esclusivo. A tale proposito, la Corte ha costantemente ricordato che il regime che essa ha sviluppato ai sensi dell'articolo 340, secondo comma, TFUE tiene segnatamente conto, inoltre, della complessità delle situazioni da disciplinare e delle difficoltà di applicazione o di interpretazione dei testi (v. sentenza del 23 novembre 2011, Sison/Consiglio, T-341/07, EU:T:2011:687, punti 36 e 37 e giurisprudenza ivi citata) o, più in generale, dell'ambito, delle condizioni e del contesto in cui la norma violata si impone all'istituzione o all'organo dell'Unione interessato (v. sentenza del 4 aprile 2017, Mediatore/Staelen, C-337/15 P, EU:C:2017:256, punto 40 e giurisprudenza ivi citata).

53 Ne deriva che soltanto la constatazione di un'irregolarità che, in circostanze analoghe, non sarebbe stata commessa da un'amministrazione normalmente prudente e diligente consente il sorgere della responsabilità dell'Unione. Spetta pertanto al giudice dell'Unione, dopo aver determinato, anzitutto, se l'istituzione interessata disponesse di un margine discrezionale, prendere in considerazione la complessità della situazione da disciplinare, le difficoltà d'applicazione o di interpretazione dei testi, il grado di chiarezza e di precisione della norma violata e l'intenzionalità o l'inescusabilità dell'errore commesso (sentenza del 3 marzo 2010, Artegodan/Commissione, T-429/05, EU:T:2010:60, punto 62).

54 Per quanto riguarda la condizione relativa all'effettività del danno, quest'ultimo dev'essere reale e certo, circostanza che spetta alla parte ricorrente provare (v. sentenza del 9 novembre 2006, Agraz e a./Commissione, C-243/05 P, EU:C:2006:708, punto 27 e giurisprudenza ivi citata). Per contro, un danno puramente ipotetico e indeterminato non dà diritto a risarcimento (v. sentenza del 26 ottobre 2011, Dufour/BCE, T-436/09, EU:T:2011:634, punto 192 e giurisprudenza ivi citata).

55 Per quanto riguarda il presupposto relativo al nesso causale, esso concerne l'esistenza di un rapporto di causa-effetto sufficientemente diretto tra il comportamento dell'istituzione e il danno, nesso di cui spetta alla parte ricorrente fornire la prova, di modo che il comportamento addebitato deve essere la causa determinante del danno (v. sentenza del 13 dicembre 2018, Unione europea/ASPLA e Armando Álvarez, C-174/17 P e C-222/17 P, EU:C:2018:1015, punto 23 e giurisprudenza ivi citata).

56 Peraltro, occorre ricordare che l'azione risarcitoria, fondata sull'articolo 340, secondo comma, TFUE, è stata istituita come un rimedio autonomo, dotato di una sua particolare funzione nell'ambito del regime dei mezzi di ricorso e subordinato, quanto al suo esercizio, a condizioni attinenti al suo specifico oggetto, di modo che la dichiarazione di irricevibilità della domanda di annullamento non comporta automaticamente quella della domanda di risarcimento danni (v. sentenza del 5 settembre 2019, Unione europea/Guardian Europe e Guardian Europe/Unione europea, C-447/17 P e C-479/17 P, EU:C:2019:672, punto 49 e giurisprudenza ivi citata).

57 Ne consegue che il rigetto della domanda di annullamento in ragione della sua irricevibilità e il rigetto della domanda in carenza in quanto non vi è più luogo a statuire su di essa, conformemente ai precedenti punti 35 e 43, non implica, di conseguenza, il rigetto in quanto irricevibili delle domande di risarcimento menzionate al precedente punto 44.

58 È alla luce di tali considerazioni che occorre esaminare le censure dedotte dal ricorrente nell'ambito delle sue domande di risarcimento danni.

Sulla prima domanda di risarcimento danni, diretta al risarcimento del danno morale derivante da una violazione del diritto di accesso alle informazioni

59 Con la sua prima domanda di risarcimento danni, il ricorrente chiede la condanna della Commissione a versargli la somma di EUR 800, a titolo di risarcimento del danno morale subito a seguito della violazione del suo diritto di accesso alle informazioni.

60 Anzitutto, il ricorrente contesta alla Commissione di non aver risposto alla richiesta di informazioni del 1º aprile 2022 entro il termine impartito e di non avergli comunicato i motivi della sua inerzia, in violazione dell'articolo 14, paragrafi 3 e 4, e dell'articolo 17, paragrafi 1 e 2, del regolamento 2018/1725 nonché del principio di trasparenza, previsto all'articolo 4, paragrafo 1, lettera a), del medesimo regolamento. Inoltre, la Commissione non avrebbe rispettato

l'articolo 17, paragrafo 1, lettera c), e paragrafo 2, del regolamento 2018/1725, in quanto la dichiarazione relativa alla tutela della vita privata, che figura sul sito Internet della CAE, non conterrebbe informazioni relative al trasferimento di dati personali verso paesi terzi e ad eventuali garanzie adeguate ai fini di detto trasferimento, come sarebbe richiesto dall'articolo 48 di detto regolamento. Inoltre, nel messaggio di posta elettronica del 3 dicembre 2021, la Commissione avrebbe fornito informazioni errate, nei limiti in cui ha negato il trasferimento di dati personali del ricorrente verso destinatari situati negli Stati Uniti.

61 Il ricorrente sostiene poi che l'inerzia illecita della Commissione gli ha impedito di controllare il trattamento dei suoi dati personali, il che costituisce un danno morale ai sensi del considerando 46 del regolamento 2018/1725. Infine, egli fa valere che tale danno morale, che egli stima in EUR 800, è direttamente causato dal comportamento illecito della Commissione.

62 La Commissione contesta tali argomenti, facendo valere, in sostanza, che nessuna delle condizioni per il sorgere della responsabilità extracontrattuale è soddisfatta nel caso di specie.

63 Anzitutto, per quanto riguarda la condizione relativa all'illegittimità del comportamento contestato, occorre verificare se il ricorrente abbia invocato la violazione di norme giuridiche preordinate a conferire diritti ai singoli.

64 A tal riguardo, occorre osservare che l'articolo 17, paragrafo 1, lettera c), del regolamento 2018/1725 sancisce un diritto di accesso dell'interessato alle informazioni riguardanti i destinatari ai quali i suoi dati personali sono stati comunicati, in particolare i destinatari stabiliti in paesi terzi. Tale disposizione concretizza quindi il principio, sancito all'articolo 4, paragrafo 1, lettera a), del regolamento 2018/1725, secondo il quale qualsiasi informazione e comunicazione relativa al trattamento dei dati personali deve essere facilmente accessibile.

65 Inoltre, l'articolo 14, paragrafo 3, del regolamento 2018/1725 impone un termine di un mese al responsabile del trattamento dei dati personali per rispondere alle richieste di informazioni. Inoltre, l'articolo 14, paragrafo 4, di tale regolamento impone al titolare del trattamento dei dati personali, nel caso in cui decida di non dare seguito alla richiesta, di informare il richiedente, entro un mese, dei motivi della sua inerzia e della possibilità di presentare un reclamo al garante europeo della protezione dei dati (GEPD) e di proporre ricorso giurisdizionale. Tali disposizioni sono quindi norme di procedura amministrativa che contribuiscono all'attuazione del diritto di accesso alle informazioni sui dati personali della persona interessata, concretizzandolo e modulandolo. Inoltre, tali disposizioni contribuiscono alla concretizzazione del diritto riconosciuto a ogni persona, in forza dell'articolo 41 della Carta, a che il suo caso sia trattato entro un termine ragionevole dalle istituzioni e dagli organi dell'Unione.

66 Di conseguenza, le disposizioni dell'articolo 4, paragrafo 1, lettera a), dell'articolo 14, paragrafi 3 e 4, e dell'articolo 17, paragrafo 1, lettera c), del regolamento 2018/1725, lette in combinato disposto, costituiscono norme giuridiche preordinate a conferire diritti ai singoli, ai sensi della giurisprudenza menzionata al precedente punto 50.

67 Occorre poi esaminare se nel caso di specie sia dimostrata una violazione di tali disposizioni da parte della Commissione.

68 Da un lato, il ricorrente sostiene che la Commissione ha violato l'articolo 17, paragrafo 1, lettera c), e paragrafo 2, del regolamento 2018/1725, in quanto la dichiarazione relativa alla tutela della vita privata che figura sul sito Internet della CAE non conterrebbe informazioni sul trasferimento di dati personali a destinatari stabiliti in paesi terzi, su eventuali garanzie adeguate relative a detto trasferimento, o sull'identificazione dei contraenti quali destinatari di tali dati.

69 Come menzionato al precedente punto 64, l'articolo 17, paragrafo 1, lettera c), e paragrafo 2, del regolamento 2018/1725 prevede che l'interessato abbia, in particolare, il diritto di ottenere informazioni sui destinatari stabiliti in paesi terzi, ai quali i dati personali sono stati comunicati, nonché sulle garanzie adeguate per i trasferimenti di dati a tali destinatari.

70 Ne consegue che tali disposizioni stabiliscono un diritto di accesso della persona interessata a talune informazioni, ma non prevedono che dette informazioni debbano figurare obbligatoriamente su un determinato documento, o addirittura su una dichiarazione relativa alla tutela della vita privata, come quella che figura sul sito Internet della CAE. In altri termini, da tali disposizioni non risulta che le informazioni di cui trattasi debbano essere divulgate mediante detta dichiarazione. Ciò premesso, il ricorrente, al pari di qualsiasi persona interessata, conserva il diritto di ottenere siffatte informazioni mediante l'esercizio del suo diritto di accesso alle informazioni, sancito all'articolo 17, paragrafo 1, lettera c), e paragrafo 2, del regolamento 2018/1725, ove tale questione eccede la portata dell'illegittimità che il ricorrente addebita alla Commissione, la quale è limitata al contenuto della dichiarazione relativa alla tutela della vita privata (v. *supra*, punto 45).

71 In ogni caso, nella specie, dal testo di detta dichiarazione relativa alla tutela della vita privata, allegata al ricorso, risulta che essa contiene informazioni riguardanti i destinatari o le categorie di destinatari ai quali i dati personali sono stati o saranno comunicati. In tal senso, al punto 7 di detta dichiarazione è menzionato, in particolare, che l'accesso ai dati è «accordato al personale autorizzato della [Commissione] e ai suoi contraenti incaricati di effettuare l'operazione di trattamento di cui trattasi, conformemente al principio della "necessità di sapere"». Inoltre, l'argomento del ricorrente relativo al fatto che detta dichiarazione non conterrebbe informazioni sul trasferimento di dati personali a destinatari stabiliti in paesi terzi è fondato sull'ipotesi secondo cui la consultazione del sito Internet della CAE implica un trasferimento di dati personali degli utenti verso un paese terzo. Tuttavia, la presente domanda di risarcimento danni è fondata sulla violazione del diritto di accesso alle informazioni e non su quella delle disposizioni relative al trasferimento di dati personali verso paesi terzi che, peraltro, è alla base della seconda domanda di risarcimento danni.

72 Pertanto, non è dimostrato nel caso di specie che la Commissione abbia violato l'articolo 17, paragrafo 1, lettera c), e paragrafo 2, del regolamento 2018/1725, per quanto riguarda la dichiarazione relativa alla tutela della vita privata che figura sul sito Internet della CAE.

73 D'altra parte, il ricorrente contesta alla Commissione di non aver risposto alla richiesta di informazioni del 1º aprile 2022 entro il termine impartito e di non averlo informato dei motivi della sua inerzia, in violazione dell'articolo 14, paragrafi 3 e 4, e dell'articolo 17, paragrafi 1 e 2, del regolamento 2018/1725 nonché del principio di trasparenza. Inoltre, la Commissione gli avrebbe comunicato informazioni errate nel messaggio di posta elettronica del 3 dicembre 2021.

74 Occorre anzitutto osservare che il ricorrente non deduce alcun argomento concreto a sostegno di una violazione del principio di trasparenza. Tale argomento non ha quindi contenuto autonomo rispetto alla censura relativa al mancato rispetto del termine di risposta alla richiesta di informazioni e all'obbligo di comunicare i motivi del superamento di tale termine.

75 Inoltre, gli argomenti del ricorrente vertenti su una violazione dell'articolo 17, paragrafi 1 e 2, del regolamento 2018/1725 nonché sul fatto che la Commissione gli avrebbe comunicato informazioni errate nel messaggio di posta elettronica del 3 dicembre 2021 sono fondati sull'ipotesi secondo cui la consultazione del sito Internet della CAE implica un trasferimento di dati personali degli utenti verso un paese terzo. Orbene, come menzionato al precedente punto 71, la presente domanda di risarcimento danni è fondata sulla violazione del diritto di accesso alle informazioni e non su quella delle disposizioni relative al trasferimento di dati personali verso paesi terzi che è alla base della seconda domanda di risarcimento danni.

76 Pertanto, non è dimostrato nel caso di specie che la Commissione abbia violato l'articolo 17, paragrafi 1 e 2, del regolamento 2018/1725.

77 Per quanto riguarda la censura del ricorrente relativa alla violazione dell'articolo 14, paragrafi 3 e 4, del regolamento 2018/1725, dal fascicolo risulta che la Commissione ha risposto alla richiesta di informazioni del 9 novembre 2021 entro il termine di un mese previsto all'articolo 14, paragrafo 3, del regolamento 2018/1725 (v. *supra*, punti 5 e 7). Per quanto riguarda la richiesta di informazioni del 1º aprile 2022, la Commissione ha informato il ricorrente, con messaggio di posta elettronica del 30 giugno 2022, di ritenere che la richiesta di informazioni del 1º aprile 2022 fosse quasi identica alla richiesta di informazioni del 9 novembre 2021 e di aver già risposto a quest'ultima con il suo messaggio di posta elettronica del 3 dicembre 2021 (v. *supra*, punto 11).

78 Ne consegue che, per quanto riguarda la richiesta di informazioni del 1º aprile 2022, la Commissione non ha rispettato il termine di un mese, previsto all'articolo 14, paragrafo 4, del regolamento 2018/1725 (v. *supra*, punto 65).

79 Dai precedenti punti da 68 a 78 risulta che l'unica illegittimità contestata alla Commissione che è accertata nel caso di specie è quella del mancato rispetto del termine previsto all'articolo 14, paragrafo 4, del regolamento 2018/1725.

80 In tali circostanze, e indipendentemente dalla questione se l'inosservanza di detto termine da parte della Commissione costituisca una violazione sufficientemente qualificata di una norma giuridica, occorre esaminare anzitutto se l'inosservanza di tale termine abbia causato al ricorrente un danno morale reale e certo, ai sensi della giurisprudenza richiamata al precedente punto 54.

81 Per quanto riguarda l'effettività del danno morale asseritamente subito, occorre ricordare che, sebbene la presentazione di un'offerta di prova non sia necessariamente considerata come una condizione per il riconoscimento di un danno morale, spetta tuttavia alla parte ricorrente dimostrare che il comportamento contestato all'istituzione interessata era idoneo a causarle un danno del genere (sentenza del 16 luglio 2009, SELEX Sistemi Integrati/Commissione, C-481/07 P, non pubblicata, EU:C:2009:461, punto 38; v., altresì, sentenza del 2 luglio 2019, Fulmen/Consiglio, T-405/15, EU:T:2019:469, punto 188 e giurisprudenza ivi citata).

82 Nel caso di specie, il ricorrente chiede il risarcimento di un danno morale di importo pari a EUR 800, sostenendo che il comportamento contestato alla Commissione gli ha impedito di controllare il trattamento dei suoi dati personali.

83 Tuttavia, è giocoforza constatare che un siffatto danno morale non è dimostrato nel caso di specie. Infatti, l'unica illegittimità accertata nel caso di specie è quella del mancato rispetto, da parte della Commissione, del termine di un mese previsto all'articolo 14, paragrafo 4, del regolamento 2018/1725 (v. *supra*, punto 79). Orbene, tale termine non è stato superato di più di due mesi (v. *supra*, punto 77). Inoltre, le richieste di informazioni del 9 novembre 2021 e del 1º aprile 2022 erano sostanzialmente le stesse (v. *supra*, punti 5 e 8), cosicché il ricorrente aveva già ricevuto una risposta ad almeno una parte della sua richiesta di informazioni il 3 dicembre 2021, data in cui la Commissione ha risposto alla richiesta di informazioni del 9 novembre 2021 (v. *supra*, punto 7).

84 Peraltro, l'argomento del ricorrente relativo alla comunicazione di informazioni errate (v. *supra*, punto 75) riguarda la fondatezza delle informazioni e non il rispetto della norma procedurale la cui violazione è stata stabilita *supra*, al punto 78, e non è quindi pertinente per dimostrare il danno morale lamentato.

85 Ne consegue che non è dimostrato che l'inosservanza, da parte della Commissione, del termine previsto all'articolo 14, paragrafo 4, del regolamento 2018/1725 fosse tale da causare al ricorrente il danno morale lamentato.

86 Di conseguenza, dal momento che una delle condizioni cumulative per il sorgere della responsabilità extracontrattuale dell'Unione, previste all'articolo 340, secondo comma, TFUE, non sussiste, occorre respingere la prima domanda di risarcimento del ricorrente.

Sulla seconda domanda di risarcimento danni, diretta alla riparazione del danno morale derivante dai trasferimenti controversi

87 Con la sua seconda domanda di risarcimento, il ricorrente chiede il versamento di EUR 400 a titolo di risarcimento del danno morale che avrebbe subito a causa dei trasferimenti controversi menzionati ai precedenti punti da 26 a 28, ossia il trasferimento controverso in occasione della consultazione del sito Internet della CAE del 30 marzo 2022, il trasferimento controverso in occasione della connessione all'EU Login del 30 marzo 2022 e il trasferimento controverso in occasione delle consultazioni del sito Internet della CAE dell'8 giugno 2022.

88 Il ricorrente sostiene, in sostanza, che i trasferimenti controversi hanno avuto luogo verso destinatari stabiliti negli Stati Uniti, paese che non ha un livello di protezione adeguato. La Commissione non avrebbe menzionato alcuna delle garanzie adeguate che potessero giustificare tali trasferimenti, previste al capo V del regolamento 2018/1725, e avrebbe quindi violato l'articolo 46 e l'articolo 48, paragrafo 1, e paragrafo 2, lettera b), di tale regolamento nonché gli articoli 7, 8 e 47 della Carta. I trasferimenti controversi avrebbero dato luogo a un rischio di accesso ai dati del ricorrente da parte dei servizi di sicurezza e di intelligence di tale paese e, di conseguenza, gli avrebbero causato un danno morale, ai sensi del considerando 46 del regolamento 2018/1725, in quanto egli è stato privato dei suoi diritti e delle sue libertà e gli è stato impedito di esercitare il controllo sui suoi dati.

89 La Commissione contesta tali argomenti, facendo valere, in sostanza, che le condizioni per il sorgere della responsabilità extracontrattuale non sono soddisfatte nel caso di specie.

– Considerazioni preliminari sulle disposizioni relative al trasferimento di dati personali verso un paese terzo

90 In primo luogo, ai sensi del suo articolo 2, paragrafo 5, il regolamento 2018/1725 si applica al trattamento, interamente o parzialmente automatizzato, di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

91 In secondo luogo, occorre interpretare la nozione di «dati personali» come corrispondente a qualsiasi informazione riguardante una persona fisica identificata o identificabile, ai sensi dell'articolo 3, punto 1, del regolamento 2018/1725.

92 In terzo luogo, occorre osservare che il trasferimento di dati costituisce un'operazione di «trattamento» di dati ai sensi dell'articolo 3, punto 3, del regolamento 2018/1725.

93 In quarto luogo, occorre osservare che i «trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali» sono disciplinati dal capo V del regolamento 2018/1725, il quale tuttavia non li definisce.

94 Tuttavia, dal considerando 63 del regolamento 2018/1725 risulta che i trasferimenti di cui al capo V di tale regolamento riguardano i dati personali trasferiti dalle istituzioni e dagli organismi dell'Unione a responsabili del trattamento, incaricati del trattamento o altri destinatari in paesi terzi o a organizzazioni internazionali.

95 Inoltre, da un'interpretazione sistematica del regolamento 2018/1725 risulta che il trasferimento di dati personali verso paesi terzi, ai sensi del suo articolo 46, richiede, in primo luogo, che il responsabile del trattamento dei dati di cui trattasi appartenga a un'istituzione o a un organismo dell'Unione e sia quindi soggetto a detto regolamento (articolo 1 del regolamento 2018/1725); in secondo luogo, che il responsabile del trattamento metta, mediante trasmissione o in altro modo, dati personali a disposizione di un destinatario, in particolare di un'altra persona fisica o giuridica (articolo 3, punti 3 e 13, del regolamento 2018/1725) e, in terzo luogo, che tale destinatario sia stabilito in un paese terzo (articolo 46 del regolamento 2018/1725), vale a dire un paese che non è membro né dell'Unione né dello Spazio economico europeo (SEE).

96 In quinto luogo, occorre constatare che le disposizioni del capo V del regolamento 2018/1725 mirano a preservare, in occasione dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali, il livello di protezione delle persone fisiche garantito nell'Unione, conformemente all'obiettivo precisato al suo considerando 63.

97 In sesto luogo, l'articolo 46 del regolamento 2018/1725 prevede un principio generale secondo cui il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale può aver luogo solo se, fatte salve le altre disposizioni di tale regolamento, il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al suo capo V.

98 In settimo luogo, per quanto riguarda le condizioni definite nel capo V del regolamento 2018/1725, occorre osservare che l'articolo 47, paragrafo 1, di tale regolamento prevede che il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale possa aver luogo se la Commissione ha deciso, mediante una decisione di adeguatezza adottata, in particolare, ai sensi dell'articolo 45, paragrafo 3, del regolamento 2016/679, che il paese o

l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato e che il trasferimento di dati personali avviene esclusivamente per consentire l'esecuzione dei compiti che rientrano nella competenza del titolare del trattamento.

99 A tal riguardo, occorre ricordare che le due decisioni di adeguatezza della Commissione relative agli Stati Uniti sono state dichiarate invalide. Da un lato, con la sentenza del 6 ottobre 2015, Schrems (C-362/14, EU:C:2015:650), la Corte ha dichiarato invalida la decisione n. 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi dell'«approdo sicuro» e dalle relative «Domande più frequenti» (FAQ) spesso sollevate, pubblicate dal Dipartimento del Commercio degli Stati Uniti (GU 2000, L 215, pag. 7). D'altra parte, con la sentenza Schrems II, la Corte ha dichiarato invalida la 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 dallo scudo UE-USA per la privacy (GU 2016, L 207, pag. 1).

100 Ne consegue 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.

101 In assenza di una decisione di adeguatezza della Commissione riguardante gli Stati Uniti, si applica l'articolo 48, paragrafo 1, del regolamento 2018/1725, secondo il quale il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale può avvenire solo se il titolare del trattamento o il responsabile del trattamento ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e di mezzi di ricorso effettivi.

102 Le garanzie adeguate di cui all'articolo 48, paragrafo 1, del regolamento 2018/1725, elencate all'articolo 48, paragrafi 2 e 3, di tale regolamento, possono essere fornite, in particolare, mediante clausole tipo di protezione dei dati, adottate dalla Commissione, conformemente all'articolo 48, paragrafo 2, lettera b), di tale regolamento.

103 Tuttavia, le clausole tipo di protezione dei dati previste all'articolo 48, paragrafo 2, lettera b), del regolamento 2018/1725 possono richiedere l'adozione di misure supplementari al fine di garantire il rispetto del livello di protezione adeguato, alla luce del diritto dell'Unione (v., per analogia, sentenza Schrems II, punti 133 e 134).

104 Inoltre, le garanzie adeguate di cui all'articolo 48, paragrafo 1, del regolamento 2018/1725 possono essere fornite, in particolare, mediante clausole contrattuali, previste all'articolo 48, paragrafo 3, lettera a), di detto regolamento, stipulate tra, da un lato, il titolare del trattamento o il responsabile del trattamento e, dall'altro, il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo, previa autorizzazione del GEPD.

105 Inoltre, occorre ricordare che gli articoli 7, 8 e 47 della Carta stabiliscono, rispettivamente, il diritto al rispetto della vita privata, il diritto alla protezione dei dati di carattere personale e il diritto a un ricorso effettivo e a un giudice imparziale.

106 Nel caso di specie, occorre anzitutto osservare che la seconda domanda di risarcimento danni del ricorrente è fondata su una violazione, da parte della Commissione, delle disposizioni dell'articolo 46 e dell'articolo 48, paragrafo 1, e paragrafo 2, lettera b), del regolamento 2018/1725 nonché degli articoli 7, 8 e 47 della Carta. Orbene, dai precedenti punti da 91 a 105 risulta che

dette 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.

107 Ne consegue che le disposizioni la cui violazione è invocata dal ricorrente a sostegno della sua seconda domanda di risarcimento danni 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.

108 Occorre ora verificare se le condizioni per il sorgere della responsabilità extracontrattuale della Commissione siano soddisfatte per ciascuno dei tre trasferimenti controversi menzionati al precedente punto 87.

109 Dato che i trasferimenti controversi menzionati ai punti 26 e 28 *supra* avrebbero avuto luogo a causa dell'utilizzo, da parte del sito Internet della CAE, della rete di diffusione di contenuti o «RDC» (in inglese, «content delivery network» o «CDN») denominato Amazon CloudFront (in prosieguo: il «servizio Amazon CloudFront»), occorre anzitutto ricercare le condizioni di funzionamento di tale servizio nell'ambito di questo sito Internet.

– *Sul funzionamento del servizio Amazon CloudFront nell'ambito del sito Internet della CAE*

110 Nel caso di specie, è pacifico che il sito Internet della CAE utilizza la rete di diffusione di contenuti Amazon CloudFront e che questa rete è attivata in occasione di ogni consultazione di detto sito Internet da parte di un utente.

111 Dal fascicolo, in particolare dalle risposte delle parti alla misura di organizzazione del procedimento del 21 luglio 2023 nonché dalle loro difese e risposte all'udienza del 17 ottobre 2023, risulta che, in primo luogo, il servizio Amazon CloudFront è un servizio Internet che accelera la distribuzione dei contenuti Internet, nella fattispecie del contenuto del sito Internet della CAE, agli utenti. Il servizio Amazon CloudFront diffonde il contenuto attraverso una rete mondiale di server o di centri dati denominati «postazioni periferiche» o «server periferici».

112 In secondo luogo, il servizio Amazon CloudFront è fondato su un meccanismo di instradamento che dirige la richiesta di un utente del sito Internet della CAE verso il server periferico che fornisce il tempo di latenza più debole, secondo un principio di prossimità al terminale dell'utente, affinché il contenuto sia trasmesso all'utente nelle migliori condizioni possibili. Se, in particolare a causa di difficoltà tecniche, il server periferico con la latenza più bassa non è disponibile, la connessione è stabilita con quello con la seconda latenza più debole e così via.

113 In terzo luogo, il servizio Amazon CloudFront è utilizzato per il sito Internet della CAE sulla base del contratto n. 2020-1742, firmato tra la Commissione e l'AWS EMEA, essendo quest'ultima una controllata detenuta dall'impresa di diritto americano Amazon.com e avente la propria sede sociale in Lussemburgo (v. punto 12 *supra*).

114 In quarto luogo, nell'ambito di tale contratto, la Commissione ha optato, per quanto riguarda il sito Internet della CAE, per la zona geografica denominata «America del Nord (Stati Uniti, Messico, Canada), Europa e Israele». Ciò significa che la diffusione del contenuto di tale sito

Internet non avviene attraverso la rete mondiale di siti periferici di Amazon CloudFront, ma unicamente attraverso coloro che si trovano nelle zone geografiche summenzionate, vale a dire negli Stati Uniti, in Messico, in Canada, in Europa e in Israele.

115 In quinto luogo, in ragione del principio di prossimità menzionato al precedente punto 112, le richieste di consultazione del sito Internet della CAE da parte di utenti dell'Unione sono solitamente dirette verso server periferici della rete Amazon CloudFront situati in tale territorio, mentre i casi in cui tali domande sono dirette verso server al di fuori dell'Unione sono rari.

116 In sesto luogo, per quanto riguarda l'infrastruttura della rete di siti periferici di Amazon CloudFront, dal fascicolo risulta che essa è fornita da un insieme di imprese, alcune delle quali appartengono al gruppo Amazon e altre sono imprese terze e il cui elenco può essere consultato sul sito Internet di Amazon Web Services, in funzione dell'area geografica interessata. Per quanto riguarda la zona geografica denominata «America del Nord (Stati Uniti, Messico, Canada), Europa e Israele», le imprese interessate sono stabilite sia negli Stati membri dell'Unione sia al di fuori dell'Unione, in particolare negli Stati Uniti, in Israele, in Messico, in Svizzera o nel Regno Unito. Ogni impresa gestisce server nel paese in cui è stabilita e, di conseguenza, l'ubicazione geografica dei server coinvolti nella prestazione del servizio Amazon CloudFront dipende anche dall'ubicazione delle imprese interessate.

117 In settimo luogo, le clausole del contratto tra la Commissione e la AWS EMEA prevedono, in particolare, quanto segue:

– la AWS EMEA deve essere in grado di garantire che i dati rimangano a riposo e in transito nel territorio del SEE (sezione 11.2 del contratto);

– la AWS EMEA non è autorizzata a modificare l'ubicazione del trattamento dei dati senza previa autorizzazione della Commissione [sezione 12.2.3, lettera a), del contratto];

– qualsiasi trasferimento di dati personali in virtù del contratto verso paesi terzi o organizzazioni internazionali deve essere pienamente conforme ai requisiti di cui al capo V del regolamento 2018/1725 [sezione 12.2.3 (b) del contratto];

– la AWS EMEA non può trasferire dati personali verso un paese al di fuori del SEE, a meno che la Commissione non abbia dato la sua autorizzazione scritta prima di tale trasferimento e il trasferimento avvenga nel rispetto delle condizioni di cui al capo V (sezione 1.8.9 del contratto);

– la AWS EMEA deve trasmettere alla Commissione qualsiasi richiesta di accesso ai dati personali e deve avvalersi di tutti i mezzi di ricorso disponibili contro tali richieste (sezioni 1.8.3, 1.8.4 e 1.8.5 del contratto);

– la AWS EMEA deve assicurarsi che tali misure siano attuate anche in caso di ricorso a subappaltatori (sezione 1.8.8 del contratto).

118 In ottavo luogo, la Commissione ha consultato il GEPD sulle clausole contrattuali summenzionate, ma esse non sono state oggetto di un'autorizzazione formale da parte di quest'ultimo, ai sensi dell'articolo 48, paragrafo 3, lettera a), del regolamento 2018/1725.

– Trasferimento controverso in occasione della consultazione del sito Internet della CAE del 30 marzo 2022

119 [Come rettificato con ordinanza del 3 giugno 2025] Il ricorrente sostiene, in sostanza, che, in occasione della consultazione del sito Internet della CAE del 30 marzo 2022, egli ha constatato che taluni dati personali ad esso appartenenti, in particolare il suo indirizzo IP e informazioni sul suo browser e sul suo terminale, erano stati trasferiti verso gli Stati Uniti. Infatti, in primo luogo, detto sito Internet utilizzerebbe una rete di diffusione di contenuti denominata «Amazon CloudFront», il cui operatore sarebbe Amazon Web Services, un'impresa americana controllata dall'impresa americana Amazon.com. In secondo luogo, in occasione di tale consultazione, alcuni dati personali del ricorrente sarebbero stati inviati al servizio Amazon CloudFront, più precisamente al server di Amazon.com ubicato a Seattle (Washington, Stati Uniti), il cui indirizzo IP sarebbe 18.66.192.74. In terzo luogo, la chiave di sicurezza utilizzata dal sito Internet della CAE (denominata «certificato SSL») sarebbe stata fornita da Amazon, ragion per cui si dovrebbe presumere che quest'ultima avesse la possibilità di decriptare tutti i dati personali del ricorrente trasferiti verso i suoi server, comprese le sue opinioni sul futuro dell'Europa. In quarto luogo, l'impresa che fornisce il servizio Amazon CloudFront sarebbe soggetta alle leggi americane e sarebbe quindi obbligata a comunicare informazioni ai servizi di sicurezza e di sorveglianza degli Stati Uniti, e ciò anche nel caso in cui i server fossero ubicati al di fuori di tale paese. Inoltre, la Commissione non avrebbe adottato «misure supplementari», ai sensi della sentenza Schrems II, al fine di garantire un livello di protezione adeguato dei dati trasferiti verso gli Stati Uniti.

120 La Commissione contesta tali argomenti.

121 Per quanto riguarda la consultazione del sito Internet della CAE del 30 marzo 2022, risulta dal fascicolo che il ricorrente ha consultato tale sito Internet in tale data (v. *supra*, punto 3) e che, durante tale consultazione, ha avuto luogo una trasmissione del suo indirizzo IP e delle informazioni sul suo browser e sul suo terminale.

122 A tal riguardo, occorre constatare che l'indirizzo IP deve essere qualificato come dato personale, ai sensi dell'articolo 3, punto 1, del regolamento 2018/1725, poiché soddisfa le due condizioni ivi previste. Da un lato, tale informazione si riferisce a una persona fisica e, dall'altro, si riferisce a una persona identificata o identificabile, nel caso di specie il ricorrente (sentenza del 26 aprile 2023, CRU/CEPD, T-557/20, con impugnazione pendente, EU:T:2023:219, punto 59; v. altresì, in tal senso e per analogia, sentenze del 24 novembre 2011, Scarlet Extended, C-70/10, EU:C:2011:771, punto 51, e del 19 ottobre 2016, Breyer, C-582/14, EU:C:2016:779, punto 49). Infatti, anche gli indirizzi IP cosiddetti «dinamici», che per loro natura cambiano, corrispondono ad un'identità precisa in un determinato momento, che, nel caso di specie, coincide con il momento in cui ha avuto luogo la consultazione del sito Internet della CAE.

123 È altresì dimostrato che il trasferimento di dati menzionato al precedente punto 121 è stato lanciato dal sito Internet della CAE, attraverso il servizio Amazon CloudFront, verso un server il cui indirizzo IP è 18.66.192.74.

124 È inoltre dimostrato che, all'epoca dei fatti, l'indirizzo IP 18.66.192.74 era attribuito a un server ubicato a Monaco di Baviera (Germania) e che tale server apparteneva all'impresa A 100 ROW GmbH, che era stabilita in Germania e faceva parte dell'elenco di imprese menzionato al precedente punto 116.

125 Ne consegue che, certamente, in occasione della consultazione del sito Internet della CAE del 30 marzo 2022, si è verificato un trasferimento di dati personali, ai sensi dell'articolo 3, punto 1, del regolamento 2018/1725, del ricorrente, in particolare del suo indirizzo IP.

126 Tuttavia, nel caso di specie non è dimostrato che, in occasione della consultazione del sito Internet della CAE del 30 marzo 2022, vi sia stato un trasferimento di dati personali del ricorrente verso un paese terzo e, in particolare, verso gli Stati Uniti.

127 Per contro, dai precedenti punti da 121 a 124 risulta che, in occasione della consultazione del sito Internet della CAE del 30 marzo 2022, il trasferimento di dati personali del ricorrente è stato lanciato dal sito Internet della CAE, attraverso il servizio Amazon CloudFront, verso un server situato a Monaco di Baviera. Detto server apparteneva ad un'impresa con sede in Germania, che faceva parte della rete di prestatori dell'infrastruttura del servizio Amazon CloudFront, la quale è fornita alla Commissione sulla base di un contratto con la AWS EMEA, impresa con sede in Lussemburgo.

128 Ne consegue che, in occasione della consultazione del sito Internet della CAE del 30 marzo 2022, i dati personali del ricorrente sono stati trasmessi a un destinatario stabilito nell'Unione.

129 Inoltre, anche ammettendo che i dati personali del ricorrente non abbiano lasciato il territorio dell'Unione, tali dati sono stati comunque trasferiti a un server appartenente alla rete di siti periferici del servizio Amazon CloudFront, il quale comprende, per quanto riguarda la diffusione del contenuto del sito Internet della CAE, una rete di siti periferici che non si limita al territorio del SEE, ma che va al di là di quest'ultimo (v. *supra*, punto 116).

130 Tuttavia, le circostanze concrete descritte al precedente punto 127 non dimostrano l'esistenza di un trasferimento di dati personali verso destinatari stabiliti al di fuori del territorio del SEE, in particolare negli Stati Uniti.

131 Il trasferimento controverso in occasione della consultazione del sito Internet della CAE del 30 marzo 2022 non corrisponde quindi a un trasferimento di dati personali verso un paese terzo, ai sensi dell'articolo 46 del regolamento 2018/1725, dato che il concetto di trasferimento verso un paese terzo richiede che i dati personali siano messi a disposizione di un destinatario stabilito al di fuori del SEE (v. *supra*, punto 93).

132 L'argomento del ricorrente relativo al fatto che la AWS EMEA sarebbe obbligata, in quanto controllata di un'impresa americana, a trasmettere dati personali alle autorità americane, anche quando tali dati sono conservati nel territorio dell'Unione, non rimette in discussione tale conclusione.

133 Se è certamente vero che l'accesso a dati personali trattati nel SEE dalle autorità di un paese terzo in forza della legislazione di tale paese costituisce un trasferimento di dati personali verso un paese terzo, ai sensi dell'articolo 46 del regolamento 2018/1725, resta il fatto che, nel caso di specie, non è dimostrato che un siffatto accesso abbia avuto luogo. Infatti, il ricorrente non ha né dimostrato o dedotto l'esistenza di una trasmissione alle autorità americane di un qualsiasi dato personale di sua proprietà, né dimostrato o dedotto l'esistenza di una domanda di tali autorità riguardante i dati che sono stati trasferiti a detto server di Amazon CloudFront, localizzato a Monaco di Baviera.

134 Pertanto, l'argomento del ricorrente non verte su una violazione diretta delle disposizioni del capo V del regolamento 2018/1725, ma unicamente sul rischio di una siffatta violazione, nell'ipotesi in cui la AWS EMEA, a causa della sua qualità di filiale di un'impresa americana, non fosse in grado di opporsi ad una domanda delle autorità americane relativa all'accesso a dati memorizzati in server ubicati nel territorio del SEE.

135 Orbene, il solo rischio di accesso a dati personali da parte di un paese terzo non può corrispondere a un trasferimento di dati, ai sensi dell'articolo 46 del regolamento 2018/1725, come interpretato al punto 93 *supra*, poiché non è dimostrato che vi sia stata una trasmissione o messa a disposizione di un destinatario stabilito in un paese terzo in altro modo dei dati personali del ricorrente. In altri termini, il rischio di una violazione di detto articolo 46 non può essere assimilato a una violazione diretta di tale disposizione.

136 Inoltre, occorre ricordare che, nell'ambito della presente domanda di risarcimento danni, l'esame del Tribunale verte sulla verifica delle condizioni per il sorgere della responsabilità extracontrattuale della Commissione e, in particolare, sulla condizione relativa all'illiceità del comportamento della Commissione, la quale richiede che sia dimostrata una violazione sufficientemente qualificata delle disposizioni del regolamento 2018/1725 e della Carta invocate dal ricorrente.

137 A tal riguardo, il solo rischio di una violazione delle disposizioni del capo V del regolamento 2018/1725 non può, in ogni caso, essere sufficiente a dimostrare un comportamento illecito della Commissione, corrispondente a una violazione sufficientemente qualificata di tali disposizioni.

138 Tale conclusione non è rimessa in discussione dall'argomento del ricorrente relativo alla sentenza Schrems II. Infatti, occorre osservare che, in tale sentenza, la Corte si è pronunciata su talune delle condizioni in presenza delle quali possono aver luogo trasferimenti di dati personali verso gli Stati Uniti e non su quelle in cui tali dati possono essere trattati, nel territorio del SEE, da filiali di società di diritto americano, come la AWS EMEA.

139 Da tutto quanto precede risulta che, per quanto riguarda il trasferimento controverso in occasione della consultazione del sito Internet della CAE del 30 marzo 2022, il ricorrente non ha dimostrato che la Commissione fosse incorsa in una violazione sufficientemente qualificata, ai sensi della giurisprudenza richiamata al precedente punto 50, delle disposizioni dell'articolo 46 e dell'articolo 48, paragrafo 1, e paragrafo 2, lettera b), del regolamento 2018/1725 nonché degli articoli 7, 8 e 47 della Carta.

140 Di conseguenza, dal momento che una delle condizioni cumulative per il sorgere della responsabilità extracontrattuale dell'Unione, previste all'articolo 340, secondo comma, TFUE, non sussiste, occorre respingere la seconda domanda di risarcimento per quanto riguarda il trasferimento controverso in occasione della consultazione del sito Internet della CAE del 30 marzo 2022, senza che sia necessario esaminare gli altri argomenti del ricorrente.

– Trasferimento controverso in occasione delle consultazioni del sito Internet della CAE dell'8 giugno 2022

141 Il ricorrente sostiene che, in occasione delle consultazioni del sito Internet della CAE dell'8 giugno 2022, si è verificato un trasferimento dei suoi dati personali, in particolare del suo indirizzo IP, verso server di Amazon CloudFront situati negli Stati Uniti. Secondo il ricorrente, tali trasferimenti non derivano dalla sua attività in qualità di utente del sito Internet, ma sono il

risultato del funzionamento del servizio Amazon CloudFront, nell'ambito del quale il rischio di trasferimento di dati verso gli Stati Uniti è inerente all'infrastruttura mondiale su cui si basa tale servizio. La situazione del ricorrente non sarebbe diversa da quella di un cittadino dell'Unione che consulta il sito Internet della CAE in occasione, ad esempio, di uno spostamento professionale negli Stati Uniti. La Commissione non darebbe prova di tutta la diligenza richiesta al fine di evitare i trasferimenti di dati verso gli Stati Uniti, dal momento che essa avrebbe optato per una rete di diffusione di contenuti basata su una struttura di livello mondiale, invece di una soluzione di hosting puramente europea.

142 Secondo il ricorrente, detto trasferimento di dati personali gli avrebbe causato un danno morale, ai sensi del considerando 46 del regolamento 2018/1725, in quanto egli ha perso il controllo dei suoi dati, che sono stati trasferiti verso gli Stati Uniti e sottoposti a una sorveglianza illecita da parte delle autorità americane, ed è stato privato dei suoi diritti e delle sue libertà.

143 La Commissione contesta tali argomenti.

144 In via preliminare e tenuto conto dell'argomento del ricorrente, occorre ricordare che, nell'ambito della presente domanda di risarcimento danni, l'esame del Tribunale non verte direttamente sulla legittimità della decisione della Commissione di utilizzare il servizio Amazon CloudFront per la diffusione del contenuto del sito Internet della CAE, bensì sulla verifica delle condizioni per il sorgere della responsabilità extracontrattuale della Commissione per quanto riguarda il trasferimento controverso in occasione delle consultazioni del sito Internet della CAE dell'8 giugno 2022.

145 Nel caso di specie, il Tribunale ritiene opportuno esaminare anzitutto la condizione relativa all'esistenza di un nesso di causalità tra l'asserito comportamento illecito della Commissione e il danno morale lamentato.

146 Risulta dalla giurisprudenza menzionata *supra* al punto 55 che il presupposto relativo al nesso causale concerne l'esistenza di un rapporto di causa-effetto sufficientemente diretto tra il comportamento delle istituzioni dell'Unione e il danno, nesso di cui spetta alla ricorrente fornire la prova, di modo che il comportamento addebitato deve essere la causa determinante del danno.

147 Inoltre, dalla giurisprudenza risulta che il nesso di causalità richiesto per far sorgere la responsabilità extracontrattuale dell'Unione ai sensi dell'articolo 340, secondo comma, TFUE sussiste quando il danno è la conseguenza diretta dell'atto illecito in questione (sentenza del 28 giugno 2007, Internationaler Hilfsfonds/Commissione, C-331/05 P, EU:C:2007:390, punto 23).

148 Per quanto riguarda il carattere diretto del nesso di causalità, il Tribunale ha già dichiarato che il danno deve risultare direttamente dall'illegittimità invocata e non da una scelta del ricorrente quanto al modo di reagire all'atto asseritamente illegittimo. Si è quindi ritenuto che il semplice fatto che il comportamento illegittimo abbia costituito una condizione necessaria (*conditio sine qua non*) per il verificarsi del danno, nel senso che quest'ultimo non si sarebbe verificato in mancanza di tale comportamento, non è sufficiente a dimostrare un nesso di causalità sufficientemente diretto ai sensi della giurisprudenza dell'Unione (v., in tal senso e per analogia, sentenze del 30 novembre 2011, Transnational Company «Kazchrome» e ENRC Marketing/Consiglio e Commissione, T-107/08, EU:T:2011:704, punto 80 e giurisprudenza ivi citata, e del 23 maggio 2019, Remag Metallhandel e Jaschinsky/Commissione, T-631/16, non pubblicata, EU:T:2019:352, punto 52 e giurisprudenza ivi citata).

149 Risulta quindi dalla giurisprudenza che un siffatto nesso di causalità non è dimostrato quando il danno invocato è la conseguenza diretta della propria decisione o della libera scelta del ricorrente e non può, di conseguenza, essere imputato all'istituzione o all'organo interessato (v., in tal senso e per analogia, sentenze del 28 giugno 2007, Internationaler Hilfsfonds/Commissione, C-331/05 P, EU:C:2007:390, punti da 22 a 29; del 17 febbraio 2017, Novar/EUIPO, T-726/14, EU:T:2017:99, punti 31 e 32, e del 28 febbraio 2018, Vakakis kai Synergates/Commissione, T-292/15, EU:T:2018:103, punto 173 e giurisprudenza ivi citata).

150 Nel caso di specie, occorre quindi verificare se il comportamento contestato alla Commissione, ossia l'utilizzo del servizio Amazon CloudFront come rete di diffusione di contenuti del sito Internet della CAE, sia la causa diretta del danno morale lamentato, consistente in una perdita del controllo sui dati personali del ricorrente che sarebbero stati oggetto di un trasferimento verso gli Stati Uniti in occasione delle sue consultazioni su detto sito Internet dell'8 giugno 2022.

151 A tal riguardo, in primo luogo, risulta dal fascicolo nonché dalle risposte delle parti ai quesiti posti in udienza che, l'8 giugno 2022, il ricorrente era a Monaco di Baviera e che ha consultato più volte il sito Internet della CAE. Durante tali consultazioni, l'indirizzo IP del ricorrente ha stabilito connessioni successive a diversi server del servizio Amazon CloudFront, geograficamente molto distanti gli uni dagli altri. Così, esso si è collegato alle ore 7:13 a un server situato a Monaco di Baviera, alle ore 11:13 a un server situato a Londra (Regno Unito), alle ore 12: 56 a un server situato a Hillsboro (Oregon, Stati Uniti), alle ore 13:05 a un server situato a Newark e alle ore 19:12 a un server situato a Francoforte sul Meno (Germania).

152 In secondo luogo, dal fascicolo risulta che l'indirizzo IP del ricorrente è stato trasferito ai diversi server del servizio Amazon CloudFront menzionati al precedente punto 151, compresi quelli ubicati negli Stati Uniti.

153 In terzo luogo, occorre ricordare che l'indirizzo IP del ricorrente costituisce un dato personale.

154 In quarto luogo, occorre osservare che, l'8 giugno 2022, il sito Internet della CAE ha contabilizzato 4 548 accessi e 18 indirizzi IP diversi. Tra questi ultimi, un solo indirizzo IP, ossia quello del ricorrente, ha stabilito una connessione con server situati al di fuori dell'Unione, vale a dire negli Stati Uniti e nel Regno Unito. A tal riguardo, occorre osservare che non è stato dimostrato e neppure asserito che, l'8 giugno 2022, il servizio Amazon CloudFront per il sito Internet della CAE avrebbe avuto problemi tecnici o di altra natura, in modo da impedire il normale funzionamento del suo meccanismo di instradamento secondo il principio di prossimità, il quale dirige le richieste degli utenti del sito Internet della CAE verso il server periferico che fornisce la latenza più debole a seconda della posizione geografica dell'utente (v. *supra*, punto 112).

155 In quinto luogo, per quanto riguarda le circostanze relative alle connessioni stabilite dall'indirizzo IP del ricorrente a server situati negli Stati Uniti, da un lato, risulta dal fascicolo nonché dalle risposte delle parti in udienza che il ricorrente sostiene che tali connessioni erano il risultato del funzionamento di Amazon CloudFront e non di una qualsivoglia manipolazione che egli avrebbe realizzato. Dall'altro lato, la Commissione osserva che tali connessioni erano atipiche e possono essere spiegate solo con una manipolazione tecnica da parte del ricorrente.

156 A tal riguardo, occorre constatare che le circostanze descritte al precedente punto 151 dimostrano che le diverse localizzazioni dei server cui si è collegato l'indirizzo IP del ricorrente non potrebbero risultare dagli spostamenti fisici del ricorrente nella stessa giornata, i quali sarebbero impossibili tenuto conto delle distanze e degli intervalli di tempo in questione. Inoltre, non è

stata dimostrata e neppure dedotta alcuna disfunzione del servizio Amazon CloudFront, il che consente di concludere che, l'8 giugno 2022, tale servizio funzionava secondo il principio di prossimità al terminale dell'utente, in quanto il suo meccanismo di instradamento dirige le richieste degli utenti dal sito Internet della CAE verso il server periferico che forniva il tempo di latenza più debole (v. *supra*, punto 154).

157 In tali circostanze, le connessioni dell'indirizzo IP del ricorrente a server ubicati negli Stati Uniti mentre si trovava in Germania non possono risultare dal normale funzionamento del servizio Amazon CloudFront, ma piuttosto da una regolazione tecnica effettuata dal ricorrente al fine di modificare la sua ubicazione apparente, presentandosi nel dominio digitale come se si trovasse nella stessa giornata successivamente in luoghi vicini a Monaco di Baviera, Londra, Hillsboro, Newark e Francoforte sul Meno.

158 Ne consegue che, certamente, è il funzionamento del servizio Amazon CloudFront, con il suo meccanismo di instradamento che funziona secondo il principio di prossimità e che copre una zona geografica più ampia del territorio del SEE, comprendente in particolare gli Stati Uniti (v. *supra*, punti 112 e 114), che ha consentito che, durante le consultazioni del sito Internet della CAE, l'indirizzo IP del ricorrente abbia stabilito connessioni a server di Amazon CloudFront localizzati negli Stati Uniti.

159 Tuttavia, sebbene l'utilizzo, da parte della Commissione, del servizio Amazon CloudFront sia una condizione necessaria per il verificarsi dei trasferimenti di dati personali verso gli Stati Uniti, menzionati al punto 152 *supra*, tale circostanza non è sufficiente, nelle circostanze del caso di specie, a dimostrare un nesso di causalità sufficientemente diretto tra il danno morale invocato dal ricorrente e il comportamento asseritamente illecito della Commissione, consistente nell'utilizzo di un siffatto servizio in violazione delle disposizioni del capo V del regolamento 2018/1725.

160 Infatti, 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.

161 Pertanto, è il ricorrente che ha posto in essere le condizioni necessarie per provocare connessioni a server situati negli Stati Uniti attraverso il funzionamento del servizio Amazon CloudFront. È 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, poiché erano questi ultimi ad avere la più debole latenza rispetto alla localizzazione apparente del ricorrente nel dominio digitale, mentre quest'ultima non corrispondeva alla sua effettiva ubicazione.

162 Peraltro, il ricorrente non è legittimato ad adottare un comportamento diretto a provocare un determinato risultato (ossia il trasferimento dei suoi dati personali verso un paese terzo) e, successivamente, a chiedere il risarcimento del danno asseritamente causato da tale risultato, di cui il suo comportamento è stato la causa diretta. Pertanto, contrariamente a quanto sostenuto dal ricorrente, nell'ambito di un ricorso per risarcimento danni come quello del caso di specie, la sua situazione non può essere valutata in modo analogo a quella di un utente che si sia effettivamente trasferito negli Stati Uniti e che, di conseguenza, abbia avuto accesso al sito Internet della CAE a partire da tale paese.

163 Da tutto quanto precede risulta che, per quanto riguarda il trasferimento controverso in occasione delle consultazioni del sito Internet della CAE dell'8 giugno 2022, non è stato dimostrato un nesso di causalità sufficientemente diretto tra il comportamento asseritamente illegittimo della Commissione e il danno morale lamentato.

164 Dal momento che una delle condizioni cumulative per il sorgere della responsabilità extracontrattuale dell'Unione non sussiste, occorre respingere la domanda di risarcimento per quanto riguarda il trasferimento controverso in occasione delle consultazioni del sito Internet della CAE dell'8 giugno 2022, senza che sia necessario esaminare le altre condizioni per il sorgere di detta responsabilità.

– *Trasferimento controverso in occasione della connessione a EU Login del 30 marzo 2022*

165 Il ricorrente sostiene che, il 30 marzo 2022, al momento della sua iscrizione all'evento «GoGreen» disponibile sul sito Internet della CAE, il suo indirizzo IP nonché informazioni sul suo browser e sul suo terminale sono stati trasferiti all'impresa Meta Platforms, con sede negli Stati Uniti, che è proprietaria del social network Facebook. Infatti, al momento di tale iscrizione, il ricorrente sarebbe stato diretto verso il servizio di autenticazione dell'Unione EU Login, il quale propone, in particolare, di connettersi attraverso diversi social network. Il ricorrente avrebbe optato per la connessione attraverso il suo account Facebook e, una volta cliccato sul collegamento ipertestuale, il link avrebbe portato a una trasmissione del suo indirizzo IP a Facebook. Il ricorrente avrebbe accettato solo i «cookie essenziali» di Facebook. Altri dati personali del ricorrente, ossia il suo indirizzo di posta elettronica, il suo nome e cognome e la sua fotografia di profilo, sarebbero stati raccolti da Facebook mediante cookie, in particolare cookie denominato «sb», e trasferiti ai server di Meta Platforms. Dalla giurisprudenza risulterebbe che i gestori di siti Internet che utilizzano Facebook nei loro siti Internet, come nel caso della Commissione, sono responsabili, congiuntamente a Facebook, del rispetto del diritto dell'Unione in materia di protezione dei dati. La Commissione sarebbe quindi corresponsabile dell'inserimento dei cookie memorizzati da Facebook. Il ricorrente avrebbe perso il controllo sui suoi dati personali trasmessi a Facebook e sarebbe privato dei suoi diritti e delle sue libertà, il che costituirebbe un danno morale ai sensi del considerando 46 del regolamento 2018/1725.

166 La Commissione contesta tali argomenti. Essa fa valere, in sostanza, di non aver effettuato né avviato trasferimenti di dati a Meta Platforms. Non sarebbe obbligatorio iscriversi tramite EU Login per partecipare all'evento «GoGreen» e, anche utilizzando EU Login, il ricorrente avrebbe avuto diverse possibilità di autenticazione, comprese possibilità che non richiederebbero l'utilizzo di un account su social network. Sarebbe quindi una scelta del ricorrente di essersi collegato al servizio EU Login con il suo account Facebook e sarebbe quindi lui, e non la Commissione, ad aver lanciato l'accesso al sito Internet di Facebook. Inoltre, sul piano tecnico, l'opzione di autenticazione da parte di Facebook sarebbe realizzata attraverso il collegamento ipertestuale pubblicato sul sito Internet EU Login, che non conterrebbe dati personali dell'utente. Contrariamente a quanto sostenuto dal ricorrente, i dati raccolti dai cookie utilizzati da Facebook non sarebbero trasferiti alla Commissione al momento della connessione al sito UE Login e non rientrerebbero nella responsabilità della Commissione. Tali cookie sono il risultato di scambi tra Facebook e il ricorrente, sulla base di consensi dati da quest'ultimo, ove la Commissione non è coinvolta in tali scambi. Inoltre, la Commissione sostiene che la giurisprudenza invocata dal ricorrente non è applicabile nel caso di specie e che, in ogni caso, l'argomento del ricorrente vertente su un'asserita responsabilità congiunta della Commissione e della Meta Platforms sarebbe un motivo nuovo dedotto per la prima volta in sede di replica che, di conseguenza, sarebbe irricevibile.

167 Nel caso di specie, occorre anzitutto esaminare il contesto di fatto in cui si inserisce il trasferimento controverso in occasione della connessione a EU Login del 30 marzo 2022, tenendo conto degli elementi risultanti dal fascicolo nonché delle risposte delle parti ai quesiti posti dal Tribunale in udienza e della misura di organizzazione del procedimento del 9 febbraio 2024.

168 A tal riguardo, occorre constatare che l'evento «GoGreen», organizzato da un organismo con sede nei Paesi Bassi, era annunciato sul sito Internet della CAE. L'iscrizione a tale evento poteva essere effettuata, in particolare, sul sito Internet della CAE, tramite il servizio EU Login.

169 Il ricorrente ha scelto di iscriversi sul sito Internet della CAE, utilizzando EU Login.

170 EU Login è il servizio di autenticazione dell'utente della Commissione, che protegge centinaia di siti Internet e di applicazioni collegati all'Unione. Nel caso di specie, la connessione a EU Login, ai fini dell'iscrizione all'evento «GoGreen», aveva lo scopo di garantire che tale iscrizione fosse effettuata mediante un indirizzo di posta elettronica verificato, riducendo i rischi connessi all'iscrizione di falsi utenti o all'usurpazione di identità.

171 EU Login visualizza diverse opzioni di connessione sulla sua pagina Internet. La prima opzione consiste nel connettersi direttamente a EU Login, compilando i dati di connessione per un conto EU Login preesistente o creando un conto per tale servizio. La seconda opzione è quella di utilizzare una carta d'identità elettronica «eID», disponibile per i cittadini di alcuni Stati membri. La terza opzione, disponibile per un numero limitato di servizi, consiste nell'utilizzare un account che l'utente possiede già su Facebook, Twitter o Google, cliccando sul collegamento ipertestuale corrispondente, visualizzato sul sito Internet di EU Login.

172 La possibilità di connettersi a EU Login tramite un account Facebook deriva dal fatto che la Commissione ha ritenuto opportuno dare agli utenti la scelta di connettersi a EU Login attraverso account preesistenti su piattaforme, al fine di offrire loro un accesso più facile e rapido, nonché la possibilità di autenticarsi senza necessità di creare un account EU Login, evitando così di moltiplicare il numero di conti e di entità con i quali gli utenti devono condividere i loro dati personali. Peraltro, la Commissione ha ritenuto che Facebook fosse affidabile ai fini della verifica degli indirizzi e-mail degli utenti, date le misure adottate. Tuttavia, il collegamento ipertestuale che consente agli utenti di connettersi tramite un account Facebook preesistente è disponibile su EU Login solo per siti web o applicazioni che richiedono solo un livello di sicurezza di base.

173 Il ricorrente ha scelto l'opzione di connettersi all'EU Login tramite il suo account Facebook, utilizzando il collegamento ipertestuale «Sign in with Facebook» che è visualizzato sul sito Internet di EU Login (in prosieguo: il «collegamento ipertestuale "connettersi a Facebook"»).

174 Il collegamento ipertestuale «connettersi a Facebook» contiene un collegamento verso un sito Internet esterno alla Commissione. Quando tale collegamento ipertestuale è attivato, cliccando sopra, esso dà accesso a un indirizzo URL del sito Internet di Facebook, vale a dire a un indirizzo individuale di tale sito Internet.

175 L'accesso all'indirizzo URL del sito Internet di Facebook dà luogo ad una comunicazione tra il browser dell'utente e detto sito Internet, nell'ambito della quale il browser trasmette l'indirizzo IP dell'utente al sito Internet di cui trattasi. Tale trasmissione è simile a quella che avviene

quando l'utente inserisce direttamente l'indirizzo URL di qualsiasi sito Internet nel suo browser, in quanto l'indirizzo IP deve necessariamente essere comunicato da ogni utente di Internet che intenda accedere a un sito Internet.

176 Attraverso il collegamento ipertestuale «connettersi a Facebook», EU Login invia alcune informazioni a Facebook, che sono necessarie ai fini del processo di autenticazione e assumono la forma del seguente esempio:

https://www.facebook.com/v3.0/dialog/oauth?response_type=code&
client_id=1200572836629487&
redirect_uri=https%3A%2F%2Fecas.ec.europa.eu%2Fcas%2FoAuthCallback&scope=email&
state=useFacebook%7CECAS_LR-5249395-
yQYIt4muQF7PyfSbvEk42Lt0Zm6AmYrUlJfVU5FfsrkYNTaFX552FQShXP9oggHF9jlEUohJx6I4ACrQJ0zPJ4-rS0vSrmBGYCzOpBivVtNak-
93Am7vhlDrqH4FT9cBOzViGrSdq4b2TrFkbOxzHB4zyingpuKF16KQfMnmu5izfXzUIIDHx1HqNS9QGEFVWzoeq0

177 Più precisamente, le informazioni contenute nel collegamento ipertestuale «connettersi a Facebook» sono le seguenti:

– in primo luogo, la parte «clienti_id = 1200572836629487» contiene un «codice identificativo unico», che identifica EU Login come applicazione. Questo numero di identificazione è lo stesso per tutti gli utenti che desiderano autenticarsi su EU Login utilizzando Facebook;

– in secondo luogo, la parte «redirect_uri = https% 3A% 2F% 2Fecas.ec.europa.eu% 2Fcas% 2FoAuthCallback» contiene l'indirizzo URL generale di EU Login, che è l'indirizzo al quale Facebook deve rinviare l'utente dopo che quest'ultimo ha acconsentito a che i suoi dati personali siano trasmessi da Facebook a EU Login;

– in terzo luogo, la parte «scope = email» contiene i dati che Facebook deve trasmettere a EU Login al fine di garantire un'autenticazione riuscita dell'utente, in particolare l'indirizzo di posta elettronica dell'utente nonché il nome e il cognome indicati sul sito Facebook al momento della creazione di un account Facebook;

– in quarto luogo, la parte «state = useFacebook» indica che la lunga catena di caratteri che segue è un valore aleatorio di sicurezza, che è utilizzato per evitare attacchi di sicurezza e ha una validità limitata nel tempo. Tale valore aleatorio di sicurezza è generato in modo aleatorio da EU Login e svolge la funzione di frase segreta, che Facebook deve ripetere al momento della trasmissione di dati a EU Login, al fine di consentire a EU Login di sapere che l'indirizzo di posta elettronica, il nome e il cognome comunicati riguardano l'utente che ha lanciato il metodo di autenticazione. Una volta scaduto il termine o l'utente già autenticato, non è più possibile utilizzare il valore di sicurezza; e

– in quinto luogo, la parte «response_type = codice» indica che la trasmissione di dati da Facebook a EU Login è ancora accompagnata da un codice unico. Tale codice unico include il summenzionato valore casuale di sicurezza. Il codice unico equivale a un numero di

registrazione unico o a un numero di serie che autentica i dati trasmessi da Facebook a EU Login.

178 Una volta che l'utente accede all'indirizzo URL di Facebook, egli si trova su tale sito Internet, sul quale, anzitutto, compare una finestra che chiede all'utente di accettare l'uso di marcatori o «cookies» da parte di Facebook. Successivamente, se i cookie sono accettati, si apre un'altra finestra che consente di compilare il nome utente e la password dell'account utente su Facebook. Infine, una volta collegato al suo account Facebook, l'utente può autorizzare Facebook a utilizzare cookie su altre applicazioni e siti Internet, rispondendo alla domanda «allow Facebook to use cookies and similar technologies placed on other apps and website?». Se l'utente acconsente a tale uso, sarà successivamente invitato ad acconsentire a che Facebook fornisca a EU Login il nome, il cognome, la fotografia del profilo e l'indirizzo di posta elettronica collegati al suo account Facebook. Peraltro, nel corso di tale processo, l'utente può interrompere l'autenticazione mediante il suo account Facebook, scegliendo l'opzione «Cancel». In tale ipotesi, esso è reindirizzato verso il sito Internet di EU Login, dove compare nuovamente la pagina con le opzioni di connessione.

179 Nel caso di specie, quando il ricorrente ha cliccato sul collegamento ipertestuale «connettersi a Facebook», il suo browser Internet ha avuto accesso all'indirizzo URL del sito Internet di Facebook e ha, di conseguenza, comunicato il suo indirizzo IP a tale sito Internet. Successivamente, quando si trovava sul sito Internet di Facebook, il ricorrente ha scelto le opzioni che consentivano a Facebook di utilizzare unicamente cookie essenziali, poi si è collegato al suo account Facebook e, infine, ha autorizzato Facebook a comunicare a EU Login il suo nome, cognome, fotografia del profilo e indirizzo di posta elettronica, come li aveva indicati sul suo account Facebook.

180 In seguito a tali autorizzazioni concesse dal ricorrente, Facebook lo ha rinviato al sito Internet dell'EU Login, conformemente alle indicazioni contenute nel collegamento ipertestuale «connettersi a Facebook» (v. *supra*, punto 177, primo e secondo trattino).

181 Al contempo, Facebook ha comunicato a EU Login il valore aleatorio di sicurezza e il codice unico menzionati al precedente punto 177, quarto e quinto trattino. Da un lato, tale comunicazione di Facebook ha consentito a EU Login di sapere che i dati personali che Facebook metteva a sua disposizione riguardavano l'utente che aveva avviato il processo di autenticazione, ossia, nel caso di specie, il ricorrente. Dall'altro lato, essa ha consentito a EU Login di accedere, per un periodo limitato, ai dati personali menzionati al precedente punto 177, terzo trattino, vale a dire, in particolare, il nome, il cognome e l'indirizzo di posta elettronica del ricorrente, quali egli li ha indicati sul suo account Facebook. La trasmissione di tali dati da parte di Facebook a EU Login è stata effettuata mediante una connessione criptata tra di essi. È sulla base dei dati messi a disposizione da Facebook che EU Login ha autenticato l'indirizzo di posta elettronica del ricorrente.

182 Inoltre, occorre osservare che il social network Facebook è detenuto da Meta Platforms, impresa con sede negli Stati Uniti.

183 Occorre peraltro rilevare che la visualizzazione di tale collegamento ipertestuale sul sito Internet di EU Login è disciplinata dalle condizioni generali della piattaforma Facebook, divulgate all'indirizzo Internet «https://developers.facebook.com/terms».

184 È alla luce di tali considerazioni che occorre esaminare se siano soddisfatte le condizioni per il sorgere della responsabilità extracontrattuale della Commissione.

185 Il ricorrente fa valere, in sostanza, che, al momento della sua connessione a EU Login del 30 marzo 2022, vi è stato un trasferimento di dati personali ad esso appartenenti, in particolare dal suo indirizzo IP, verso server della social network Facebook, di cui l'impresa proprietaria ha sede negli Stati Uniti. Tale trasferimento sarebbe stato effettuato in violazione dell'articolo 46 del regolamento 2018/1725 e avrebbe causato al ricorrente un danno morale consistente in una perdita del controllo dei suoi dati e in una privazione dei suoi diritti e delle sue libertà.

186 In via preliminare, occorre ricordare che, come risulta dal precedente punto 95, un trasferimento di dati personali verso un paese terzo, ai sensi dell'articolo 46 del regolamento 2018/1725, richiede che un'istituzione, un organismo o un organismo dell'Unione metta, mediante trasmissione o in altro modo, dati personali a disposizione di un destinatario stabilito in un paese terzo, vale a dire un paese che non è membro né dell'Unione né del SEE.

187 Nel caso di specie, è dimostrato che, in primo luogo, tra le opzioni di connessione a EU Login, il ricorrente ha scelto di collegarsi al suo account Facebook. In secondo luogo, il collegamento ipertestuale «connettersi a Facebook» contiene un link verso un indirizzo URL del sito Internet di Facebook. In terzo luogo, quando il ricorrente ha attivato tale collegamento ipertestuale cliccando sopra, il suo browser ha acceduto all'indirizzo URL del sito Internet di Facebook e, successivamente, ha trasmesso il suo indirizzo IP a Facebook (v. *supra*, punti da 173 a 175).

188 Ne consegue che la Commissione, tramite il collegamento ipertestuale «connettersi a Facebook», visualizzato sulla pagina Internet di EU Login, ha creato le condizioni che consentono di trasmettere l'indirizzo IP del ricorrente a Facebook. Orbene, tale indirizzo IP costituisce un dato personale del ricorrente (v. *supra*, punto 122) che, tramite detto collegamento ipertestuale, è stato trasmesso a Meta Platforms, impresa con sede negli Stati Uniti. Tale trasmissione corrisponde quindi a un trasferimento di dati personali verso un paese terzo, ai sensi dell'articolo 46 del regolamento 2018/1725.

189 Inoltre, nel caso di specie è dimostrato che, al momento di tale trasferimento di dati, ossia il 30 marzo 2022, non esisteva alcuna decisione di adeguatezza, ai sensi dell'articolo 47 del regolamento 2018/1725, per quanto riguarda gli Stati Uniti (v. *supra*, punto 100).

190 In mancanza di una decisione di adeguatezza della Commissione per quanto riguarda gli Stati Uniti, il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale può avvenire solo se il titolare del trattamento o l'incaricato del trattamento ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi, conformemente all'articolo 48, paragrafo 1, del regolamento 2018/1725 (v. *supra*, punto 101).

191 Nel caso di specie, la Commissione non ha dimostrato, e neppure dedotto, l'esistenza di una garanzia adeguata, in particolare di una clausola tipo di protezione dei dati o di una clausola contrattuale adottate alle condizioni previste all'articolo 48, paragrafi 2 e 3, del regolamento 2018/1725 (v. *supra*, punti da 102 a 104). Per contro, è dimostrato che la visualizzazione del collegamento ipertestuale «connettersi con Facebook» sul sito Internet di EU Login è semplicemente disciplinata dalle condizioni generali della piattaforma Facebook (v. *supra*, punto 183).

192 Di conseguenza, la Commissione ha creato le condizioni affinché si sia verificato un trasferimento di dati personali del richiedente verso un paese terzo, senza tuttavia rispettare le condizioni di cui all'articolo 46 del regolamento 2018/1725.

193 Si deve quindi concludere, senza che sia necessario esaminare gli altri argomenti del ricorrente, che la Commissione ha commesso una violazione sufficientemente qualificata, ai sensi della giurisprudenza richiamata al precedente punto 50, dell'articolo 46 del regolamento 2018/1725, per quanto riguarda il trasferimento controverso al momento della connessione a EU Login del 30 marzo 2022.

194 Occorre quindi esaminare se le altre condizioni per il sorgere della responsabilità extracontrattuale della Commissione, relative al danno e al nesso di causalità, siano soddisfatte nel caso di specie.

195 Il ricorrente afferma che il trasferimento illegittimo del suo indirizzo IP a un'impresa stabilita negli Stati Uniti gli ha causato un danno morale consistente nella perdita del controllo dei suoi dati e in una privazione dei suoi diritti e delle sue libertà.

196 A tal riguardo, si deve considerare che l'articolo 65 del regolamento 2018/1725 dà diritto a un risarcimento non solo del danno materiale, ma anche del danno morale subito a causa di una violazione di tale regolamento, senza che sia necessario dimostrare una qualsivoglia soglia di gravità [v., in tal senso e per analogia, sentenza del 4 maggio 2023, Österreichische Post (Danno morale connesso al trattamento di dati personali), C-300/21, EU:C:2023:370, punti 45 e 51].

197 Nel caso di specie, il danno morale invocato dal ricorrente deve essere considerato reale e certo, ai sensi della giurisprudenza richiamata al precedente punto 54, in quanto il trasferimento menzionato al precedente punto 188, effettuato in violazione dell'articolo 46 del regolamento 2018/1725, ha posto il ricorrente in una situazione di incertezza quanto al trattamento dei suoi dati personali, in particolare del suo indirizzo IP.

198 Inoltre, sussiste un nesso di causalità sufficientemente diretto, ai sensi della giurisprudenza richiamata al precedente punto 55, tra la violazione, da parte della Commissione, dell'articolo 46 del regolamento 2018/1725 e il danno morale subito dal ricorrente.

199 Nelle circostanze del caso di specie, occorre valutare ex aequo et bono l'importo del danno morale causato dalla Commissione nella somma di EUR 400.

200 Di conseguenza, occorre condannare la Commissione a versare al ricorrente la somma di EUR 400 a titolo di risarcimento del danno morale subito a seguito del trasferimento controverso in occasione della connessione con EU Login del 30 marzo 2022.

Sulle spese

201 Ai sensi dell'articolo 134, paragrafo 3, del regolamento di procedura del Tribunale, se le parti soccombono rispettivamente su uno o più capi, le spese sono compensate. Tuttavia, qualora ciò appaia giustificato alla luce delle circostanze del caso di specie, il Tribunale può decidere che una parte sostenga, oltre alle proprie spese, una quota delle spese della controparte.

202 Nel caso di specie, il ricorrente è rimasto soccombente sul primo e sul secondo capo della domanda nonché su una parte del suo terzo capo della domanda. Tuttavia, il terzo capo della domanda è stato parzialmente accolto e la Commissione è condannata a pagare l'importo che il ricorrente ha chiesto a titolo di risarcimento del danno morale che ha subito a causa del trasferimento controverso in occasione della connessione con EU Login del 30 marzo 2022. In tali circostanze, la Commissione deve essere condannata a sopportare le proprie spese e la metà delle spese sostenute dal ricorrente. Il ricorrente sopporterà la metà delle proprie spese.

Per questi motivi,

IL TRIBUNALE (Sesta Sezione ampliata)

dichiara e statuisce:

1) Il ricorso è respinto in quanto irricevibile nella parte relativa alla domanda di annullamento.

2) Non vi è più luogo a statuire sulla domanda volta a far dichiarare che la Commissione europea ha illegittimamente omesso di prendere posizione sulla richiesta di informazioni del sig. Thomas Bindl del 1º aprile 2022.

3) La Commissione è condannata a versare al sig. Bindl la somma di EUR 400 a titolo di risarcimento del danno morale subito.

4) La domanda di risarcimento è respinta quanto al resto.

5) La Commissione è condannata a farsi carico delle proprie spese nonché della metà delle spese sopportate dal sig. Bindl.

6) Il sig. Bindl è condannato a farsi carico della metà delle proprie spese.

Costeira Kancheva Öberg

Zilgalvis Tichy-Fisslberger

Così deciso e pronunciato a Lussemburgo l'8 gennaio 2025.

Firme

Indice

Fatti all'origine della controversia e fatti successivi alla presentazione del ricorso . . . 2

Conclusioni delle parti . . . 3

In diritto . . . 4

Considerazioni preliminari sulla protezione dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione . . . 4

Sulla ricevibilità . . . 5

Ricevibilità della domanda di annullamento . . . 5

Ricevibilità della domanda di declaratoria di carenza . . . 7

Sulla richiesta di risarcimento danni . . . 8

Considerazioni preliminari sulle condizioni per il sorgere della responsabilità extracontrattuale dell'Unione nell'ambito del regolamento 2018/1725 . . . 8

Sulla prima domanda di risarcimento danni, diretta al risarcimento del danno morale derivante da una violazione del diritto di accesso alle informazioni . . . 10

Sulla seconda domanda di risarcimento danni, diretta alla riparazione del danno morale derivante dai trasferimenti controversi . . . 14

– Considerazioni preliminari sulle disposizioni relative al trasferimento di dati personali verso un paese terzo . . . 15

– Sul funzionamento del servizio Amazon CloudFront nell'ambito del sito Internet della CAE . . . 17

– Trasferimento controverso in occasione della consultazione del sito Internet della CAE del 30 marzo 2022 . . . 19

– Trasferimento controverso in occasione delle consultazioni del sito Internet della CAE dell'8 giugno 2022 . . . 21

– Trasferimento controverso in occasione della connessione a EU Login del 30 marzo 2022 . . . 25

Sulle spese . . . 30