Decisione 01/2020 relativa alla controversia sorta sul progetto di decisione dell'autorità di controllo irlandese concernente Twitter International Company ai sensi dell'articolo 65, paragrafo 1, lettera a), RGPD

Adottata il 9 novembre 2020

Indice

Il comitato europeo per la protezione dei dati

visto l'articolo 63 e l'articolo 65, paragrafo 1, lettera a), del 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) (in appresso: «**RGPD**») ([1]),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo n. 37 dello stesso, modificati dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018 ([2]),

visto l'articolo 11 e l'articolo 22 del proprio regolamento interno ([3]),

considerando quanto segue:

(1) Il ruolo principale del comitato europeo per la protezione dei dati (in appresso: l'«**EDPB**» o il «**comitato**») è assicurare l'applicazione coerente del RGPD in tutto il SEE. A tal fine, dall'articolo 60 del RGPD risulta che l'autorità di controllo capofila (in appresso: «**autorità capofila**») coopera con le altre autorità di controllo interessate (in appresso «**autorità interessate**») nell'impegno per raggiungere un consenso, che l'autorità capofila e le autorità interessate si scambiano tutte le informazioni utili e che l'autorità capofila comunica senza indugio le informazioni utili sulla questione alle altre autorità di controllo interessate. L'autorità capofila trasmette senza indugio alle altre autorità interessate un progetto di decisione per ottenere il loro parere e tiene debitamente conto delle loro opinioni.

(2) Se una delle autorità interessate solleva un'obiezione pertinente e motivata («**RRO**») al progetto di decisione conformemente all'articolo 4, paragrafo 24, e all'articolo 60, paragrafo 4, RGPD, e l'autorità capofila non intende dare seguito all'obiezione o ritiene l'obiezione non pertinente o non motivata, l'autorità capofila sottopone la questione al meccanismo di coerenza di cui all'articolo 63 del RGPD.

(3) Ai sensi dell'articolo 65, paragrafo 1, lettera a), RGPD, l'EDPB adotta una decisione vincolante che riguarda tutte le questioni oggetto delle RRO, in particolare qualora sussista una violazione del RGPD.

(4) La decisione vincolante dell'EDPB è adottata da parte di una maggioranza di due terzi dei membri del comitato, ai sensi dell'articolo 65, paragrafo 2, RGPD, in combinato disposto con l'articolo 11, paragrafo 4, del regolamento interno dell'EDPB, entro un mese dalla decisione del presidente e dell'autorità di controllo competente in merito alla completezza del fascicolo. La scadenza può essere prorogata di un ulteriore mese, tenendo conto della complessità dell'argomento, per decisione del presidente, di propria iniziativa o su richiesta di almeno un terzo dei membri dell'EDPB.

(5) Conformemente all'articolo 65, paragrafo 3, RGPD, se, nonostante tale proroga, l'EDPB non è stato in grado di adottare una decisione entro il termine previsto, dovrà farlo entro due settimane dalla scadenza della proroga a maggioranza semplice dei suoi membri.

([1]) GU L 119 del 4.5.2016, pag. 1.
([2]) Nella presente decisione, con «Stati membri» ci si riferisce agli «Stati membri del SEE». I riferimenti alla «UE» vanno intesi, se del caso, come riferimenti al «SEE».
([3]) Regolamento interno dell'EDPB, adottato il 25 maggio 2018, modificato da ultimo e adottato l'8 ottobre 2020.

1 SINTESI DELLA CONTROVERSIA

1. Il presente documento contiene una decisione vincolante adottata dall'EDPB ai sensi dell'articolo 65, paragrafo 1, lettera a), RGPD. La decisione riguarda la controversia sorta a seguito di un progetto di decisione (in appresso: «**progetto di decisione**») emesso dall'autorità di controllo irlandese («Data Protection Commission», in appresso: «**AC IE**», in questo contesto anche l'«**autorità capofila**») e delle successive obiezioni espresse da una serie di autorità interessate («Österreichische Datenschutzbehörde», in appresso: «**AC AT**»; «Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit» ([4]), in appresso: «**AC DE**»; «Datatilsynet», in appresso «**AC DK**»; «Agencia Española de Protección de Datos», in appresso: «**AC ES**»; «Commission Nationale de l'Informatique et des Libertés», in appresso: «**AC FR**»; «Nemzeti Adatvédelmi és Információszabadság Hatóság», in appresso: «**AC HU**»; «Garante per la protezione dei dati personali», in appresso: «**AC IT**»; «Autoriteit Persoonsgegevens», in appresso: «**AC NL**»). Il progetto di decisione in questione si riferisce a una «indagine d'ufficio» avviata dall'AC IE a seguito della **notifica di una violazione di dati personali** in data 8 gennaio 2019 (la «**violazione**») da parte di Twitter International Company, una società con sede a Dublino, Irlanda (in appresso: «**TIC**») ([5]).

2. La violazione di dati è stata provocata da **un bug nella progettazione di Twitter** a causa del quale, se un utente su un dispositivo Android cambiava l'indirizzo e-mail associato al suo account Twitter, i tweet protetti diventavano non protetti e quindi accessibili a un pubblico più ampio (e non solo ai follower dell'utente) a sua insaputa ([6]). Il bug è stato scoperto il 26 dicembre 2018 dal contraente esterno che gestisce il «programma bug bounty» della società, un programma che consente a chiunque di segnalare l'esistenza di bug ([7]).

3. Durante l'indagine, Twitter ha scoperto altre azioni degli utenti che avrebbero comportato lo stesso risultato involontario. Il bug è stato **ricondotto a una modifica del codice effettuata il 4 novembre 2014** ([8]).

4. TIC ha informato l'AC IE che, per quanto era in grado di identificare, tra il 5 settembre 2017 e l'11 gennaio 2019, **sono stati interessati da questo bug 88 726 utenti dell'UE e del SEE**. Twitter ha confermato la datazione del bug al 4 novembre 2014, ma ha anche confermato di poter identificare gli utenti interessati solo a partire dal 5 settembre 2017 a causa di una politica di conservazione applicabile ai log ([9]). Di conseguenza, TIC ha riconosciuto la possibilità che un numero maggiore di utenti sia stato colpito dalla violazione ([10]).

([4]) L'obiezione dell'autorità di controllo di Amburgo è stata presentata anche in rappresentanza delle autorità seguenti: «Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg», «Berliner Beauftragte für Datenschutz und Informationsfreiheit, «Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern», «Die Landesbeauftragte für den Datenschutz Niedersachsen». L'obiezione è stata coordinata anche con altre autorità di controllo tedesche.
([5]) Progetto di decisione, paragrafi 1.1-1.2.
([6]) Progetto di decisione, paragrafo 1.9.
([7]) Progetto di decisione, paragrafi 2.7 e 4.7.
([8]) Progetto di decisione, paragrafo 2.10.
([9]) Progetto di decisione, paragrafo 2.10.
([10]) Progetto di decisione, paragrafi 1.10, 2.10, 14.2 e 14.3.

5. La decisione dell'AC IE di avviare l'indagine è stata presa in circostanze in cui TIC, nel modulo di notifica della violazione, aveva identificato come **«significativo» il potenziale impatto per le persone interessate** ([11]).

6. Nel progetto di decisione, l'AC IE ha dichiarato che c'erano i presupposti tali per cui l'AC IE stessa fosse l'autorità capofila, ai sensi del RGPD, in relazione a TIC, in qualità di titolare del trattamento transfrontaliero dei dati personali che sono stati oggetto della violazione, effettuato da TIC stessa ([12]).

7. La tabella che segue presenta un calendario riassuntivo degli eventi oggetto della procedura che ha comportato la presentazione della questione al meccanismo di coerenza:

26.12.2018	Twitter, Inc., una società costituita negli Stati Uniti, riceve una segnalazione di bug attraverso il suo programma bug bounty. La relazione è stata inviata da un terzo contraente che gestisce il programma bug bounty (contraente 1) al terzo contraente incaricato da Twitter, Inc. di cercare e valutare i bug (contraente 2).
29.12.2018	Il contraente 2 condivide il risultato con Twitter, Inc. tramite un ticket JIRA.
02.01.2019	Il team responsabile della sicurezza informatica di Twitter, Inc. esamina il ticket JIRA e decide che non si tratta di un problema di sicurezza, ma che potrebbe trattarsi di un problema di protezione dei dati.
02.01.2019	Viene informato il team legale di Twitter, Inc.
03.01.2019	Il team legale di Twitter, Inc. decide che la questione deve essere trattata come un incidente.
04.01.2019	Twitter, Inc. attiva la **procedura di intervento in caso di incidente** ma, a causa di un errore nell'applicazione della procedura interna, il responsabile globale della protezione dei dati non viene aggiunto come «osservatore» al ticket, pertanto non viene informato.
07.01.2019	Il responsabile globale della protezione dei dati viene informato della violazione dei dati durante una riunione.
08.01.2019	TIC **informa della violazione** l'AC IE utilizzando il modulo di notifica di violazione transfrontaliera della stessa.
22.01.2019	L'ambito di applicazione e la base giuridica dell'indagine sono stati definiti nell'avviso di avvio dell'indagine inviato a TIC il 22 gennaio 2019. L'AC IE avvia l'indagine e chiede informazioni a TIC.
dal 28.05.2019 al 21.10.2019	Fase della relazione d'indagine: - l'AC IE prepara un **progetto di relazione d'indagine** e la presenta a TIC per consentire a TIC di presentare le proprie osservazioni in merito al progetto di relazione stesso; - TIC fornisce le proprie osservazioni in merito al progetto di relazione d'indagine;

([11]) Progetto di decisione, paragrafo 2.8.

([12]) L'AC IE ha confermato che la sua valutazione al riguardo si basava sulla determinazione secondo la quale 1) TIC, in qualità di fornitore del servizio Twitter nell'UE/SEE, è il relativo titolare del trattamento, e 2) lo stabilimento principale di TIC nell'UE si trova a Dublino, Irlanda, dove TIC adotta le decisioni sulle finalità e i mezzi di trattamento dei dati personali degli utenti di Twitter nell'UE/SEE, ai sensi dell'articolo 4, paragrafo 16, RGPD. Progetto di decisione, paragrafi 2.2-2.3.

	) l'AC IE chiede chiarimenti in relazione alle osservazioni di TIC;) l'AC IE presenta la relazione d'indagine finale.
21.10.2019	L'AC IE avvia la fase decisionale.
11.11.2019 e 28.11.2019	L'AC IE scrive a TIC e la invita a presentare ulteriori osservazioni scritte.
2.12.2019	TIC presenta ulteriori osservazioni all'AC IE in risposta alla corrispondenza della stessa dell'11 e 28 novembre 2019.
14.03.2020	L'AC IE presenta un **progetto preliminare di decisione** (in appresso: «**il progetto preliminare di decisione**») a TIC, concludendo che TIC ha violato l'articolo 33, paragrafi 1 e 5, RGPD; l'AC IE intende pertanto rivolgere un ammonimento ai sensi dell'articolo 52, paragrafo 2, RGPD e infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 58, paragrafo 2, lettera i), e dell'articolo 83, paragrafo 2, RGPD.
27.04.2020	TIC fornisce osservazioni sul progetto preliminare di decisione all'AC IE.
27.04.2020 - 22.05.2020	L'AC IE tiene conto delle osservazioni di TIC in relazione al progetto preliminare di decisione e prepara il progetto di decisione da presentare alle autorità interessate in conformità dell'articolo 60 del RGPD.
22.05.2020 - 20.06.2020	L'AC IE condivide il progetto di decisione con le autorità interessate, conformemente all'articolo 60, paragrafo 3, RGPD. Diverse autorità interessate [AC AT, AC DE (rappresentata da AC DE-Amburgo), AC DK, AC ES, AC FR, AC HU, AC IT e AC NL) sollevano **obiezioni** ai sensi dell'articolo 60, paragrafo 4, RGPD.
15.07.2020	L'AC IE emette un memorandum composito che contiene le risposte a tali obiezioni e lo condivide con le autorità interessate (in appresso: «**memorandum composito**»). L'AC IE chiede alle autorità interessate competenti di confermare se, dopo aver considerato la sua posizione, esposta nel memorandum composito, in relazione alle obiezioni, intendono mantenere le loro obiezioni.
27.07.2020 e 28.07.2020	Alla luce delle argomentazioni avanzate dall'AC IE nel memorandum composito, l'AC DK informa l'AC IE che non manterrà la sua obiezione e l'AC ES informa l'AC IE che ritirerà parzialmente la sua obiezione. Le altre autorità interessate (ossia le AC AT, DE, ES, FR, HU, IT e NL) confermano all'AC IE che manterranno le loro restanti obiezioni.
19.08.2020	L'AC IE deferisce la questione all'EDPB conformemente all'articolo 60, paragrafo 4, RGPD, avviando così la procedura di risoluzione delle controversie ai sensi dell'articolo 65, paragrafo 1, lettera a).

8. L'AC IE ha attivato la procedura di risoluzione delle controversie tramite l'IMI il 19 agosto 2020. In seguito alla presentazione della questione da parte dell'autorità capofila all'EDPB ai sensi dell'articolo 60, paragrafo 4, RGPD, il segretariato del comitato ha valutato la completezza del fascicolo per conto del presidente, in linea con l'articolo 11, paragrafo 2, del regolamento interno dell'EDPB. Il 20 agosto 2020 il segretariato del comitato ha contattato per la prima volta l'AC IE per richiedere documenti e informazioni supplementari da caricare nell'IMI e chiedere all'AC IE di confermare la completezza del fascicolo. L'AC IE ha fornito i documenti e le informazioni e ha confermato la completezza del fascicolo il 21 agosto 2020. Una questione di particolare importanza esaminata dal segretariato dell'EDPB è stata il diritto di essere ascoltati, come previsto dall'articolo 41, paragrafo 2, lettera a), della Carta dei diritti fondamentali. Il 4 settembre 2020 il segretariato ha contattato l'AC IE con ulteriori domande per confermare se a TIC è stata data la possibilità di esercitare il suo diritto di

essere ascoltata in merito a tutti i documenti presentati al comitato per la decisione. L'8 settembre 2020 l'AC IE ha confermato che ciò è avvenuto e ha fornito i documenti per dimostrarlo ([13]).

9. L'8 settembre 2020 è stata presa la decisione sulla completezza del fascicolo, che è stata trasmessa dal segretariato dell'EDPB a tutti i membri del comitato.

10. Il presidente ha deciso, in conformità dell'articolo 65, paragrafo 3, RGPD, in combinato disposto con l'articolo 11, paragrafo 4, del regolamento interno dell'EDPB, di prorogare di un ulteriore mese il termine di un mese per l'adozione, in considerazione della complessità della materia.

2 CONDIZIONI PER L'ADOZIONE DI UNA DECISIONE VINCOLANTE

11. Le condizioni generali per l'adozione di una decisione vincolante da parte del comitato sono stabilite dall'articolo 60, paragrafo 4, e dall'articolo 65, paragrafo 1, lettera a), RGPD ([14]).

2.1 Obiezioni espresse dalle autorità interessate in relazione a un progetto di decisione

12. L'EDPB osserva che le autorità interessate hanno sollevato obiezioni al progetto di decisione tramite il sistema di informazione e comunicazione di cui all'articolo 17 del regolamento interno dell'EDPB, ossia il sistema di informazione del mercato interno. Le obiezioni sono state sollevate ai sensi dell'articolo 60, paragrafo 4, RGPD.

13. Più nello specifico, le autorità interessate hanno sollevato obiezioni in relazione alle questioni seguenti:

- la competenza dell'autorità capofila;
- la qualifica dei ruoli di TIC e Twitter, Inc. rispettivamente;
- le violazioni del RGPD individuate dall'autorità capofila;
- l'esistenza di possibili violazioni ulteriori (o alternative) del RGPD;
- la mancanza di un ammonimento;
- la quantificazione della sanzione pecuniaria proposta.

14. Ciascuna di queste obiezioni è stata presentata entro il termine previsto dall'articolo 60, paragrafo 4, RGPD.

2.2 L'autorità capofila non dà seguito alle obiezioni pertinenti e motivate al progetto di decisione o ritiene che non siano pertinenti e motivate

([13]) Tra i documenti inviati dall'AC IE vi erano e-mail del responsabile globale della protezione dei dati che confermavano la ricezione dei documenti pertinenti.
([14]) Ai sensi dell'articolo 65, paragrafo 1, lettera a), RGPD, il comitato adotta una decisione vincolante quando un'autorità di controllo ha sollevato un'obiezione pertinente e motivata a un progetto di decisione dell'autorità capofila o l'autorità capofila ha rigettato tale obiezione in quanto non pertinente o non motivata.

15. Il 15 luglio 2020 l'AC IE ha fornito alle autorità interessate un'analisi dettagliata delle obiezioni sollevate dalle stesse nel memorandum composito, nella quale ha indicato se considerava le obiezioni «pertinenti e motivate» ai sensi dell'articolo 4, paragrafo 24, RGPD, e se decideva di darvi seguito ([15]).

16. Più nello specifico, l'AC IE riteneva che solo le obiezioni sollevate dalle autorità interessate in relazione alla quantificazione della sanzione pecuniaria soddisfacessero la soglia di cui all'articolo 4, paragrafo 24, RGPD, nella misura in cui si riferiscono al rispetto del RGPD da parte dell'azione prevista in relazione al titolare o al responsabile del trattamento e, inoltre, espongono i rischi posti riguardo ai diritti e alle libertà fondamentali degli interessati ([16]). Tuttavia, l'AC IE ha concluso che non avrebbe dato seguito alle obiezioni, per le ragioni esposte nel memorandum composito e in appresso.

17. L'AC IE ha ritenuto che le altre obiezioni espresse dalle autorità interessate non fossero «pertinenti e motivate» ai sensi dell'articolo 4, paragrafo 24, RGPD.

2.3 Conclusione

18. Il caso in questione soddisfa tutti gli elementi elencati dall'articolo 65, paragrafo 1, lettera a), RGPD, in quanto diverse autorità interessate hanno sollevato obiezioni a un progetto di decisione dell'autorità capofila entro il termine previsto dall'articolo 60, paragrafo 4, RGPD, e l'autorità capofila non ha dato seguito alle obiezioni o le ha respinte in quanto non pertinenti o motivate.

19. L'EDPB è pertanto competente ad adottare una decisione vincolante, che riguarda tutte le questioni oggetto delle obiezioni pertinenti e motivate, in particolare l'eventuale violazione del RGPD ([17]).

20. Tutti i risultati della presente decisione non pregiudicano eventuali valutazioni o decisioni vincolanti elaborate in altri casi dall'EDPB, anche con le stesse parti, sulla base di risultati ulteriori e/o nuovi.

3 IL DIRITTO A UNA BUONA AMMINISTRAZIONE

21. L'EDPB è soggetto all'articolo 41 della Carta dei diritti fondamentali dell'Unione, in particolare all'articolo 41 (diritto a una buona amministrazione). Ciò si riflette anche nell'articolo 11, paragrafo 1, del regolamento interno dell'EDPB ([18]).

22. La decisione dell'EDPB «*è motivata e trasmessa all'autorità di controllo capofila e a tutte le autorità di controllo interessate ed è per esse vincolante*» (articolo 65, paragrafo 2, RGPD) e non intende rivolgersi direttamente a terzi. Tuttavia, come misura precauzionale per affrontare la possibilità che TIC possa essere interessata dalla decisione dell'EDPB, quest'ultimo ha valutato se a TIC sia stata offerta la possibilità di esercitare il diritto di essere ascoltata in relazione alla procedura condotta dall'autorità capofila e in particolare se tutti i documenti ricevuti in questa procedura e utilizzati dal comitato per

([15]) Lo scopo del documento, come dichiarato dall'AC IE, era quello di agevolare l'ulteriore cooperazione con le autorità interessate in relazione al progetto di decisione e rispettare il requisito di cui all'articolo 60, paragrafo 1, RGPD, secondo cui l'autorità capofila coopera con le altre autorità interessate nell'impegno per raggiungere un consenso.
([16]) Memorandum composito, paragrafo 5.59.
([17]) Articolo 65, paragrafo 1, lettera a), RGPD. Alcune autorità interessate hanno formulato osservazioni e non obiezioni di per sé, che pertanto non sono state prese in considerazione dall'EDPB.
([18]) Regolamento interno dell'EDPB, adottato il 25 maggio 2018, modificato da ultimo e adottato l'8 ottobre 2020.

prendere la sua decisione siano già stati condivisi in precedenza con TIC e se quest'ultima sia stata ascoltata in merito a essi.

23. Considerando che TIC è già stata ascoltata dall'AC IE su tutte le informazioni ricevute dall'EDPB e utilizzate per prendere la sua decisione ([19]) e che l'autorità capofila ha condiviso con il comitato le osservazioni scritte di TIC, in linea con l'articolo 11, paragrafo 2, del regolamento interno dell'EDPB ([20]), in relazione alle questioni sollevate in questo specifico progetto di decisione, l'EDPB ritiene che l'articolo 41 della Carta dei diritti fondamentali dell'Unione sia stato rispettato.

4 SULLA QUALIFICA DEL TITOLARE E DEL RESPONSABILE DEL TRATTAMENTO E SULLA COMPETENZA DELL'AUTORITÀ CAPOFILA

4.1 Analisi dell'autorità capofila nel progetto di decisione

24. Il progetto di decisione stabilisce che «*all'inizio dell'indagine l'accertatore nominato internamente [all'AC IE] [...] riteneva che ci fossero i presupposti tali per cui TIC è il titolare del trattamento, ai sensi dell'articolo 4, paragrafo 7, RGPD, in relazione ai dati personali oggetto della violazione*» e che «*a tal proposito, TIC ha confermato di essere il titolare del trattamento*» nel modulo di notifica della violazione dei dati e nella corrispondenza con l'AC IE ([21]). Il progetto di decisione stabilisce inoltre che «*TIC ha inoltre confermato che la violazione è avvenuta nell'ambito di un trattamento effettuato per suo conto da Twitter Inc., il responsabile del trattamento*» ([22]) e che «*TIC è il titolare del trattamento dei dati personali oggetto dell'indagine. TIC ha stipulato un accordo con Twitter Inc. (il responsabile del trattamento) per la fornitura di servizi di trattamento dei dati*» ([23]).

25. Inoltre, il progetto di decisione specifica che l'AC IE riteneva inoltre che ci fossero i presupposti tali per cui fosse competente ad agire in qualità di autorità capofila in riferimento al trattamento transfrontaliero effettuato da TIC, in relazione ai dati personali oggetto della violazione ([24]).

26. A questo proposito, il progetto di decisione stabilisce inoltre che TIC ha confermato all'AC IE, nel comunicare la violazione, che si trattava di «*una società irlandese*» e del «*fornitore dei servizi di Twitter in Europa*», e che la politica sulla privacy di TIC (aggiornata al gennaio 2016) informava gli utenti dei servizi di Twitter nell'UE che avevano il diritto di sollevare dubbi presso la rispettiva autorità di controllo locale o presso l'autorità capofila di TIC, l'AC IE ([25]).

27. L'AC IE ha inoltre incluso nel progetto di decisione un estratto della relazione annuale e del bilancio di TIC relativo all'esercizio finanziario chiuso al 31 dicembre 2018, specificando che «*la parte che detiene il controllo finale e il più grande gruppo di imprese per le quali viene redatto il bilancio del gruppo, e di*

([19]) Progetto preliminare di decisione dell'AC IE (14 marzo 2020); progetto di decisione dell'AC IE (22 maggio 2020); obiezioni e commenti sollevati dalle autorità interessate (18-20 giugno 2020); memorandum composito preparato dall'AC IE (15 luglio 2020); e i restanti commenti e obiezioni delle autorità interessate (27-28 luglio 2020).
([20]) Regolamento interno dell'EDPB, adottato il 25 maggio 2018, modificato da ultimo e adottato l'8 ottobre 2020.
([21]) Progetto di decisione, paragrafo 2.2.
([22]) Progetto di decisione, paragrafo 4.2.
([23]) Progetto di decisione, paragrafo 4.6.
([24]) Progetto di decisione, paragrafo 2.3.
([25]) Progetto di decisione, paragrafo 2.3.

cui la società è membro, è Twitter, Inc., società costituita negli Stati Uniti d'America e quotata alla Borsa di New York» ([26]).

28. L'AC IE ha inizialmente dovuto affrontare l'incertezza derivante dall'uso dei termini «noi» e «nostro» nel modulo di notifica della violazione dei dati per riferirsi in modo intercambiabile a TIC e Twitter, Inc. L'AC IE ha chiesto chiarimenti a questo proposito e TIC ha indicato che i dipendenti di TIC e Twitter, Inc. usano abitualmente «noi» e «nostro» per riferirsi in modo generico al gruppo con il suo nome. Inoltre, TIC ha indicato che, pur essendo il titolare del trattamento e prendendo decisioni in merito alle finalità e ai mezzi del trattamento dei dati, TIC non opera da sola: «*TIC e i suoi dipendenti fanno parte [...] del Gruppo Twitter [...]. Tutti i dipendenti del Gruppo Twitter utilizzano gli stessi sistemi informatici, aderiscono alle stesse politiche generali... e lavorano insieme per garantire il supporto globale 24 ore su 24 necessario per mantenere operativa la piattaforma di Twitter*»[27].

4.2 Sintesi delle obiezioni sollevate dalle autorità interessate

29. Nella sua obiezione, l'**AC ES** afferma che **il progetto di decisione non giustifica sufficientemente il ruolo di titolare del trattamento di TIC**. L'AC ES sottolinea che si dovrebbe effettuare una valutazione circa quale entità decida realmente le finalità e i mezzi, oltre a un'analisi critica di tutti i fatti che si sono verificati. Secondo l'AC ES, gli elementi alla base del progetto di decisione sembrano suggerire una conclusione diversa da quella raggiunta dall'AC IE. In particolare, l'AC ES ritiene che le decisioni sulle finalità essenziali del trattamento dei dati siano effettivamente prese da Twitter, Inc. L'AC ES ha sostenuto il suo ragionamento elencando alcuni fattori che, a suo avviso, potrebbero suggerire che TIC non decide in merito alle finalità e ai mezzi. In primo luogo, l'AC ES ha ricordato che TIC è una società controllata da Twitter, Inc. e ha sottolineato che sarebbe quindi difficile comprendere come TIC possa «*impartire ordini*» a Twitter, Inc. in relazione al trattamento dei dati personali degli utenti SEE. Secondo l'AC ES, TIC non è mai stata in grado di scegliere autonomamente Twitter, Inc. come suo responsabile del trattamento e non sarebbe in grado di sostituirlo. Inoltre, l'AC ES ha sostenuto che Twitter, Inc. non sembra agire come responsabile del trattamento a causa della «*mancanza di un canale diretto*» fra le due società nella gestione dei casi di violazione dei dati, a parte l'invio di una e-mail con il responsabile globale della protezione dei dati in copia. In terzo luogo, l'AC ES ha dichiarato che non era chiaro come TIC avrebbe potuto adottare o influenzare in modo indipendente le decisioni che hanno portato alla correzione del bug informatico nel sistema gestito e controllato da Twitter, Inc., e che è stata piuttosto Twitter, Inc. a prendere decisioni relative alla soluzione della violazione, i cui effetti non erano limitati solo agli utenti europei.

30. L'**AC NL** ha inoltre sollevato un'obiezione in merito alla qualifica giuridica di TIC e Twitter, Inc. rispettivamente come titolare e responsabile del trattamento. In particolare, l'obiezione si riferisce al modo in cui l'AC IE ha sostenuto che in questo caso TIC è l'unico titolare del trattamento e che Twitter, Inc. è un responsabile del trattamento che agisce per conto di TIC. L'AC NL ritiene che la valutazione della titolarità del trattamento sia un aspetto fondamentale del caso in esame e che pertanto qualsiasi conclusione relativa al ruolo di titolare, responsabile o contitolare del trattamento debba essere suffragata da elementi di fatto e di diritto. Nella sua obiezione**, l'AC NL sostiene essenzialmente che il progetto di decisione non contiene prove sufficienti per stabilire di fatto e di diritto i ruoli delle entità interessate**, in particolare per sostenere la conclusione i) che TIC è (unico) titolare e ii) che Twitter, Inc. è semplicemente un responsabile del trattamento che agisce su istruzione di TIC per il funzionamento del servizio globale di Twitter e/o le finalità che sono rilevanti nel presente caso. Secondo l'AC NL, l'autorità capofila dovrebbe verificare **se le dichiarazioni legali dell'organizzazione e/o la sua politica**

([26]) Progetto di decisione, paragrafo 2.4.
([27]) Progetto di decisione, paragrafo 4.5.

sulla privacy corrispondono alla sua attività effettive. L'AC NL ha chiesto all'AC IE di includere maggiori informazioni e/o una descrizione dei fattori che portano alla determinazione dei ruoli nello stesso documento del progetto di decisione. L'AC NL menziona inoltre, come esempi di fattori da prendere in considerazione: istruzioni da TIC a Twitter, Inc., o altre prove oggettive o indizi concreti derivanti da operazioni quotidiane, nonché esempi di registri scritti come un accordo di trattamento dei dati.

31. Nella sua obiezione, l'**AC DE** sostiene che **il rapporto tra Twitter, Inc. e TIC non è un rapporto fra titolare e responsabile del trattamento**, ma piuttosto un rapporto fra contitolari del trattamento. L'obiezione si basa in primo luogo sul fatto che Twitter, Inc. e TIC non gestiscono sistemi di trattamento dei dati separati. Secondo l'AC DE, il sistema di base gestito da Twitter, Inc. viene modificato in base alle decisioni prese da TIC e a quelle per gli utenti del SEE, mentre il sistema di trattamento principale rimane lo stesso. L'AC DE ha inoltre sottolineato che tutti i dipendenti del gruppo utilizzano lo stesso sistema informatico e aderiscono alle stesse politiche generali.

32. Infine, l'**AC FR** ha sollevato un'obiezione in merito alla competenza dell'AC IE, affermando che sembra che l'AC IE sia giunta alla conclusione che il potere decisionale sulle finalità e sui mezzi del trattamento in questione sia stato esercitato da TIC. Secondo l'AC FR, **il progetto di decisione non indica chiaramente che altri elementi oltre alle dichiarazioni della società TIC siano stati presi in considerazione dall'autorità per considerare che tale società avesse un potere decisionale sul trattamento**. L'AC FR ha inoltre specificato che il progetto di decisione non indica chiaramente se la competenza dell'autorità si basi sul fatto che la società TIC debba essere considerata il titolare, o sul fatto che debba essere considerata lo stabilimento principale come definito dall'articolo 4, paragrafo 16, RGPD. L'AC FR ha concluso che, allo stato attuale, il progetto di decisione non impedisce il rischio di scelta opportunistica del foro, che il meccanismo dello sportello unico intende evitare. L'AC FR ha invitato l'AC IE a fornire ulteriori elementi che permettano di dimostrare che la società TIC ha un potere decisionale per quanto riguarda le finalità e i mezzi del trattamento per il social network Twitter.

4.3 Posizione dell'autorità capofila in merito alle obiezioni

33. Nel memorandum composito, l'AC IE ha ritenuto che un'obiezione basata sul ruolo o sulla designazione delle parti come titolare e responsabile del trattamento e/o sulla sua competenza «*non contesta l'accertamento di una violazione né l'azione prevista e, pertanto, non soddisfa la definizione di cui all'articolo 4, paragrafo 24*» e che «*non rientra nella definizione di obiezione "pertinente e motivata" ai sensi dell'articolo 4, paragrafo 24*» ([28]). L'AC IE ha tuttavia analizzato tali obiezioni e, nel farlo, ha esposto i fattori che aveva considerato nel determinare lo status di titolare del trattamento e di stabilimento principale di TIC. A questo proposito, l'AC IE ha delineato (in sintesi) ([29]) i fatti e l'analisi giuridica che hanno portato alla sua conclusione in merito allo status di titolare del trattamento di TIC, in sostanza:

- la precedente conferma da parte di Twitter, nel 2015, della sua proposta di rendere TIC in Irlanda il titolare del trattamento dei dati personali degli utenti di Twitter nell'UE ([30]);

([28]) Memorandum composito, paragrafo 5.39.
([29]) Memorandum composito, paragrafo 5.35.
([30]) A questo proposito, il memorandum composito spiega che TIC ha informato l'AC IE in data 8 aprile 2015 di aver proposto di rendere TIC in Irlanda il titolare del trattamento dei dati personali dei suoi utenti al di fuori degli USA e che TIC ha comunicato questo fatto ad altre autorità di controllo dell'UE nel maggio 2015 (paragrafo 5.15).

- la conferma da parte di TIC di essere il titolare del trattamento dei dati personali interessati dalla violazione sia nella notifica della stessa all'AC IE, sia nel corso dell'indagine;
- la conferma da parte di TIC dell'esistenza di un accordo di trattamento dei dati tra la stessa e Twitter, Inc. in qualità di suo responsabile del trattamento, il quale include le disposizioni richieste dall'articolo 28 del RGPD;
- le interazioni tra TIC e Twitter, Inc. dopo il 7 gennaio 2019, quando TIC (attraverso il suo responsabile della protezione dei dati) è stata effettivamente informata della violazione, dimostrando secondo l'AC IE che TIC esercitava il controllo e l'autorità decisionale su Twitter, Inc. per quanto riguarda le attività di riparazione e la notifica della violazione e in relazione al relativo trattamento dei dati personali interessati dalla violazione; e
- le azioni di Twitter, Inc. al momento della notifica dell'incidente da parte del contraente 2, anch'esse secondo l'AC IE a sostegno dello status del rapporto esistente tra le due entità come uno in cui TIC esercitava l'autorità e assumeva responsabilità in qualità di titolare del trattamento.

34. L'AC IE ha quindi esposto, in sintesi ([31]), i fatti e l'analisi giuridica che hanno portato alla conclusione secondo la quale lo stabilimento principale di TIC è in Irlanda, in sostanza (oltre ai punti precedenti):
    - la designazione e la dichiarazione di TIC stessa come stabilimento principale;
    - la conferma da parte di TIC nella sua politica sulla privacy dello status di titolare del trattamento rilevante dei dati personali degli utenti di Twitter nell'UE;
    - la sede dell'amministrazione centrale di TIC si trova a Dublino, e conta circa 170 dipendenti;
    - l'assunzione diretta da parte di TIC di un responsabile globale della protezione dei dati ai fini del RGPD, la linea di segnalazione per lo stesso all'interno di TIC e la rappresentazione di TIC da parte del responsabile globale della protezione dei dati su una serie di attività relative alla privacy e al trattamento dei dati, compresa la possibilità di porre il veto al trattamento dei dati;
    - il controllo storico e continuativo di TIC da parte dell'AC IE, durante il quale è emerso che TIC determina le finalità e i mezzi per i quali i dati personali sono trattati all'interno dell'UE.

    L'AC IE ha ribadito che, nonostante la sua risposta alla sostanza delle obiezioni sollevate sulle questioni di competenza e/o sulla designazione delle parti, non ha ritenuto che le obiezioni in relazione a tali questioni soddisfacessero la definizione di «obiezione pertinente e motivata» ai sensi dell'articolo 4, paragrafo 24, RGPD. L'AC IE ha dichiarato che, sia alla luce della sua valutazione secondo cui tali questioni non soddisfano la definizione di cui all'articolo 4, paragrafo 24, del RGPD, sia alla luce della sua dimostrazione di aver affrontato adeguatamente le questioni circa lo stabilimento principale, la sua competenza e la designazione del titolare e del responsabile del trattamento nel suo progetto di decisione, non intendeva dare seguito alle obiezioni su tali questioni ([32]).

4.4 Analisi dell'EDPB

([31]) Memorandum composito, paragrafo 5.36.
([32]) Memorandum composito, paragrafo 5.40.

4.4.1 *Valutazione della pertinenza e della motivazione delle obiezioni*

35. L'EDPB inizierà la sua analisi delle obiezioni sollevate valutando se le suddette obiezioni debbano essere considerate «obiezioni pertinenti e motivate» ai sensi dell'articolo 4, paragrafo 24, RGPD.

36. L'articolo 4, paragrafo 24, RGPD definisce «l'obiezione pertinente e motivata» come «*un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione*» ([33]).

37. Come chiarito nelle linee guida relative al concetto di obiezione pertinente e motivata, un'obiezione deve essere sia «pertinente» che «motivata». Affinché l'obiezione sia «pertinente», deve sussistere un collegamento diretto tra l'obiezione e il progetto di decisione e deve riguardare sia l'esistenza di una violazione del RGPD, sia la conformità dell'azione prevista in relazione al titolare o al responsabile del trattamento al RGPD ([34]).

38. Secondo le stesse linee guida ([1]), un'obiezione è «motivata» quando è coerente, chiara, precisa e dettagliata nel fornire chiarimenti e argomentazioni sui motivi per cui viene proposta una modifica della decisione e su come la modifica comporterebbe una conclusione diversa ([35]) e quando dimostra chiaramente l'importanza dei rischi posti dal progetto di decisione per i diritti e le libertà fondamentali degli interessati e, se del caso, per la libera circolazione dei dati personali all'interno dell'Unione europea. L'autorità interessata dovrebbe quindi «*mostrare le implicazioni che il progetto di decisione avrebbe per i valori tutelati* (...) *avanzando argomenti sufficienti a dimostrare che tali rischi sono sostanziali e plausibili*» ([36]). La valutazione dei rischi per i diritti e le libertà degli interessati ([37]) può basarsi, tra l'altro, sull'adeguatezza, la necessità e la proporzionalità delle misure previste ([38]) e sulla possibile riduzione delle future violazioni del RGPD ([39]).

39. In termini di contenuto, l'obiezione può, come prima alternativa, riguardare l'esistenza di una violazione del RGPD. In tal caso, dovrebbe spiegare perché l'autorità interessata non è d'accordo sul fatto che le attività svolte dal titolare o dal responsabile del trattamento abbiano portato alla violazione di una determinata disposizione del RGPD e a quale violazione (o violazioni) in particolare ([40]). Tale obiezione può anche comprendere un disaccordo sulle conclusioni da trarre dai risultati dell'indagine (ad esempio dichiarando che i risultati costituiscono una violazione

([33]) RGPD, articolo 4, paragrafo 24.
Cfr. anche le linee guida 9/2020 dell'EDPB relative al concetto di obiezione pertinente e motivata, versione per la consultazione pubblica (in appresso: «**Linee guida relative alla RRO**»), paragrafo 12, attualmente oggetto di consultazione pubblica, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-092020-relevant-and-reasoned-objection_en. Le linee guida sono state adottate l'8 ottobre 2020, dopo l'avvio dell'indagine da parte dell'AC IE relativa a questo caso particolare.
([35]) Linee guida relative alla RRO, paragrafi 17 e 20.
([36]) Linee guida relative alla RRO, paragrafo 37.
([37]) Gli «interessati» i cui diritti e le cui libertà possono essere pregiudicati possono essere sia quelli i cui dati personali sono trattati dal titolare/responsabile del trattamento, sia quelli i cui dati personali possono essere trattati in futuro. Linee guida relative alla RRO, paragrafo 43.
([38]) Linee guida relative alla RRO, paragrafo 42.
([39]) Linee guida relative alla RRO, paragrafo 43.
([40]) Linee guida relative alla RRO, paragrafo 25.

diversa/supplementare rispetto a quelle già analizzate) ([41]) o potrebbe arrivare fino all'individuazione di lacune nel progetto di decisione che giustifichino la necessità di ulteriori indagini da parte dell'autorità capofila ([42]). Tuttavia, è meno probabile che ciò avvenga quando l'obbligo per l'autorità capofila di cooperare con le autorità interessate e di scambiarsi tutte le informazioni pertinenti è stato debitamente rispettato nel periodo precedente la presentazione del progetto di decisione ([43]). In alternativa, il contenuto dell'obiezione può fare riferimento alla conformità dell'azione in relazione al titolare o al responsabile del trattamento (misura correttiva o altro), prevista nel progetto di decisione, rispetto al RGPD, spiegando perché l'azione prevista non è in linea con il RGPD ([44]).

40. L'EDPB ritiene possibile che un'obiezione relativa all'esistenza di una violazione del RGPD riguardi l'assenza o l'insufficienza della valutazione o della motivazione (con la conseguenza che la conclusione contenuta nel progetto di decisione non è adeguatamente corroborata dalla valutazione effettuata e dalle prove presentate, come richiesto dall'articolo 58 del RGPD), purché sia rispettato nella sua interezza il requisito di soglia stabilito dall'articolo 4, paragrafo 24, RGPD e purché vi sia un nesso tra l'analisi asseritamente insufficiente e l'esistenza di una violazione del RGPD o la conformità dell'azione prevista al RGPD ([45]).

41. L'EDPB ritiene che un'obiezione relativa al ruolo o alla designazione delle parti possa rientrare nella definizione di obiezione «pertinente e motivata» di cui all'articolo 4, paragrafo 24, RGPD, poiché ciò può incidere sulla determinazione dell'esistenza di una violazione del presente regolamento o della conformità al presente regolamento delle azioni previste in relazione al titolare o al responsabile del trattamento. Tuttavia, l'EDPB ritiene che un'obiezione in merito alla competenza dell'autorità di controllo che agisce in qualità di autorità capofila non debba essere sollevata tramite un'obiezione ai sensi dell'articolo 60, paragrafo 4, RGPD e non rientri nel campo di applicazione dell'articolo 4, paragrafo 24, RGPD ([46]).

a) Valutazione dell'obiezione sollevata dall'AC NL

42. L'obiezione sollevata dall'AC NL in prima istanza si riferisce a una «*assenza o insufficienza di valutazione o di motivazione*» ([47]) che porta alle conclusioni dell'AC IE in merito alla qualifica giuridica di TIC e Twitter, Inc. Come sottolinea l'AC NL, la valutazione della titolarità del trattamento è in effetti un aspetto fondamentale del caso. Una diversa conclusione in merito alla qualifica giuridica di TIC e Twitter, Inc. influenzerebbe le conclusioni dell'autorità di controllo, sia in relazione all'accertamento

([41]) Linee guida relative alla RRO, paragrafo 27.
([42]) Linee guida relative alla RRO, paragrafo 28 (che specifica inoltre che «[a] questo proposito occorre distinguere tra, da un lato, le indagini d'ufficio e, dall'altro, le indagini avviate a seguito di reclami o di segnalazioni di potenziali violazioni condivise dalle autorità di controllo interessate»).
([43]) Linee guida relative alla RRO, paragrafo 27.
([44]) Linee guida relative alla RRO, paragrafo 33. Ciò significa che l'obiezione può, tra l'altro, contestare gli elementi su cui si è fatto affidamento per la quantificazione della sanzione pecuniaria (linee guida relative alla RRO, paragrafo 34).
([45]) Linee guida relative alla RRO, paragrafo 29.
([46]) La procedura di cui all'articolo 65, paragrafo 1, lettera b), RGPD è applicabile in questo caso e può essere avviata in qualsiasi fase; cfr. linee guida relative alla RRO, paragrafo 31.
([47]) Linee guida relative alla RRO, paragrafo 29. Un'obiezione pertinente e motivata riguardante l'esistenza di una violazione del RGPD può riguardare «*informazioni fattuali o una descrizione del caso in questione insufficienti», un «disaccordo sulle conclusioni da trarre dai risultati dell'indagine*» (Linee guida relative alla RRO, paragrafo 27) o fare riferimento a una «*assenza o insufficienza di valutazione o di motivazione (con la conseguenza che la conclusione nel progetto di decisione non è adeguatamente supportata dalla valutazione effettuata e dalle prove presentate, come richiesto dall'articolo 58 del RGPD)*» (Linee guida relative alla RRO, paragrafo 29).

di una violazione dell'articolo 33 del RGPD, sia in relazione alla decisione sulle misure correttive risultanti dall'indagine.

43. L'EDPB ricorda che ogni misura giuridicamente vincolante adottata da un'autorità di controllo deve essere motivata ([48]). La determinazione dell'esistenza di una violazione del presente regolamento o della conformità delle azioni previste nei confronti del titolare o del responsabile del trattamento al presente regolamento dipende dalla corretta identificazione dei ruoli delle parti che sono oggetto del provvedimento. Pertanto, un progetto di decisione deve contenere sufficienti elementi di fatto e di diritto a sostegno della decisione proposta ([49]). Di conseguenza, l'EDPB ritiene che l'obiezione sollevata dall'AC NL riguardi sia «l'esistenza di una violazione del RGPD» sia «la conformità o meno dell'azione prevista con il RGPD».

44. L'EDPB ritiene pertanto che l'obiezione dell'AC NL sia pertinente e contenga argomentazioni giuridiche a sostegno della sua posizione, ma che non avanzi argomentazioni sul modo in cui tali conseguenze comporterebbero rischi significativi per i diritti e le libertà degli interessati e/o per la libera circolazione dei dati ([50]). L'EDPB ricorda che l'obbligo di dimostrare chiaramente l'importanza del rischio posto dal progetto di decisione (stabilito dal RGPD) spetta all'autorità interessata ([51]). Mentre la possibilità per le autorità interessate di fornire tale dimostrazione può anche dipendere dal grado di dettaglio del progetto di decisione stesso e dai precedenti scambi di informazioni ([52]), tale circostanza, ove applicabile, non può esonerare completamente l'autorità interessata dall'obbligo di esporre chiaramente i motivi per cui ritiene che il progetto di decisione, se lasciato invariato, comporti rischi significativi per i diritti e le libertà delle persone.

45. L'EDPB ritiene che l'obiezione sollevata dall'AC NL non dimostri chiaramente i rischi per i diritti e le libertà delle persone in quanto tali. Su tale base, l'EDPB ritiene che l'obiezione sollevata dall'AC NL non soddisfi i requisiti di cui all'articolo 4, paragrafo 24, RGPD.

b) Valutazione dell'obiezione sollevata dall'AC ES

46. L'obiezione sollevata dall'AC ES contesta anche la sufficienza della valutazione o della motivazione in relazione alle conclusioni tratte dall'AC IE in merito alla qualifica giuridica di TIC e Twitter, Inc. L'obiezione chiarisce inoltre che la corretta qualifica di TIC e di Twitter, Inc. è fondamentale per determinare le rispettive responsabilità, nonché per la competenza dell'AC IE. Di conseguenza, l'EDPB ritiene che anche l'obiezione sollevata dall'AC ES riguardi sia «l'esistenza di una violazione del RGPD» sia «la conformità dell'azione prevista al RGPD». L'obiezione dell'AC ES espone inoltre i motivi per cui ritiene necessaria una modifica del progetto di decisione e il modo in cui tale modifica porterebbe a una diversa conclusione.

47. L'EDPB ritiene che l'obiezione dell'AC ES sia pertanto pertinente e contenga argomentazioni giuridiche a sostegno della sua posizione, ma che non spieghi chiaramente perché la decisione, se lasciata invariata al riguardo, comporterebbe rischi significativi per i diritti e le libertà degli interessati e, ove

([48]) Cfr. il considerando 129 del RGPD.
([49]) Tali informazioni sono necessarie anche per garantire l'efficacia del meccanismo di cooperazione e di coerenza, in modo tale da consentire alle autorità interessate di decidere con cognizione di causa se accettare o meno o esprimere un'obiezione pertinente e motivata.
([50]) Linee guida relative alla RRO, paragrafo 19.
([51]) Linee guida relative alla RRO, paragrafo 36 e articolo 4, paragrafo 24, RGPD.
([52]) Linee guida relative alla RRO, paragrafo 36.

applicabile, per la libera circolazione dei dati personali. Su questa base l'EDPB ritiene che l'obiezione sollevata dall'AC ES non soddisfi i requisiti di cui all'articolo 4, paragrafo 24, RGPD.

c) Valutazione dell'obiezione sollevata dall'AC DE

48. Mentre le obiezioni espresse dalle AC NL ed ES si riferiscono principalmente a una «mancanza di motivazione» che giustifichi la conclusione secondo la quale TIC agisce come (unico) titolare, l'AC DE non concorda con le conclusioni da trarre dai risultati dell'indagine ([53]). In particolare, l'AC DE ritiene che gli elementi di fatto inclusi nel fascicolo siano sufficienti a giustificare la conclusione per cui Twitter, Inc. non si qualifica come responsabile, ma piuttosto come contitolare del trattamento, insieme a TIC.

49. Nella sua obiezione l'AC DE espone anche il motivo per cui la qualifica delle parti è rilevante per determinare «l'esistenza di una violazione». In particolare, l'AC DE sostiene che la valutazione giuridica della relazione fra Twitter, Inc. e TIC influisce sulla determinazione del momento in cui si viene a conoscenza della violazione. Secondo l'AC DE, la conoscenza deve essere ugualmente attribuita a entrambi i (con)titolari del trattamento alla luce dell'articolo 26, paragrafo 1, RGPD. Tenendo conto di ciò, l'AC DE sostiene che la data rilevante in cui TIC, in qualità di contitolare del trattamento, è venuta a conoscenza (o meglio sarebbe dovuta venire a conoscenza) deve essere riconsiderata dall'AC IE.

50. L'EDPB ritiene che l'obiezione sollevata dall'AC DE indichi chiaramente perché si ritiene necessario modificare il progetto di decisione e in che modo l'obiezione, se seguita, porterebbe a una diversa conclusione. Ciò detto, l'EDPB non ritiene che l'obiezione sollevata dall'AC DE contenga una chiara dichiarazione sui rischi posti dal progetto di decisione per quanto riguarda i diritti e le libertà fondamentali degli interessati in relazione alla qualifica delle parti in quanto tali. Su tale base, l'EDPB ritiene che l'obiezione sollevata dall'AC DE non soddisfi i requisiti di cui all'articolo 4, paragrafo 24, RGPD.

d) Valutazione dell'obiezione sollevata dall'AC FR

51. In sostanza, anche l'AC FR ritiene che il progetto di decisione soffra di «assenza o insufficienza di valutazione o di motivazione», in quanto non indica chiaramente che l'AC IE abbia preso in considerazione altri elementi diversi dalle dichiarazioni di TIC per ritenere che quest'ultima esercitasse il potere decisionale sul trattamento. Analogamente alle AC NL ed ES, anche l'AC FR sottolinea l'importanza che la decisione dell'autorità capofila sia sufficientemente motivata. A differenza delle AC NL ed ES, tuttavia, l'AC FR si concentra, nella sua obiezione, principalmente sull'importanza di includere tale ragionamento nell'accertamento della competenza dell'autorità capofila, in particolare al fine di evitare la scelta opportunistica del foro.

52. L'EDPB ricorda che un'eccezione sulla competenza dell'autorità di controllo che agisce in qualità di autorità capofila ad adottare una decisione nel caso specifico non dovrebbe essere sollevata tramite un'obiezione ai sensi dell'articolo 60, paragrafo 4, RGPD e non rientra nel campo di applicazione dell'articolo 4, paragrafo 24, RGPD ([54]). L'EDPB ritiene che l'obiezione sollevata dall'AC FR non contenga argomenti sufficienti a chiara dimostrazione dell'importanza del rischio per i diritti e le libertà degli interessati rappresentato dal progetto di decisione. Di conseguenza, l'EDPB ritiene che l'obiezione sollevata dall'AC FR non costituisca un'obiezione pertinente e motivata ai sensi dell'articolo 4, paragrafo 24, RGPD.

([53]) Linee guida relative alla RRO, paragrafo 27.
([54]) Linee guida relative alla RRO, paragrafo 31. Le linee guida precisano inoltre che, a differenza dell'obiezione ai sensi dell'articolo 60, paragrafo 4, RGPD, la procedura di cui all'articolo 65, paragrafo 1, lettera b), RGPD è applicabile in qualsiasi fase.

4.4.2 Conclusione

53. L'EDPB ritiene che le suddette obiezioni soddisfino diversi criteri di cui all'articolo 4, paragrafo 24, RGPD. Diversamente dalla conclusione dell'AC IE, l'EDPB ritiene che ciascuna obiezione soddisfi la condizione di far riferimento, alternativamente, all'esistenza di una violazione del presente regolamento o alla conformità al regolamento stesso delle azioni previste nei confronti del titolare o del responsabile del trattamento. Inoltre, l'EDPB ritiene che un'obiezione relativa al ruolo o alla qualificazione giuridica delle parti possa, in linea di principio, rientrare nella definizione di obiezione «pertinente e motivata» di cui all'articolo 4, paragrafo 24, RGPD.

54. Tuttavia, come indicato in precedenza, le suddette obiezioni non soddisfano il requisito di soglia che prevede di fornire una chiara dimostrazione dell'importanza dei rischi posti dal progetto di decisione per quanto riguarda i diritti e le libertà fondamentali degli interessati e, ove applicabile, la libera circolazione dei dati personali all'interno dell'Unione europea.

55. Inoltre, per quanto riguarda la summenzionata obiezione sollevata dall'AC FR, oltre a non fornire una sufficiente argomentazione per dimostrare chiaramente l'importanza del rischio per i diritti e le libertà degli interessati posto dal progetto di decisione, l'obiezione riguarda un disaccordo sulla competenza dell'autorità di controllo che agisce in qualità di autorità capofila. L'EDPB ricorda che tale eccezione non deve essere sollevata tramite un'obiezione ai sensi dell'articolo 60, paragrafo 4, RGPD e non rientra nel campo di applicazione dell'articolo 4, paragrafo 24, RGPD ([55]).

56. Pertanto, l'EDPB ritiene che le suddette obiezioni non soddisfino i requisiti di cui all'articolo 4, paragrafo 24, RGPD.

57. Di conseguenza, **l'EDPB non prende posizione sul merito di eventuali questioni sostanziali sollevate da tali obiezioni**. **L'EDPB ribadisce che la sua attuale decisione non pregiudica le valutazioni che il comitato può essere chiamato a effettuare in altri casi, anche con le stesse parti, tenendo conto del contenuto del relativo progetto di decisione e delle obiezioni sollevate dalle autorità interessate**.

5 SULLE VIOLAZIONI DEL RGPD RISCONTRATE DALL'AUTORITÀ CAPOFILA

5.1 Sull'accertamento di una violazione dell'articolo 33, paragrafo 1, RGPD

5.1.1 Analisi dell'autorità capofila nel progetto di decisione

58. L'AC IE ha concluso che TIC non ha rispettato gli obblighi di titolare del trattamento ai sensi dell'articolo 33, paragrafo 1, RGPD, che «*non può essere considerato isolatamente e deve essere inteso nel contesto dei più ampi obblighi dei titolari del trattamento ai sensi del RGPD, in particolare l'obbligo di responsabilizzazione ai sensi dell'articolo 5, paragrafo 2, il rapporto tra titolari e responsabili del trattamento (articolo 28), e l'obbligo di attuare misure tecniche e organizzative adeguate (ed efficaci)*» ([56]).

([55]) Linee guida relative alla RRO, paragrafo 31.
([56]) Progetto di decisione, paragrafo 6.20. Cfr. anche progetto di decisione, paragrafi 6.5, 6.7 e 6.13. Il progetto di decisione (paragrafo 7.129, punto i)) stabilisce inoltre che «*il requisito di cui all'articolo 33, paragrafo 1 [...] si basa sul fatto che il titolare garantisca di disporre di sistemi e procedure interni (e, se del caso, di sistemi e*

59. Per quanto riguarda il momento in cui il titolare del trattamento è venuto a conoscenza della violazione, il progetto di decisione ha concluso che, nel caso in cui la violazione sia stata subita dal responsabile del trattamento, il titolare del trattamento ne viene a conoscenza quando viene informato della violazione dal responsabile del trattamento ([57]), ma il titolare del trattamento deve garantire di disporre di misure sufficienti per agevolare tale presa di conoscenza ([58]). Poiché TIC, in qualità di titolare del trattamento, era responsabile della supervisione delle operazioni di trattamento effettuate dal responsabile del trattamento Twitter, Inc. ([59]), il progetto di decisione ha stabilito che, qualora il responsabile del trattamento non segua la procedura o la procedura fallisca in altro modo, il titolare del trattamento non può giustificare la propria notifica tardiva sulla base della colpa del responsabile del trattamento ([60]), in quanto l'adempimento dell'obbligo di notifica da parte di un titolare del trattamento non può essere subordinato al rispetto da parte del responsabile del trattamento dei suoi obblighi ai sensi dell'articolo 33, paragrafo 2, RGPD ([61]). L'AC IE ha rilevato che in tali circostanze si deve ritenere che il titolare del trattamento venga a conoscenza in modo costruttivo della violazione dei dati tramite il responsabile del trattamento ([62]) e che tale interpretazione riflette la responsabilità e la responsabilizzazione del titolare del trattamento nel RGPD ([63]).

60. Secondo il progetto di decisione, quindi, TIC è venuta effettivamente a conoscenza della violazione il 7 gennaio 2019 ([64]), ma avrebbe dovuto esserne venuta a conoscenza al più tardi entro il 3 gennaio 2019, poiché in quella data Twitter, Inc., in qualità di responsabile del trattamento, ha valutato l'incidente come una potenziale violazione dei dati e il team legale di Twitter, Inc. ha dato istruzioni di aprire la procedura di incidente ([65]). Il progetto di decisione affermava inoltre che, anche nelle particolari circostanze di questa situazione (in cui si erano verificati anche ritardi precedenti) ([66]), eventuali accordi in essere con Twitter, Inc. avrebbero dovuto consentire ciò ([67]). Invece, a causa

procedure in atto con qualsiasi soggetto esterno, compresi i responsabili del trattamento) che siano configurati e seguiti, in modo tale da agevolare la rapida presa di coscienza e la tempestiva notifica delle violazioni».

([57]) Progetto di decisione, paragrafo 7.129, punto iii).

([58]) Progetto di decisione, paragrafo 7.98.

([59]) Progetto di decisione, paragrafo 7.129, punto iv).

([60]) Progetto di decisione, paragrafo 7.129, punto iv).

([61]) Progetto di decisione, paragrafo 7.129, punto x).

([62]) Progetto di decisione, paragrafo 7.129, punto v).

([63]) Progetto di decisione, paragrafo 7.98. Secondo il progetto di decisione, un'interpretazione alternativa che porta a ritenere che un titolare del trattamento sia «consapevole» solo quando è informato dal responsabile del trattamento, lascia una lacuna significativa nella protezione fornita dal RGPD, in quanto potrebbe far sì che il titolare del trattamento eviti le responsabilità anche in caso di ritardi rilevanti se dimostra di aver adempiuto ai propri obblighi nella scelta di un responsabile del trattamento e di disporre di sistemi adeguati, ma che tali sistemi non vengono presi in considerazione dal responsabile del trattamento (progetto di decisione, paragrafo 7.99). L'AC IE ha inoltre sottolineato nel progetto di decisione che «l'applicazione alternativa dell'articolo 33, paragrafo 1, e quella suggerita da TIC, secondo cui l'adempimento dell'obbligo di notifica da parte di un titolare del trattamento è essenzialmente subordinato al rispetto da parte del responsabile del trattamento degli obblighi di cui all'articolo 33, paragrafo 2, comprometterebbe l'efficacia degli obblighi di cui all'articolo 33 da parte di un titolare del trattamento [e che] un tale approccio sarebbe in contrasto con lo scopo generale del RGPD e con l'intenzione del legislatore dell'UE».

([64]) Progetto di decisione, paragrafo 7.129, punto vi).

([65]) Progetto di decisione, paragrafo 7.129, punto vi).

([66]) Nell'individuare il 3 gennaio 2019 come data in cui TIC avrebbe dovuto essere a conoscenza della violazione, l'AC IE ha tenuto conto anche del fatto che si era verificato un precedente ritardo nel periodo trascorso tra la data in cui l'incidente era stato notificato per la prima volta dal contraente esterno (contraente 2) a Twitter, Inc., il 29 dicembre 2018, alla data in cui Twitter, Inc. ha avviato la revisione dello stesso, il 2 gennaio 2019. TIC ha confermato, nel corso dell'indagine, che la causa di ciò è legata al «*programma delle vacanze natalizie*».

[67] Progetto di decisione, paragrafo 7.129, punto ix).

dell'«inefficacia del processo» nelle «particolari circostanze» del caso in questione e/o «un'incapacità del personale [del responsabile del trattamento] di seguire il processo di gestione degli incidenti», si è verificato un ritardo a causa del quale la comunicazione al titolare del trattamento è avvenuta solo il 7 gennaio 2019 ([68]). Ciò ha portato alla violazione dell'articolo 33, paragrafo 1, RGPD, anche se sono trascorse meno di 72 ore tra il momento in cui TIC è venuto effettivamente a conoscenza della violazione (7 gennaio 2019) e la notifica (8 gennaio 2019).

5.1.2 Sintesi delle obiezioni sollevate dalle autorità interessate

61. L'**AC FR** ha sollevato un'obiezione affermando che i risultati non corrispondono a una violazione dell'articolo 33, paragrafo 1, RGPD, ma piuttosto degli articoli 28 o 32 del RGPD, che stabiliscono gli obblighi del titolare del trattamento quando decide di ricorrere a un responsabile del trattamento. Tale argomentazione si basa sul fatto che l'accertamento della violazione dell'articolo 33, paragrafo 1, si basa principalmente sulle carenze nell'applicazione della procedura stabilita tra TIC e il responsabile del trattamento in caso di violazione dei dati, mentre l'articolo 33, paragrafo 1, RGPD si riferisce solo all'obbligo del titolare del trattamento di notificare le violazioni dei dati all'autorità competente.

62. Le obiezioni dell'**AC DE**, invece, si sono concentrate sul ragionamento che ha portato a concludere che l'articolo 33, paragrafo 1, RGPD è stato violato, senza contestare tale conclusione di per sé, e si riferivano più nello specifico alla determinazione del *dies a quo* del termine di 72 ore.

63. Nella sua obiezione, l'AC DE ha sostenuto che la questione dell'assegnazione dei ruoli incide sulla determinazione del momento di presa di coscienza della violazione, in quanto la conoscenza di una violazione deve essere attribuita in egual misura a entrambi i contitolari del trattamento. Secondo l'AC DE, ciò potrebbe portare a considerare il 26 dicembre 2018 come data in cui TIC, in qualità di contitolare del trattamento, è venuta a conoscenza/dovrebbe essere venuta a conoscenza della violazione.

5.1.3 Posizione dell'autorità capofila in merito alle obiezioni

64. Per quanto riguarda l'obiezione sollevata dall'AC FR, l'AC IE ritiene che essa richieda l'esame di disposizioni alternative del RGPD e che la richiesta da parte delle autorità interessate di prendere in considerazione disposizioni alternative del RGPD mirerebbe essenzialmente a ridefinire l'ambito di applicazione dell'indagine condotta ([69]): l'AC IE ha concluso che tale obiezione non rientra nella definizione di «obiezione pertinente e motivata» ai fini dell'articolo 4, paragrafo 24, RGPD ([70]). L'AC IE ha inoltre sottolineato la sua opinione secondo la quale si è verificata una violazione dell'articolo 33, paragrafo 1, RGPD e non ha proposto di considerare le violazioni di altre disposizioni del RGPD come un'alternativa all'articolo 33, paragrafo 1 ([71]), sottolineando che l'estensione della gamma delle violazioni ad altri obblighi del RGPD su richiesta delle autorità interessate «*metterebbe a repentaglio l'intera procedura d'indagine a norma dell'articolo 60 esponendola al rischio di rivendicazioni di iniquità procedurale*» ([72]). L'AC IE ha inoltre sottolineato che sta esaminando il rispetto da parte di TIC degli obblighi più ampi previsti dal RGPD nel contesto di un'altra indagine in corso ([73]).

([68]) Progetto di decisione, paragrafo 7.129, punto vi).
([69]) Memorandum composito, paragrafo 5.45.
([70]) Memorandum composito, paragrafo 5.45.
([71]) Memorandum composito, paragrafo 5.47.
([72]) Memorandum composito, paragrafo 5.44, lettera c).
([73]) Memorandum composito, paragrafo 5.44, lettera d).

65. Per quanto riguarda l'obiezione sollevata dall'AC DE, con specifico riferimento alla determinazione del momento della presa di coscienza della violazione, l'AC IE ha sostenuto che, anche se esistesse un rapporto di titolarità congiunta del trattamento (un'opinione che, come indicato precedentemente alla sezione 4.3, l'AC IE non condivide), ciò non significherebbe necessariamente che la presa di coscienza della violazione possa essere attribuita in egual misura a entrambi i contitolari del trattamento ([74]).

5.1.4 Analisi dell'EDPB

5.1.4.1 Valutazione della pertinenza e della motivazione delle obiezioni

66. Come ricordato in precedenza (cfr. sezione 4.4.1), è necessario valutare se le obiezioni sollevate dalle autorità interessate soddisfino la soglia fissata dall'articolo 4, paragrafo 24, RGPD.

67. Sebbene l'obiezione dell'**AC FR** sia pertinente, in quanto delinea un disaccordo sul fatto che nel caso specifico si sia verificata una particolare violazione del RGPD e comprende argomentazioni giuridiche a sostegno dell'obiezione, essa non soddisfa la norma dell'articolo 4, paragrafo 24, RGPD, in quanto non include giustificazioni relative alle conseguenze dell'adozione di una decisione senza le modifiche proposte nell'obiezione e al modo in cui tali conseguenze comporterebbero rischi significativi per i diritti e le libertà degli interessati ([75]). Pertanto, non si può affermare che l'obiezione «dimostri chiaramente» l'importanza dei rischi posti dall'adozione del progetto di decisione (se dovesse essere adottato in via definitiva), in quanto non fornisce argomenti sufficienti per spiegare perché tali diritti e libertà degli interessati, con specifico riferimento all'accertamento di una violazione dell'articolo 33, paragrafo 1 (anziché degli articoli 32/28), RGPD, siano sostanziali e plausibili ([76]). Pertanto, l'EDPB conclude che l'obiezione dell'**AC FR** non è pertinente e motivata a causa della mancanza di una chiara dimostrazione dei rischi, come specificamente richiesto dall'articolo 4, paragrafo 24, RGPD.

68. Inoltre, per quanto riguarda l'obiezione dell'**AC DE**, in particolare in relazione alla determinazione del *dies a quo* per la violazione dell'articolo 33, paragrafo 1, RGPD, in quanto dipende dalla qualifica delle parti, l'EDPB desidera ricordare l'analisi effettuata nella sezione 4.4 precedente e ritiene che l'obiezione non dimostri le implicazioni che il progetto di decisione con il suo contenuto attuale (in particolare per quanto riguarda il ragionamento alla base dell'accertamento di una violazione dell'articolo 33, paragrafo 1, RGPD) avrebbe per i valori tutelati ([77]) (diritti e libertà degli interessati o, ove applicabile, libera circolazione dei dati personali).

5.1.4.2 Conclusione

69. L'EDPB ritiene che le obiezioni summenzionate soddisfino la condizione di far riferimento alternativamente all'esistenza di una violazione del presente regolamento o alla conformità al regolamento stesso delle azioni previste nei confronti del titolare del trattamento o del responsabile del trattamento, ma che non dimostrino chiaramente l'importanza dei rischi posti dal progetto di decisione per quanto riguarda i diritti e le libertà fondamentali degli interessati e, ove applicabile, la libera circolazione dei dati personali all'interno dell'Unione europea.

([74]) Memorandum composito, paragrafo 5.34 (che si riferisce anche alla sentenza della CGUE nella causa *Wirtschaftsakademie*, C-210/16, punto 43).
([75]) Linee guida relative alla RRO, paragrafo 19.
([76]) Linee guida relative alla RRO, paragrafo 37.
([77]) Linee guida relative alla RRO, paragrafo 37.

70. Pertanto, le obiezioni delle AC FR e DE non soddisfano i requisiti di cui all'articolo 4, paragrafo 24, RGPD ([78]).

5.2 Sull'accertamento di una violazione dell'articolo 33, paragrafo 5, RGPD

5.2.1 Analisi dell'autorità capofila nel progetto di decisione

71. Nel progetto di decisione, l'AC IE ha ritenuto che TIC non abbia rispettato i suoi obblighi ai sensi dell'articolo 33, paragrafo 5, RGPD, di documentare la violazione, poiché si è ritenuto che la documentazione fornita da TIC nel corso dell'indagine non contenesse informazioni sufficienti e non contenesse un registro o un documento relativo, nello specifico, a una «violazione di dati personali», in quanto si trattava di «documentazione di natura più generale» ([79]).

72. D'altro canto, l'AC IE ha riconosciuto che TIC ha cooperato pienamente durante l'indagine (sebbene ciò non sia stato considerato un fattore attenuante) ([80]).

5.2.2 Sintesi delle obiezioni sollevate dalle autorità interessate

73. L'EDPB coglie l'occasione per sottolineare, a fini di chiarezza, che nessuna delle obiezioni sollevate ha contestato la conclusione secondo cui TIC ha violato l'articolo 33, paragrafo 5, RGPD.

74. Tuttavia, l'**AC IT** ha sollevato un'obiezione sostenendo che la conclusione relativa alla violazione dell'articolo 33, paragrafo 5, RGPD non sembra coerente con il ragionamento e le elaborazioni avanzate dall'autorità capofila, in quanto l'inadeguatezza della documentazione prodotta nel corso di un'indagine così approfondita, basata su molteplici interazioni fra l'autorità capofila e il titolare del trattamento, indicherebbe la scarsa collaborazione di quest'ultimo con l'autorità per la protezione dei dati. Secondo l'AC IT, la constatazione contenuta nel progetto di decisione secondo cui TIC ha fornito piena collaborazione durante la fase d'indagine dovrebbe essere riesaminata, in quanto tale piena collaborazione può essere considerata esistente solo se il titolare del trattamento mette a disposizione una documentazione adeguata ed esaustiva in modo inequivocabile.

5.2.3 Posizione dell'autorità capofila in merito alle obiezioni

75. L'AC IE ritiene che l'obbligo di cui all'articolo 33, paragrafo 5, RGPD si applichi indipendentemente dall'obbligo di cui all'articolo 31 del RGPD di cooperare con l'autorità di controllo e dal modo in cui TIC si è comportata e ha interagito con l'autorità capofila nel momento in cui quest'ultima ha avviato le attività di regolamentazione relative alla violazione da parte di TIC ([81]). L'AC IE ha sostenuto che le carenze nel modo in cui TIC ha documentato la violazione non sono necessariamente correlate a una mancanza di cooperazione da parte sua ([82]). Inoltre, l'AC IE ha sottolineato che TIC ha collaborato con essa durante l'indagine rispondendo a tutte le richieste di informazioni e fornendo tutti i documenti richiesti, senza cercare di disturbare o ostacolare in alcun modo l'indagine ([83]). In ogni caso, l'AC IE non

([78]) Di conseguenza, l'EDPB non prende posizione sul merito di eventuali questioni sostanziali sollevate da tali obiezioni. L'EDPB ribadisce che la sua attuale decisione non pregiudica le valutazioni che il comitato può essere chiamato a effettuare in altri casi, anche con le stesse parti, tenendo conto del contenuto del progetto di decisione pertinente e delle obiezioni sollevate dalle autorità interessate.
([79]) Progetto di decisione, paragrafo 10.46.
([80]) Progetto di decisione, paragrafo 14.50.
([81]) Memorandum composito, paragrafo 5.87.
([82]) Memorandum composito, paragrafo 5.87.
([83]) Memorandum composito, paragrafo 5.87.

ha considerato la cooperazione di TIC come un'attenuante ([84]). Per le ragioni sopra esposte, l'AC IE ha ritenuto «discutibile» definire che l'obiezione sollevata dall'AC IT sia pertinente e motivata, in quanto, pur riguardando una violazione del RGPD, non dimostra come la posizione dell'AC IE sul grado di cooperazione di TIC si traduca in rischi posti dal progetto di decisione in materia di diritti e libertà fondamentali degli interessati ([85]). L'AC IE ha concluso che non avrebbe dato seguito a tale obiezione ([86]).

5.2.4 Analisi dell'EDPB

5.2.4.1 Valutazione della pertinenza e della motivazione delle obiezioni

76. L'AC IT nella sua obiezione non contesta che si sia verificata una violazione dell'articolo 33, paragrafo 5, RGPD. Un'obiezione pertinente e motivata può mettere in discussione il ragionamento alla base delle conclusioni raggiunte dall'autorità capofila nel progetto di decisione solo se tale ragionamento ha un legame con tali conclusioni, in tal caso l'obiezione è adeguatamente motivata. In questo caso, l'obiezione non argomenta chiaramente in che modo, se le venisse dato seguito, ciò potrebbe comportare una modifica del progetto di decisione. Inoltre, l'obiezione non soddisfa i criteri di cui all'articolo 4, paragrafo 24, RGPD perché non dimostra chiaramente l'importanza dei rischi posti dal progetto di decisione, in quanto non mostra le implicazioni che il presunto errore nel progetto di decisione avrebbe per i valori tutelati.

5.2.4.2 Conclusione

77. Poiché l'obiezione dell'AC IT non soddisfa i requisiti dell'articolo 4, paragrafo 24, RGPD, il comitato non prende posizione sul merito delle questioni sostanziali sollevate da tale obiezione. L'EDPB ribadisce che la sua attuale decisione non pregiudica le valutazioni che il comitato può essere chiamato a effettuare in altri casi, anche con le stesse parti, tenendo conto del contenuto del progetto di decisione pertinente e delle obiezioni sollevate dalle autorità interessate.

6 IN MERITO A POTENZIALI VIOLAZIONI ULTERIORI (O ALTERNATIVE) DEL RGPD INDIVIDUATE DALLE AUTORITÀ INTERESSATE

6.1 Analisi dell'autorità capofila nel progetto di decisione

78. Sulla base delle informazioni fornite da TIC al momento della notifica della violazione all'AC IE, quest'ultima ha osservato che dal modulo di notifica della violazione risultava trascorso un periodo di oltre 72 ore dal momento in cui TIC (in qualità di titolare del trattamento) è venuto a conoscenza della violazione ([87]). Per questo motivo, l'AC IE ha deciso di avviare, d'ufficio, un'indagine per esaminare se TIC avesse rispettato i suoi obblighi ai sensi dell'articolo 33, paragrafi 1 e 5, RGPD ([88]).

79. Al fine di determinare se TIC rispetta gli obblighi di cui all'articolo 33, paragrafo 1, RGPD, l'AC IE li ha considerati nel contesto degli obblighi più ampi di un titolare del trattamento, compresi quelli di responsabilizzazione (articolo 5, paragrafo 2, RGPD), ricorso a un responsabile del trattamento

([84]) Memorandum composito, paragrafo 5.87.
([85]) Memorandum composito, paragrafo 5.88.
([86]) Memorandum composito, paragrafo 5.88.
([87]) Progetto di decisione, paragrafo 2.11.
([88]) Progetto di decisione, paragrafo 2.11.

(articolo 28 del RGPD) e in relazione alla sicurezza del trattamento dei dati personali (articolo 32 del RGPD) ([89]). Tuttavia, se da una parte l'AC IE ha preso in considerazione i fattori e le questioni di fatto che hanno portato al ritardo di TIC nell'essere messa a conoscenza della violazione da parte del responsabile del trattamento e, in ultima analisi, nel notificare la violazione, dall'altra l'AC IE non ha considerato se TIC si sia conformata o meno a uno o a ciascuno di questi obblighi se non al fine di valutare l'adempimento di TIC ai suoi obblighi ai sensi dell'articolo 33, paragrafi 1 e 5, RGPD ([90]).

6.2 Sintesi delle obiezioni sollevate dalle autorità interessate

80. Le AC DE, FR, HU e IT hanno sollevato obiezioni sul fatto che TIC ha violato altre disposizioni del RGPD in aggiunta o in sostituzione dell'articolo 33, paragrafi 1 e 5, RGPD.

6.2.1 violazione dell'articolo 5, paragrafo 1, lettera f), RGPD sul principio di integrità e riservatezza

81. L'**AC DE** ha sollevato un'obiezione affermando che il «bug sottostante» nell'applicazione di TIC che ha portato alla violazione notificata all'AC IE avrebbe dovuto essere considerato dall'AC IE nel suo progetto di decisione, in modo tale da determinare se tale bug costituisse effettivamente una violazione significativa della riservatezza dei dati personali, violando in ultima analisi l'articolo 5, paragrafo 1, lettera f), RGPD, oltre all'articolo 33, paragrafi 1 e 5, RGPD.

82. L'**AC HU** ha sollevato un'obiezione affermando che, dato il «bug» nell'applicazione di TIC nel corso degli anni e la sua grave natura in materia di sicurezza dei dati, l'AC IE dovrebbe indagare se TIC abbia anche violato l'articolo 5, paragrafo 1, lettera f), RGPD sul principio di integrità e riservatezza.

6.2.2 violazione dell'articolo 5, paragrafo 2, RGPD sul principio di responsabilizzazione

83. L'**AC IT** ha sollevato un'obiezione affermando che la violazione dell'articolo 33, paragrafo 1, RGPD evidenzia una violazione molto più grave del principio di responsabilizzazione (ai sensi dell'articolo 5, paragrafo 2, RGPD), poiché la mancanza di politiche aziendali per gestire gli incidenti di sicurezza o il mancato rispetto di tali politiche dimostra che le misure attuate dal titolare del trattamento sono inadeguate a garantire la conformità e a documentarla. L'AC IT ha sostenuto che tali carenze procedurali sono evidenziate dal progetto di decisione, ma che quest'ultimo non le sottopone a un'analisi specifica. Poiché ciò può influire anche sul trattamento di future violazioni dei dati, secondo l'AC IT anche i risultati relativi alla conformità di TIC all'articolo 5, paragrafo 2, RGPD dovrebbero far parte della decisione finale dell'AC IE. L'AC IT ha inoltre ritenuto che la violazione dell'articolo 5, paragrafo 2, RGPD sia confermata dall'incapacità del titolare del trattamento di indicare il numero esatto e la natura dei dati personali interessati o il numero totale degli interessati.

6.2.3 violazione dell'articolo 24 del RGPD sulla responsabilità del titolare del trattamento

84. L'**AC DE** ha sollevato un'obiezione affermando che il progetto di decisione non è chiaro circa il motivo per cui l'AC IE non ha valutato se la violazione significativa della riservatezza dei dati personali causata da un «bug sottostante» sia dovuta a una violazione dei requisiti di cui all'articolo 24 RGPD.

([89]) Progetto di decisione, paragrafi 6.13-6.20, 7.111-7.112, 7.122-7.124.
([90]) Progetto di decisione, paragrafi 6.13, 7.111, 7.122-7.124.

6.2.4 violazione dell'articolo 28 del RGPD sul rapporto con i responsabili del trattamento

85. L'**AC FR** ha espresso un'obiezione affermando che TIC non ha rispettato l'obbligo del titolare del trattamento di verificare la validità delle procedure istituite dal responsabile del trattamento. Pertanto, l'AC FR ritiene che non vi sia violazione dell'articolo 33, paragrafo 1, RGPD, ma dell'articolo 28 del RGPD (o dell'articolo 32 del RGPD; cfr. sezione 6.2.5 di seguito). L'AC FR ha sostenuto che, se il responsabile del trattamento di TIC è la sua società madre, «*era tanto più facile per TIC verificare la validità delle procedure stabilite dalla società madre e chiedere una correzione, se necessario*».

86. L'**AC IT** ha espresso un'obiezione affermando che il mancato coinvolgimento da parte di TIC del responsabile globale della protezione dei dati nel team di rilevamento e risposta del responsabile del trattamento (Twitter, Inc.), nonostante tale pratica fosse prevista nelle politiche interne di TIC, dimostra che le garanzie fornite dal responsabile del trattamento in termini di attuazione delle misure organizzative appropriate ai sensi dell'articolo 28, paragrafo 1, RGPD non sono sufficientemente ampie. Inoltre, l'AC IT ha sostenuto nelle sue obiezioni che il responsabile del trattamento ha violato l'obbligo di assistere il titolare del trattamento, ai sensi dell'articolo 28, paragrafo 3, lettera f), RGPD.

6.2.5 violazione dell'articolo 32 del RGPD sulla sicurezza del trattamento

87. L'**AC DE** ha sollevato obiezioni affermando che l'AC IE avrebbe dovuto esaminare se tutte le misure tecniche e organizzative adeguate (ai sensi dell'articolo 32 del RGPD) fossero state rispettate in questo caso e se le violazioni in questo ambito avrebbero dovuto essere oggetto dei procedimenti in questione. L'AC DE sostiene inoltre che nel progetto di decisione non è chiaro il motivo per cui l'AC IE non ha valutato se la violazione significativa della riservatezza dei dati personali provocata da un «bug sottostante» sia dovuta a una violazione dei requisiti dell'articolo 32 del RGPD.

88. L'**AC FR** ha espresso un'obiezione riguardo alla caratterizzazione giuridica dei fatti effettuata dall'AC IE e ha dichiarato che il mancato rispetto da parte di TIC dell'obbligo del titolare del trattamento di verificare la validità delle procedure istituite dal responsabile del trattamento corrisponde a una violazione dell'articolo 32 del RGPD (o dell'articolo 28 RGPD; cfr. sezione 6.2.4 sopra), piuttosto che dell'articolo 33, paragrafo 1, RGPD. L'AC FR ha sostenuto che, se il responsabile del trattamento di TIC è la sua società madre, «*era tanto più facile per TIC verificare la validità delle procedure stabilite dalla sua società madre e chiedere una correzione, se necessario*».

89. L'**AC HU** ha sollevato obiezioni affermando che, dato il «bug» nell'applicazione di TIC nel corso degli anni e la sua grave natura in materia di sicurezza dei dati, l'AC IE dovrebbe indagare se TIC abbia violato anche l'articolo 32 RGPD circa gli obblighi di sicurezza del trattamento.

6.2.6 violazione dell'articolo 33, paragrafo 3, RGPD sul contenuto della notifica di una violazione dei dati personali in materia di sicurezza del trattamento

90. L'**AC DE** ha espresso obiezioni, affermando che l'esame dell'AC IE è carente per quanto riguarda la portata delle informazioni da fornire in caso di notifica, che è prevista come vincolante dall'articolo 33, paragrafo 3, RGPD. Sulla base delle osservazioni di TIC sulla violazione da essa fornita ai sensi dell'articolo 33, paragrafo 5, RGPD e della descrizione dell'indagine sui fatti del caso, è ovvio che TIC non ha rispettato pienamente l'obbligo di documentazione quando ha segnalato la violazione per la prima volta l'8 gennaio 2019. L'AC DE ha ritenuto che vi siano quindi numerose indicazioni secondo le quali il risultato potrebbe consistere anche in una violazione dell'articolo 33, paragrafo 3, RGPD.

6.2.7 *violazione dell'articolo 34 del RGPD sulla comunicazione all'interessato di una violazione dei dati personali*

91. L'**AC HU** ha sollevato obiezioni affermando che, dato il «bug» nell'applicazione di TIC nel corso degli anni e la sua grave natura in materia di sicurezza dei dati, l'AC IE doveva indagare se TIC avesse violato anche l'articolo 34 del RGPD sull'obbligo di informare gli interessati in merito alla violazione.

6.3 Posizione dell'autorità capofila in merito alle obiezioni

92. L'autorità capofila ha fornito una risposta in merito alle obiezioni relative a potenziali violazioni ulteriori (o alternative) del RGPD collettivamente nel suo memorandum composito condiviso con le autorità interessate. L'autorità capofila ha spiegato di «*aver esercitato il suo potere discrezionale [...] di limitare l'ambito dell'indagine alla considerazione di due questioni discrete, ossia se TIC avesse rispettato gli obblighi di titolare del trattamento ai sensi dell'articolo 33, paragrafo 1, in relazione alla notifica della violazione, e se avesse rispettato gli obblighi ai sensi dell'articolo 33, paragrafo 5, di documentare la violazione*» ([91]). L'autorità capofila si è basata sull'articolo 110, paragrafo 1, dell'Irish Data Protection Act 2018, che prevede che l'AC IE possa «*far sì che l'indagine venga condotta nel modo che ritiene opportuno*» ([92]). Lo scopo dell'indagine descritta dall'AC IE era quindi «*unicamente quello di esaminare le circostanze relative all'apparente ritardo della notifica della violazione da parte di TIC [...] e alla documentazione della violazione*», una questione considerata dall'AC IE «*di notevole importanza dato che, considerando le quasi 200 000 violazioni notificate in due anni in tutta l'UE, è necessario fare chiarezza su ciò che è richiesto in base ai requisiti del RGPD di notifica e di documentazione della violazione* » ([93]).

93. Nell'ambito del memorandum composito ([94]), l'AC IE sostiene che le obiezioni sollevate nel contesto dell'articolo 60, paragrafo 4, RGPD non possono avere l'effetto di contestare la portata di un'indagine. Nel caso in esame, l'autorità capofila ricorda di aver informato TIC all'inizio dell'indagine del fatto che il suo scopo era di verificare la conformità di TIC all'articolo 33, paragrafi 1 e 5, RGPD, in relazione alla notifica da parte sua di una violazione all'autorità stessa in data 8 gennaio 2019. L'intero processo di indagine è stato pertanto condotto in tale ambito, così come la stesura del progetto di decisione, e a TIC è stato riconosciuto il diritto di essere ascoltata a tale riguardo in ogni fase della procedura. Pertanto, l'autorità capofila sostiene che, se dovesse dare seguito alle obiezioni delle autorità interessate e includere altre violazioni nella sua decisione finale «*sulla base del solo materiale contenuto nel progetto di decisione*», ciò metterebbe a repentaglio «*l'intero processo di indagine a norma dell'articolo 60, esponendolo al rischio di rivendicazioni di iniquità procedurale*» ([95]).

94. Inoltre, l'autorità capofila spiega di avere un'altra indagine in corso in relazione ad altre violazioni di dati comunicatele da TIC prima della notifica che riguarda il caso in questione. In quest'altra indagine, avviata prima di quella in questione, l'autorità capofila sottolinea che l'ambito di applicazione dell'indagine riguarda la possibile non conformità con «*tra gli altri, gli articoli 5, 24, 25, 28, 29 e 32*» del RGPD ([96]). L'autorità capofila ritiene che tale indagine parallela stia effettivamente valutando il rispetto da parte di TIC dei suoi obblighi più ampi nell'ambito del RGPD per determinare se siano state

([91]) Memorandum composito, paragrafo 1.7.
([92]) Memorandum composito, paragrafo 1.5.
([93]) Memorandum composito, paragrafo 1.9.
([94]) Memorandum composito, paragrafo 5.44.
([95]) Memorandum composito, paragrafo 5.44, lettera c).
([96]) Memorandum composito, paragrafo 1.10.

le lacune di conformità a provocare le violazioni dei dati. Di conseguenza, l'autorità capofila è del parere che le autorità interessate avranno la possibilità di considerare tali possibili violazioni nel contesto di quest'altra indagine, in quanto saranno consultate in merito al relativo progetto di decisione, conformemente all'articolo 60, paragrafo 4, RGPD ([97]).

95. TIC ha sostenuto che, poiché il progetto di decisione afferma che «*un esame dettagliato delle misure tecniche e organizzative va oltre l'ambito dell'indagine* ([98]), *non sarebbe ragionevole o adeguato, e offenderebbe principi consolidati di "giustizia naturale", se la decisione dovesse produrre risultati o imporre sanzioni a TIC in relazione a obblighi e principi che non fanno parte dell'indagine del DPC, dal momento che TIC non ha avuto l'opportunità di rispondere a eventuali dubbi che il DPC o le autorità interessate potrebbero avere riguardo ai processi di TIC in questi ambiti*» ([99]).

6.4 Analisi dell'EDPB

6.4.1 Valutazione della pertinenza e della motivazione delle obiezioni

6.4.1.1 violazione dell'articolo 5, paragrafo 1, lettera f), RGPD sul principio di integrità e riservatezza

96. L'EDPB osserva che l'obiezione dell'**AC DE** all'articolo 5, paragrafo 1, lettera f), RGPD si riferisce all'esistenza o meno di una violazione del RGPD ed esprime disaccordo rispetto alle conclusioni da trarre dai risultati dell'indagine. L'obiezione avanzava inoltre argomenti a sostegno della conclusione secondo cui occorre valutare la conformità all'articolo 5, paragrafo 1, lettera f), RGPD. L'obiezione dell'AC DE dimostra chiaramente l'importanza dei rischi posti dal progetto di decisione per i diritti e le libertà degli interessati, in particolare sottolineando che i fatti costituiscono una violazione «significativa» e «sostanziale» della riservatezza dei dati personali e che un gran numero di persone è stato interessato per un periodo di tempo considerevole. Inoltre, l'AC DE ha sostenuto che vi erano indicazioni per considerare l'esistenza di un «errore sistemico», che avrebbe richiesto un esame più approfondito al di là del singolo bug specifico in questione.

97. Anche l'obiezione dell'**AC HU** può essere considerata rilevante in quanto riguarda l'esistenza di una violazione del RGPD. Inoltre, fa (solo) brevemente riferimento ad argomentazioni fattuali a sostegno della necessità di valutare tale disposizione aggiuntiva (la durata del bug e la sua grave natura che incide sulla sicurezza dei dati), ma non «dimostra chiaramente» l'importanza dei rischi posti dal progetto di decisione per i diritti e le libertà delle persone in quanto non avanza argomenti o giustificazioni riguardanti le conseguenze dell'adozione di una decisione senza le modifiche proposte nell'obiezione ([100]).

98. Di conseguenza, l'EDPB ritiene che l'obiezione sollevata dall'AC DE in relazione alla potenziale violazione ulteriore dell'articolo 5, paragrafo 1, lettera f), RGPD sia pertinente e motivata ai fini

([97]) Memorandum composito, paragrafo 5.44, lettera d).
([98]) Progetto di decisione, paragrafo 7.19.
([99]) «Dichiarazioni in risposta alle obiezioni e ai commenti delle autorità interessate» presentate da TIC (14 agosto 2020), paragrafo 4.1. L'EDPB desidera sottolineare che le obiezioni sollevate dalle autorità interessate sono state portate all'attenzione di TIC dall'AC IE e che TIC ha presentato le suddette dichiarazioni in merito alle obiezioni, che sono state prese in considerazione dall'AC IE prima dell'avvio del procedimento ai sensi dell'articolo 65 e fanno parte del fascicolo all'esame del comitato nell'ambito del presente procedimento. Cfr. anche nota a piè di pagina 19.
([100]) Linee guida relative alla RRO, paragrafo 19.

dell'articolo 4, paragrafo 24, RGPD, ma ritiene che l'obiezione dell'AC HU in relazione allo stesso argomento non soddisfi i requisiti dell'articolo 4, paragrafo 24 ([101]).

99. L'EDPB valuterà la fondatezza delle questioni sostanziali sollevate dall'obiezione dell'AC DE in relazione alla potenziale violazione ulteriore dell'articolo 5, paragrafo 1, lettera f), RGPD (cfr. sezione 6.4.2 sotto).

6.4.1.2 violazione dell'articolo 5, paragrafo 2, RGPD sul principio di responsabilizzazione

100. L'obiezione sollevata dall'**AC IT** è da considerarsi «pertinente» in quanto, se seguita, porterebbe a una diversa conclusione circa l'esistenza di una violazione del RGPD ([102]). Più nello specifico, essa comprende un «disaccordo circa le conclusioni da trarre dai risultati dell'indagine», poiché afferma che «*tali risultati rimandano alla violazione di una disposizione del RGPD [...] oltre a [...] quelle già analizzate dal progetto di decisione*» ([103]).

101. Inoltre, l'obiezione è «motivata» in quanto include chiarimenti sul motivo per cui viene proposta la modifica della decisione ([104]): la modifica proposta si basa sulla «*mancanza di politiche aziendali formalizzate per la gestione degli incidenti di sicurezza [...] o il mancato rispetto di tali politiche*», sul fatto che tali «*carenze procedurali sono ripetutamente evidenziate dall'[AC IE]*» nel progetto di decisione, e sull'incapacità del titolare del trattamento di indicare il numero esatto e la natura dei dati personali/degli interessati.

102. L'**AC IT** ha chiaramente dimostrato l'importanza dei rischi posti dal progetto di decisione per i diritti e le libertà fondamentali degli interessati, mostrando le «implicazioni che il progetto di decisione avrebbe per i valori tutelati» ([105]) e più nello specifico «l'impatto sui diritti e le libertà degli interessati i cui dati personali potrebbero essere trattati in futuro» ([106]); l'obiezione dimostra ciò sostenendo che gli aspetti menzionati sono «*di natura strutturale per quanto riguarda l'organizzazione del titolare del trattamento» e «destinati a produrre effetti non solo sul caso in questione, ma anche sul trattamento di eventuali violazioni di dati personali che potrebbero verificarsi in futuro*».

103. Di conseguenza, l'obiezione dell'AC IT in merito all'articolo 5, paragrafo 2, RGPD soddisfa i requisiti di cui all'articolo 4, paragrafo 24, RGPD. L'EDPB analizzerà pertanto la fondatezza delle questioni sostanziali sollevate da tale obiezione ([107]).

6.4.1.3 violazione dell'articolo 24 del RGPD sulla responsabilità del titolare del trattamento

104. L'obiezione dell'**AC DE** si riferisce nello specifico al capo 5 «Questioni per la determinazione» del progetto di decisione ([108]) e si oppone a quest'ultimo in merito alla violazione dell'articolo 24 del RGPD

([101]) Di conseguenza, l'EDPB non prende posizione sul merito di eventuali questioni sostanziali sollevate dall'obiezione dell'AC HU. L'EDPB ribadisce che la sua attuale decisione non pregiudica le valutazioni che il comitato può essere chiamato a effettuare in altri casi, anche con le stesse parti, tenendo conto del contenuto del progetto di decisione pertinente e delle obiezioni sollevate dalle autorità interessate.
([102]) Linee guida relative alla RRO, paragrafo 13.
([103]) Linee guida relative alla RRO, paragrafo 27.
([104]) Linee guida relative alla RRO, paragrafo 17.
([105]) Linee guida relative alla RRO, paragrafo 37.
([106]) Linee guida relative alla RRO, paragrafo 43.
([107]) Cfr. sezione 6.4.2 sotto.
([108]) Linee guida relative alla RRO, paragrafo 20.

da parte di TIC ([109]). Essa si basa sui fatti ([110]) esposti nel progetto di decisione secondo cui «*se un utente di Twitter con un account protetto, utilizzando Twitter per Android, cambiasse il suo indirizzo e-mail, il bug comporterebbe la mancata protezione del suo account*» ([111]) e i suoi tweet protetti sarebbero resi disponibili al pubblico tramite il servizio. Più precisamente, l'AC DE si chiede perché l'AC IE non abbia esaminato, nel progetto di decisione, le cause della violazione, in particolare alla luce dell'articolo 24 del RGPD, e perché non abbia spiegato nel progetto di decisione il motivo per cui non ha effettuato tale esame.

105. L'AC DE sostiene che, poiché la notifica di violazione ha rivelato «*carenze nel rispetto del RGPD, ... [una] società che non è in grado, con mezzi e risorse proprie, attraverso ispezioni di squadre di sicurezza interne o esterne, di trovare un bug di tale rilievo e portata dovrebbe essere soggetta a un esame più approfondito delle sue impostazioni di sicurezza e di trattamento dei dati, al di là del singolo bug specifico in questione*».

106. Secondo l'AC DE, un esame più approfondito della configurazione del trattamento dei dati di TIC «*potrebbe comportare, a seconda dei casi, l'ordine al titolare del trattamento di rendere le operazioni di trattamento conformi alle disposizioni del RGPD. Il caso in questione non rispecchia questo compito. Ciò rende ancora più urgente l'esame dei poteri correttivi di cui all'articolo 58, paragrafo 2, RGPD in questo contesto*».

107. Pertanto, l'AC DE ha indicato quella che considerava una mancanza di valutazione, con la conseguenza che le conclusioni tratte dai risultati dell'indagine dell'autorità capofila potrebbero essere diverse ([112]).

108. L'obiezione dell'AC DE afferma che «*[s]econdo l'art. 83, par. 1, RGPD, le sanzioni pecuniarie devono essere "in ogni singolo caso effettive, proporzionate e dissuasive". Una sanzione è effettiva e dissuasiva se, da un lato, è idonea come misura preventiva generale per dissuadere il pubblico dal commettere violazioni e per affermare la fiducia del pubblico nella validità del diritto dell'Unione, ma, dall'altro, è anche idonea come misura preventiva per dissuadere il trasgressore dal commettere ulteriori violazioni*». Di conseguenza, l'AC DE dimostra come non modificare il progetto di decisione per includere una valutazione del rispetto dell'articolo 24 del RGPD comporterebbe rischi significativi per i diritti e le libertà fondamentali degli interessati ([113]).

109. Nelle linee guida relative alla RRO, l'EDPB accetta che un'obiezione possa contestare la conclusione dell'autorità capofila, ritenendo che i risultati di quest'ultima portino effettivamente a concludere che sia stata violata un'altra disposizione del RGPD in aggiunta o in sostituzione della disposizione individuata dall'autorità capofila ([114]). L'EDPB ritiene che questa sia esattamente l'essenza dell'obiezione dell'AC DE, che non le impedisce quindi di essere pertinente e motivata.

110. Inoltre, l'obiezione dell'AC DE dimostra chiaramente l'importanza dei rischi posti dal progetto di decisione per i diritti e le libertà degli interessati, anche evidenziando che un gran numero di persone è stato interessato per un periodo di tempo altrettanto considerevole, il che riflette un errore sistemico che richiede un esame più approfondito, che va al di là del singolo bug specifico in questione. Di conseguenza, l'obiezione dell'AC DE in merito all'articolo 24 del RGPD soddisfa la soglia di cui all'articolo 4, paragrafo 24, RGPD.

([109]) Linee guida relative alla RRO, paragrafo 12.
([110]) Linee guida relative alla RRO, paragrafo 14.
([111]) Progetto di decisione, paragrafo 2.7.
([112]) Linee guida relative alla RRO, paragrafo 29.
([113]) Linee guida relative alla RRO, paragrafo 19.
([114]) Linee guida relative alla RRO, paragrafo 27.

111. Alla luce della valutazione di cui sopra, l'EDPB ritiene che l'obiezione dell'AC DE relativa a una possibile violazione dell'articolo 24 del RGPD sia pertinente e motivata in conformità dell'articolo 4, paragrafo 24, RGPD. Di conseguenza, l'EDPB sta valutando la fondatezza delle questioni sostanziali sollevate da tale obiezione (cfr. sezione 6.4.2 sotto).

6.4.1.4 violazione dell'articolo 28 del RGPD sul rapporto con i responsabili del trattamento

112. L'obiezione dell'**AC FR** si riferisce nello specifico al paragrafo 7.129, punti iii), iv) e v), del progetto di decisione ([115]) e si oppone a quest'ultimo in merito alla violazione dell'articolo 28 del RGPD da parte di TIC invece che dell'articolo 33, paragrafo 1, RGPD ([116]). Essa si basa sui fatti ([117]) esposti nel progetto di decisione e sui risultati dell'autorità capofila secondo cui «TIC non ha rispettato l'obbligo del titolare del trattamento di verificare la validità delle procedure stabilite dal responsabile del trattamento».

113. Secondo l'AC FR, poiché l'articolo 28, paragrafo 3, lettera h), RGPD stabilisce gli obblighi del titolare del trattamento quando si avvale di un responsabile del trattamento, i risultati avrebbero dovuto portare l'autorità capofila a concludere che è stato violato l'articolo 28, paragrafo 3, lettera h), RGPD anziché l'articolo 33, paragrafo 1, RGPD. In definitiva, per l'AC FR ciò significa che la sanzione emessa sotto forma di sanzione pecuniaria dovrebbe riguardare diverse violazioni.

114. Nelle linee guida relative alla RRO, l'EDPB accetta che un'obiezione possa contestare la conclusione dell'autorità capofila, ritenendo che i risultati di quest'ultima portino effettivamente a concludere che sia stata violata un'altra disposizione del RGPD in aggiunta o in sostituzione della disposizione individuata dall'autorità capofila ([118]). L'EDPB ritiene che questa sia esattamente l'essenza dell'obiezione dell'AC FR, che non le impedisce quindi di essere pertinente. L'obiezione presenta inoltre argomentazioni adeguate a sostegno della conclusione proposta. Al tempo stesso, l'EDPB osserva che l'obiezione dell'AC FR non dimostra chiaramente i rischi significativi posti dal progetto di decisione per i diritti e le libertà fondamentali degli interessati, in particolare per quanto riguarda la mancata conclusione sulla violazione di questa specifica disposizione ([119]). Alla luce di tale valutazione, l'EDPB ritiene che l'obiezione dell'AC FR relativa a una possibile violazione dell'articolo 28 del RGPD invece che dell'articolo 33, paragrafo 1, RGPD non sia pertinente e motivata ai sensi dell'articolo 4, paragrafo 24, RGPD ([120]).

115. L'AC IT si oppone al progetto di decisione in merito alla violazione da parte di TIC dell'articolo 28 del RGPD, tra gli altri, in aggiunta all'articolo 33, paragrafo 1, RGPD ([121]).

116. L'AC IT si basa sui fatti esposti nel progetto di decisione e sui risultati dell'autorità capofila secondo cui il responsabile globale della protezione dei dati in pratica non è stato coinvolto, nonostante il suo coinvolgimento nel team di rilevamento e risposta del responsabile del trattamento, Twitter, Inc., sia previsto nelle politiche interne di TIC. L'AC IT osserva inoltre che Twitter, Inc., in qualità di responsabile del trattamento, non ha fornito assistenza a TIC.

([115]) Linee guida relative alla RRO, paragrafo 20.
([116]) Linee guida relative alla RRO, paragrafo 12.
([117]) Linee guida relative alla RRO, paragrafo 14.
([118]) Linee guida relative alla RRO, paragrafo 27.
([119]) Linee guida relative alla RRO, paragrafo 29.
([120]) Di conseguenza, l'EDPB non prende posizione sul merito di eventuali questioni sostanziali sollevate da tali obiezioni. L'EDPB ribadisce che la sua attuale decisione non pregiudica le valutazioni che il comitato può essere chiamato a effettuare in altri casi, anche con le stesse parti, tenendo conto del contenuto del progetto di decisione pertinente e delle obiezioni sollevate dalle autorità interessate.
([121]) Linee guida relative alla RRO, paragrafo 12.

117. Secondo l'AC IT, considerando che l'articolo 28, paragrafo 1, RGPD, impone ai titolari del trattamento di utilizzare solo responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate e l'articolo 28, paragrafo 3, lettera f), RGPD, impone che il contratto tra il titolare del trattamento e il responsabile del trattamento preveda che quest'ultimo assista «il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento», i risultati avrebbero dovuto portare l'autorità capofila a concludere che anche l'articolo 28, paragrafo 1 e paragrafo 3, lettera f), RGPD è stato violato.

118. L'EDPB ritiene che l'obiezione dell'AC IT in relazione all'articolo 28, paragrafo 1 e paragrafo 3, lettera f), RGPD debba essere considerata «pertinente» poiché, se seguita, porterebbe a una diversa conclusione in merito all'esistenza di una violazione del RGPD ([122]). Più nello specifico, essa comprende un «disaccordo sulle conclusioni da trarre dai risultati dell'indagine», poiché afferma che «tali risultati equivalgono alla violazione di una disposizione del RGPD [...] oltre a [...] quelle già analizzate dal progetto di decisione» ([123]).

119. Inoltre, secondo l'EDPB, l'obiezione è «motivata» in quanto contiene chiarimenti sul motivo per cui si propone di modificare la decisione ([124]): la modifica proposta si basa sul fatto che il titolare del trattamento non si è conformato alle sue politiche interne secondo le quali il responsabile della protezione dei dati di TIC dovrebbe essere coinvolto. Oltretutto, l'obiezione solleva il punto secondo il quale il responsabile del trattamento non ha rispettato l'obbligo contrattuale di assistere il titolare del trattamento, conformemente all'articolo 28, paragrafo 3, lettera f), RGPD.

120. Tuttavia, l'EDPB osserva che l'obiezione dell'AC IT relativa all'articolo 28, paragrafo 1 e paragrafo 3, lettera f), RGPD non dimostra chiaramente i rischi significativi posti dal progetto di decisione per i diritti e le libertà fondamentali degli interessati ([125]). Di conseguenza, l'obiezione sollevata dall'AC IT non soddisfa i requisiti di cui all'articolo 4, paragrafo 24, RGPD ([126]).

6.4.1.5 violazione dell'articolo 32 del RGPD sulla sicurezza del trattamento

121. L'obiezione dell'**AC DE**, se seguita, comporterebbe un cambiamento che porterebbe a una conclusione diversa in merito all'esistenza di una violazione del RGPD, poiché individua un «*disaccordo circa le conclusioni da trarre dai risultati dell'indagine*» ([127]), sottolineando che tali risultati possono indicare una violazione anche dell'articolo 32 del RGPD. L'EDPB ritiene pertanto che vi sia un nesso tra il contenuto dell'obiezione e la potenziale conclusione diversa ([128]). Inoltre, tale obiezione è legata a specifici elementi di fatto e di diritto del progetto di decisione ([129]).

122. Inoltre, l'obiezione dell'AC DE dimostra chiaramente l'importanza dei rischi posti dal progetto di decisione per i diritti e le libertà degli interessati, in particolare sottolineando che i fatti costituiscono una violazione «significativa» e «sostanziale» della riservatezza dei dati personali e che un gran numero

([122]) Linee guida relative alla RRO, paragrafo 13.
([123]) Linee guida relative alla RRO, paragrafo 27.
([124]) Linee guida relative alla RRO, paragrafo 17.
([125]) Linee guida relative alla RRO, paragrafo 29.
([126]) Di conseguenza, l'EDPB non prende posizione sul merito di eventuali questioni sostanziali sollevate da tali obiezioni. L'EDPB ribadisce che la sua attuale decisione non pregiudica le valutazioni che il comitato può essere chiamato a effettuare in altri casi, anche con le stesse parti, tenendo conto del contenuto del progetto di decisione pertinente e delle obiezioni sollevate dalle autorità interessate.
([127]) Linee guida relative alla RRO, paragrafo 28.
([128]) Linee guida relative alla RRO, paragrafo 13.
([129]) Linee guida relative alla RRO, paragrafo 14.

di persone sono state interessate per un periodo di tempo considerevole. Inoltre, l'AC DE ha anche sostenuto che vi erano indicazioni per considerare l'esistenza di un «errore sistemico», che avrebbe richiesto un esame più approfondito al di là del singolo bug specifico in questione.

123. Alla luce della valutazione di cui sopra, l'EDPB ritiene che l'obiezione dell'AC DE relativa a una possibile violazione dell'articolo 32 del RGPD sia pertinente e motivata conformemente all'articolo 4, paragrafo 24, RGPD. Di conseguenza, l'EDPB sta valutando la fondatezza delle questioni sostanziali sollevate da tale obiezione (cfr. punto 6.4.2 sotto).

124. Per quanto riguarda l'obiezione dell'**AC FR**, l'EDPB la ritiene conforme al criterio della «pertinenza» perché, se l'autorità capofila l'avesse seguita, si sarebbe giunti a una conclusione diversa in merito all'esistenza di una violazione del RGPD ([130]). L'obiezione dell'AC FR si basa sul ragionamento fornito dall'AC IE nel suo progetto di decisione e tale ragionamento è legato alla conclusione secondo cui una violazione del RGPD è stata correttamente individuata ([131]). L'EDPB ricorda che l'autorità interessata deve presentare i fatti che porterebbero a una conclusione diversa ([132]) e osserva che nel caso in questione l'obiezione analizza i fatti che porterebbero alla violazione dell'articolo 32, paragrafo 1, lettera d), RGPD, anziché alla violazione dell'articolo 33, paragrafo 1, RGPD, e lo fa in modo coerente, chiaro e preciso, indicando chiaramente con quali parti della decisione dell'AC IE non è d'accordo. L'obiezione dell'AC FR è chiaramente pertinente, in quanto evidenzia un disaccordo sull'esistenza o meno di una violazione del RGPD. Tuttavia, tale obiezione spiega solo succintamente le ragioni della sua proposta di modifica e non dimostra chiaramente l'importanza dei rischi posti dal progetto di decisione per quanto riguarda i diritti e le libertà fondamentali degli interessati in relazione al mancato accertamento di una violazione dell'articolo 32 del RGPD. Di conseguenza, l'obiezione sollevata dall'AC FR non soddisfa i requisiti di cui all'articolo 4, paragrafo 24, RGPD ([133]).

125. Anche l'obiezione dell'**AC HU** si riferiva all'eventuale violazione del RGPD, sostenendo la necessità di indagare anche in merito alla possibile violazione del principio di integrità e riservatezza. L'obiezione dell'AC HU è chiaramente pertinente, poiché sottolinea che si sarebbe dovuto indagare su un'ulteriore disposizione del RGPD (ossia sull'articolo 32). Tuttavia, l'AC HU non spiega in che modo il progetto di decisione comporterebbe tali rischi, né spiega pienamente il motivo per cui aspetti specifici della decisione sono carenti dal suo punto di vista ([134]). L'obiezione dell'AC HU non soddisfa il criterio di fornire una valida motivazione della sua obiezione, facendo riferimento ad argomentazioni di fatto o di diritto. Al contrario, si limita a raccomandare che l'AC IE indaghi anche sulla conformità all'articolo 32 del RGPD da parte del titolare del trattamento. Di conseguenza, l'obiezione sollevata dall'AC HU non soddisfa i requisiti di cui all'articolo 4, paragrafo 24, RGPD ([135]).

([130]) Linee guida relative alla RRO, paragrafo 13.
([131]) Linee guida relative alla RRO, paragrafo 16.
([132]) Linee guida relative alla RRO, paragrafo 18.
([133]) Di conseguenza, l'EDPB non prende posizione sul merito di eventuali questioni sostanziali sollevate da tali obiezioni. L'EDPB ribadisce che la sua attuale decisione non pregiudica le valutazioni che il comitato può essere chiamato a effettuare in altri casi, anche con le stesse parti, tenendo conto del contenuto del progetto di decisione pertinente e delle obiezioni sollevate dalle autorità interessate.
([134]) Linee guida relative alla RRO, paragrafo 18.
([135]) Di conseguenza, l'EDPB non prende posizione sul merito di eventuali questioni sostanziali sollevate da tali obiezioni. L'EDPB ribadisce che la sua attuale decisione non pregiudica le valutazioni che il comitato può essere chiamato a effettuare in altri casi, anche con le stesse parti, tenendo conto del contenuto del progetto di decisione pertinente e delle obiezioni sollevate dalle autorità interessate.

6.4.1.6 violazione dell'articolo 33, paragrafo 3, RGPD sul contenuto della notifica di una violazione dei dati personali in materia di sicurezza del trattamento

126. L'**AC DE** ritiene che il progetto di decisione indichi che l'articolo 33, paragrafo 3, RGPD potrebbe essere stato violato in aggiunta ad altre disposizioni del RGPD. In tal senso, si tratta di «stabilire se vi sia stata una violazione» del RGPD e se essa non sia stata esaminata e affrontata dalla proposta di decisione. Pertanto, l'AC DE ritiene che, se modificata, la proposta di decisione porterebbe alla conclusione che sussistono ulteriori violazioni del RGPD.

127. Tuttavia, l'AC DE non dimostra chiaramente i rischi significativi che la proposta di decisione comporta per i diritti e le libertà fondamentali degli interessati. Di conseguenza, l'obiezione dell'AC DE in merito all'articolo 33, paragrafo 3, RGPD non soddisfa i requisiti di cui all'articolo 4, paragrafo 24, RGPD ([136]).

6.4.1.7 violazione dell'articolo 34 del RGPD sulla comunicazione all'interessato di una violazione dei dati personali

128. L'**AC HU** ritiene che il progetto di decisione indichi che l'articolo 34 del RGPD potrebbe essere stato violato in aggiunta ad altre disposizioni del RGPD, soprattutto alla luce del fatto che il bug è durato nel corso degli anni e data la grave natura che incide sulla sicurezza del titolare del trattamento. In tal senso, si tratta di «stabilire se vi sia stata una violazione» del RGPD e se essa non sia stata esaminata e affrontata dalla proposta di decisione. Pertanto, l'AC HU ritiene che, se modificata, la proposta di decisione porterebbe alla conclusione che sussistono ulteriori violazioni del RGPD.

129. Tuttavia, l'AC HU non dimostra chiaramente i rischi significativi che il progetto di decisione comporta per i diritti e le libertà fondamentali degli interessati. Di conseguenza, l'obiezione dell'AC HU in merito all'articolo 34 del RGPD non soddisfa i requisiti di cui all'articolo 4, paragrafo 24, RGPD ([137]).

6.4.2 Valutazione del merito delle questioni sostanziali sollevate dalle obiezioni pertinenti e motivate e conclusione

130. Il comitato analizza ora le obiezioni ritenute pertinenti e motivate, in particolare le obiezioni dell'AC DE in merito all'articolo 5, paragrafo 1, lettera f), e in merito agli articoli 24 e 32 del RGPD, nonché l'obiezione dell'AC IT in merito all'articolo 5, paragrafo 2, RGPD, nonché la risposta dell'autorità capofila a tali obiezioni e le dichiarazioni di TIC.

131. Conformemente all'articolo 65, paragrafo 1, lettera a), RGPD, nell'ambito di una procedura di risoluzione delle controversie l'EDPB adotta una decisione vincolante in merito a tutte le questioni oggetto delle obiezioni pertinenti e motivate, in particolare se vi è una violazione del RGPD. L'EDPB può (e deve) prendere una decisione vincolante che, ove possibile, tenendo conto degli elementi del fascicolo e del diritto della parte convenuta a essere ascoltata, fornisce una conclusione definitiva sull'applicazione del RGPD in relazione al caso in questione. L'autorità capofila sarà quindi obbligata ad attuare le modifiche nella sua decisione finale.

([136]) Di conseguenza, l'EDPB non prende posizione sul merito di eventuali questioni sostanziali sollevate da tali obiezioni. L'EDPB ribadisce che la sua attuale decisione non pregiudica le valutazioni che il comitato può essere chiamato a effettuare in altri casi, anche con le stesse parti, tenendo conto del contenuto del progetto di decisione pertinente e delle obiezioni sollevate dalle autorità interessate.

([137]) Di conseguenza, l'EDPB non prende posizione sul merito di eventuali questioni sostanziali sollevate da tali obiezioni. L'EDPB ribadisce che la sua attuale decisione non pregiudica le valutazioni che il comitato può essere chiamato a effettuare in altri casi, anche con le stesse parti, tenendo conto del contenuto del progetto di decisione pertinente e delle obiezioni sollevate dalle autorità interessate.

132. Il comitato ritiene che gli elementi di fatto disponibili inclusi nel progetto di decisione e nelle obiezioni non siano sufficienti per consentire all'EDPB di stabilire l'esistenza di violazioni ulteriori (o alternative) dell'articolo 5, paragrafo 1, lettera f), e dell'articolo 5, paragrafo 2, nonché degli articoli 24 e 32 del RGPD.

133. Il comitato ritiene che, in generale, la portata limitata dell'indagine dell'AC IE, incentrata sin dall'inizio solo sull'esistenza di violazioni dell'articolo 33, paragrafi 1 e 5, RGPD da parte di TIC, incida direttamente sul suo mandato ai fini dell'indagine e sull'ulteriore accertamento dei fatti, nonché sulla capacità delle autorità interessate di presentare elementi sufficienti affinché l'EDPB possa sostenere le obiezioni.

134. L'EDPB ricorda il dovere dell'autorità capofila di «adoperarsi per raggiungere un consenso» con le autorità interessate (articolo 60, paragrafo 1, RGPD) e di fornire loro, senza indugio, «le informazioni utili» sulla questione (articolo 60, paragrafo 3, RGPD). Anche nel caso di un'indagine d'ufficio, le linee guida relative alle obiezioni pertinenti e motivate stabiliscono che l'autorità capofila «dovrebbe cercare un consenso sulla portata della procedura (ossia sugli aspetti del trattamento dei dati in esame) prima di avviare formalmente la procedura» ([138]), anche nel contesto di un eventuale nuovo procedimento.

135. Sebbene l'EDPB ritenga che le autorità di controllo godano di un certo grado di discrezionalità per decidere come inquadrare la portata delle loro indagini, il comitato ricorda che uno dei principali obiettivi del RGPD è quello di garantire la coerenza in tutta l'Unione europea, e la cooperazione tra l'autorità capofila e le autorità interessate è uno dei mezzi per raggiungere questo obiettivo. L'EDPB ricorda inoltre l'esistenza di una gamma completa di strumenti di cooperazione previsti dal RGPD (compresi gli articoli 61 e 62), tenendo presente l'obiettivo di raggiungere un consenso all'interno del meccanismo di cooperazione e la necessità di scambiare tutte le informazioni pertinenti, al fine di garantire la tutela dei diritti e delle libertà fondamentali degli interessati.

136. L'EDPB ritiene che un'autorità capofila, nel determinare la portata dell'indagine anche qualora essa sia limitata, dovrebbe inquadrarla in modo tale da consentire alle autorità interessate di svolgere efficacemente il loro ruolo, a fianco dell'autorità capofila, nel determinare se vi sia stata una violazione del RGPD.

7 SULLE MISURE CORRETTIVE DECISE DALL'AUTORITÀ CAPOFILA, IN PARTICOLARE L'IMPOSIZIONE DI UN AMMONIMENTO

7.1 Analisi dell'autorità capofila nel progetto di decisione

137. Il progetto di decisione spiega che, mentre nel progetto preliminare di decisione tra i poteri correttivi proposti figuravano sia un ammonimento, ai sensi dell'articolo 58, paragrafo 2, lettera b), RGPD, sia una sanzione amministrativa pecuniaria, ai sensi dell'articolo 58, paragrafo 2, lettera i), RGPD, il progetto di decisione finale consiste nell'imposizione di una sola sanzione amministrativa pecuniaria a TIC in qualità di titolare del trattamento ([139]).

138. Nelle sue osservazioni in relazione al progetto preliminare di decisione, TIC ha contestato la decisione di emettere un ammonimento, sostenendo che le violazioni dell'articolo 33, paragrafi 1 e 5, RGPD non

([138]) Linee guida relative alla RRO, paragrafo 28.
([139]) Progetto di decisione, paragrafo 12.1.

comprendono «operazioni di trattamento», mentre l'articolo 58, paragrafo 2, lettera b), RGPD conferisce alle autorità di controllo il potere di rivolgere ammonimenti ove i trattamenti abbiano violato le disposizioni del RGPD ([140]). L'argomentazione di TIC si basava principalmente sul fatto che né il ritardo nella notifica all'autorità di controllo né la mancata tenuta di registri adeguati costituiscono di per sé un'operazione di trattamento ([141]).

139. Nel suo progetto di decisione, l'AC IE ha spiegato la sua decisione di non rivolgere un ammonimento ricordando l'argomentazione avanzata da TIC nelle sue osservazioni in relazione al progetto preliminare di decisione, sostenendo che le violazioni dell'articolo 33, paragrafi 1 e 5, RGPD non comprendono «operazioni di trattamento», mentre l'articolo 58, paragrafo 2, lettera b), RGPD conferisce alle autorità di controllo il potere di rivolgere ammonimenti ove i trattamenti abbiano violato le disposizioni del RGPD ([142]). L'AC IE ha considerato che il termine «operazioni di trattamento» compare 50 volte nel RGPD e sembra essere utilizzato per indicare il trattamento o l'utilizzo di dati personali (o, in altre parole, azioni eseguite su di essi) controllati da un titolare del trattamento, ma che al tempo stesso la definizione di «trattamento» fornita dal RGPD è molto ampia, il che fa ritenere che, trattandosi di una violazione dei dati personali, ne consegue che l'obbligo di notifica (nella misura in cui deve intrinsecamente comportare un esame di ciò che è accaduto ai dati personali o di come sono stati interessati) è intrinsecamente connesso a una o più operazioni di trattamento ([143]). L'AC IE non ha ritenuto necessario trarre conclusioni definitive circa il significato e l'effetto del termine «operazioni di trattamento» nel progetto di decisione, ma «a conti fatti» ha ritenuto che l'argomentazione giuridica di TIC fosse «plausibile», decidendo di non procedere con un ammonimento rivolto a TIC ([144]).

7.2 Sintesi delle obiezioni sollevate dalle autorità interessate

140. L'**AC DE** ha sollevato un'obiezione in merito al fatto che, mentre nel progetto preliminare di decisione erano previsti sia un ammonimento che una sanzione pecuniaria, nel progetto di decisione è stata inclusa solo quest'ultima. L'AC DE non concordava con il ragionamento avanzato dall'AC IE in merito alla decisione di non rivolgere un ammonimento. Secondo l'AC DE, il ragionamento giuridico accettato dall'autorità capofila come «plausibile» non è convincente in quanto l'interpretazione giuridica richiede non solo un esame della formulazione della disposizione, ma anche del suo significato e della sua finalità, della storia del suo sviluppo e della sua sistematica integrazione nell'intero complesso normativo.

7.3 Posizione dell'autorità capofila in merito alle obiezioni

141. Nel memorandum composito, l'AC IE ha ritenuto che, sebbene l'obiezione dell'AC DE prenda in considerazione «se l'azione prevista in relazione a un titolare del trattamento o a un responsabile del trattamento sia conforme [al RGPD]», essa non dimostra come non rivolgere un ammonimento a TIC possa comportare rischi significativi per gli interessati ([145]); l'obiezione sulla decisione di non rivolgere

([140]) Osservazioni di TIC in relazione al progetto preliminare di decisione, paragrafo 11.1.
([141]) Progetto di decisione, paragrafo 12.4.
([142]) Osservazioni di TIC in relazione al progetto preliminare di decisione, paragrafo 11.1.
([143]) Progetto di decisione, paragrafo 12.5.
([144]) Progetto di decisione, paragrafo 12.5. Le altre argomentazioni separate avanzate da TIC in merito alle ragioni per cui l'imposizione di un ammonimento non è stata considerata adeguata (osservazioni di TIC in relazione al progetto preliminare di decisione, paragrafi 11.2-11.4) non sono state considerate separatamente, alla luce della suddetta decisione (progetto di decisione, paragrafo 12.6).
([145]) Memorandum composito, paragrafo 5.79.

un ammonimento non è quindi stata ritenuta pertinente e motivata ai sensi dell'articolo 4, paragrafo 24, RGPD.

142. Ciononostante, prendendo in esame i meriti delle questioni sostanziali sollevate dalle obiezioni, l'autorità capofila ha spiegato che considerava il termine «operazioni di trattamento» in linea con il significato e l'applicazione ad esso attribuiti in tutto il RGPD, osservando che questo termine è utilizzato per i poteri delle autorità di controllo soltanto ai sensi dell'articolo 58 del RGPD. A seguito delle osservazioni presentate da TIC nella sua risposta alle obiezioni delle autorità interessate su questo punto, l'autorità capofila ha deciso, in considerazione dell'ambito dell'indagine incentrata sugli obblighi del titolare del trattamento in relazione alla notifica della violazione, che la sua indagine «*non comportava l'accertamento che le "operazioni di trattamento" sottostanti relative alla violazione violassero [...] il RGPD*» ([146]). Pertanto, l'autorità capofila ha ritenuto che non vi fosse motivo di rivedere la propria decisione di non rivolgere un ammonimento alla luce dell'obiezione dell'AC DE.

143. L'autorità capofila ha osservato che la sua posizione nel progetto di decisione di non rivolgere un ammonimento è applicabile solo alle circostanze specifiche di questo caso; pertanto non pregiudica le future decisioni sugli ammonimenti che potrebbero essere prese dall'autorità capofila o da qualsiasi altra autorità interessata ([147]).

7.4 Analisi dell'EDPB

7.4.1 Valutazione della pertinenza e della motivazione delle obiezioni

144. L'obiezione dell'**AC DE** si riferisce alla conformità dell'azione prevista con il RGPD, in quanto indica quale azione correttiva, a suo avviso, dovrebbe essere inclusa dall'autorità capofila nella decisione finale: si tratta quindi di un'obiezione pertinente, che mostra adeguatamente la diversa conclusione proposta. Inoltre, essa include un ragionamento giuridico a sostegno del suo punto di vista e propone un'interpretazione giuridica alternativa. Tuttavia, l'obiezione non dimostra chiaramente l'importanza del rischio posto dal progetto di decisione per i diritti e le libertà degli interessati e/o la libera circolazione dei dati personali. In particolare, non fornisce alcuna motivazione circa il modo in cui la mancata imposizione di un ammonimento in questo caso specifico, in cui viene anche comminata una sanzione pecuniaria, possa far scattare rischi per i diritti e le libertà fondamentali degli interessati.

7.4.2 Conclusione

145. L'EDPB ritiene che tale obiezione non soddisfi i requisiti dell'articolo 4, paragrafo 24, RGPD.

146. L'EDPB prende atto della posizione dell'autorità capofila secondo cui la sua posizione di non rivolgere un ammonimento è applicabile solo alle circostanze specifiche di questo caso, pertanto non pregiudica le future decisioni sugli ammonimenti che potrebbero essere prese dall'autorità capofila o da qualsiasi altra autorità interessata ([148]).

147. Come già indicato in precedenza, la decisione dell'EDPB di non valutare la fondatezza del merito dell'obiezione sollevata non pregiudica le future decisioni dell'EDPB sullo stesso argomento o su questioni analoghe.

([146]) Memorandum composito, paragrafo 5.78.
([147]) Memorandum composito, paragrafo 5.78.
([148]) Memorandum composito, paragrafo 5.78.

8 SULLE MISURE CORRETTIVE, IN PARTICOLARE LA QUANTIFICAZIONE DELLA SANZIONE AMMINISTRATIVA PECUNIARIA

8.1 Analisi dell'autorità capofila nel progetto di decisione

148. Il progetto di decisione spiega il modo in cui l'AC IE ha considerato i criteri di cui all'articolo 83, paragrafo 2, RGPD nel decidere se imporre una sanzione amministrativa pecuniaria e come determinarne l'importo ([149]).

149. Per quanto riguarda il calcolo della sanzione pecuniaria, il progetto di decisione ha analizzato, in primo luogo, **la natura, la gravità e la durata della violazione**, ai sensi dell'articolo 83, paragrafo 2, lettera a), RGPD ([150]). La proposta di decisione ha tenuto in considerazione «*la natura, l'oggetto o la finalità del trattamento*» facendo riferimento alla natura delle operazioni di trattamento effettuate da Twitter (una piattaforma di «microblogging» e social media su cui gli utenti hanno la possibilità di documentare le loro riflessioni tramite «tweet»), alla natura del trattamento che ha dato origine alla violazione (derivante da un bug che ha fatto sì che tweet precedentemente «protetti» diventassero «non protetti» e accessibili al pubblico, nei casi in cui utenti Android hanno cambiato l'indirizzo e-mail), e all'ambito di applicazione del trattamento (il bug ha interessato almeno 88 726 utenti UE/SEE, in quanto sono state coinvolte altre persone nel periodo compreso tra la data in cui si è verificato il bug, il 4 novembre 2014, e la sua completa riparazione, il 14 gennaio 2019, ma non è stato possibile identificarle tutte) ([151]).

150. Il progetto di decisione ha preso in considerazione anche il **numero di interessati lesi dal danno e il livello del danno da essi subito** ([152]), concludendo che il numero di interessati che potrebbero essere stati coinvolti dalla notifica tardiva e il potenziale danno per gli stessi derivante dalla conseguente valutazione tardiva da parte dell'autorità di controllo erano fattori rilevanti da prendere in considerazione ([153]). È stato ricordato che l'impatto sui singoli utenti e la possibilità che ne derivi un danno si ripercuoterà sul livello e sulla natura dei dati personali resi pubblici e che il ritardo delle azioni correttive poteva comportare almeno potenzialmente un danno agli interessati ([154]). La posizione dell'AC IE nel progetto preliminare affermava che, *«sebbene TIC non avesse confermato la natura precisa dei dati resi pubblici nella violazione, era ragionevole dedurre che, data l'entità degli utenti interessati e la natura del servizio offerto da TIC, alcuni dei dati personali pubblicati in relazione, almeno, ad alcuni degli utenti avranno incluso categorie sensibili di dati e altro materiale particolarmente privato*» ([155]). Questa posizione è stata ulteriormente precisata nel progetto di decisione alla luce delle osservazioni di TIC, in quanto l'AC IE ha deciso che «*dovrebbe essere attribuito meno peso a questo fattore*», sulla base del fatto che, «*sebbene non si possa affermare in via definitiva*

([149]) Progetto di decisione, paragrafi 14.1-14.62.
([150]) L'articolo 83, paragrafo 2, lettera a), RGPD cita «*la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito*».
([151]) Progetto di decisione, paragrafo 14.2.
([152]) Progetto di decisione, paragrafi 14.3-14.5.
([153]) Progetto di decisione, paragrafo 14.5.
([154]) Progetto di decisione, paragrafo 14.5 (il progetto di decisione osserva che «Chiaramente, l'impatto sui singoli utenti e la possibilità che ne derivi un danno dipenderà dal livello dei dati personali resi pubblici e, inoltre, dalla natura di tali dati personali»).
([155]) Progetto di decisione, paragrafo 14.5.

che nessun utente interessato dalla violazione sia stato interessato dalla notifica tardiva, non vi era alcuna prova diretta di un danno derivante da quest'ultima» ([156]).

151. Per quanto riguarda la **natura della violazione**, il progetto di decisione ha evidenziato che le violazioni dell'articolo 33, paragrafi 1 e 5, RGPD non riguardano la questione sostanziale della violazione ([157]). L'AC IE ha inoltre ritenuto che la natura degli obblighi di cui all'articolo 33, paragrafi 1 e 5, RGPD, è tale per cui il rispetto degli stessi è fondamentale per il funzionamento complessivo del regime di controllo e di esecuzione messo in atto dalle autorità di controllo in relazione sia alla questione specifica delle violazioni dei dati personali, sia all'individuazione e alla valutazione di questioni più ampie di mancato rispetto da parte dei titolari del trattamento, e il mancato rispetto di tali obblighi ha gravi conseguenze in quanto rischia di compromettere l'effettivo esercizio delle funzioni delle autorità di controllo di cui al RGPD ([158]).

152. Per quanto riguarda la **gravità della violazione** dell'articolo 33, paragrafo 1, RGPD, il progetto di decisione ha tenuto conto di come essa ha interferito con la finalità generale di comunicare una violazione dei dati personali all'autorità di controllo, del fatto che non è stato dimostrato alcun danno materiale agli interessati, che le misure correttive di TIC si sono limitate a un'azione rivolta al futuro per la cessazione del bug (e non hanno rappresentato un'analisi retrospettiva per individuare i rischi per gli interessati derivanti dalla violazione) e dell'apparente mancanza di una valutazione formale del rischio da parte di TIC ([159]). Il progetto di decisione non ha considerato l'affermazione di TIC secondo cui la violazione è stata causata da un guasto isolato (che ha portato al ritardo nella notifica al responsabile della protezione dei dati) di peso sufficiente a ridurre la gravità della violazione (ma ha tenuto conto di tale natura isolata dell'incidente, discostandosi dal punto di vista provvisorio del progetto preliminare, secondo cui la violazione era indicativa di un problema più ampio e sistemico) ([160]). Per quanto riguarda la gravità della violazione dell'articolo 33, paragrafo 5, RGPD, il progetto di decisione ha sottolineato che è necessaria un'adeguata documentazione delle violazioni per consentire a un'autorità di controllo di verificare il rispetto dell'articolo 33 RGPD ([161]) da parte del titolare del trattamento e che l'AC IE era tenuta a sollevare molteplici interrogativi per ottenere chiarezza sui fatti relativi alla notifica della violazione ([162]), ma ha riconosciuto che le carenze della documentazione derivavano da un malinteso in buona fede dei requisiti (che risultano, tuttavia, chiari dalla formulazione della disposizione) ([163]). Il progetto di decisione ha concluso che ogni violazione si collocava all'«*estremità bassa o moderata della scala di gravità*» ([164]).

153. Per quanto riguarda la **durata della violazione** dell'articolo 33, paragrafo 1, RGPD, il progetto di decisione ha ritenuto che si trattasse di un periodo di due giorni e lo ha valutato alla luce del termine complessivo generalmente consentito per le notifiche di violazione (72 ore), osservando che non si trattava di un periodo banale o insignificante ([165]). Per quanto riguarda la durata della violazione

([156]) Progetto di decisione, paragrafo 14.5.
([157]) Progetto di decisione, paragrafo 14.6.
([158]) Progetto di decisione, paragrafo 14.11.
([159]) Progetto di decisione, paragrafi 14.16-14.18.
([160]) Progetto di decisione, paragrafo 14.19.
([161]) Progetto di decisione, paragrafo 14.20.
([162]) Progetto di decisione, paragrafo 14.21.
([163]) Progetto di decisione, paragrafo 14.24.
([164]) Progetto di decisione, paragrafo 14.24.
([165]) Progetto di decisione, paragrafo 14.26 [è iniziato alla scadenza delle 72 ore a partire dal 3 gennaio 2019 (cioè il 6 gennaio 2019) e si è concluso al momento della notifica della violazione da parte di TIC l'8 gennaio 2019].

dell'articolo 33, paragrafo 5, RGPD, il progetto di decisione ha concluso che era attualmente in corso ([166]).

154. In relazione all'**articolo 83, paragrafo 2, lettera b), RGPD** (il carattere doloso o colposo della violazione), nel progetto di decisione l'AC IE ha concluso che la violazione dell'articolo 33, paragrafo 1, RGPD ([167]) da parte di TIC aveva **carattere colposo**, sottolineando che il ritardo nella notifica del responsabile globale della protezione dei dati si era verificato perché una parte del protocollo interno del gruppo Twitter non era stata completata come prescritto e il protocollo non era così chiaro come avrebbe potuto essere ([168]). Ciò ha portato alla conclusione che il ritardo è stato provocato da una negligenza da parte del titolare del trattamento, ma è stata accettata l'affermazione di TIC secondo cui la notifica tardiva non era indicativa di un problema sistemico più ampio e costituiva un evento isolato ([169]). L'AC IE non ha individuato alcuna prova di comportamento doloso in relazione alla violazione dell'articolo 33, paragrafo 1, RGPD ([170]). Il progetto di decisione ha inoltre individuato il carattere colposo della violazione dell'articolo 33, paragrafo 5, RGPD ([171]) da parte di TIC, in quanto non vi era alcuna conoscenza e volontà di provocare la violazione (il che sarebbe equivalso a dolo), ma la documentazione non era sufficiente a consentire di verificare il rispetto dell'articolo 33 ([172]).

155. Per quanto riguarda l'**articolo 83, paragrafo 2, lettera c), RGPD**, ossia le misure adottate dal titolare del trattamento per **attenuare il danno subito dagli interessati**, il progetto di decisione ha ritenuto che fossero state adottate misure correttive per evitare il ripetersi del problema e per correggere il bug, che sono state considerate come l'unico fattore attenuante nella valutazione dell'importo della sanzione pecuniaria da infliggere ([173]).

156. Il progetto di decisione ha preso in considerazione l'**articolo 83, paragrafo 2, lettera d), RGPD**, ossia il **grado di responsabilità** del titolare o del responsabile del trattamento, prendendo atto delle misure tecniche e organizzative esistenti e successivamente potenziate attuate da TIC in qualità di titolare del trattamento, tra cui la modifica del protocollo interno del gruppo Twitter (che secondo l'AC IE non era così chiaro come avrebbe potuto essere) e le misure di formazione del personale adottate successivamente da Twitter, Inc. (una formazione supplementare è stata fornita internamente, sottolineando l'importanza di menzionare il team del responsabile della protezione dei dati, e quindi TIC come titolare del trattamento, nel sistema interno di ticket), nonché l'esistenza di strutture e di garanzie interne riguardanti la responsabilità per le questioni di sicurezza informatica e l'esistenza di una revisione esterna ricorrente di esperti esterni del programma di sicurezza informatica di Twitter, Inc. ([174]). Sebbene le questioni emerse non siano state ritenute indicative di un problema sistemico più ampio ([175]) e TIC abbia dimostrato un approccio generalmente responsabile e affidabile nei confronti della sicurezza dei dati ([176]), si è ritenuto che vi fosse un livello di responsabilità da moderato a elevato

([166]) Progetto di decisione, paragrafo 14.29.
([167]) Progetto di decisione, paragrafo 14.34.
([168]) Progetto di decisione, paragrafi 14.33-14.34.
([169]) Progetto di decisione, paragrafo 14.34.
([170]) Progetto di decisione, paragrafo 14.35.
([171]) Progetto di decisione, paragrafo 14.38.
([172]) Progetto di decisione, paragrafi 14.36 e 14.38.
([173]) Progetto di decisione, paragrafi 14.39-14.42.
([174]) Progetto di decisione, paragrafi 14.43-14.47.
([175]) Progetto di decisione, paragrafo 14.45.
([176]) Progetto di decisione, paragrafo 14.47.

dimostrato dal titolare del trattamento, in quanto la mancanza di chiarezza del protocollo è stata dimostrata anche dalla sua successiva modifica ([177]).

157. È stato valutato il **grado di cooperazione** con l'autorità di controllo, in linea con l'**articolo 83, paragrafo 2, lettera f)**, **RGPD**, e non è risultato essere un fattore attenuante ([178]). L'AC IE ha riconosciuto che TIC ha cooperato pienamente, ma ha osservato che si trattava di un obbligo di legge e che TIC non è andata oltre tale obbligo ([179]).

158. In relazione all'**articolo 83, paragrafo 2, lettera g), RGPD** relativo alle **categorie di dati personali interessate**, il progetto di decisione ha concluso che qualsiasi categoria di dati personali avrebbe potuto essere interessata dalla notifica tardiva e che non si può affermare in via definitiva che non vi sia stato alcun danno per gli interessati o che non vi siano categorie di dati personali interessate ([180]).

159. La **maniera in cui l'AC IE è venuta a conoscenza della violazione** è stata considerata un fattore pertinente per la determinazione dell'importo della sanzione pecuniaria (in linea con l'articolo 83, paragrafo 2, lettera h), RGPD), poiché, sebbene TIC abbia collaborato nel fornire tutta la documentazione disponibile, i registri non hanno consentito all'AC IE di verificare il rispetto dell'articolo 33 del RGPD e le informazioni originariamente fornite nella notifica all'AC IE erano di natura imprecisa ([181]).

160. I criteri di cui all'**articolo 83, paragrafo 2, lettere e), i) e j), RGPD**, non sono risultati applicabili e non sono stati individuati ulteriori elementi in relazione all'**articolo 83, paragrafo 2, lettera k), RGPD** ([182]).

161. L'AC IE ha sottolineato nel suo progetto di decisione che, in mancanza di orientamenti specifici a livello dell'UE sul calcolo delle sanzioni pecuniarie, non era tenuta ad applicare una metodologia particolare o a utilizzare un punto di partenza finanziario fisso ([183]) e che l'espressione «dovuta considerazione» fornisce alle autorità di controllo un'ampia discrezionalità su come soppesare i fattori di cui all'articolo 83, paragrafo 2, RGPD ([184]).

162. Per quanto riguarda l'identificazione dell'impresa interessata per calcolare il limite massimo della sanzione pecuniaria stabilito dall'**articolo 83, paragrafo 4, RGPD**, l'AC IE ha sottolineato che il fatto che TIC goda di autonomia nella titolarità del trattamento dei dati non significa che cessi di far parte di un'**unica entità economica** con la sua società madre e ha osservato che, oltre alla proprietà di TIC da parte di Twitter, Inc., il consulente generale di Twitter, Inc. sembra essere uno dei tre direttori di TIC ([185]).

163. Per questo motivo, il limite massimo del valore dell'eventuale sanzione pecuniaria inflitta è stato calcolato dall'autorità capofila con riferimento al fatturato di Twitter, Inc. ([186]). Poiché il fatturato

([177]) Progetto di decisione, paragrafo 14.47.
([178]) Progetto di decisione, paragrafo 14.50.
([179]) Progetto di decisione, paragrafo 14.49.
([180]) Progetto di decisione, paragrafo 14.54.
([181]) Progetto di decisione, paragrafo 14.58.
([182]) Progetto di decisione, paragrafi 14.48, 14.59, 14.60, 14.61.
([183]) Progetto di decisione, paragrafo 15.2.
([184]) Progetto di decisione, paragrafo 15.1.
([185]) Progetto di decisione, paragrafo 15.13.
([186]) Progetto di decisione, paragrafo 15.14.

annuo di Twitter, Inc., nel 2018 ammontava a 3 miliardi di USD, il massimale è stato considerato pari a 60 milioni di USD (2 % di 3 miliardi di USD) ([187]).

164. Nell'applicare i principi di **efficacia, proporzionalità e dissuasività** (**articolo 83, paragrafo 1, RGPD**), il progetto di decisione ha ritenuto che una sanzione pecuniaria non può essere efficace se non ha un'importanza relativa alle entrate del titolare del trattamento, che la violazione non deve essere considerata in astratto, indipendentemente dall'impatto sul titolare del trattamento, e che le violazioni future devono essere scoraggiate ([188]).

165. L'AC IE ha proposto di infliggere una sanzione amministrativa pecuniaria compresa tra 150 000 e 300 000 USD, ossia tra lo 0,005 % e lo 0,01 % del fatturato annuo dell'impresa o tra lo 0,25 % e lo 0,5 % dell'importo massimo della sanzione pecuniaria che può essere applicata in relazione a tali violazioni. Ciò equivale a una sanzione pecuniaria in euro compresa tra 135 000 e 275 000 ([189]).

8.2 Sintesi delle obiezioni sollevate dalle autorità interessate

166. L'**AC AT** ha sollevato un'obiezione in merito all'importo della sanzione pecuniaria proposta e al fatto che l'autorità capofila ha proposto un intervallo di importi invece di una somma fissa. Per quanto riguarda l'articolo 83, paragrafo 2, lettera a), RGPD, l'AC AT ha sottolineato che almeno 88 726 persone (ma probabilmente di più) sono state colpite dalla violazione e che «*è molto probabile che siano stati divulgati dati sensibili a un pubblico più vasto*».

167. L'obiezione sollevata dall'AC AT ha espresso un disaccordo sul modo in cui il *momento in cui il titolare del trattamento deve essere considerato a conoscenza di una violazione dei dati* è stato analizzato nel progetto di decisione. Più nello specifico, l'AC AT ha sostenuto nella sua obiezione che TIC avrebbe dovuto effettuare una notifica di violazione dei dati entro 72 ore dal ricevimento della segnalazione di bug da parte del responsabile del trattamento, venendo così a conoscenza della violazione. L'AC AT ha sottolineato che TIC è responsabile della supervisione delle operazioni di trattamento effettuate dal responsabile del trattamento e che un titolare del trattamento non dovrebbe cercare di nascondere una mancanza del responsabile del trattamento con cui ha un rapporto contrattuale e che è stato scelto dal titolare stesso. Ciò contribuisce alla valutazione della violazione dell'articolo 33, paragrafo 1, RGPD da parte dell'AC AT come «grave».

168. Per quanto riguarda il «*carattere doloso o colposo della violazione*» (articolo 83, paragrafo 2, lettera b), RGPD), l'AC AT ha sostenuto che il comportamento di TIC dovrebbe essere etichettato come «doloso», sulla base dei criteri di conoscenza e intenzionalità stabiliti nelle Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie («WP253») del Gruppo di lavoro articolo 29, approvate dall'EDPB ([190]). Per quanto riguarda il criterio relativo alle *misure adottate per attenuare il danno* subito dagli interessati (articolo 83, paragrafo 2, lettera c), RGPD), l'AC AT ha sottolineato che «*inizialmente non era intenzione di TIC informare gli utenti interessati dalla violazione*» e che «*le misure adottate da Twitter, Inc. per correggere il bug sono l'unico fattore attenuante*». Infine, l'AC AT ritiene

([187]) Progetto di decisione, paragrafo 15.19.
([188]) Progetto di decisione, paragrafo 15.18.
([189]) Progetto di decisione, paragrafo 15.20 (il valore più elevato dell'intervallo proposto nel progetto di decisione è inferiore a quello del progetto preliminare di decisione, al fine di riflettere i cambiamenti di opinione in relazione alla gravità, al grado di responsabilità del titolare del trattamento e al fatto che le violazioni fossero sistemiche). Al paragrafo 15.21 del progetto di decisione è sottolineato che, al fine di tutelare i diritti procedurali di TIC, per la sanzione pecuniaria è stato proposto un intervallo, anziché una cifra fissa, e si riconosce la possibilità che le autorità interessate si pronuncino circa dove dovesse situarsi la sanzione in tale intervallo.
([190]) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

che l'intervallo proposto per la sanzione pecuniaria dall'AC IE non sia né effettivo, né proporzionato, né dissuasivo alla luce dei criteri elencati all'articolo 83, paragrafo 2, lettere da a) a k), RGPD. In conclusione, l'AC AT ha proposto l'imposizione di una sanzione amministrativa pecuniaria più elevata, che potrebbe soddisfare i requisiti di efficacia, proporzionalità e dissuasività (ossia «*un importo minimo dell'1 % del fatturato annuo dell'impresa*»).

169. L'**AC DE** ha sollevato un'obiezione sostenendo che la sanzione pecuniaria proposta dall'autorità capofila è «troppo bassa» e «non è conforme alle disposizioni dell'articolo 83, paragrafo 1, RGPD». Più nello specifico, l'AC DE ha sostenuto che l'ammenda non è dissuasiva. L'obiezione ha ricordato che una sanzione può essere considerata effettiva e dissuasiva se è adatta sia come misura preventiva generale, per dissuadere il pubblico dal commettere violazioni e per affermare la fiducia del pubblico nella validità del diritto dell'Unione, sia come misura preventiva speciale, per dissuadere il trasgressore dal commettere ulteriori violazioni. L'AC DE sostiene inoltre che la capacità finanziaria di un'impresa (in termini di fatturato) può fornire un'indicazione importante degli importi necessari per ottenere un effetto dissuasivo: ciò può significare prendere in considerazione la parte di fatturato generata dai prodotti per i quali è stata commessa la violazione, che può fornire un'indicazione dell'entità delle violazioni. L'AC DE sostiene inoltre che l'effetto dissuasivo di sanzioni pecuniarie elevate può essere ottenuto solo se gli importi imposti non possono essere pagati facilmente a causa di beni ingenti o di redditi elevati, evidenziando che la sanzione pecuniaria deve avere un effetto dissuasivo, in particolare in relazione a specifici trattamenti di dati. Di conseguenza, la sanzione pecuniaria minacciata deve essere sufficientemente elevata da rendere il trattamento dei dati antieconomico e oggettivamente inefficiente. Poiché il modello aziendale di Twitter si basa sul trattamento dei dati e poiché Twitter genera fatturato principalmente attraverso di esso, l'AC DE ritiene che una sanzione pecuniaria dissuasiva in questo caso specifico dovrebbe quindi essere così elevata da rendere non redditizio il trattamento illegale dei dati. Sulla base del concetto di sanzione pecuniaria applicabile alle AC DE, la sanzione pecuniaria per la violazione descritta nel progetto di decisione andrebbe da circa 7 348 035,00 EUR a 22 044 105,00 EUR.

170. L'**AC HU** ha sostenuto che, sebbene «*le sanzioni pecuniarie siano giustificate per le violazioni commesse*», «*la sanzione pecuniaria stabilita nel progetto è irragionevolmente bassa, inadeguata e quindi non dissuasiva in considerazione della gravità della violazione commessa e del potere di mercato mondiale del titolare del trattamento*».

171. L'**AC IT** ha chiesto all'autorità capofila di «*rivedere il progetto di decisione in relazione anche alla quantificazione della sanzione amministrativa pecuniaria, tenendo conto di specifici elementi aggravanti del caso per quanto riguarda la natura del titolare del trattamento dei dati, la gravità e la durata della violazione dei dati*».

8.3 Posizione dell'autorità capofila in merito alle obiezioni

172. L'AC IE ha ritenuto che le obiezioni sollevate dalle AC AT, DE e HU in relazione alla sanzione amministrativa pecuniaria fossero «pertinenti e motivate» ai sensi dell'articolo 4, paragrafo 24, RGPD. Allo stesso tempo, l'AC IE non ha dato seguito a tali obiezioni per le ragioni esposte nel memorandum composito ([191]).

173. In particolare, per quanto riguarda le obiezioni delle AC AT e DE, l'AC IE ritiene che la sua valutazione e l'applicazione dei fattori di cui all'articolo 83, paragrafo 2, lettere a) e b), RGPD, elaborate nel suo

([191]) Memorandum composito, paragrafi 5.60-5.72.

progetto di decisione, siano adeguate. Per quanto riguarda l'obiezione dell'AC AT, l'AC IE sostiene che la violazione dell'articolo 33, paragrafi 1 e 5, RGPD da parte di TIC sia stata il risultato di una negligenza di TIC piuttosto che di un'omissione intenzionale ([192]). Pertanto, l'AC IE ritiene che la sanzione pecuniaria proposta dall'AC AT non sia proporzionata ([193]). Inoltre, l'AC IE sostiene che la preoccupazione espressa dall'AC AT circa l'intervallo per la sanzione pecuniaria proposta nel progetto di decisione, anziché una somma fissa, non sia stata ben elaborata e chiarita da quest'autorità interessata ([194]). Per quanto riguarda l'obiezione dell'AC DE, l'AC IE ha preso atto dell'obiezione in merito alla necessità che la sanzione pecuniaria soddisfi il requisito della dissuasività, ma ritiene che il livello di sanzione pecuniaria proposto dall'AC DE non sia proporzionato in questo caso ([195]). Per le ragioni sopra esposte, l'AC IE ritiene che tali obiezioni siano pertinenti e motivate, ma propone di non darvi seguito ([196]).

174. L'AC IE ha tenuto in debito conto il punto di vista dell'AC AT in relazione alla tempistica della presa di coscienza e della notifica della violazione da parte di TIC, ma ha concluso che, nonostante l'effettiva «presa di coscienza» della violazione da parte di TIC il 7 gennaio 2019, TIC avrebbe dovuto esserne a conoscenza al più tardi entro il 3 gennaio 2019 ([197]). Nell'individuare il 3 gennaio 2019 come data in cui TIC avrebbe dovuto essere a conoscenza della violazione, l'AC IE ha tenuto conto del fatto che si era verificato un precedente ritardo nel periodo che va da quando l'incidente è stato comunicato per la prima volta da un contraente a Twitter, Inc. a quando Twitter, Inc. ha iniziato la revisione ([198]). Inoltre, l'AC IE chiarisce che non sta suggerendo che, «*in linea generale, i titolari del trattamento dei dati dovrebbero essere considerati automaticamente consapevoli delle violazioni dei dati nel momento stesso in cui il responsabile del trattamento viene a conoscenza della violazione*» ([199]). Inoltre, l'AC IE afferma che «*di solito accade che un responsabile del trattamento che subisce una violazione viene a conoscenza dell'evento in un momento precedente rispetto al titolare del trattamento e che, a condizione che il processo concordato tra il titolare e il responsabile del trattamento sia efficace e/o sia seguito, il titolare del trattamento viene "messo a conoscenza" della violazione [...] in modo tale da poter adempiere all'obbligo di notifica*» ([200]).

8.4 Analisi dell'EDPB

8.4.1 Valutazione della pertinenza e della motivazione delle obiezioni

175. Per quanto riguarda la possibilità di contestare l'importo delle sanzioni pecuniarie proposte tramite obiezioni pertinenti e motivate sulla conformità al RGPD dell'azione prevista in relazione al titolare o al responsabile del trattamento ([201]), l'EDPB ha recentemente chiarito che «*è possibile che l'obiezione contesti gli elementi su cui ci si è basati per la quantificazione dell'importo della sanzione pecuniaria*» ([202]). Ciò può equivalere a un esempio di obiezione relativa alla conformità al RGPD dell'azione prevista in relazione al titolare o al responsabile del trattamento.

([192]) Memorandum composito, paragrafo 5.62.
([193]) Memorandum composito, paragrafo 5.63.
([194]) Memorandum composito, paragrafo 5.64.
([195]) Memorandum composito, paragrafo 5.68.
([196]) Memorandum composito, paragrafi 5.65 e 5.68.
([197]) Memorandum composito, paragrafo 5.48.
([198]) Memorandum composito, paragrafo 5.50.
([199]) Memorandum composito, paragrafo 5.50.
([200]) Memorandum composito, paragrafo 5.50.
([201]) RGPD, articolo 4, paragrafo 24.
([202]) Linee guida relative alla RRO, paragrafo 34.

176. Nel caso in esame, l'obiezione dell'**AC AT** contesta gli elementi su cui si è basata l'AC IE nella quantificazione dell'importo della sanzione pecuniaria e riguarda quindi la conformità al RGPD dell'azione proposta nei confronti del titolare del trattamento. L'AC AT ha chiarito il collegamento tra la sua obiezione e il progetto di decisione e ha dimostrato come le modifiche proposte porterebbero a una diversa conclusione. Inoltre, ha fornito argomentazioni sul motivo per cui propone di modificare la decisione, fornendo un'interpretazione alternativa di tre dei criteri elencati dall'articolo 83 del RGPD e facendo riferimento ad argomenti di fatto e di diritto. L'AC AT dimostra chiaramente l'importanza dei rischi posti dal progetto di decisione, in primo luogo sostenendo che la sanzione pecuniaria proposta non è sufficientemente effettiva e dissuasiva e ricordando che a tal fine deve essere in grado di dissuadere il pubblico dal commettere una violazione analoga e di confermare la fiducia del pubblico nell'applicazione del diritto dell'Unione, nonché di dissuadere il titolare del trattamento dal commettere ulteriori violazioni. Inoltre, nella valutazione della gravità della violazione, l'obiezione si riferisce anche alla misura in cui gli interessati (in un numero probabilmente superiore a quello identificato) sono stati colpiti dalla violazione (ad esempio a causa dell'esposizione al pubblico generale dei loro tweet precedentemente protetti, che probabilmente includevano dati sensibili). Il presunto dolo della violazione, secondo l'AC AT, implica un impatto molto maggiore sulla capacità di distinguere ciò che è giusto da ciò che è sbagliato rispetto a una violazione colposa. Alla luce della valutazione di cui sopra, l'EDPB ritiene che l'obiezione dell'AC AT sia pertinente e motivata ai sensi dell'articolo 4, paragrafo 24, RGPD. Di conseguenza, l'EDPB valuterà il merito delle questioni sostanziali sollevate da tale obiezione (cfr. sezione 8.4.2 sotto).

177. Anche l'obiezione dell'**AC DE** è da considerarsi pertinente in quanto riguarda la conformità dell'azione prevista con il RGPD, contestando gli elementi su cui ci si è basati per la quantificazione dell'importo della sanzione pecuniaria. Più nello specifico, essa sostiene che la sanzione pecuniaria inflitta dall'AC IE non sia dissuasiva e che quindi la quantificazione effettuata non sia conforme all'articolo 83, paragrafo 1, RGPD. L'AC DE ha chiarito che una sanzione si considera effettiva e dissuasiva quando serve come misura preventiva generale per dissuadere il pubblico dal commettere violazioni e per affermare la sua fiducia nella validità del diritto dell'Unione, ma anche quando dissuade il trasgressore dal commettere ulteriori violazioni. Inoltre, l'AC DE dimostra chiaramente l'importanza dei rischi che il progetto di decisione comporta per i diritti e le libertà degli interessati, poiché la mancata imposizione di una sanzione dissuasiva ed effettiva può non essere in grado di dissuadere il titolare del trattamento dal commettere ulteriori violazioni.

178. Un altro argomento fornito dall'AC DE per dimostrare l'importanza dei rischi è che la mancata gestione adeguata della violazione suggerisce un «*errore sistemico*», che avrebbe richiesto di sottoporre il titolare del trattamento a un esame più approfondito, al di là del singolo incidente specifico. L'AC DE ha inoltre ricordato che un gran numero di persone è stato interessato e che il periodo di tempo è stato altrettanto rilevante e ha concluso che i poteri correttivi imposti sulla base dell'articolo 58, paragrafo 2, RGPD devono essere esaminati alla luce di questi elementi. In conclusione, l'EDPB ritiene che l'obiezione dell'AC DE sia pertinente e motivata ai sensi dell'articolo 4, paragrafo 24, RGPD. Di conseguenza, l'EDPB valuterà il merito delle questioni sostanziali sollevate da tale obiezione (cfr. sezione 8.4.2 sotto).

179. L'obiezione dell'**AC HU** è pertinente in quanto anch'essa riguarda la conformità dell'azione prevista con il RGPD, affermando che la sanzione pecuniaria proposta è «*irragionevolmente bassa, sproporzionata e quindi non dissuasiva*». Tuttavia, sebbene l'obiezione si riferisca al «*"bug" nell'applicazione del titolare del trattamento negli anni» e alla «sua grave natura che incide sulla sicurezza dei dati*», nonché alla «*gravità della violazione commessa*» e al «*potere di mercato mondiale del titolare del trattamento*», essa non dimostra chiaramente l'importanza dei rischi per i diritti e le

libertà degli interessati posti dall'importo della sanzione pecuniaria proposto dall'AC IE. Di conseguenza, l'EDPB ritiene che tale obiezione non soddisfi i requisiti dell'articolo 4, paragrafo 24, RGPD ([203]).

180. Infine, la pertinenza dell'obiezione sollevata dall'**AC IT** è dimostrata anche dal riferimento alla conformità dell'azione proposta con il RGPD, in quanto sostiene che l'AC IE dovrebbe rivedere il progetto di decisione in relazione alla quantificazione della sanzione amministrativa pecuniaria. Facendo riferimento alle «*obiezioni di cui sopra*» e quindi al fatto che gli aspetti menzionati sono «*di natura strutturale per quanto riguarda l'organizzazione del titolare del trattamento*» e «*destinati a produrre effetti non solo sul caso in questione, ma anche su qualsiasi violazione dei dati che possa verificarsi in futuro*», l'obiezione dell'AC IT dimostra chiaramente l'importanza dei rischi per i diritti e le libertà degli interessati in relazione alla quantificazione della sanzione pecuniaria.

181. Pertanto, l'EDPB ritiene che l'obiezione dell'AC IT sia pertinente e motivata e che soddisfi i requisiti dell'articolo 4, paragrafo 24, RGPD. Di conseguenza, l'EDPB valuterà il merito delle questioni sostanziali sollevate da tale obiezione.

8.4.2 Valutazione del merito delle questioni sostanziali sollevate dalle obiezioni pertinenti e motivate

182. L'EDPB ritiene che le obiezioni riscontrate come pertinenti e motivate nella presente sottosezione ([204]) richiedano di valutare se il progetto di decisione propone una sanzione pecuniaria in linea con i criteri stabiliti dall'articolo 83 del RGPD e dalle Linee guida del Gruppo di lavoro articolo 29 riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679 («WP253») (approvate dall'EDPB) ([205]).

183. In effetti, il meccanismo di coerenza può essere utilizzato anche per promuovere un'applicazione coerente delle sanzioni amministrative pecuniarie ([206]): qualora un'obiezione pertinente e motivata contesti gli elementi su cui l'autorità capofila si è basata per quantificare l'importo della sanzione pecuniaria, l'EDPB può incaricare l'autorità capofila di procedere a una nuova quantificazione della sanzione pecuniaria proposta, eliminando le lacune nella determinazione dei nessi causali tra i fatti in questione e il modo in cui la sanzione pecuniaria proposta è stata quantificata sulla base dei criteri di cui all'articolo 83 del RGPD e delle norme comuni stabilite dall'EDPB ([207]). Una sanzione pecuniaria dovrebbe essere effettiva, proporzionata e dissuasiva, come richiesto dall'articolo 83, paragrafo 1, RGPD, tenendo conto dei fatti del caso ([208]). Inoltre, nel decidere l'importo della sanzione pecuniaria, l'autorità capofila tiene conto dei criteri elencati all'articolo 83, paragrafo 2, RGPD.

184. Per quanto riguarda la natura, la gravità e la durata della violazione di cui all'articolo 33, paragrafi 1 e 5, RGPD, l'**articolo 83, paragrafo 2, lettera a), RGPD** impone di tenere conto, tra l'altro, **della natura,**

([203]) Di conseguenza, l'EDPB non prende posizione sul merito di eventuali questioni sostanziali sollevate da tali obiezioni. L'EDPB ribadisce che la sua attuale decisione non pregiudica le valutazioni che il comitato può essere chiamato a effettuare in altri casi, anche con le stesse parti, tenendo conto del contenuto del progetto di decisione pertinente e delle obiezioni sollevate dalle autorità interessate.
([204]) Tali obiezioni sono quelle delle AC AT, DE e IT.
([205]) Linee guida del Gruppo di lavoro articolo 29 riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679, WP253, adottate il 3 ottobre 2017 (approvate dall'EDPB il 25 maggio 2020).
([206]) Cfr. il considerando 150 del RGPD.
([207]) Linee guida relative alla RRO, paragrafo 34.
([208]) Linee guida dell'EDPB relative alle sanzioni amministrative pecuniarie, pag. 7.

dell'oggetto e della finalità del trattamento in questione, nonché **del numero di interessati lesi dal danno** e **del livello del danno** da essi subito.

185. L'EDPB concorda con l'AC IE sul fatto che la violazione da considerare non è la violazione in quanto tale, ma la conformità all'articolo 33, paragrafi 1 e 5, RGPD nel comunicare tale violazione all'autorità di controllo competente e nel documentarla.

186. L'EDPB osserva che l'AC IE tiene conto della natura del trattamento e del numero di interessati lesi dal danno. Per quanto riguarda la **natura del trattamento**, l'AC IE lo descrive come una piattaforma di «microblogging» e social media sulla quale gli utenti hanno la possibilità di documentare le loro opinioni tramite «tweet». L'EDPB ritiene che, nel valutare la natura del trattamento, si debba tenere conto anche del fatto che il «trattamento in questione» riguardava comunicazioni di interessati che avevano deliberatamente scelto di limitare il pubblico di tali comunicazioni. L'EDPB prende atto del fatto che il progetto di decisione dell'AC IE ne ha tenuto conto: «*l'impatto sui singoli utenti e la possibilità che ne derivi un danno dipenderà dal livello dei dati personali resi pubblici e, inoltre, dalla natura di tali dati personali. A questo proposito, nel progetto preliminare si è indicato che, sebbene TIC non abbia confermato l'esatta natura dei dati resi pubblici nella violazione, è ragionevole dedurre che, data l'entità degli utenti interessati e la natura del servizio offerto da TIC, alcuni dei dati personali pubblicati in relazione almeno ad alcuni utenti avranno incluso categorie sensibili di dati e altro materiale particolarmente privato*» ([209]). Tuttavia, l'AC IE, sulla base delle osservazioni di TIC, ha dato meno peso a questo fattore rispetto a quanto gliene avesse dato nel progetto preliminare, dal momento che non vi erano prove dirette di danni ([210]). L'EDPB ritiene tuttavia che l'AC IE, al momento di valutare la natura del trattamento in questione, avrebbe comunque dovuto dare un peso significativo al fatto che tale trattamento riguarda comunicazioni di interessati che hanno deliberatamente scelto di limitarne il pubblico. In particolare, l'AC IE avrebbe dovuto dare un peso significativo a questo fatto, dato che lo ha ricordato nel progetto di decisione, in cui la stessa ha ritenuto che «*l'ampia portata del segmento di utenti interessati dà luogo alla possibilità di uno spettro molto più ampio di danni derivanti dalla violazione, in particolare data la natura del servizio offerto da TIC*» e «*la probabilità che molti utenti si siano affidati alla funzione di mantenere privati i "tweet" per condividere informazioni o punti di vista (nella certezza di trovarsi in quello che ritengono essere un ambiente privato e controllato) che normalmente non renderebbero di pubblico dominio*» ([211]).

187. Inoltre, per quanto riguarda l'oggetto del trattamento in questione in quanto tale, l'AC IE sembra sostituirlo con il numero degli interessati. L'EDPB ritiene che la **natura e l'oggetto del "trattamento**" da prendere in considerazione per determinare la sanzione pecuniaria non sia l'operazione di trattamento consistente nella (accidentale) divulgazione (violazione di dati personali), o la causa della stessa, ma piuttosto l'oggetto del trattamento sottostante effettuato da TIC, come descritto nel paragrafo precedente.

188. Secondo l'**AC AT**, il momento in cui il titolare del trattamento è venuto a conoscenza della violazione ha un impatto sulla gravità della violazione dell'articolo 33, paragrafo 1, RGPD. L'obiezione sollevata dall'AC AT ha espresso un disaccordo su come determinare o valutare il momento in cui il titolare del trattamento deve essere considerato a conoscenza di una violazione dei dati. Più nello specifico, l'AC AT ha sostenuto nella sua obiezione che TIC avrebbe dovuto effettuare una notifica di violazione dei dati entro 72 ore dal momento in cui il responsabile del trattamento è venuto a conoscenza del bug.

([209]) Progetto di decisione, paragrafo 14.51.
([210]) Si veda il paragrafo 150 sopra.
([211]) Progetto di decisione, paragrafo 14.51.

Ciò contribuisce alla valutazione della violazione dell'articolo 33, paragrafo 1, RGPD da parte dell'AC AT come «grave».

189. A questo proposito, l'EDPB ricorda che le Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento 2016/679 («WP250») ([212]), approvate dal comitato, stabiliscono che «*(q)ualsiasi piano di risposta alle violazioni dovrebbe mirare a proteggere le persone fisiche e i loro dati personali. Di conseguenza, la notifica della violazione deve essere vista come uno strumento per migliorare la conformità in materia di protezione dei dati personali*» ([213]).

190. Secondo le Linee guida sulla notifica delle violazioni dei dati personali, un titolare del trattamento deve essere considerato «a conoscenza» nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali ([214]). Poiché il titolare del trattamento si serve del responsabile del trattamento per conseguire le proprie finalità, in linea di principio esso dovrebbe considerarsi «a conoscenza» non appena il responsabile del trattamento gli notifica la violazione ([215]). Tuttavia, il RGPD impone al titolare del trattamento di attuare le misure necessarie per assicurarsi di venire «a conoscenza» di eventuali violazioni in maniera tempestiva in modo da poter adottare le misure appropriate ([216]) e spiega che «*il titolare del trattamento può effettuare una <u>breve</u> indagine per stabilire se la violazione si sia effettivamente verificata. Durante il periodo di indagine il titolare del trattamento non può essere considerato "a conoscenza"*» ([217]). Tuttavia, le Linee guida chiariscono che l'indagine iniziale dovrebbe iniziare il più presto possibile e che un'indagine più dettagliata può quindi seguire ([218]).

191. Le linee guida chiariscono quindi che il titolare del trattamento e, per estensione, il responsabile del trattamento devono agire rapidamente. «Nella maggior parte dei casi queste azioni preliminari dovrebbero essere completate subito dopo l'allerta iniziale (ossia *quando il titolare o il responsabile del trattamento sospetta che si sia verificato un incidente di sicurezza che potrebbe interessare dati personali*)*;* dovrebbe richiedere più tempo soltanto in casi eccezionali» ([219]).

192. Alla luce di quanto precede, l'EDPB concorda con la posizione della valutazione dell'AC IE secondo cui non ci si può aspettare che il titolare del trattamento sia venuto a conoscenza del fatto nel momento in cui il responsabile del trattamento si è reso conto che si era verificato un incidente di sicurezza. Come previsto dalle Linee guida del Gruppo di lavoro articolo 29 sulla notifica delle violazioni dei dati personali, approvate dall'EDPB, occorre un certo grado di certezza che si sia verificata una violazione di dati personali prima che si possa stabilire di esserne a conoscenza. Dai fatti in questione non è chiaro, come risulta dal progetto di decisione, che ciò sia avvenuto prima del 3 gennaio 2019. Nel caso in questione, l'AC AT non ha dimostrato che TIC abbia raggiunto il necessario grado di certezza in merito al fatto che si era verificata una violazione dei dati precedentemente al momento in cui l'AC IE ha ritenuto che TIC fosse «a conoscenza» della violazione. Di conseguenza, l'EDPB ritiene che non sia necessario adeguare la valutazione della gravità della violazione alla luce di una diversa

([212]) Linee guida del Gruppo di lavoro articolo 29 sulla notifica delle violazioni dei dati personali ai sensi del regolamento 2016/679, WP250 rev.01, approvate dall'EDPB (in appresso: «Linee guida sulla notifica delle violazioni dei dati personali»).
([213]) Linee guida sulla notifica delle violazioni dei dati personali, pag. 5.
([214]) Linee guida sulla notifica delle violazioni dei dati personali, pag. 11.
([215]) Linee guida sulla notifica delle violazioni dei dati personali, pag. 14-15.
([216]) Linee guida sulla notifica delle violazioni dei dati personali, pag. 11.
([217]) Linee guida sulla notifica delle violazioni dei dati personali, pag. 12 (corsivo e enfasi aggiunti).
([218]) Linee guida sulla notifica delle violazioni dei dati personali, pag. 12.
([219]) Linee guida sulla notifica delle violazioni dei dati personali, pag. 13 (corsivo aggiunto).

determinazione del momento in cui il titolare del trattamento è venuto a conoscenza della violazione dei dati.

193. Inoltre, per quanto riguarda **la gravità della violazione**, l'EDPB concorda con l'AC IE sul fatto che il rispetto dell'articolo 33, paragrafi 1 e 5, RGPD è fondamentale per il funzionamento complessivo del regime di controllo e di esecuzione.

194. Per quanto riguarda l'obiezione sollevata dall'AC AT in merito alla **natura dolosa della violazione**, l'EDPB ritiene che l'obiezione non abbia dimostrato a sufficienza che, dal momento in cui il titolare del trattamento è venuto a conoscenza della violazione, esso abbia intenzionalmente ignorato il suo dovere di diligenza.

195. Tuttavia, per quanto riguarda la natura colposa della violazione, l'EDPB ritiene che una società per la quale il trattamento dei dati personali è al centro delle attività commerciali dovrebbe disporre di procedure sufficienti per la documentazione delle violazioni dei dati personali, comprese azioni correttive, che le consentano di adempiere anche all'obbligo di notifica ai sensi dell'articolo 33, paragrafo 1, RGPD. Questo elemento implica un ulteriore elemento da prendere in considerazione nell'analisi della gravità della violazione.

196. L'EDPB ricorda che la CGUE ha costantemente sostenuto che una sanzione dissuasiva è una sanzione che ha un **reale effetto deterrente** ([220]). A tale riguardo, si può distinguere tra dissuasione generale (scoraggiare altri dal commettere la stessa violazione in futuro) e dissuasione specifica (dissuadere il destinatario della sanzione pecuniaria dal commettere nuovamente la stessa violazione) ([221]). Inoltre, la severità delle sanzioni deve essere adeguata alla gravità delle violazioni che esse reprimono ([222]). Ne consegue che gli importi delle ammende non devono essere sproporzionati rispetto agli scopi perseguiti, vale a dire rispetto alle norme sulla protezione dei dati e che l'importo dell'ammenda inflitta ad un'impresa deve essere proporzionato all'infrazione, valutata complessivamente, tenendo conto, in particolare, della gravità di quest'ultima ([223]).

197. Sebbene l'autorità capofila nel progetto di decisione facesse riferimento al requisito secondo il quale la sanzione pecuniaria deve essere **dissuasiva e proporzionata**, l'EDPB ritiene che l'autorità capofila non abbia motivato a sufficienza il modo in cui la sanzione pecuniaria proposta risponde a tali requisiti. In particolare, l'EDPB osserva che l'autorità capofila passa dalla quantificazione dell'importo massimo della sanzione pecuniaria (fissato a 60 milioni di dollari) all'indicazione dell'intervallo per la sanzione pecuniaria proposto (compreso tra 150 000 dollari e 300 000 dollari), senza ulteriori spiegazioni su quali elementi particolari abbiano indotto l'autorità capofila a individuare questo intervallo specifico ([224]). Al di là del riferimento generale ai fattori pertinenti di cui all'articolo 83, paragrafo 2, RGPD, non vi è una chiara motivazione per la scelta della percentuale proposta (tra lo 0,25 % e lo 0,5 %) della sanzione pecuniaria massima applicabile ai sensi dell'articolo 83, paragrafo 4, RGPD.

198. A questo proposito, l'EDPB ha illustrato in precedenza le ragioni per cui l'autorità capofila nel progetto di decisione avrebbe dovuto dare maggior peso all'elemento relativo alla natura, all'oggetto e al

([220]) Cfr. conclusioni dell'avvocato generale Geelhoed del 29 aprile 2004 nella sentenza del 12 luglio 2005, Commissione/Francia, C-304/02, EU:C:2005:444, paragrafo 39.
([221]) Cfr., tra l'altro, la sentenza del 13 giugno 2013, Versalis Spa / Commissione, C-511/11, ECLI:EU:C:2013:386, punto 94.
([222]) Sentenza della CGUE del 25 aprile 2013, Asociaţia Accept, C-81/12.
([223]) Tribunale dell'UE, Marine - Harvest, T-704/14, 26 ottobre 2017.
([224]) Progetto di decisione, paragrafi 15.19 e 15.20.

carattere colposo della violazione e ritiene pertanto che l'intervallo della sanzione pecuniaria proposta debba essere adeguato di conseguenza.

8.4.3 Conclusione

199. In seguito a ciò, l'EDPB ritiene che la sanzione pecuniaria proposta nel progetto di decisione sia troppo bassa e non soddisfi quindi la sua finalità di misura correttiva, e che in particolare non soddisfi i requisiti di cui all'articolo 83, paragrafo 1, RGPD di essere efficace, dissuasiva e proporzionata.

200. Pertanto, l'EDPB chiede all'AC IE di riesaminare gli elementi su cui si basa per quantificare l'importo della sanzione pecuniaria fissata ([225]) da infliggere a TIC in modo da garantire che sia adeguata ai fatti del caso.

201. L'EDPB osserva che l'analisi delle obiezioni si limita alla sostanza delle obiezioni da considerare pertinenti e motivate. La portata dell'analisi dell'EDPB relativa alla quantificazione della sanzione pecuniaria è pertanto limitata all'analisi del metodo di quantificazione delle sanzioni pecuniarie in quanto tale. Essa non costituisce una convalida implicita o esplicita da parte dell'EDPB dell'analisi effettuata dall'autorità capofila in merito alla violazione dell'articolo 33, paragrafi 1 o 5, RGPD, o della qualifica giuridica di Twitter Inc. e TIC. L'EDPB ribadisce che la sua attuale decisione non pregiudica le valutazioni che il comitato può essere chiamato a effettuare in altri casi, anche con le stesse parti, tenendo conto del contenuto del progetto di decisione pertinente e delle obiezioni sollevate dalle autorità interessate.

9 DECISIONE VINCOLANTE

202. Alla luce di quanto sopra e in conformità con il compito dell'EDPB ai sensi dell'articolo 70, paragrafo 1, lettera t), RGPD di adottare decisioni vincolanti ai sensi dell'articolo 65 del RGPD, il comitato adotta la seguente decisione vincolante ai sensi dell'articolo 65, paragrafo 1, lettera a), RGPD.

203. <u>In merito alle obiezioni relative alla qualifica del titolare del trattamento e responsabile del trattamento e alla competenza dell'autorità capofila</u>

- L'EDPB decide che l'AC IE non è tenuta a modificare il suo progetto di decisione sulla base delle obiezioni sollevate, in quanto esse non soddisfano i requisiti di cui all'articolo 4, paragrafo 24, RGPD.

204. <u>In merito alle obiezioni relative alle violazioni dell'articolo 33, paragrafi 1 e 5, RGPD rilevate dall'autorità capofila</u>

- In relazione all'obiezione dell'AC FR sull'assenza di una violazione dell'articolo 33, paragrafo 1, RGPD, all'obiezione dell'AC DE sulla determinazione del *dies a quo* per la violazione dell'articolo 33, paragrafo 1, RGPD, e all'obiezione dell'AC IT sulla violazione dell'articolo 33, paragrafo 5, RGPD, l'EDPB decide che l'AC IE non è tenuta a modificare il progetto di decisione sulla base delle obiezioni sollevate, in quanto non soddisfano i requisiti di cui all'articolo 4, paragrafo 24, RGPD.

205. <u>In merito alle obiezioni relative alle possibili violazioni ulteriori (o alternative) del RGPD individuate dalle autorità interessate</u>

([225]) Ciò dovrebbe preferibilmente essere già previsto nel progetto di decisione ai sensi dell'articolo 60 del RGPD.

- In relazione all'obiezione dell'AC DE sulle possibili violazioni dell'articolo 5, paragrafo 1, lettera f), dell'articolo 24 e dell'articolo 32, RGPD e all'obiezione dell'AC IT sulla possibile violazione dell'articolo 5, paragrafo 2, RGPD, l'EDPB decide che, pur soddisfacendo i requisiti di cui all'articolo 4, paragrafo 24, RGPD, l'AC IE non è tenuta a modificare il progetto di decisione perché gli elementi di fatto disponibili inclusi in esso e nelle obiezioni non sono sufficienti a consentire all'EDPB di stabilire l'esistenza di violazioni dell'articolo 5, paragrafo 1, lettera f), e dell'articolo 5, paragrafo 2, dell'articolo 24 e dell'articolo 32, RGPD.

- In relazione all'obiezione dell'AC DE relativa alla possibile violazione dell'articolo 33, paragrafo 3, RGPD, all'obiezione dell'AC FR relativa alla possibile violazione degli articoli 28 e 32 del RGPD, all'obiezione dell'AC HU relativa alla possibile violazione dell'articolo 5, paragrafo 1, lettera f), e degli articoli 32 e 34 del RGPD, nonché all'obiezione dell'AC IT relativa alla possibile violazione dell'articolo 28 del RGPD, l'EDPB decide che l'AC IE non è tenuta a modificare il progetto di decisione sulla base delle obiezioni sollevate in quanto esse non soddisfano i requisiti di cui all'articolo 4, paragrafo 24, RGPD.

206. In merito all'obiezione relativa alla decisione dell'autorità capofila di non rivolgere un ammonimento

- In relazione all'obiezione dell'AC DE in merito alla decisione dell'AC IE di non rivolgere un ammonimento, l'EDPB decide che l'AC IE non è tenuta a modificare il suo progetto di decisione sulla base dell'obiezione sollevata in quanto essa non soddisfa i requisiti di cui all'articolo 4, paragrafo 24, RGPD.

207. In merito all'obiezione relativa alla quantificazione della sanzione pecuniaria suggerita dall'autorità capofila

- In relazione all'obiezione dell'AC HU sulla natura non sufficientemente dissuasiva della sanzione pecuniaria, l'EDPB decide che l'AC IE non è tenuta a modificare il progetto di decisione sulla base dell'obiezione sollevata in quanto essa non soddisfa i requisiti di cui all'articolo 4, paragrafo 24, RGPD.

- In relazione alle obiezioni delle AC AT, DE e IT sulla natura non sufficientemente dissuasiva della sanzione pecuniaria, l'EDPB decide che esse soddisfano i requisiti di cui all'articolo 4, paragrafo 24, RGPD e che l'AC IE è tenuta a rivalutare **gli elementi su cui si basa per quantificare l'importo della sanzione pecuniaria fissata** da infliggere a TIC e a modificare il progetto di decisione aumentando il livello della sanzione pecuniaria per garantire che essa soddisfi la sua finalità di misura correttiva nonché i requisiti di efficacia, dissuasività e proporzionalità stabiliti dall'articolo 83, paragrafo 1, RGPD e tenendo conto dei criteri di cui all'articolo 83, paragrafo 2, RGPD.

10 OSSERVAZIONI FINALI

208. La presente decisione vincolante è destinata all'AC IE e alle autorità interessate. L'AC IE adotta la decisione finale sulla base della presente decisione vincolante ai sensi dell'articolo 65, paragrafo 6, RGPD.

209. Per quanto riguarda le obiezioni ritenute non conformi ai requisiti di cui all'articolo 4, paragrafo 24, RGPD, l'EDPB non prende posizione sul merito di eventuali questioni sostanziali sollevate da tali obiezioni. L'EDPB ribadisce che la sua attuale decisione non pregiudica le valutazioni che il comitato

può essere chiamato a effettuare in altri casi, anche con le stesse parti, tenendo conto del contenuto del progetto di decisione pertinente e delle obiezioni sollevate dalle autorità interessate.

210. Ai sensi dell'articolo 65, paragrafo 6, RGPD, l'AC IE comunica la decisione finale al presidente entro un mese dal ricevimento della decisione vincolante.

211. Una volta effettuata tale comunicazione da parte dell'AC IE, la decisione vincolante sarà resa pubblica ai sensi dell'articolo 65, paragrafo 5, RGPD.

212. Ai sensi dell'articolo 70, paragrafo 1, lettera y), RGPD, l'AC IE comunica la decisione definitiva all'EDPB affinché sia inserita nel registro delle decisioni soggette al meccanismo di coerenza.

Per il comitato europeo per la protezione dei dati

La presidente

(Andrea Jelinek)