Decizia 1/2020 privind litigiul declanșat privind proiectul de decizie al autorității de supraveghere din Irlanda cu privire la Twitter International Company în temeiul articolului 65 alineatul (1) litera (a) din RGPD

Adoptată la 9 noiembrie 2020

Cuprins

Comitetul european pentru protecția datelor,

având în vedere articolul 63 și articolul 65 alineatul (1) litera (a) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (denumit în continuare „**RGPD**”)[1],

având în vedere Acordul privind SEE, în special anexa XI și Protocolul 37 la acesta, astfel cum au fost modificate prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018[2],

având în vedere articolele 11 și 22 din Regulamentul său de procedură[3],

întrucât:

(1) Rolul principal al Comitetului european pentru protecția datelor (denumit în continuare „**CEPD**” sau „**comitetul**”) este de a asigura aplicarea coerentă a RGPD pe întreg teritoriul SEE. În acest sens, din articolul 60 din RGPD rezultă că autoritatea de supraveghere principală (denumită în continuare „**ASP**”) cooperează cu celelalte autorități de supraveghere vizate (denumite în continuare „**ASV**”), în încercarea de a ajunge la un consens, că ASP și ASV își comunică reciproc toate informațiile relevante și că ASP comunică fără întârziere informațiile relevante referitoare la această chestiune celorlalte autorități de supraveghere vizate. ASP transmite fără întârziere un proiect de decizie celorlalte ASV, pentru a obține avizul lor, și ține seama în mod corespunzător de opiniile acestora.

(2) În cazul în care oricare dintre celelalte ASV exprimă o obiecție relevantă și motivată („**ORM**”) la proiectul de decizie, în conformitate cu articolul 4 alineatul (24) și articolul 60 alineatul (4) din RGPD, iar ASP nu intenționează să dea curs ORM sau consideră că obiecția nu este relevantă sau motivată, ASP sesizează mecanismul pentru asigurarea coerenței menționat la articolul 63 din RGPD.

(3) În temeiul articolului 65 alineatul (1) litera (a) din RGPD, CEPD emite o decizie obligatorie cu privire la toate chestiunile care fac obiectul ORM, în special dacă a fost încălcat RGPD.

(4) Decizia obligatorie a CEPD se adoptă cu o majoritate de două treimi a membrilor CEPD, în temeiul articolului 65 alineatul (2) din RGPD coroborat cu articolul 11 alineatul (4) din Regulamentul de procedură al CEPD, în termen de o lună de la decizia președintelui și a autorității de supraveghere privind caracterul complet al dosarului. Acest termen poate fi prelungit cu o lună, ținându-se seama de complexitatea chestiunii, în urma deciziei președintelui din proprie inițiativă sau la cererea a cel puțin o treime dintre membrii CEPD.

(5) În conformitate cu articolul 65 alineatul (3) din RGPD, dacă, în pofida unei astfel de prelungiri, CEPD nu a fost în măsură să adopte o decizie în termenul respectiv, acesta adoptă decizia în termen de două săptămâni de la data expirării prelungirii cu o majoritate simplă a membrilor săi.

[1] JO L 119, 4.5.2016, p. 1.
[2] Referirile la „statele membre” din această decizie trebuie înțelese ca referiri la „statele membre ale SEE”. Referirile la „UE” trebuie înțelese, acolo unde este necesar, ca referiri la „SEE”.
[3] Regulamentul de procedură al CEPD, adoptat la 25 mai 2018, așa cum a fost modificat ultima dată și adoptat la 8 octombrie 2020.

1 REZUMATUL LITIGIULUI

1. Acest document conține o decizie obligatorie adoptată de CEPD în conformitate cu articolul 65 alineatul (1) litera (a) din RGPD. Prezenta decizie se referă la litigiul rezultat în urma unui proiect de decizie (denumit în continuare „**proiectul de decizie**”) emis de autoritatea de supraveghere din Irlanda („Comisia pentru protecția datelor”, denumită în continuare „**AS IE**”, denumită în continuare în acest context și „**ASP**”) și la obiecțiile ulterioare exprimate de o serie de ASV („Österreichische Datenschutzbehörde”, denumită în continuare „**AS AT**”; „Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit”[4], denumită în continuare „**AS DE**”; „Datatilsynet”, denumită în continuare „**AS DK**”; „Agencia Española de Protección de Datos”, denumită în continuare „**AS ES**”; „Commission Nationale de l'Informatique et des Libertés”, denumită în continuare „**AS FR**”; „Nemzeti Adatvédelmi és Információszabadság Hatóság”, denumită în continuare „**AS HU**”; „Garante per la protezione dei dati personali”, denumită în continuare „**AS IT**”; „Autoriteit Persoonsgegevens”, denumită în continuare „**AS NL**”). Proiectul de decizie în cauză se referă la o „anchetă din proprie inițiativă” care a fost inițiată de AS IE în urma **notificării unei încălcări a securității datelor cu caracter personal** din data de 8 ianuarie 2019 („**încălcarea securității**”) de către Twitter International Company, societate cu sediul la Dublin, în Irlanda (denumită în continuare „**TIC**”)[5].

2. Încălcarea securității datelor a rezultat în urma **unei erori în proiectarea Twitter**, din cauza căreia, în cazul în care un utilizator de pe un dispozitiv Android modifica adresa de e-mail asociată contului său de Twitter, mesajele Tweet protejate deveneau neprotejate și, prin urmare, accesibile unui public mai larg (iar nu doar urmăritorilor utilizatorului), fără ca utilizatorul să aibă cunoștință de acest lucru[6]. Eroarea a fost descoperită la 26 decembrie 2018 de către contractantul extern care gestiona „programul de recompense pentru semnalarea erorilor” al societății, acesta fiind un program prin care oricine poate transmite un raport privind o eroare[7].

3. În timpul investigațiilor sale, Twitter a descoperit alte acțiuni ale utilizatorilor care generau același rezultat neintenționat. S-a constatat că eroarea din cod **a avut drept cauză o modificare a codului, efectuată la 4 noiembrie 2014**[8].

4. TIC a informat AS IE că, potrivit celor identificate, între 5 septembrie 2017 și 11 ianuarie 2019, **88 726 de utilizatori din UE și din SEE au fost afectați** de această eroare. Twitter a confirmat că data erorii este 4 noiembrie 2014, însă a confirmat și că poate identifica numai utilizatorii afectați începând din 5 septembrie 2017, din cauza unei politici privind păstrarea datelor, aplicabilă jurnalelor[9]. Prin urmare, TIC a recunoscut posibilitatea ca mai mulți utilizatori să fi fost afectați de încălcarea securității[10].

[4] Obiecția exprimată de AS Hamburg a fost transmisă și cu reprezentarea „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”. De asemenea, obiecția a fost coordonată și cu alte AS din Germania.
[5] Proiectul de decizie, punctele 1.1-1.2.
[6] Proiectul de decizie, punctul 1.9.
[7] Proiectul de decizie, punctele 2.7 și 4.7.
[8] Proiectul de decizie, punctul 2.10.
[9] Proiectul de decizie, punctul 2.10.
[10] Proiectul de decizie, punctele 1.10, 2.10, 14.2 și 14.3.

5. Decizia AS IE de a iniția ancheta a fost luată în situația în care TIC, în formularul său de notificare a încălcării securității, a identificat **impactul potențial asupra persoanelor afectate ca fiind „semnificativ”**.[11]

6. AS IE a afirmat în proiectul de decizie că recunoaște că AS IE este ASP, în sensul RGPD, pentru TIC, în calitate de operator în ceea ce privește prelucrarea transfrontalieră a datelor, efectuată de TIC, care a făcut obiectul încălcării securității[12].

7. Tabelul de mai jos prezintă un rezumat al cronologiei evenimentelor care fac parte din procedura ce a determinat înaintarea chestiunii către mecanismul de asigurare a coerenței:

26.12.2018	Twitter, Inc., societate constituită în USA, primește un raport privind o eroare prin programul său de recompense pentru semnalarea erorilor. Raportul a fost transmis de un contractant terț care gestiona programul de recompense pentru semnalarea erorilor (contractantul 1) către contractantul terț angajat de Twitter, Inc. pentru a căuta și evalua erorile (contractantul 2).
29.12.2018	Contractantul 2 comunică rezultatul companiei Twitter, Inc., printr-un tichet JIRA.
02.01.2019	Echipa de securitate a informațiilor a companiei Twitter, Inc. examinează tichetul JIRA și decide că nu este o chestiune de securitate, dar că ar putea fi o chestiune de protecție a datelor.
02.01.2019	Se transmite o notificare echipei juridice a Twitter Inc..
03.01.2019	Echipa juridică a Twitter, Inc. decide că această chestiune trebuie să fie tratată ca un incident.
04.01.2019	Twitter, Inc. declanșează un **proces de reacție la incident** însă, din cauza unei greșeli în aplicarea procedurii interne, responsabilul cu protecția datelor de la nivel global nu este adăugat ca „observator” la tichet. Prin urmare, acesta nu este notificat.
07.01.2019	Responsabilul cu protecția datelor de la nivel global este notificat cu privire la încălcarea securității datelor în timpul unei ședințe.
08.01.2019	TIC **notifică încălcarea securității** către AS IE, utilizând formularul AS IE de notificare a unei încălcări transfrontaliere a securității.
22.01.2019	Domeniul de aplicare și temeiul juridic al anchetei au fost stabilite în notificarea privind declanșarea anchetei, care a fost transmisă către TIC la 22 ianuarie 2019. AS IE începe ancheta și solicită informații de la TIC.
28.05.2019 până la 21.10.2019	Etapa Raportului de anchetă: - AS IE elaborează un **proiect de raport** și îl transmite către TIC pentru a-i permite acesteia să prezinte observații în legătură cu proiectul de raport de anchetă;

[11] Proiectul de decizie, punctul 2.8.

[12] AS IE a confirmat că evaluarea sa în acest sens a avut la bază atât constatarea sa că (1) TIC, în calitate de furnizor al serviciului Twitter în UE/SEE, este operatorul relevant, cât și (2) că sediul principal al TIC în UE se află la Dublin, în Irlanda, unde TIC ia deciziile privind scopurile și mijloacele de prelucrare a datelor cu caracter personal ale utilizatorilor Twitter din UE/SEE, în conformitate cu articolul 4 alineatul (16) din RGPD. Proiectul de decizie, punctele 2.2-2.3.

	J TIC transmite observațiile în legătură cu proiectul de raport de anchetă; J AS IE solicită clarificări în ceea ce privește observațiile transmise de TIC; J AS IE emite raportul final de anchetă.
21.10.2019	AS IE începe etapa decizională.
11 și 28.11.2019	AS IE corespondează cu TIC și o invită să transmită observații suplimentare în scris.
2.12.2019	TIC transmite observații suplimentare către AS IE, ca răspuns la corespondența transmisă de AS IE în 11 și 28 noiembrie 2019.
14.3.2020	AS IE transmite un **proiect preliminar de decizie** (denumit în continuare „**proiectul preliminar de decizie**") către TIC, concluzionând că TIC a încălcat articolul 33 alineatele (1) și (5) din RGPD; prin urmare, intenționează să emită o mustrare în conformitate cu articolul 52 alineatul (2) din RGPD și o amendă administrativă în conformitate cu articolul 58 alineatul (2) litera (i) și articolul 83 alineatul (2) din RGPD.
27.4.2020	TIC transmite către AS IE observații privind proiectul preliminar de decizie.
27.4.2020 - 22.5.2020	AS IE ia în considerare observațiile TIC în ceea ce privește proiectul preliminar de decizie și își pregătește proiectul de decizie în vederea transmiterii către ASV în conformitate cu articolul 60 din RGPD.
22.5.2020 - 20.6.2020	AS IE transmite proiectul de decizie autorităților de supraveghere vizate în conformitate cu articolul 60 alineatul (3) din RGPD. Câteva autorități de supraveghere vizate (AS AT, AS DE (reprezentată de AS DE-Hamburg), AS DK, AS ES, AS FR, AS HU, AS IT și AS NL) ridică **obiecții** în conformitate cu articolul 60 alineatul (4) din RGPD.
15.7.2020	AS IE emite un memorandum compus în care precizează răspunsurile la aceste obiecții și îl comunică autorităților de supraveghere vizate (denumit în continuare „**memorandumul compus**"). AS IE solicită autorităților de supraveghere vizate relevante să confirme dacă, după ce au luat în considerare poziția AS IE în ceea ce privește obiecțiile, astfel cum au fost stabilite în memorandumul compus, autoritățile de supraveghere vizate intenționează să își mențină obiecțiile.
27 și 28.7.2020	Prin prisma argumentelor înaintate de AS IE în memorandumul compus, AS DK informează AS IE că nu își menține obiecția, iar AS ES informează AS IE că își retrage parțial obiecția. Celelalte ASV (respectiv AS AT, DE, ES, FR, HU, IT și NL), transmit către AS IE confirmarea că își mențin obiecțiile nesoluționate.
19.8.2020	AS IE trimite chestiunea către CEPD, în conformitate cu articolul 60 alineatul (4) din RGPD, inițiind astfel procedura de soluționare a litigiilor în temeiul articolului 65 alineatul (1) litera (a).

8. AS IE a declanșat procedura de soluționare a litigiilor în Sistemul de informare al pieței interne (IMI) la 19 august 2020. În urma trimiterii acestei chestiuni de către ASP la CEPD, în conformitate cu articolul 60 alineatul (4) din RGPD, secretariatul CEPD a evaluat caracterul complet al dosarului în numele președintelui, conform articolului 11 alineatul (2) din Regulamentul de procedură al CEPD. Secretariatul CEPD a contactat AS IE pentru prima oară la 20 august 2020, solicitând depunerea de documente și informații suplimentare în IMI și solicitând AS IE să confirme caracterul complet al dosarului. AS IE a furnizat documentele și informațiile și a confirmat caracterul complet al dosarului la

21 august 2020. O chestiune de importanță deosebită, care a fost examinată de Secretariatul CEPD, a fost dreptul de a fi ascultat, potrivit celor impuse de articolul 41 alineatul (2) litera (a) din Carta drepturilor fundamentale. La 4 septembrie 2020, secretariatul a contactat AS IE cu întrebări suplimentare pentru a confirma dacă TIC a avut posibilitatea de a-și exercita „dreptul de a fi ascultată" cu privire la toate documentele care au fost înaintate comitetului în vederea adoptării deciziei sale. La 8 septembrie 2020, AS IE a confirmat acest lucru și a furnizat documentele justificative în acest sens[13].

9. La 8 septembrie 2020, s-a luat decizia privind caracterul complet al dosarului, aceasta fiind comunicată de secretariatul CEPD tuturor membrilor CEPD.

10. Președintele a decis, în conformitate cu articolul 65 alineatul (3) din RGPD, coroborat cu articolul 11 alineatul (4) din Regulamentul de procedură al CEPD, să prelungească termenul standard de adoptare de o lună cu încă o lună, din cauza complexității chestiunii.

2 CONDIȚII PENTRU ADOPTAREA UNEI DECIZII OBLIGATORII

11. Condițiile generale pentru adoptarea unei decizii obligatorii a comitetului sunt prezentate la articolul 60 alineatul (4) și la articolul 65 alineatul (1) litera (a) din RGPD[14].

2.1 Obiecțiile exprimate de ASV în ceea ce privește un proiect de decizie

12. CEPD constată că ASV au formulat obiecții la proiectul de decizie prin sistemul informațional și de comunicare menționat la articolul 17 din Regulamentul de procedură al CEPD, respectiv Sistemul de informare al pieței interne. Obiecțiile au fost formulate în temeiul articolului 60 alineatul (4) din RGPD.

13. Mai exact, ASV au formulat obiecții cu privire la următoarele chestiuni:

- competența ASP;
- calificarea rolurilor îndeplinite de TIC și, respectiv, Twitter, Inc.;
- încălcările RGPD identificate de ASP;
- existența unor posibile încălcări suplimentare (sau alternative) ale RGPD;
- lipsa unei mustrări;
- calculul amenzii propuse.

14. Fiecare dintre aceste obiecții a fost transmisă în termenul prevăzut la articolul 60 alineatul (4) din RGPD.

2.2 ASP nu dă curs obiecțiilor relevante și motivate la proiectul de decizie sau este de părere că obiecțiile nu sunt relevante sau motivate

[13] Printre documentele transmise de AS IE s-au regăsit e-mailuri de la RPD de la nivel global, prin care se confirmă primirea documentelor relevante.
[14] În conformitate cu articolul 65 alineatul (1) litera (a) din RGPD, comitetul va emite o decizie obligatorie atunci când o autoritate de supraveghere a formulat o obiecție relevantă și motivată la un proiect de decizie al ASP sau când ASP a respins o astfel de obiecție ca nefiind relevantă sau motivată.

15. La 15 iulie 2020, AS IE a furnizat ASV o analiză detaliată a obiecțiilor formulate de autoritățile de supraveghere vizate în memorandumul compus, în care a subliniat dacă a considerat că obiecțiile sunt „relevante și motivate” în conformitate cu articolul 4 alineatul (24) din RGPD și dacă a decis să dea curs oricăror obiecții[15].

16. Mai exact, AS IE a considerat că numai obiecțiile formulate de ASV-uri în ceea ce privește calculul amenzii îndeplinesc cerințele specificate la articolul 4 alineatul (24) din RGPD în măsura în care se referă la conformitatea cu RGPD a măsurii preconizate în raport cu operatorul sau persoana împuternicită de operator și, de asemenea, în măsura în care stabilesc riscurile pe care le prezintă în ceea ce privește drepturile și libertățile fundamentale ale persoanelor vizate[16]. Cu toate acestea, AS IE a concluzionat că nu va da curs obiecțiilor, din motivele prezentate în memorandumul compus și în cele ce urmează.

17. AS IE a considerat că celelalte obiecții exprimate de ASV-uri nu sunt „relevante și motivate” în sensul articolului 4 alineatul (24) din RGPD.

2.3 Concluzie

18. Cauza în discuție îndeplinește toate elementele enumerate la articolul 65 alineatul (1) litera (a) din RGPD, deoarece mai multe ASV-uri au formulat obiecții la un proiect de decizie al ASP în termenul prevăzut la articolul 60 alineatul (4) din RGPD, iar ASP nu a dat curs obiecțiilor sau le-a respins ca nefiind relevante sau motivate.

19. Prin urmare, CEPD are competența de a adopta o decizie obligatorie, care se referă la toate chestiunile vizate de obiecția (obiecțiile) relevantă (relevante) și motivată (motivate), în special la chestiunea privind încălcarea RGPD[17].

20. Toate rezultatele din prezenta decizie nu aduc atingere niciunei evaluări sau decizii obligatorii adoptate în alte cauze de către CEPD, inclusiv cu aceleași părți, acestea depinzând de constatări suplimentare și/sau noi.

3 DREPTUL LA BUNĂ ADMINISTRARE

21. CEPD se supune articolului 41 din Carta drepturilor fundamentale a UE, în special articolului 41 (dreptul la bună administrare). Acesta se regăsește și la articolul 11 alineatul (1) din Regulamentul de procedură al CEPD[18].

22. Decizia CEPD *„se motivează și se adresează autorității de supraveghere principale și tuturor autorităților de supraveghere vizate, fiind obligatorie pentru acestea.”* [articolul 65 alineatul (2) din RGPD]. Aceasta nu își propune să se adreseze direct unei părți terțe. Cu toate acestea, ca măsură de precauție pentru a aborda posibilitatea ca TIC să fie afectată de decizia CEPD, CEPD a evaluat dacă TIC a avut posibilitatea să-și exercite dreptul de a fi ascultată în ceea ce privește procedura desfășurată de

[15] Scopul documentului, potrivit celor declarate de AS IE, a fost de a facilita cooperarea viitoare cu ASV în ceea ce privește proiectul de decizie și de a respecta cerința prevăzută la articolul 60 alineatul (1) din RGPD ca ASP să coopereze cu celelalte autorități de supraveghere vizate, încercând să ajungă la un consens.
[16] Memorandumul compus, punctul 5.59.
[17] Articolul 65 alineatul (1) litera (a) din RGPD. Anumite ASV-uri au prezentat observații, și nu obiecții propriu-zise care, prin urmare, nu au fost luate în considerare de către CEPD.
[18] Regulamentul de procedură al CEPD, adoptat la 25 mai 2018, așa cum a fost modificat ultima dată și adoptat la 8 octombrie 2020.

ASP și în special dacă toate documentele primite în cadrul acestei proceduri și folosite de CEPD pentru a lua o decizie au fost deja comunicate către TIC în prealabil și dacă TIC a fost audiată în acest sens.

23. Având în vedere că TIC a fost deja audiată de AS IE cu privire la toate informațiile primite de CEPD și utilizate pentru adoptarea deciziei sale[19], iar ASP a comunicat CEPD observațiile scrise ale TIC, în conformitate cu articolul 11 alineatul (2) din Regulamentul de procedură al CEPD[20], în ceea ce privește chestiunile formulate în prezentul proiect de decizie, CEPD consideră că articolul 41 din Carta drepturilor fundamentale a UE a fost respectat.

4 DESPRE CALIFICAREA OPERATORULUI ȘI A PERSOANEI ÎMPUTERNICITE DE OPERATOR ȘI COMPETENȚA ASP

4.1 Analiza efectuată de ASP în cadrul proiectului de decizie

24. Proiectul de decizie afirmă că: *„[l]a inițierea anchetei, investigatorul desemnat din cadrul [AS IE] [...] a considerat că TIC este operatorul, în sensul articolului 4 alineatul (7) din RGPD, cu privire la datele cu caracter personal care au făcut obiectul încălcării securității”* și că *„[î]n acest sens, TIC a confirmat că este operatorul”* în formularul de notificare a încălcării securității datelor și în corespondența cu AS IE[21]. În plus, proiectul de decizie afirmă că *„de asemenea, TIC a confirmat că încălcarea securității a apărut în contextul unei prelucrări efectuate în numele său de Twitter Inc., care este persoana împuternicită de operator”*[22] și că *„TIC este operatorul de date pentru datele cu caracter personal care fac obiectul anchetei. TIC are un contract încheiat cu Twitter Inc. (persoana împuternicită de operator) pentru prestarea de servicii de prelucrare a datelor”*[23].

25. În plus, proiectul de decizie specifică faptul că AS IE consideră în continuare că deține și competența de a acționa în calitate de ASP cu privire la prelucrarea transfrontalieră efectuată de TIC în ceea ce privește datele cu caracter personal care au făcut obiectul încălcării securității[24].

26. În acest sens, proiectul de decizie afirmă, de asemenea, că TIC a confirmat pentru AS IE, la notificarea încălcării securității, că este *„societate irlandeză”* și *„furnizorul serviciilor Twitter în Europa”* și că politica TIC privind confidențialitatea (actualizată în ianuarie 2016) informa utilizatorii serviciului Twitter din UE că au dreptul să-și exprime preocupările fie la autoritatea de supraveghere de la nivel local, fie la ASP a TIC, respectiv AS IE[25].

27. De asemenea, AS IE a inclus în proiectul de decizie un extras din Raportul anual și din situațiile financiare ale TIC, referitoare la exercițiul financiar încheiat la 31 decembrie 2018, specificând că *„partea care deține controlul suprem și cel mai mare grup de întreprinderi pentru care se întocmesc*

[19] Proiectul preliminar de decizie al AS IE (14 martie 2020); proiectul de decizie al AS IE (22 mai 2020); obiecțiile și observațiile formulate de ASV-uri (18-20 iunie 2020); memorandumul compus elaborat de AS IE (15 iulie 2020); și celelalte observații și obiecții de la ASV-uri (27-28 iulie 2020).
[20] Regulamentul de procedură al CEPD, adoptat la 25 mai 2018, așa cum a fost modificat ultima dată și adoptat la 8 octombrie 2020.
[21] Proiectul de decizie, punctul 2.2.
[22] Proiectul de decizie, punctul 4.2.
[23] Proiectul de decizie, punctul 4.6.
[24] Proiectul de decizie, punctul 2.3.
[25] Proiectul de decizie, punctul 2.3.

situațiile financiare și din care face parte societatea este Twitter, Inc., o societate constituită în Statele Unite ale Americii și listată la Bursa de Valori de la New York" [26].

28. Inițial, AS IE s-a confruntat cu incertitudini generate de utilizarea termenilor „noi" și „nostru/noastră/noștri/noastre" în formularul de notificare a încălcării securității datelor pentru a se referi alternativ la TIC și la Twitter, Inc. AS IE a solicitat clarificări în acest sens, iar TIC a indicat că angajații TIC și ai Twitter, Inc. folosesc de obicei „noi" și „nostru" în sens larg pentru a face referire la grup după numele său. În plus, TIC a indicat că, deși TIC este operatorul și decide în ceea ce privește scopurile și mijloacele prelucrării datelor, aceasta nu își desfășoară activitatea singură: *„TIC și angajații săi fac parte din [...] Grupul Twitter [...]. Toți angajații Grupului Twitter utilizează aceleași sisteme informatice, respectă aceleași politici generale [...] și colaborează pentru a asigura asistența globală fără întrerupere necesară pentru a menține platforma Twitter funcțională"*[27].

4.2 Rezumatul obiecțiilor formulate de ASV-uri

29. În obiecția sa, **AS ES** afirmă că **proiectul de decizie nu justifică suficient rolul de operator al TIC**. AS ES subliniază că ar trebui să se realizeze o evaluare privind care entitate decide cu adevărat cu privire la scopuri și mijloace, alături de o analiză critică a tuturor faptelor care au avut loc. Potrivit AS ES, elementele care stau la baza proiectului de decizie par să sugereze o concluzie diferită de cea la care a ajuns AS IE. În special, AS ES consideră că deciziile privind scopurile esențiale ale prelucrării datelor sunt luate, de fapt, de către Twitter, Inc. AS ES și-a susținut raționamentul enumerând câțiva factori care, din punctul său de vedere, ar putea sugera că TIC nu decide cu privire la scopuri și mijloace. În primul rând, AS ES a reamintit că TIC este o subsidiară a Twitter, Inc. și a accentuat că, prin urmare, ar fi greu de înțeles cum ar putea TIC *„să emită ordine"* către Twitter, Inc. în ceea ce privește prelucrarea datelor cu caracter personal ale utilizatorilor din SEE. Potrivit AS ES, TIC nu a fost niciodată în situația de a alege independent pe Twitter, Inc. drept persoană împuternicită de operator și nu ar putea să o înlocuiască. În plus, AS ES a susținut că Twitter, Inc. nu pare să acționeze ca persoană împuternicită de operator din cauza *„lipsei unui canal direct"* între cele două societăți în gestionarea cazurilor de încălcare a securității datelor, altul decât trimiterea unui e-mail, cu RPD de la nivel global în copie. În al treilea rând, AS ES a afirmat că nu era clar cum TIC ar fi putut să adopte independent sau să influențeze deciziile care să determine corectarea erorii informatice în sistemul gestionat și controlat de Twitter, Inc. și că mai degrabă Twitter, Inc. a fost cea care a luat decizii referitoare la soluționarea încălcarea securității, ale cărei efecte nu se limitau numai la utilizatorii europeni.

30. De asemenea, **AS NL** a formulat o obiecție referitoare la calificarea legală a TIC și a Twitter, Inc. ca operator și, respectiv, persoană împuternicită de operator. Mai exact, obiecția se referă la modul în care AS IE a susținut că TIC este unicul operator în acest caz și că Twitter, Inc. este o persoană împuternicită de operator, care acționează în numele acesteia. AS NL consideră că evaluarea controlului constituie un aspect fundamental al acestei cauze și, prin urmare, orice concluzie referitoare la rolul de operator, persoană împuternicită de operator sau de operatori asociați trebuie să fie susținută prin dovezi juridice și faptice. În obiecția sa, **AS NL arată în esență că proiectul de decizie nu conține dovezi suficiente pentru a stabili din punct de vedere juridic și faptic rolurile entităților în cauză**, în special pentru a susține concluzia (i) că TIC este (unicul) operator și (ii) că Twitter, Inc. este doar o persoană împuternicită de operator, care acționează potrivit instrucțiunilor furnizate de TIC pentru operarea serviciului global Twitter și/sau în scopurile relevante în această cauză. Potrivit AS NL, ASP trebuie să verifice **dacă declarațiile legale ale organizației și/sau politica sa de confidențialitate corespund activităților sale efective.** AS NL a solicitat AS IE să includă mai multe

[26] Proiectul de decizie, punctul 2.4.
[27] Proiectul de decizie, punctul 4.5.

informații cu privire la factorii care au determinat stabilirea rolurilor și/sau o descriere a acestora chiar în documentul proiectului de decizie. De asemenea, AS NL menționează, ca exemple de factori care trebuie să fie luați în considerare: instrucțiunile transmise de TIC către Twitter, Inc. sau alte dovezi obiective sau indicii practice din operațiunile de zi cu zi, precum și exemple din evidențele scrise, precum acordul privind prelucrarea datelor.

31. În obiecția sa, **AS DE** susține că **relația dintre Twitter, Inc. și TIC nu este o relație operator-persoană împuternicită de operator**, ci, mai degrabă, o relație între operatori asociați. Obiecția în primă instanță are la bază faptul că Twitter, Inc. și TIC nu operează sisteme separate de prelucrare a datelor. Conform AS DE, sistemul de bază operat de Twitter, Inc. este modificat în baza deciziilor luate de TIC și a celor pentru utilizatorii din SEE, în timp ce sistemul principal de prelucrare rămâne la fel. De asemenea, AS DE a evidențiat că toți angajații grupului utilizează același sistem informatic și respectă aceleași politici generale.

32. În final, **AS FR** a formulat o obiecție privind competența AS IE, afirmând că se pare că AS IE a ajuns la concluzia că competențele decizionale privind scopurile și mijloacele prelucrării în cauză sunt exercitate de TIC. Potrivit AS FR, **proiectul de decizie nu indică în mod clar că autoritatea a ținut cont de alte elemente în afara declarațiilor societății TIC pentru a considera că această societate avea competențe decizionale cu privire la prelucrare.** De asemenea, AS FR a specificat că proiectul de decizie nu indică în mod clar dacă la baza competenței autorității se află faptul că societatea TIC trebuie să fie considerată operator sau că TIC trebuie să fie considerată ca fiind sediul principal, conform celor definite la articolul 4 alineatul (16) din RGPD. AS FR a concluzionat că, în starea sa actuală, proiectul de decizie nu previne riscul de alegere a unei instanțe mai favorabile, pe care mecanismul ghișeului unic trebuie să îl evite. AS FR a invitat AS IE să ofere mai multe elemente, care să permită dovedirea faptului că societatea TIC are competențe decizionale privind scopurile și mijloacele prelucrării pentru site-ul de socializare în rețea Twitter.

4.3 Poziția ASP cu privire la obiecții

33. În memorandumul său compus, AS IE a considerat că o obiecție care are la bază rolul sau desemnarea părților în calitate de operator sau persoană împuternicită de operator și/sau competența AS IE *„nu contestă constatarea unei neîndepliniri a obligațiilor și nici măsura preconizată și, prin urmare, nu respectă definiția de la articolul 4 alineatul (24)”* și că aceasta *„nu se încadrează în definiția unei obiecții „relevante și motivate” de la articolul 4 alineatul (24)”*[28]. Cu toate acestea, AS IE a analizat aceste obiecții și, astfel, a prezentat factorii pe care i-a luat în considerare la determinarea statutului TIC de operator și de sediu principal. În acest sens, AS IE a prezentat (în rezumat[29]) faptele și analiza juridică care au determinat-o să ia concluzia în ceea ce privește statutul de operator al TIC, în esență:

- Confirmarea anterioară oferită de Twitter în anul 2015 prin care s-a propus ca TIC din Irlanda să fie operatorul pentru datele cu caracter personal ale utilizatorilor Twitter din UE[30];
- Confirmarea TIC că a fost operatorul pentru datele cu caracter personal afectate de încălcarea securității transmisă către AS IE și pe parcursul anchetei;

[28] Memorandumul compus, punctul 5.39.
[29] Memorandumul compus, punctul 5.35.
[30] În acest sens, memorandumul compus explică faptul că, la 8 aprilie 2015, TIC a informat AS IE că a propus să desemneze societatea TIC din Irlanda în calitate de operator pentru datele cu caracter personal ale utilizatorilor săi din afara SUA și că TIC a notificat acest lucru altor autorități de supraveghere din UE în mai 2015 (punctul 5.15).

- Confirmarea TIC că există un acord privind prelucrarea datelor între aceasta și Twitter, Inc. în calitate de persoană împuternicită de operator, care include prevederile impuse de articolul 28 din RGPD;
- interacțiunile dintre TIC și Twitter, Inc. de după 7 ianuarie 2019, când TIC (prin responsabilul său cu protecția datelor) a luat efectiv cunoștință de încălcarea securității, demonstrând, conform AS IE, că TIC exercita controlul și autoritatea decizională asupra Twitter, Inc. cu privire la activitățile de remediere și notificarea încălcării securității și cu privire la prelucrarea datelor cu caracter personal afectate de încălcarea securității, care a stat la baza acestora; și
- acțiunile Twitter, Inc. atunci când aceasta a fost notificată cu privire la incident de către contractantul 2 care, potrivit AS IE, sprijină, de asemenea, statutul relației dintre cele două entități ca fiind una în care TIC exercita autoritate și avea responsabilități în calitate de operator.

34. Apoi, AS IE a prezentat, în rezumat[31], faptele și analiza juridică care au dus la concluzia că TIC are sediul principal în Irlanda, în esență (în plus față de punctele de mai sus):
    - Desemnarea TIC și declarația sa că este sediu principal;
    - confirmarea TIC în cadrul politicii sale privind confidențialitatea a statutului său de operator relevant pentru datele cu caracter personal ale utilizatorilor Twitter din UE;
    - Sediul central al TIC se află la Dublin, unde are aproximativ 170 de angajați;
    - Angajarea directă de către TIC a unui RPD la nivel global în scopul RGPD, linia de raportare pentru RPD de la nivel global din cadrul TIC și reprezentarea societății TIC de către RPD de la nivel global cu privire la o serie de activități legate de confidențialitate și prelucrarea datelor, inclusiv dreptul de veto privind prelucrarea datelor;
    - supravegherea în trecut și în prezent a TIC de către AS IE, perioadă în care a fost evident că TIC stabilește scopurile și mijloacele pentru care datele cu caracter personal sunt prelucrate în UE.

    AS IE a reiterat că, prin excepție de la răspunsul său privind substanța obiecțiilor formulate în legătură cu chestiunile de competență și/sau desemnarea părților, aceasta nu consideră că obiecțiile privind aceste chestiuni respectă definiția pentru o „obiecție relevantă și motivată” de la articolul 4 alineatul (24) din RGPD. AS IE a afirmat că, pe baza evaluării sale conform căreia aceste chestiuni nu corespund definiției de la articolul 4 alineatul (24) din RGPD și pe baza faptului că a demonstrat o abordare adecvată a chestiunilor privind sediul principal, competența sa, desemnarea operatorului și a persoanei împuternicite de operator în proiectul său de decizie, nu intenționează să dea curs obiecțiilor privind aceste chestiuni[32].

4.4 Analiza CEPD

4.4.1 Evaluarea caracterului relevant și motivat al obiecțiilor

35. CEPD își va începe analiza obiecțiilor formulate evaluând dacă obiecțiile sus-menționate trebuie să fie considerate ca fiind „obiecții relevante și motivate” în sensul articolului 4 alineatul (24) din RGPD.

36. Articolul 4 alineatul (24) din RGPD definește o „obiecție relevantă și motivată” drept o *„obiecție la un proiect de decizie în scopul de a stabili dacă există o încălcare a prezentului regulament sau dacă*

[31] Memorandumul compus, punctul 5.36.
[32] Memorandumul compus, punctul 5.40.

măsurile preconizate în ceea ce privește operatorul sau persoana împuternicită de operator respectă prezentul regulament, care demonstrează în mod clar importanța riscurilor pe care le prezintă proiectul de decizie în ceea ce privește drepturile și libertățile fundamentale ale persoanelor vizate și, după caz, libera circulație a datelor cu caracter personal în cadrul Uniunii"[33].

37. Potrivit celor clarificate în Orientările privind conceptul unei obiecții relevante și motivate, o obiecție trebuie să fie atât „relevantă", cât și „motivată". Pentru ca obiecția să fie „relevantă", trebuie să existe o legătură directă între obiecție și proiectul de decizie și aceasta trebuie să țină cont de posibilitatea existenței unei încălcări a RGPD sau de respectarea RGPD prin măsura preconizată cu privire la operator sau persoana împuternicită de operator[34].

38. Potrivit orientărilor, o obiecție este „motivată" atunci când este coerentă, clară, precisă și detaliată în furnizarea unor clarificări și argumente privind motivul pentru care se propune modificarea deciziei și modul în care ar determina o concluzie diferită[35] și atunci când demonstrează clar semnificația riscurilor pe care le prezintă proiectul de decizie în ceea ce privește drepturile și libertățile fundamentale ale persoanelor vizate și, după caz, libera circulație a datelor cu caracter personal în cadrul Uniunii Europene. Astfel, ASV ar trebui *„să prezinte implicațiile pe care le-ar avea proiectul de decizie asupra valorilor protejate"*, *„oferind suficiente argumente pentru a arăta că aceste riscuri sunt substanțiale și plauzibile"*[36]. Evaluarea riscurilor pe care le prezintă în ceea ce privește drepturile și libertățile persoanelor vizate[37] poate să aibă la bază, printre altele, caracterul adecvat, necesitatea și proporționalitatea măsurilor preconizate[38], precum și posibila reducere a încălcărilor viitoare ale RGPD[39].

39. În ceea ce privește conținutul, obiecția poate să se refere, ca o primă alternativă, la existența unei încălcări a RGPD. În acest caz, aceasta trebuie să explice de ce ASV nu este de acord că activitățile desfășurate de operator sau de persoana împuternicită de operator au determinat încălcarea unei anumite dispoziții a RGPD, precum și despre ce încălcare (încălcări) este vorba mai exact[40]. De asemenea, această obiecție poate să includă un dezacord privind concluziile obținute din constatările investigației (de exemplu, afirmând că respectivele constatări reprezintă o încălcare alta decât/suplimentară față de cele care au fost analizate deja)[41] sau ar putea chiar să identifice deficiențele din proiectul de decizie, justificând necesitatea efectuării unei investigări suplimentare de către ASP[42]. Însă este mai puțin probabil ca acest lucru să se întâmple atunci când obligația ASP de a

[33] RGPD, articolul 4 alineatul (24).
[34] Vezi, de asemenea, Orientările CEPD 9/2020 privind conceptul obiecției relevante și motivate (denumite în continuare „**Orientările privind ORM"**), punctul 12, supuse în prezent consultării publice, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-092020-relevant-and-reasoned-objection_en Orientările au fost adoptate la 8 octombrie 2020, după inițierea anchetei de către AS IE referitoare la această cauză specifică.
[35] Orientările privind ORM, punctele 17 și 20.
[36] Orientările privind ORM, punctul 37.
[37] „Persoanele vizate" ale căror drepturi și libertăți pot fi afectate pot fi atât cele ale căror date cu caracter personal sunt prelucrate de operator/persoana împuternicită de operator, cât și cele ale căror date cu caracter personal pot fi prelucrate în viitor. Orientările privind ORM, punctul 43.
[38] Orientările privind ORM, punctul 42.
[39] Orientările privind ORM, punctul 43.
[40] Orientările privind ORM, punctul 25.
[41] Orientările privind ORM, punctul 27.
[42] Orientările privind ORM, punctul 28 (care specifică, de asemenea, că: „În acest sens, trebuie să se facă o distincție între anchetele din proprie inițiativă, pe de o parte, și investigațiile declanșate de plângerile sau de rapoartele privind încălcările potențiale comunicate de autoritățile de supraveghere în cauză, pe de altă parte").

coopera cu ASV-urile și de a comunica toate informațiile a fost respectată în mod corespunzător în perioada care precedă emiterea proiectului de decizie[43]. În mod alternativ, conținutul obiecției poate să facă referire la conformitatea măsurii cu RGPD în raport cu operatorul sau persoana împuternicită de operator (acțiune corectivă sau de alt tip) avută în vedere în proiectul de decizie, explicând de ce măsura prevăzută nu corespunde RGPD[44].

40. CEPD consideră că este posibil ca o obiecție privind existența unei încălcări a RGPD să vizeze absența sau insuficiența unei evaluări sau a unei motivări (cu consecința că concluzia din proiectul de decizie nu este susținută în mod adecvat de evaluarea efectuată și de dovezile prezentate, conform celor impuse de articolul 58 din RGPD), dacă sunt îndeplinite toate condițiile din articolul 4 alineatul (24) din RGPD și dacă există o legătură între analiza care se presupune că este insuficientă și existența unei încălcări a RGPD sau dacă măsura preconizată respectă RGPD[45].

41. CEPD consideră că o obiecție privind rolul sau desemnarea părților poate corespunde definiției unei obiecții „relevante și motivate" în temeiul articolului 4 alineatul (24) din RGPD, deoarece aceasta poate să afecteze stabilirea existenței unei încălcări a acestui regulament sau a respectării acestui regulament de către măsura preconizată în ceea ce privește operatorul sau persoana împuternicită de operator. Cu toate acestea, CEPD consideră că o obiecție privind competența autorității de supraveghere care acționează în calitate de ASP nu trebuie formulată printr-o obiecție în temeiul articolului 60 alineatul (4) din RGPD și nu intră în domeniul de aplicare al articolului 4 alineatul (24) din RGPD[46].

a) Evaluarea obiecției formulate de AS NL

42. Obiecțiile formulate de AS NL în primă instanță se referă la *„absența sau insuficiența evaluării sau a motivării"* [47] care duce la concluziile AS IE în ceea ce privește calificarea legală a TIC și a Twitter, Inc. Astfel cum semnalează AS NL, evaluarea controlului este, într-adevăr, un aspect fundamental al cauzei. O altă concluzie în ceea ce privește calificarea TIC și a Twitter, Inc. ar afecta concluziile autorității de supraveghere, atât în ceea ce privește stabilirea unei încălcări a articolului 33 din RGPD, cât și în ceea ce privește decizia privind măsurile de remediere rezultate în urma investigației.

43. CEPD reamintește că fiecare măsură obligatorie adoptată de o autoritate de supraveghere trebuie să prezinte motivele care stau la baza acesteia[48]. Stabilirea existenței unei încălcări a acestui regulament sau a respectării regulamentului prin măsura vizată în raport cu operatorul sau cu persoana împuternicită de operator se bazează pe identificarea corectă a rolurilor părților care vor face obiectul măsurii. Prin urmare, un proiect de decizie trebuie să conțină suficiente elemente juridice și faptice

[43] Orientările privind ORM, punctul 27.
[44] Orientările privind ORM, punctul 33. Aceasta înseamnă că obiecția poate, printre altele, să conteste elementele care stau la baza calculării valorii amenzii (Orientările privind ORM, punctul 34).
[45] Orientările privind ORM, punctul 29.
[46] Procedura în temeiul articolului 65 alineatul (1) litera (b) din RGPD este aplicabilă în acest caz și poate fi inițiată în orice etapă - Orientările privind ORM, punctul 31.
[47] Orientările privind ORM, punctul 29. O obiecție relevantă și motivată referitoare la existența unei încălcări a RGPD poate viza *„informații faptice insuficiente sau descriere insuficientă privind cauza în discuție",* un *„dezacord privind concluziile care urmează să fie extrase din constatările investigației"*(Orientările privind ORM, punctul 27) sau se poate referi la *„absența sau insuficiența evaluării sau a motivării (cu consecința că concluzia din proiectul de decizie nu este sprijinită în mod adecvat de evaluarea efectuată și de dovezile prezentate, astfel cum se impune la articolul 58 din RGPD)"* (Orientările privind ORM, punctul 29).
[48] Considerentul (129) din RGPD.

care să sprijine decizia propusă[49]. Drept rezultat, CEPD consideră că obiecția formulată de AS NL se referă atât la „existența unei încălcări a RGPD sau la lipsa unei astfel de încălcări", cât și la „conformitatea sau neconformitatea măsurii preconizate cu RGPD".

44. Deși CEPD consideră că obiecția AS NL este, prin urmare, relevantă, și include argumente juridice care îi susțin poziția, acesta nu oferă argumente cu privire la modul în care aceste consecințe ar prezenta riscuri semnificative pentru drepturile și libertățile persoanelor vizate și/sau libera circulație a datelor[50]. CEPD reamintește că obligația de a demonstra în mod clar semnificația riscului prezentat de proiectul de decizie - stabilit de RGPD - revine ASV[51]. Deși posibilitatea ca ASV-urile să ofere o astfel de demonstrație poate depinde și de gradul de detaliu al proiectului de decizie în sine și de schimburile anterioare de informații[52], o astfel de situație, dacă este cazul, nu poate exonera complet ASV de obligația de a indica în mod clar de ce consideră că proiectul de decizie, dacă ar rămâne neschimbat, generează riscuri semnificative pentru drepturile și libertățile persoanelor.

45. CEPD constată că obiecția formulată de AS NL nu demonstrează în mod clar riscurile pentru drepturile și libertățile persoanelor ca atare. Pe acest temei, CEPD consideră că obiecția formulată de AS NL nu îndeplinește cerințele articolului 4 alineatul (24) din RGPD.

b) Evaluarea obiecției formulate de AS ES

46. Obiecția formulată de AS ES contestă, de asemenea, suficiența evaluării sau a motivării în raport cu concluziile AS IE în ceea ce privește calificarea legală a TIC și, respectiv, a Twitter, Inc. De asemenea, obiecția clarifică faptul că o calificare corectă a TIC și Twitter, Inc. este esențială pentru determinarea responsabilităților lor, precum și pentru competența AS IE. Drept rezultat, CEPD consideră, de asemenea, că obiecția formulată de AS ES se referă atât la „existența unei încălcări a RGPD sau la lipsa unei astfel de încălcări", cât și la „conformitatea sau neconformitatea măsurii preconizate cu RGPD". Obiecția AS ES indică și de ce aceasta consideră că este necesară o modificare a Proiectului de decizie, precum și modul în care modificarea ar duce la o concluzie diferită.

47. Deși CEPD consideră că obiecția AS ES este, prin urmare, relevantă, și cuprinde argumente juridice care îi susțin poziția, acesta nu exprimă clar motivul pentru care, în cazul în care ar rămâne nemodificată în acest sens, decizia ar prezenta riscuri semnificative pentru drepturile și libertățile persoanelor vizate și, dacă este cazul, pentru libera circulație a datelor. Pe această bază, CEPD consideră că obiecția formulată de AS ES nu îndeplinește cerințele expuse la articolul 4 alineatul (24) din RGPD.

c) Evaluarea obiecției formulate de AS DE

48. Dacă obiecțiile exprimate de AS NL și ES se referă în primul rând la o „absență a motivării", justificând concluzia că TIC acționează ca operator (unic), AS DE nu este de acord în ceea ce privește concluziile care urmează să fie extrase din constatările investigației[53]. În special, AS DE consideră că elementele faptice incluse în dosar sunt suficiente pentru justificarea concluziei că Twitter, Inc. nu se califică drept persoană împuternicită de operator ci mai degrabă drept operator asociat, împreună cu TIC.

49. În obiecția sa, AS DE prezintă și motivele pentru care calificarea părților este relevantă pentru a se stabili „dacă există sau nu o încălcare". În special, AS DE susține că evaluarea juridică a relației dintre

[49] De asemenea, aceste informații sunt necesare pentru a asigura eficacitatea mecanismului de cooperare și de coerență, astfel încât să le ofere ASV-urilor posibilitatea de a lua o decizie în cunoștință de cauză cu privire la un acord sau dezacord sau la formularea unei obiecții relevante și motivate.
[50] Orientările privind ORM, punctul 19.
[51] Orientările privind ORM, punctele 36 și articolul 4 alineatul (24) din RGPD.
[52] Orientările privind ORM, punctul 36.
[53] Orientările privind ORM, punctul 27.

Twitter, Inc. și TIC afectează stabilirea momentului în care s-a luat cunoștință de încălcarea securității. Conform AS DE, cunoașterea trebuie să fie atribuită în mod egal ambilor operatori (asociați) în temeiul articolului 26 alineatul (1) din RGPD. Ținând cont de aceasta, AS DE susține că data relevantă la care TIC, în calitate de operator asociat, a luat cunoștință (sau mai degrabă ar fi trebuit să ia cunoștință) trebuie să fie reexaminată de AS IE.

50. CEPD consideră că obiecția formulată de AS DE indică în mod clar de ce modificarea Proiectului de decizie este considerată necesară și modul în care obiecția, dacă i s-ar da curs, ar duce la o concluzie diferită. Acestea fiind spuse, CEPD nu consideră că obiecția formulată de AS DE include o afirmație clară referitoare la riscurile pe care le prezintă Proiectul de decizie în ceea ce privește drepturile și libertățile fundamentale ale persoanelor vizate în raport cu calificarea părților ca atare. Pe această bază, CEPD consideră că obiecția formulată de AS DE nu îndeplinește cerințele expuse la articolul 4 alineatul (24) din RGPD.

d) Evaluarea obiecției formulate de AS FR

51. În esență, AS FR consideră, de asemenea, că Proiectul de decizie suferă de „absența sau insuficiența evaluării sau a motivării" prin faptul că nu indică în mod clar că AS IE a luat în considerare alte elemente în afară de afirmațiile proprii ale TIC pentru a examina dacă TIC a exercitat competențe decizionale asupra prelucrării. Asemenea AS NL și AS ES, AS FR subliniază și importanța motivării suficiente a deciziei ASP. Cu toate acestea, spre deosebire de AS NL și AS ES, AS FR se concentrează, în obiecția sa, în primul rând asupra importanței includerii motivării respective în stabilirea competenței unei autorități a ASP, în special în vederea prevenirii alegerii unei instanțe mai favorabile.

52. CEPD reamintește că un dezacord privind competența autorității de supraveghere care acționează în calitate de ASP de a emite o decizie într-un anumit caz nu trebuie semnalat printr-o obiecție în temeiul articolului 60 alineatul (4) din RGPD și nu intră în domeniul de aplicare a articolului 4 alineatul (24) din RGPD[54]. CEPD consideră că obiecția formulată de AS FR nu prezintă argumente suficiente pentru a demonstra clar semnificația riscurilor pentru drepturile și libertățile persoanelor vizate pe care le prezintă proiectul de decizie. Prin urmare, CEPD consideră că obiecția formulată de AS FR nu constituie o obiecție relevantă și motivată în sensul articolului 4 alineatul (24) din RGPD.

4.4.2 Concluzie

53. CEPD consideră că obiecțiile sus-menționate îndeplinesc câteva dintre criteriile articolului 4 alineatul (24) din RGPD. Spre deosebire de concluzia AS IE, CEPD consideră că fiecare dintre obiecțiile respective îndeplinea condiția de a se referi în mod alternativ la existența sau inexistența unei încălcări a acestui regulament sau la conformitatea cu regulamentul a măsurii preconizate în raport cu operatorul sau cu persoana împuternicită de operator. În plus, CEPD consideră că o obiecție care are la bază rolul sau desemnarea părților poate să respecte în principiu definiția obiecției „relevante și motivate" de la articolul 4 alineatul (24) din RGPD.

54. Cu toate acestea, potrivit afirmațiilor de mai sus, obiecțiile sus-menționate nu îndeplinesc condiția de a oferi o demonstrație clară în ceea ce privește semnificația riscurilor prezentate de proiectul de decizie în ceea ce privește drepturile și libertățile fundamentale ale persoanelor vizate și, dacă este cazul, libera circulație a datelor cu caracter personal în Uniunea Europeană.

[54] Orientările privind ORM, punctul 31. Orientările continuă prin a afirma că, spre deosebire de obiecția în temeiul articolului 60 alineatul (4) din RGPD, procedura în temeiul articolului 65 alineatul (1) litera (b) din RGPD este aplicabilă în orice etapă.

55. În plus, cu privire la obiecția sus-menționată, formulată de AS FR, pe lângă faptul că nu oferă suficiente argumente pentru a demonstra în mod clar semnificația riscurilor pentru drepturile și libertățile persoanelor vizate pe care le prezintă proiectul de decizie, obiecția se referă la un dezacord privind competența autorității de supraveghere care îndeplinește rolul de ASP. CEPD reamintește că un astfel de dezacord nu trebuie formulat printr-o obiecție în temeiul articolului 60 alineatul (4) din RGPD și nu intră în domeniul de aplicare al articolului 4 alineatul (24) din RGPD[55].

56. În consecință, CEPD consideră că obiecțiile sus-menționate nu îndeplinesc cerințele expuse la articolul 4 alineatul (24) din RGPD.

57. În consecință, **CEPD nu se pronunță cu privire la fondul oricărora dintre chestiunile semnificative semnalate de aceste obiecții. CEPD reiterează că decizia sa actuală nu aduce atingere evaluărilor care pot fi solicitate CEPD în alte cauze, inclusiv cu aceleași părți, ținând cont de conținutul proiectului de decizie relevant și de obiecțiile formulate de ASV-uri.**

5 DESPRE ÎNCĂLCĂRILE RGPD CONSTATATE DE ASP

5.1 Despre constatările privind o încălcare a articolului 33 alineatul (1) din RGPD

5.1.1 Analiza efectuată de ASP în cadrul proiectului de decizie

58. AS IE a concluzionat că TIC nu și-a îndeplinit obligațiile în calitate de operator în temeiul articolului 33 alineatul (1) din RGPD, care „nu pot fi luate în considerare izolat și trebuie să fie înțelese în contextul obligațiilor mai ample care le revin operatorilor în temeiul RGPD, în special obligația privind responsabilitatea, în temeiul articolului 5 alineatul (2), relația dintre operatori și persoanele împuternicite de operatori (articolul 28) și obligația de a pune în aplicare măsuri tehnice și organizatorice adecvate (și eficace)”[56].

59. În ceea ce privește momentul în care operatorul a luat cunoștință de încălcarea securității, proiectul de decizie a concluzionat că, în cazul în care persoana împuternicită de operator face obiectul încălcării securității, operatorul ia cunoștință când este notificat cu privire la încălcarea securității de către persoana împuternicită de operator[57], însă operatorul trebuie să se asigure că a pus în aplicare suficiente măsuri pentru a facilita această conștientizare[58]. Deoarece TIC, în calitate de operator, avea răspunderea de a supraveghea operațiunile de prelucrare efectuate de persoana împuternicită de operator, Twitter, Inc.[59], proiectul de decizie a afirmat că, dacă persoana împuternicită de operator nu respectă procedura sau procedura eșuează într-un alt mod, operatorul nu își poate scuza propria întârziere în transmiterea notificării prin vina persoanei împuternicite de operator[60], întrucât respectarea obligației operatorului de a notifica nu poate depinde de respectarea de către persoana

[55] Orientările privind ORM, punctul 31.
[56] Proiectul de decizie, punctul 6.20. Vezi, de asemenea, Proiectul de decizie, punctele 6.5, 6.7 și 6.13. Proiectul de decizie (punctul 7.129 subpunctul (i)) afirmă, de asemenea, că *„cerința de la articolul 33 alineatul (1) [...] se bazează pe faptul că operatorul se asigură că deține sistemele și procedurile interne (și, dacă este cazul, sistemele și procedurile puse în aplicare la orice alte părți externe, inclusiv la persoanele împuternicite de operatori) care sunt configurate și respectate în așa fel încât să faciliteze conștientizarea fără întârziere și notificarea în timp util a situațiilor de încălcare a securității”.*
[57] Proiectul de decizie, punctul 7.129 subpunctul (iii).
[58] Proiectul de decizie, punctul 7.98.
[59] Proiectul de decizie, punctul 7.129 subpunctul (iv).
[60] Proiectul de decizie, punctul 7.129 subpunctul (iv).

împuternicită de operator a obligațiilor sale în temeiul articolului 33 alineatul (2) din RGPD[61]. AS IE a constatat că, în aceste situații, trebuie să se considere că operatorul are cunoștință în mod constructiv de încălcarea securității datelor cu caracter personal prin persoana împuternicită de operator[62] și că o astfel de interpretare reflectă responsabilitatea și răspunderea operatorului din RGPD[63].

60. Prin urmare, conform proiectului de decizie, TIC a luat efectiv cunoștință de încălcarea securității la 7 ianuarie 2019 [64], dar ar fi trebuit să aibă cunoștință de încălcarea securității cel puțin de la data de 3 ianuarie 2019, deoarece, la data respectivă, Twitter, Inc., în calitate de persoană împuternicită de operator, a evaluat pentru prima oară incidentul ca fiind o potențială încălcare a securității datelor, iar echipa juridică a Twitter, Inc. a transmis instrucțiuni ca incidentul să fie deschis[65]. De asemenea, proiectul de decizie a afirmat că, și în circumstanțele specifice ale acestei situații (unde apăruseră întârzieri și înainte)[66], acordurile stabilite cu Twitter, Inc. ar fi trebuit să permită acest lucru[67]. În schimb, din cauza „ineficacității procesului", în „circumstanțele specifice" ale cazului în discuție și/sau a „nerespectarea de către personalul [persoanei împuternicite de operator] a procesului său de gestionare a incidentelor", a existat o întârziere, care a determinat notificarea operatorului numai la 7 ianuarie 2019[68]. Acest lucru a determinat încălcarea articolului 33 alineatul (1) din RGPD, chiar dacă au trecut mai puțin de 72 de ore între momentul în care TIC a luat de fapt cunoștință de încălcarea securității (7 ianuarie 2019) și notificare (8 ianuarie 2019).

5.1.2 Rezumatul obiecțiilor formulate de ASV-uri

61. **AS FR** a formulat o obiecție în care a afirmat că constatările nu corespund unei încălcări a articolului 33 alineatul (1) din RGPD, ci mai degrabă a articolului 28 sau a articolului 32 din RGPD, care stabilește obligațiile operatorului atunci când acesta decide să recurgă la o persoană împuternicită de operator. Acest argument se bazează pe faptul că constatarea încălcării articolului 33 alineatul (1) are la bază în principal erorile în aplicarea procedurii stabilite între TIC și persoana împuternicită de operator în cazul unei încălcări a securității datelor, în timp ce articolul 33 alineatul (1) din RGPD se referă numai la obligația operatorului de a notifica situațiile de încălcare a securității către autoritatea competentă.

[61] Proiectul de decizie, punctul 7.129 subpunctul (x).
[62] Proiectul de decizie, punctul 7.129 subpunctul (v).
[63] Proiectul de decizie, punctul 7.98. Conform Proiectului de decizie, o interpretare alternativă, care a determină aprecierea că un operator are „cunoștință" numai când este informat de persoana împuternicită de operator, lasă o lacună semnificativă în protecția oferită de RGPD, întrucât aceasta ar putea avea drept rezultat evitarea responsabilităților, chiar și în cazul unor întârzieri majore, dacă acesta a demonstrat că și-a îndeplinit obligațiile de a alege o persoană împuternicită de operator și de a deține sistemele adecvate, însă aceste sisteme nu au fost luate în considerare de persoana împuternicită de operator (Proiectul de decizie, punctul 7.99). De asemenea, AS IE a subliniat în proiectul de decizie că „aplicarea alternativă a articolului 33 alineatul (1) și cea sugerată de TIC, prin care îndeplinirea obligației unui operator de a transmite o notificare depinde, în esență, de respectarea de către persoana împuternicită de operator a obligațiilor sale în temeiul articolului 33 alineatul (2), ar periclita eficacitatea obligațiilor din articolul 33 care revin unui operator [și că] [o] astfel de abordare ar contraveni scopului general al RGPD și intenției organului legislativ al Uniunii".
[64] Proiectul de decizie, punctul 7.129 (vi).
[65] Proiectul de decizie, punctul 7.129 (vi).
[66] Pentru identificarea datei de 3 ianuarie 2019 ca fiind data la care TIC ar fi trebuit să aibă cunoștință de încălcarea securității, AS IE a luat în considerare și faptul că se produsese o întârziere și înainte, în perioada de la data la care incidentul a fost notificat pentru prima oară de Contractantul extern (Contractantul 2) către Twitter, Inc. la 29 decembrie 2018 până când Twitter, Inc. a început examinarea acestuia, la 2 ianuarie 2019. TIC a confirmat, în timpul anchetei, că acest lucru *„s-a datorat programului din perioada sărbătorilor de iarnă"*.
[67] Proiectul de decizie, punctul 7.129 (ix).
[68] Proiectul de decizie, punctul 7.129 (vi).

62. În schimb, obiecțiile **AS DE** s-au concentrat asupra motivării care a generat concluzia că a fost încălcat articolul 33 alineatul (1) din RGPD, fără a contesta această concluzie în sine, și s-au referit mai specific la determinarea *dies a quo* pentru termenul de 72 de ore.

63. AS DE a susținut, în obiecția sa, că aspectul alocării rolurilor afectează determinarea momentului în care se ia cunoștință de încălcarea securității, deoarece cunoașterea unei încălcări a securității trebuie să fie atribuită în mod egal ambilor operatori asociați. Potrivit AS DE, aceasta poate duce la aprecierea că data de 26 decembrie 2018 este data la care TIC, în calitate de operator asociat a luat cunoștință/ar fi trebuit să ia cunoștință de încălcarea securității.

5.1.3 Poziția ASP cu privire la obiecții

64. În ceea ce privește obiecția formulată de AS FR, AS IE consideră că aceasta impune luarea în considerare a unor dispoziții alternative ale RGPD și că solicitarea ASV de a lua în considerare dispozițiile alternative ale RGPD ar urmări în esență să restabilească domeniul de aplicare al anchetei desfășurate[69]: AS IE a concluzionat că o astfel de obiecție nu respectă definiția obiecției relevante și motivate în sensul articolului 4 alineatul (24) din RGPD[70]. De asemenea, AS IE a subliniat că, din punctul său de vedere, s-a produs o încălcare a articolului 33 alineatul (1) din RGPD și nu a propus să se ia în considerare încălcările oricăror alte dispoziții ale RGPD ca alternativă la articolul 33 alineatul (1)[71], subliniind că extinderea seriei de încălcări la alte obligații din cadrul RGPD, la cererea ASV, *„ar pune în pericol ancheta în ansamblu și procesul desfășurat în temeiul articolului 60, expunând-o la riscul de invocare a inechității procedurale”*[72]. De asemenea, AS IE a evidențiat că examinează respectarea de către TIC a obligațiilor sale mai ample în temeiul RGPD în contextul unei alte anchete în curs[73].

65. În ceea ce privește obiecția formulată de AS DE, cu referire specială la stabilirea momentului în care s-a luat cunoștință de încălcarea securității, AS IE a arătat că, și dacă ar fi existat o relație de control comun (un punct de vedere pe care, potrivit celor descrise în secțiunea 4.3~~4.3~~, AS IE nu îl împărtășea), acest lucru nu ar însemna neapărat că cunoașterea încălcării securității ar putea fi atribuită în mod egal ambilor operatori asociați[74].

Formatted: Font color: Black

5.1.4 Analiza CEPD

5.1.4.1 Evaluarea caracterului relevant și motivat al obiecțiilor

66. Astfel cum se reamintește mai sus (vezi secțiunea 4.4.1), este necesar să se evalueze dacă obiecțiile formulate de ASV-uri îndeplinesc condițiile stabilite de articolul 4 alineatul (24) din RGPD.

67. Deși obiecția **AS FR** este relevantă, întrucât subliniază un dezacord cu privire la producerea unei anumite încălcări a RGPD în acest caz specific și include argumente juridice care sprijină obiecția, nu îndeplinește standardul din articolul 4 alineatul (24) din RGPD, deoarece nu include justificări privind consecințele emiterii unei decizii fără modificările propuse în obiecție și privind modul în care aceste consecințe ar prezenta riscuri semnificative pentru drepturile și libertățile persoanelor vizate[75]. Astfel,

[69] Memorandumul compus, punctul 5.45.
[70] Memorandumul compus, punctul 5.45.
[71] Memorandumul compus, punctul 5.47.
[72] Memorandumul compus, punctul 5.44 (c).
[73] Memorandumul compus, punctul 5.44 (d).
[74] Memorandumul compus, punctul 5.34 (care face referire și la hotărârea CJUE în cauza *Wirtschaftsakademie*, C-210/16, punctul 43).
[75] Orientările privind ORM, punctul 19.

nu se poate spune că obiecția „demonstrează în mod clar" importanța riscurilor pe care le prezintă emiterea proiectului de decizie (dacă acesta ar fi emis în formă finală), întrucât nu oferă argumente suficiente cu privire la motivul pentru care aceste drepturi și libertăți ale persoanelor vizate, ținându-se cont în mod special de constatarea unei încălcări a articolului 33 alineatul (1) (în locul articolului 32/28) din RGPD, sunt semnificative și plauzibile[76]. Prin urmare, CEPD concluzionează că obiecția **AS FR** nu este relevantă și motivată din cauza lipsei unei demonstrații clare a riscurilor, potrivit celor impuse în mod specific de articolul 4 alineatul (24) din RGPD.

68. În plus, în ceea ce privește obiecția **AS DE**, în mod specific cu privire la faptul că determinarea *dies a quo* pentru încălcarea articolului 33 alineatul (1) din RGPD depinde de calificarea părților, CEPD ar dori să reamintească de analiza efectuată mai sus în secțiunea 4.4 și constată că obiecția nu prezintă implicațiile pe care le-ar avea proiectul de decizie, cu conținutul său actual, - în special cu privire la motivarea care stă la baza constatării unei încălcări a securității din articolul 33 alineatul (1) din RGPD - în ceea ce privește valorile protejate[77] (drepturile și libertățile persoanelor vizate sau, dacă este cazul, libera circulație a datelor cu caracter personal).

5.1.4.2 Concluzie

69. CEPD consideră că obiecțiile menționate mai sus au îndeplinit condiția de a se referi în mod alternativ la existența sau inexistența unei încălcări a prezentului regulament sau la respectarea sau nerespectarea prezentului regulament prin măsurile preconizate în ceea ce privește operatorul sau persoana împuternicită de operator, dar acestea nu demonstrează în mod clar importanța riscurilor pe care le prezintă proiectul de decizie în ceea ce privește drepturile și libertățile fundamentale ale persoanelor vizate și, după caz, libera circulație a datelor cu caracter personal în cadrul Uniunii Europene.

70. Prin urmare, obiecțiile AS FR și DE nu îndeplinesc cerințele din articolul 4 alineatul (24) din RGPD[78].

5.2 Despre constatările privind o încălcare a articolului 33 alineatul (5) din RGPD

5.2.1 Analiza efectuată de ASP în cadrul proiectului de decizie

71. În proiectul de decizie, AS IE a constatat că TIC nu și-a respectat obligațiile în temeiul articolului 33 alineatul (5) din RGPD pentru a documenta încălcarea securității, deoarece nu s-a considerat că documentația furnizată de TIC pe parcursul anchetei conține informații suficiente și nu s-a considerat că aceasta conține o evidență sau un document specific de „încălcare a securității datelor cu caracter personal", întrucât acestea reprezintă „o documentație cu un caracter mai general" [79].

72. În altă ordine de idei, AS IE a recunoscut că TIC a cooperat pe deplin pe perioada anchetei (deși acest lucru nu a fost considerat circumstanță atenuantă)[80].

[76] Orientările privind ORM, punctul 37.
[77] Orientările privind ORM, punctul 37.
[78] În consecință, CEPD nu se pronunță cu privire la fondul chestiunilor semnificative semnalate de aceste obiecții. CEPD reiterează că decizia sa actuală nu aduce atingere evaluărilor care pot fi solicitate CEPD în alte cauze, inclusiv cu aceleași părți, ținând cont de conținutul proiectului de decizie relevant și de obiecțiile formulate de ASV-uri.
[79] Proiectul de decizie, punctul 10.46.
[80] Proiectul de decizie, punctul 14.50.

5.2.2 Rezumatul obiecțiilor formulate de ASV-uri

73. CEPD profită de ocazie pentru a evidenția, din motive de claritate, faptul că niciuna dintre obiecțiile formulate nu contesta concluzia că TIC a încălcat articolul 33 alineatul (5) din RGPD.

74. Cu toate acestea, **AS IT** a formulat o obiecție, susținând că constatarea referitoare la încălcarea articolului 33 alineatul (5) din RGPD nu pare să fie consecventă cu motivarea și cu elaborările prezentate de ASP, deoarece se presupune că inadecvarea documentației întocmite pe parcursul unei investigații atât de ample, având la bază multiple interacțiuni între ASP și operator, semnalează cooperarea slabă a operatorului cu APD. Conform AS IT, constatarea din proiectul de decizie potrivit căreia TIC a oferit cooperare deplină în faza de investigație trebuie să fie revizuită, întrucât se poate considera că această cooperare deplină există numai dacă operatorul pune la dispoziție documentație adecvată și exhaustivă, în mod direct.

5.2.3 Poziția ASP cu privire la obiecții

75. AS IE este de părere că obligația în temeiul articolului 33 alineatul (5) din RGPD se aplică independent de obligația în temeiul articolului 31 din RGPD de a coopera cu autoritatea de supraveghere și de comportamentul TIC în relația cu ASP și de interacțiunea sa cu aceasta în momentul în care aceasta din urmă și-a inițiat activitățile de reglementare privind încălcarea securității de către TIC[81]. AS IE a susținut că deficiențele privind modul în care TIC a documentat încălcarea securității nu se corelează neapărat cu o lipsă de cooperare a TIC[82]. În plus, AS IE a subliniat că TIC a cooperat cu AS IE în timpul anchetei, răspunzând la toate solicitările de informații și furnizând toate documentele solicitate, fără a urmări să perturbe sau să obstrucționeze ancheta în niciun mod[83]. În orice caz, AS IE nu a considerat cooperarea TIC ca fiind circumstanță atenuantă[84]. Din motivele sus-menționate, AS IE a considerat că este „îndoielnic" dacă obiecția formulată de AS IT este motivată și relevantă, deoarece, deși aceasta se referă la o încălcare a RGPD, nu demonstrează modul în care poziția AS IE privind gradul de cooperare al TIC generează riscuri prezentate de proiectul de decizie privind drepturile și libertățile fundamentale ale persoanelor vizate[85]. AS IE a concluzionat că nu va da curs obiecției respective[86].

5.2.4 Analiza CEPD

5.2.4.1 Evaluarea caracterului relevant și motivat al obiecțiilor

76. În obiecția sa, AS IT nu contestă faptul că s-a produs o încălcare a articolului 33 alineatul (5) din RGPD. O obiecție relevantă și motivată poate să conteste motivarea care stă la baza concluziilor la care a ajuns ASP în proiectul de decizie numai în măsura în care motivarea respectivă are o legătură cu concluziile, obiecția este motivată în mod adecvat. În acest caz, obiecția nu susține clar modul în care, dacă i s-ar da curs, ar implica o modificare a proiectului de decizie. În plus, obiecția nu respectă criteriile subliniate la articolul 4 alineatul (24) din RGPD, deoarece nu demonstrează clar importanța riscurilor prezentate de proiectul de decizie, întrucât nu indică implicațiile pe care presupusa greșeală din proiectul de decizie le-ar avea în ceea ce privește valorile protejate.

[81] Memorandumul compus, punctul 5.87.
[82] Memorandumul compus, punctul 5.87.
[83] Memorandumul compus, punctul 5.87.
[84] Memorandumul compus, punctul 5.87.
[85] Memorandumul compus, punctul 5.88.
[86] Memorandumul compus, punctul 5.88.

5.2.4.2 Concluzie

77. Deoarece obiecția AS IT nu îndeplinește cerințele articolului 4 alineatul (24) din RGPD, comitetul nu se pronunță cu privire la fondul chestiunilor semnificative semnalate de această obiecție. CEPD reiterează că decizia sa actuală nu aduce atingere evaluărilor care pot fi solicitate CEPD în alte cauze, inclusiv cu aceleași părți, ținând cont de conținutul proiectului de decizie relevant și de obiecțiile formulate de ASV-uri.

6 DESPRE POSIBILELE ÎNCĂLCĂRI SUPLIMENTARE (SAU ALTERNATIVE) ALE RGPD, IDENTIFICATE DE ASV-URI.

6.1 Analiza efectuată de ASP în cadrul proiectului de decizie

78. În baza informațiilor furnizate de TIC în momentul în care a notificat încălcarea securității către AS IE, AS IE a observat că, din formularul de notificare a încălcării securității, reiese că s-au scurs mai mult de 72 de ore din momentul în care TIC (în calitate de operator) a luat cunoștință de încălcarea securității[87]. Din acest motiv, AS IE a decis să demareze o anchetă, din proprie inițiativă, pentru a examina dacă TIC și-a respectat obligațiile în temeiul articolului 33 alineatele (1) și (5) din RGPD[88].

79. Pentru a stabili dacă TIC își respectă obligațiile în temeiul articolului 33 alineatul (1) din RGPD, AS IE le-a luat în considerare în contextul obligațiilor mai ample ale unui operator, inclusiv cea de responsabilitate [articolul 5 alineatul (2) din RGPD], de recrutare a unei persoane împuternicite de operator (articolul 28 din RGPD) și în ceea ce privește securitatea prelucrării datelor cu caracter personal (articolul 32 din RGPD)[89]. Cu toate acestea, dacă AS IE a luat în considerare factorii și chestiunile faptice care au generat întârzierea cu care persoana împuternicită de operator a adus la cunoștința TIC încălcarea securității, și în cele din urmă, întârzierea acesteia din urmă în a notifica încălcarea securității, AS IE nu a luat în considerare dacă TIC a respectat sau nu oricare dintre aceste obligații sau fiecare dintre acestea cu scopul de a evalua respectarea obligațiilor de către TIC, în temeiul articolului 33 alineatul (1) și al articolului 33 alineatul (5) din RGPD[90].

6.2 Rezumatul obiecțiilor formulate de ASV-uri

80. AS DE, FR, HU și IT au formulat obiecții conform cărora TIC a încălcat și alte dispoziții ale RGPD, pe lângă sau în locul dispozițiilor articolului 33 alineatele (1) și (5).

6.2.1 Încălcarea articolului 5 alineatul (1) litera (f) din RGPD privind principiul integrității și al confidențialității

81. **AS DE** a formulat o obiecție în care a afirmat că AS IE ar fi trebuit să ia în considerare în proiectul său de decizie „eroarea subiacentă" din aplicația TIC, care a generat notificarea încălcării securității către AS IE, pentru a determina dacă această eroare constituie de fapt o încălcare considerabilă a confidențialității datelor cu caracter personal, încălcând în final articolul 5 alineatul (1) litera (f) din RGPD, în plus față de articolul 33 alineatele (1) și (5) din RGPD.

[87] Proiectul de decizie, punctul 2.11.
[88] Proiectul de decizie, punctul 2.11.
[89] Proiectul de decizie, punctele 6.13-6.20, 7.111-7.112, 7.122-7.124.
[90] Proiectul de decizie, punctele 6,13, 7,111, 7.122-7.124.

82. **AS HU** a formulat o obiecție în care a afirmat că, având în vedere „eroarea” din aplicația TIC de-a lungul timpului, precum și natura sa gravă, care afectează securitatea datelor, AS IE trebuie să investigheze dacă TIC a încălcat și articolul 5 alineatul (1) litera (f) din RGPD, privind principiul integrității și confidențialității.

6.2.2 Încălcarea articolului 5 alineatul (2) din RGPD privind principiul responsabilității

83. **AS IT** a formulat o obiecție în care a afirmat că încălcarea articolului 33 alineatul (1) din RGPD evidențiază o încălcare mult mai gravă a principiului responsabilității (în temeiul articolului 5 alineatul (2) din RGPD), deoarece lipsa politicilor corporative pentru tratarea incidentelor de securitate sau nerespectarea lor demonstrează că măsurile puse în aplicare de operator sunt inadecvate pentru a asigura conformitatea și pentru a o documenta. AS IT a susținut că aceste deficiențe procedurale sunt evidențiate în proiectul de decizie, care însă nu face din acestea obiectul unei analize specifice. Întrucât acest lucru poate afecta și gestionarea situațiilor viitoare de încălcare a securității datelor, constatările referitoare la respectarea de către TIC a articolului 5 alineatul (2) din RGPD ar trebui să facă parte din hotărârea finală a AS IE, în opinia AS IT. De asemenea, AS IT a considerat că încălcarea articolului 5 alineatul (2) din RGPD este confirmată de incapacitatea operatorului de a afirma numărul exact al datelor cu caracter personal afectate și natura acestora sau numărul total de persoane vizate implicate.

6.2.3 Încălcarea articolului 24 din RGPD privind responsabilitatea operatorului

84. **AS DE** a formulat o obiecție în care afirma că proiectul de decizie nu specifica în mod clar motivul pentru care AS IE nu a evaluat dacă încălcarea semnificativă a datelor cu caracter personal, cauzată de o „eroare subiacentă” se datorează unei încălcări a cerințelor articolului 24 din RGPD.

6.2.4 Încălcarea articolului 28 din RGPD privind relația cu persoanele împuternicite de operator

85. **AS FR** a exprimat o obiecție în care afirma că TIC nu a respectat obligația operatorului de a verifica validitatea procedurilor stabilite de persoana împuternicită de operator. Prin urmare, AS FR consideră că nu există o încălcare a articolului 33 alineatul (1) din RGPD, ci, în schimb, a articolului 28 din RGPD (sau a articolului 32 din RGPD - vezi secțiunea 6.2.5 de mai jos). AS FR a susținut că, dacă persoana împuternicită de operator pentru TIC este societatea-mamă a acesteia, *„era cu atât mai ușor ca TIC să verifice validitatea procedurilor stabilite de societatea-mamă și să solicite o corecție, în cazul în care aceasta era necesară”.*

86. **AS IT** a exprimat o obiecție, afirmând că neimplicarea responsabilului cu protecția datelor de la nivel local din echipa de depistare și reacție a persoanei împuternicite de operator (Twitter, Inc.), în pofida faptului că această practică era prevăzută în politicile interne ale TIC, indică faptul că garanțiile oferite de persoana împuternicită de operator în ceea ce privește punerea în aplicare a măsurilor organizatorice adecvate în temeiul articolului 28 alineatul (1) din RGPD nu sunt suficient de ample. În plus, AS IT a susținut în obiecțiile sale că persoana împuternicită de operator și-a încălcat obligația de a ajuta operatorul, conform articolului 28 alineatul (3) litera (f) din RGPD.

6.2.5 Încălcarea articolului 32 din RGPD privind securitatea prelucrării

87. **AS DE** a formulat obiecții în care a afirmat că AS IE ar fi trebuit să examineze dacă au fost respectate toate măsurile tehnice și organizatorice adecvate în acest caz (conform articolului 32 din RGPD) și dacă încălcările în acest domeniu ar fi trebuit să constituie obiectul acestor proceduri. De asemenea, **AS DE**

susține că proiectul de decizie nu specifică în mod clar motivul pentru care AS IE nu a evaluat dacă încălcarea semnificativă a datelor cu caracter personal, cauzată de o „eroare subiacentă” se datorează unei încălcări a cerințelor articolului 32 din RGPD.

88. **AS FR** a exprimat o obiecție privind caracterizarea juridică a faptelor efectuate de AS IE și a afirmat că nerespectarea de către TIC a obligației operatorului de a verifica validitatea procedurilor stabilite de persoana împuternicită de operator corespunde unei încălcări a articolului 32 din RGPD (sau a articolului 28 din RGPD - vezi secțiunea 6.2.4 de mai sus), în locul încălcării articolului 33 alineatul (1) din RGPD. AS FR a susținut că, dacă persoana împuternicită de operator pentru TIC este societatea-mamă a acesteia, *„era cu atât mai ușor ca TIC să verifice validitatea procedurilor stabilite de societatea-mamă și să solicite o corecție, în cazul în care aceasta era necesară”.*

89. **AS HU** a formulat obiecții în care a afirmat că, având în vedere „eroarea” care a existat în aplicația TIC de-a lungul anilor, precum și natura sa gravă, care afectează securitatea datelor, AS IE ar trebui să investigheze dacă TIC a încălcat și articolul 32 din RGPD, privind obligațiile TIC de a asigura securitatea prelucrării.

6.2.6 Încălcarea articolului 33 alineatul (3) din RGPD privind conținutul notificării în cazul încălcării securității datelor cu caracter personal privind securitatea prelucrării

90. **AS DE** a exprimat obiecții în care a afirmat că examinarea efectuată de AS IE are deficiențe în ceea ce privește sfera de cuprindere a informațiilor care trebuie furnizate în cazul unei notificări, care este obligatorie, potrivit celor specificate la articolul 33 alineatul (3) din RGPD. În baza observațiilor TIC privind încălcarea securității, furnizate în temeiul articolului 33 alineatul (5) din RGPD și în baza descrierii investigării faptelor cauzei, este evident că TIC nu și-a respectat obligația de documentare atunci când a raportat prima oară încălcarea securității la 8 ianuarie 2019. Prin urmare, AS DE a considerat că există numeroase indicații că rezultatul ar putea fi, de asemenea, o încălcare a articolului 33 alineatul (3) din RGPD.

6.2.7 Încălcarea articolului 34 din RGPD privind informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal

91. **AS HU** a formulat obiecții în care a afirmat că, având în vedere „eroarea” care a existat în aplicația TIC de-a lungul anilor, precum și natura sa gravă, care afectează securitatea datelor, AS IE a trebuit să investigheze dacă TIC a încălcat și articolul 34 din RGPD referitor la obligațiile TIC de a informa persoanele vizate cu privire la încălcarea securității.

6.3 Poziția ASP cu privire la obiecții

92. ASP și-a furnizat răspunsul în ceea ce privește obiecțiile referitoare la încălcările potențiale suplimentare (sau alternative) ale RGPD în mod colectiv în Memorandumul său compus comunicat ASV-urilor. ASP a explicat că „și-a exercitat puterea de apreciere [...] pentru a limita domeniul de aplicare al anchetei la analiza a două chestiuni diferite, și anume dacă TIC și-a respectat sau nu obligațiile în calitate de operator în temeiul articolului 33 alineatul (1) în ceea ce privește notificarea încălcării securității și dacă și-a respectat sau nu obligațiile în temeiul articolului 33 alineatul (5) pentru a documenta încălcarea securității”[91]. ASP s-a bazat pe secțiunea 110 alineatul (1) din Legea irlandeză

[91] Memorandumul compus, punctul 1.7.

privind protecția datelor din 2018, care prevede că AS IE poate „determina desfășurarea anchetei respective astfel cum consideră potrivit”[92]. Astfel, scopul anchetei, potrivit celor descrise de AS IE, a fost „exclusiv de a examina circumstanțele din jurul notificării care se pare că a fost transmisă cu întârziere de TIC cu privire la încălcarea securității [...] și documentarea încălcării securității de către aceasta”, o chestiune considerată de AS IE ca fiind „de importanță considerabilă, având în vedere faptul că, înregistrându-se notificarea a aproape 200 000 de încălcări ale securității în doi ani în întreaga UE, este nevoie de claritate cu privire la ceea ce este necesar în temeiul notificării încălcării securității și al cerințelor de documentare din RGPD”[93].

93. În Memorandumul său compus[94], AS IE își menține opinia că obiecțiile formulate în contextul articolului 60 alineatul (4) din RGPD nu pot avea efectul de a contesta domeniul de aplicare al unei anchete. În cazul de față, ASP reamintește că a informat TIC la începutul anchetei că scopul său a constat în verificarea conformității TIC cu articolul 33 alineatele (1) și (5) din RGPD în ceea ce privește notificarea acesteia privind o încălcare a securității către ASP din data de 8 ianuarie 2019. Prin urmare, întregul proces de anchetă a fost desfășurat în respectivul domeniu de aplicare, la fel ca proiectul de decizie, iar TIC a beneficiat de dreptul de a fi ascultată în acest sens, în fiecare etapă a procedurii. Prin urmare, ASP susține că, în cazul în care ar da curs obiecțiilor ASV și ar include și alte încălcări în decizia sa finală, *„numai în baza materialului inclus în proiectul de decizie”*, acest lucru *„ar pune în pericol ancheta în ansamblu și procesul desfășurat în temeiul articolului 60, expunând-o la riscul de invocare a inechității procedurale”*[95].

94. În plus, ASP explică faptul că are o altă anchetă în curs în raport cu alte încălcări ale securității datelor notificate ASP de către TIC înainte de notificarea care vizează cauza în discuție. În cealaltă anchetă, inițiată înainte de cea în discuție, ASP subliniază că domeniul de aplicare al investigației se referă la posibila nerespectare a ”*articolelor 5, 24, 25, 28, 29 și 32, între altele*” din RGPD[96]. ASP consideră că această anchetă paralelă evaluează, într-adevăr, respectarea de către TIC a obligațiilor sale mai ample în temeiul RGPD, pentru a stabili dacă deficiențele de conformitate au cauzat încălcarea securității datelor. În consecință, ASP este de opinie că ASV-urile vor avea posibilitatea de a lua în considerare aceste posibile încălcări în contextul celeilalte anchete, întrucât acestea vor fi consultate în proiectul de decizie, în conformitate cu articolul 60 alineatul (4) din RGPD[97].

95. TIC a transmis că, întrucât proiectul de decizie afirmă că *„o examinare detaliată a măsurilor tehnice și organizatorice depășește domeniul de aplicare al anchetei”*[98], *„nu ar fi rezonabil sau adecvat și ar contraveni principiilor consacrate ale echității dacă decizia ar include constatări sau ar impune sancțiuni asupra TIC în ceea ce privește obligațiile și principiile care nu au făcut parte din investigația coordonatorului pentru protecția datelor, deoarece TIC nu a avut ocazia de a aborda niciuna dintre preocupările semnalate de coordonatorul pentru protecția datelor sau de ASV-uri cu privire la procesele TIC în aceste domenii”*[99].

[92] Memorandumul compus, punctul 1.5.
[93] Memorandumul compus, punctul 1.9.
[94] Memorandumul compus, punctul 5.44.
[95] Memorandumul compus, punctul 5.44 (c).
[96] Memorandumul compus, punctul 1.10.
[97] Memorandumul compus, punctul 5.44 (d).
[98] Proiectul de decizie, punctul 7.19.
[99] „Declarații ca răspuns la obiecțiile și observațiile primite de la ASV-uri”, transmise de TIC (14 august 2020), punctul 4.1. CEPD dorește să sublinieze că obiecțiile formulate de ASV-uri au fost aduse în atenția TIC de către AS IE, iar TIC a emis declarațiile menționate mai sus cu privire la obiecții, care au fost luate în considerare de AS IE înainte de inițierea procedurii în temeiul articolului 65 și sunt incluse în dosarul luat în considerare de CEPD în contextul acestei proceduri. Vezi, de asemenea, nota de subsol 19.

6.4 Analiza CEPD

6.4.1 Evaluarea caracterului relevant și motivat al obiecțiilor

6.4.1.1 Încălcarea articolului 5 alineatul (1) litera (f) din RGPD privind principiul integrității și al confidențialității

96. CEPD reține că obiecția **AS DE** cu privire la articolul 5 alineatul (1) litera (f) din RGPD se referă la existența sau inexistența unei încălcări a RGPD, exprimând un dezacord în ceea ce privește concluziile care urmează să fie extrase din constatările investigației. De asemenea, obiecția oferă argumente pentru a sprijini concluzia că trebuie evaluată conformitatea cu articolul 5 alineatul (1) litera (f) din RGPD. Obiecția AS DE demonstrează în mod clar că semnificația riscurilor prezentate de proiectul de decizie în ceea ce privește drepturile și libertățile persoanelor vizate, în special din cauză că subliniază că faptele reprezintă o încălcare „importantă" și „semnificativă" a confidențialității datelor cu caracter personal și că a fost vizat un număr mare de persoane, pentru o perioadă de timp semnificativă. În plus, AS DE a susținut, de asemenea, că existau indicii pentru a se lua în considerare o „eroare sistemică", iar aceasta ar fi necesitat un control mai aprofundat, dincolo de eroarea specifică unică în cauză.

97. De asemenea, obiecția înaintată de **AS HU** poate fi considerată relevantă, deoarece se referă la existența sau inexistența unei încălcări a RGPD. În plus, aceasta face referință (doar) pe scurt la argumentele faptice, care susțin necesitatea de a aborda această dispoziție suplimentară (durata erorii și caracterul său grav, care afectează securitatea datelor), însă nu „demonstrează în mod clar" importanța riscurilor pe care le prezintă proiectul de decizie pentru riscurile privind drepturile și libertățile persoanelor, întrucât nu oferă argumente sau justificări privind consecințele emiterii unei decizii fără schimbările propuse în obiecție[100].

98. În consecință, CEPD consideră că obiecția formulată de AS DE în ceea ce privește potențiala încălcare a articolului 5 alineatul (1) litera (f) din RGPD în scopurile relevante și motivate ale articolului 4 alineatul (24) din RGPD, însă consideră că obiecția AS HU în ceea ce privește același subiect nu îndeplinește cerințele articolului 4 alineatul (24)[101].

99. CEPD va evalua fondul chestiunilor semnificative semnalate de obiecția AS DE în ceea ce privește potențiala încălcare suplimentară a articolului 5 alineatul (1) litera (f) din RGPD (vezi secțiunea 6.4.2 de mai jos).

6.4.1.2 Încălcarea articolului 5 alineatul (2) din RGPD privind principiul responsabilității

100. Obiecția formulată de **AS IT** trebuie să fie considerată „relevantă" deoarece, dacă i s-ar da curs, ar duce la o concluzie diferită în ceea ce privește existența sau inexistența unei încălcări a RGPD[102]. Mai precis, aceasta include un „dezacord în ceea ce privește concluziile care trebuie să fie formulate în urma

[100] Orientările privind ORM, punctul 19.
[101] În consecință, CEPD nu se pronunță cu privire la fondul niciuneia dintre chestiunile semnificative semnalate de obiecția AS HU. CEPD reiterează că decizia sa actuală nu aduce atingere evaluărilor care pot fi solicitate CEPD în alte cauze, inclusiv cu aceleași părți, ținând cont de conținutul proiectului de decizie relevant și de obiecțiile formulate de ASV-uri.
[102] Orientările privind ORM, punctul 13.

constatărilor investigației", deoarece afirmă că *„constatările reprezintă o încălcare a unei dispoziții a RGPD [...] în plus față de [...] cele analizate deja în proiectul de decizie"*[103].

101. În plus, obiecția este „motivată", deoarece conține clarificări privind motivul pentru care se propune modificarea deciziei[104]: schimbarea propusă se bazează pe *„lipsa unor politici corporative formale pentru gestionarea incidentelor de securitate [...] sau nerespectarea politicilor respective"* privind faptul că aceste *„deficiențe procedurale sunt evidențiate în mod repetat de către [AS IE]"* în proiectul de decizie și privind incapacitatea operatorului de a specifica numărul exact și natura datelor cu caracter personal / persoanele vizate afectate.

102. **AS IT** a demonstrat în mod clar importanța riscurilor prezentate de proiectul de decizie în ceea ce privește drepturile și libertățile fundamentale ale persoanelor vizate, indicând „implicațiile pe care proiectul de decizie le-ar avea în ceea ce privește valorile protejate"[105] și, mai specific, „impactul asupra drepturilor și libertăților persoanelor vizate ale căror date ar putea fi prelucrate în viitor"[106]: obiecția susține astfel că aspectele menționate sunt *„de natură structurală în ceea ce privește organizația operatorului" și „sigur vor produce efect nu numai asupra cauzei în discuție, ci și asupra tratării situațiilor de încălcare a securității datelor cu caracter personal care se pot produce în viitor"*.

103. În consecință, obiecția AS IT privind articolul 5 alineatul (2) din RGPD îndeplinește cerințele expuse la articolul 4 alineatul (24) din RGPD. Prin urmare, CEPD va analiza fondul chestiunilor semnificative semnalate de această obiecție[107].

6.4.1.3 Încălcarea articolului 24 din RGPD privind responsabilitatea operatorului

104. Obiecția **AS DE** se referă în mod specific la capitolul 5, „Chestiuni de determinat" din proiectul de decizie[108] și aduce obiecții la proiectul de decizie cu privire la încălcarea sau nu a articolului 24 din RGPD de către TIC[109]. Aceasta se bazează pe faptele[110] prezentate în proiectul de decizie, potrivit cărora, *„dacă un utilizator Twitter cu un cont protejat, care folosea Twitter pentru Android, își schimbă adresa de e-mail, eroarea ar face ca respectivul cont să fie neprotejat"*[111] și mesajele tweet protejate ale acestora devin publice prin intermediul serviciului. Mai exact, AS DE contestă motivul pentru care AS DE nu a examinat, în proiectul de decizie, cauzele încălcării securității, în special prin prisma articolului 24 din RGPD și motivul pentru care AS IE nu a explicat în proiectul de decizie de ce nu a efectuat această examinare.

105. AS DE susține că, având în vedere faptul că notificarea încălcării securității a dezvăluit *„deficiențe în ceea ce privește conformitatea cu RGPD... [o] societate care nu este capabilă, prin mijloacele și resursele proprii, prin inspecții ale echipelor de securitate interne sau externe să găsească o eroare atât de importantă și de amplă trebuie să facă obiectul unui control mai aprofundat privind securitatea sa și structura de prelucrare a datelor, dincolo de eroarea specifică unică în cauză"*.

[103] Orientările privind ORM, punctul 27.
[104] Orientările privind ORM, punctul 17.
[105] Orientările privind ORM, punctul 37.
[106] Orientările privind ORM, punctul 43.
[107] Vezi secțiunea 6.4.2 de mai jos.
[108] Orientările privind ORM, punctul 20.
[109] Orientările privind ORM, punctul 12.
[110] Orientările privind ORM, punctul 14.
[111] Proiectul de decizie, punctul 2.7.

106. Potrivit AS DE*, un control sporit în ceea ce privește structura de prelucrare a datelor de către TIC „ar putea determina, după caz, un ordin al operatorului de a aduce operațiunile de prelucrare în conformitate cu dispozițiile RGPD. Cauza în discuție nu reflectă această sarcină. Din acest motiv, este cu atât mai urgent să se examineze competențele corective în temeiul articolului 58 alineatul (2) din RGPD în acest context”.*

107. Prin urmare, AS DE a evidențiat ceea ce considera o lipsă a evaluării, având drept consecințe concluzii posibil diferite extrase de ASP din constatări[112].

108. Obiecția AS DE potrivit căreia „În conformitate cu *articolul 83 alineatul (1) din RGPD, amenzile trebuie să fie «în fiecare caz, eficace, proporționale și disuasive». O sancțiune este eficace și disuasivă dacă, pe de o parte, este adecvată ca măsură preventivă generală pentru a descuraja publicul larg să comită încălcări și pentru a consolida încrederea publicului larg în validitatea dreptului Uniunii, însă, pe de altă parte, este adecvată și ca măsură preventivă pentru a descuraja infractorii să comită alte încălcări”.* În consecință, AS DE demonstrează modul în care, dacă nu s-ar modifica proiectul de decizie astfel încât să includă o evaluare a conformității cu articolul 24 din RGPD, acesta ar prezenta riscuri considerabile la adresa drepturilor și libertăților fundamentale ale persoanelor vizate[113].

109. În Orientările sale privind ORM, CEPD acceptă faptul că o obiecție poate să conteste concluzia ASP, luând în considerare faptul că constatările ASP conduc, de fapt, la concluzia că a fost încălcată o altă dispoziție a RGPD, în plus față de dispoziția identificată de ASP sau în locul acesteia[114]. CEPD consideră că tocmai aceasta este esența obiecției AS DE și, prin urmare, acest lucru nu o împiedică să fie relevantă și motivată.

110. În plus, obiecția AS DE demonstrează în mod clar semnificația riscurilor pe care le prezintă proiectul de decizie în ceea ce privește drepturile și libertățile persoanelor vizate, inclusiv prin evidențierea faptului că a fost vizat un număr mare de persoane, de-a lungul unei perioade de timp la fel de semnificative, reflectând o eroare sistemică ce impune un control mai aprofundat, dincolo de eroarea specifică în cauză. În consecință, obiecția AS DE privind articolul 24 din RGPD îndeplinește cerințele expuse la articolul 4 alineatul (24) din RGPD.

111. Prin prisma evaluării de mai sus, CEPD consideră că obiecția AS DE cu privire la posibila încălcare a articolului 24 din RGPD este relevantă și motivată în conformitate cu articolul 4 alineatul (24) din RGPD. În consecință, CEPD evaluează fondul chestiunilor semnificative semnalate de această obiecție (vezi secțiunea 6.4.2 de mai jos).

6.4.1.4 Încălcarea articolului 28 din RGPD privind relația cu persoanele împuternicite de operator

112. Obiecția **AS FR** se referă în mod specific la punctele 7.129 iii), iv) și v) din proiectul de decizie[115] și aduce obiecții la proiectul de decizie cu privire la încălcarea sau nu a articolului 28 din RGPD de către TIC în locul articolului 33 alineatul (1) din RGPD[116]. Aceasta se bazează pe faptele[117] prezentate în proiectul de decizie și pe constatările ASP, potrivit cărora „TIC nu și-a respectat obligația de operator de a verifica validitatea procedurilor stabilite de persoana împuternicită de operator.”

[112] Orientările privind ORM, punctul 29.
[113] Orientările privind ORM, punctul 19.
[114] Orientările privind ORM, punctul 27.
[115] Orientările privind ORM, punctul 20.
[116] Orientările privind ORM, punctul 12.
[117] Orientările privind ORM, punctul 14.

113. Potrivit AS FR, deoarece articolul 28 alineatul (3) litera (h) stabilește îndatoririle operatorului atunci când acesta utilizează o persoană împuternicită de operator, constatările ar fi trebuit să determine ASP să ajungă la concluzia că a fost încălcat articolul 28 alineatul (3) litera (h) din RGPD, nu articolul 33 alineatul (1) din RGPD. În final, acest lucru înseamnă, pentru AS FR, că sancțiunea emisă sub formă de amendă ar trebui să se refere la încălcări diferite.

114. În Orientările sale privind ORM, CEPD acceptă faptul că o obiecție poate să conteste concluzia ASP, luând în considerare faptul că constatările ASP conduc, de fapt, la concluzia că a fost încălcată încă o dispoziție a RGPD, în plus față de dispoziția identificată de ASP sau în locul acesteia[118]. CEPD consideră că tocmai aceasta este esența obiecției AS FR și, prin urmare, acest lucru nu o împiedică să fie relevantă. De asemenea, obiecția oferă, în mod adecvat, argumente care sprijină concluzia propusă. În același timp, CEPD reține că obiecția AS FR nu demonstrează clar importanța riscurilor prezentate de proiectul de decizie la adresa drepturilor și libertăților fundamentale ale persoanelor vizate, acordându-se atenție în mod special lipsei unei concluzii cu privire la încălcarea acestei dispoziții specifice[119]. Prin prisma acestei evaluări, CEPD consideră că obiecția AS FR cu privire la posibila încălcare a articolului 28 din RGPD în locul articolului 33 alineatul (1) din RGPD nu este relevantă și motivată în conformitate cu articolul 4 alineatul (24) din RGPD[120].

115. AS IT aduce obiecții proiectului de decizie cu privire la încălcarea sau nu de către TIC a articolului 28 din RGPD, printre altele, în plus față de articolul 33 alineatul (1) din RGPD[121].

116. AS IT se bazează pe faptele prezentate în proiectul de decizie și pe constatările ASP potrivit cărora, deși implicarea RPD de la nivel global în Echipa de depistare și reacție a persoanei împuternicite de operator, și anume Twitter Inc., este prevăzută în politicile interne ale TIC, în practică RPD de la nivel global nu a fost implicat. De asemenea, AS IT reține că Twitter, Inc., în calitate de persoană împuternicită de operator, nu a sprijinit TIC.

117. Potrivit AS IT, având în vedere articolul 28 alineatul (1) din RGPD, care impune operatorilor nu numai să recurgă la persoane împuternicite care oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, și articolul 28 alineatul (3) litera (f) din RGPD, care impune să se specifice în contractul dintre operator și persoana împuternicită de acesta că operatorul „ajută operatorul să asigure respectarea obligațiilor prevăzute la articolele 32-36, ținând seama de caracterul prelucrării și de informațiile aflate la dispoziția persoanei împuternicite de operator”, constatările ar fi trebuit să conducă ASP la concluzia că au fost încălcate și articolul 28 alineatul (1) și articolul 28 alineatul (3) litera (f) din RGPD.

118. CEPD consideră că obiecția formulată de AS IT în ceea ce privește articolul 28 alineatul (1) și articolul 28 alineatul (3) litera (f) din RGPD trebuie să fie considerată „relevantă” deoarece, dacă i s-ar da curs, ar duce o concluzie diferită în ceea ce privește existența sau inexistența unei încălcări a RGPD[122]. Mai precis, aceasta include un „dezacord în ceea ce privește concluziile care trebuie să fie formulate în

[118] Orientările privind ORM, punctul 27.
[119] Orientările privind ORM, punctul 29.
[120] În consecință, CEPD nu se pronunță cu privire la fondul niciuneia dintre chestiunile semnificative semnalate de aceste obiecții. CEPD reiterează că decizia sa actuală nu aduce atingere evaluărilor care pot fi solicitate CEPD în alte cauze, inclusiv cu aceleași părți, ținând cont de conținutul proiectului de decizie relevant și de obiecțiile formulate de ASV-uri.
[121] Orientările privind ORM, punctul 12.
[122] Orientările privind ORM, punctul 13.

urma constatărilor investigației", deoarece afirmă că „constatările reprezintă o încălcare a unei dispoziții a RGPD [...] în plus față de [...] cele analizate deja în proiectul de decizie"[123].

119. În plus, potrivit CEPD, obiecția este „motivată", deoarece include clarificări privind motivul pentru care se propune modificarea deciziei[124]: schimbarea propusă se bazează pe faptul că operatorul nu și-a respectat politicile interne, potrivit cărora ar fi trebuit să fie implicat responsabilul cu protecția datelor desemnat de TIC. În plus, obiecția aduce în discuție ideea că persoana împuternicită de operator nu și-a respectat obligațiile contractuale de a ajuta operatorul, în conformitate cu articolul 28 alineatul (3) litera (f) din RGPD.

120. Cu toate acestea, CEPD reține că obiecția AS IT referitoare la articolul 28 alineatul (1) și articolul 28 alineatul (3) litera (f) din RGPD nu demonstrează clar riscurile semnificative prezentate de proiectul de decizie la adresa drepturilor și libertăților fundamentale ale persoanelor vizate[125]. În consecință, această obiecție formulată de AS IT nu îndeplinește cerințele expuse la articolul 4 alineatul (24) din RGPD[126].

6.4.1.5 Încălcarea articolului 32 din RGPD privind securitatea prelucrării

121. Dacă s-ar da curs obiecției **AS DE**, aceasta ar implica o schimbare ce ar conduce la o concluzie diferită în ceea ce privește existența sau inexistența unei încălcări a RGPD, deoarece aceasta a identificat un *„dezacord în ceea ce privește concluziile care se pot formula din constatările investigației"*[127], atrăgând atenția ca aceste constatări pot să indice și o încălcare a articolului 32 din RGPD. Prin urmare, CEPD consideră că există o legătură între conținutul obiecției și concluzia diferită posibilă[128]. În plus, această obiecție se referă la conținutul juridic și faptic specific al proiectului de decizie[129].

122. În plus, obiecția AS DE demonstrează în mod clar că semnificația riscurilor prezentate de proiectul de decizie în ceea ce privește drepturile și libertățile persoanelor vizate, în special din cauză că subliniază că faptele reprezintă o încălcare „considerabilă" și „semnificativă" a confidențialității datelor cu caracter personal și că a fost vizat un număr mare de persoane, pentru o perioadă de timp semnificativă. În plus, AS DE a susținut, de asemenea, că existau indicii pentru a se lua în considerare existența unei „erori sistemice", iar aceasta ar fi necesitat un control mai aprofundat, dincolo de eroarea specifică unică în cauză.

123. Prin prisma evaluării de mai sus, CEPD consideră că obiecția AS DE cu privire la posibila încălcare a articolului 32 din RGPD este relevantă și motivată în conformitate cu articolul 4 alineatul (24) din RGPD. În consecință, CEPD evaluează fondul chestiunilor semnificative semnalate de această obiecție (vezi punctul 6.4.2 de mai jos).

124. În ceea ce privește obiecția **AS FR**, CEPD consideră că aceasta îndeplinește criteriul de a fi „relevantă", deoarece dacă ASP i-ar fi dat curs, concluzia în ceea ce privește existența sau inexistența unei încălcări

[123] Orientările privind ORM, punctul 27.
[124] Orientările privind ORM, punctul 17.
[125] Orientările privind ORM, punctul 29.
[126] În consecință, CEPD nu se pronunță cu privire la fondul oricărora dintre chestiunile semnificative semnalate de aceste obiecții. CEPD reiterează că decizia sa actuală nu aduce atingere evaluărilor care pot fi solicitate CEPD în alte cauze, inclusiv cu aceleași părți, ținând cont de conținutul proiectului de decizie relevant și de obiecțiile formulate de ASV-uri.
[127] Orientările privind ORM, punctul 28.
[128] Orientările privind ORM, punctul 13.
[129] Orientările privind ORM, punctul 14.

a RGPD ar fi fost diferită[130]. Obiecția AS FR se bazează pe motivația oferită de AS IE în proiectul de decizie, iar această motivare este legată de concluzia referitoare la identificarea corectă sau incorectă a unei încălcări a RGPD[131]. CEPD reamintește că ASV trebuie să prezinte faptele care se presupune că generează o concluzie diferită[132] și reține că, în cauza în discuție, obiecția analizează faptele care ar conduce la încălcarea articolului 32 alineatul (1) litera (d) din RGPD, în loc să conducă la încălcarea articolului 33 alineatul (1) din RGPD și face acest lucru într-un mod coerent, clar și precis, indicând în mod clar cu ce părți ale deciziei AS IE nu este de acord. Obiecția AS FR este relevantă în mod clar, prin faptul că subliniază un dezacord referitor la existența sau inexistența unei încălcări a RGPD. Cu toate acestea, obiecția AS FR explică numai pe scurt motivele pentru schimbarea propusă și nu demonstrează în mod clar importanța riscurilor pe care le prezintă proiectul de decizie în ceea ce privește drepturile și libertățile fundamentale ale persoanelor vizate în legătură cu lipsa constatării unei încălcări a articolului 32 din RGPD. În consecință, această obiecție formulată de AS FR nu îndeplinește cerințele expuse la articolul 4 alineatul (24) din RGPD[133].

125. De asemenea, obiecția **AS HU** s-a referit la existența sau inexistența unei încălcări a RGPD, susținând că ar trebui să fie investigată și posibila încălcare a principiului integrității și confidențialității. Obiecția AS HU este în mod clar relevantă prin faptul că subliniază că ar fi trebuit să fie investigată o dispoziție suplimentară din RGPD (și anume articolul 32 din RGPD). Cu toate acestea, AS HU nu explică modul în care proiectul de decizie ar prezenta aceste riscuri și nici nu explică pe deplin de ce anumite aspecte specifice ale deciziei sunt insuficiente din punctul său de vedere[134]. Obiecția AS HU nu îndeplinește criteriul de a oferi o motivare solidă pentru obiecția sa, făcând referire la argumente juridice sau faptice. Dimpotrivă, aceasta recomandă doar ca AS HU să investigheze respectarea articolului 32 din RGPD de către operator. În consecință, această obiecție formulată de AS HU nu îndeplinește cerințele stabilite de articolul 4 alineatul (24) din RGPD[135].

6.4.1.6 Încălcarea articolului 33 alineatul (3) din RGPD privind conținutul notificării în cazul încălcării securității datelor cu caracter personal privind securitatea prelucrării

126. **AS DE** consideră că proiectul de decizie indică faptul că este posibil ca articolul 33 alineatul (3) din RGPD să fi fost încălcat, în plus față de alte dispoziții ale RGPD. În acest sens, se referă la „existența sau inexistența unei încălcări" a RGPD și la faptul că aceasta nu a fost examinată și abordată de proiectul de decizie. Prin urmare, AS DE consideră că, dacă ar fi schimbat, proiectul de decizie ar conduce la concluzia unor încălcări suplimentare ale RGPD.

127. Cu toate acestea, AS DE nu demonstrează clar riscurile considerabile prezentate de proiectul de decizie în ceea ce privește drepturile și libertățile fundamentale ale persoanelor vizate. În consecință, obiecția

[130] Orientările privind ORM, punctul 13.
[131] Orientările privind ORM, punctul 16.
[132] Orientările privind ORM, punctul 18.
[133] În consecință, CEPD nu se pronunță cu privire la fondul niciuneia dintre chestiunile semnificative semnalate de aceste obiecții. CEPD reiterează că decizia sa actuală nu aduce atingere evaluărilor care pot fi solicitate CEPD în alte cauze, inclusiv cu aceleași părți, ținând cont de conținutul proiectului de decizie relevant și de obiecțiile formulate de ASV-uri.
[134] Orientările privind ORM, punctul 18.
[135] În consecință, CEPD nu se pronunță cu privire la fondul niciuneia dintre chestiunile semnificative semnalate de aceste obiecții. CEPD reiterează că decizia sa actuală nu aduce atingere evaluărilor care pot fi solicitate CEPD în alte cauze, inclusiv cu aceleași părți, ținând cont de conținutul proiectului de decizie relevant și de obiecțiile formulate de ASV-uri.

AS DE privind articolul 33 alineatul (3) din RGPD nu îndeplinește cerințele expuse la articolul 4 alineatul (24) din RGPD[136].

6.4.1.7 Încălcarea articolului 34 din RGPD privind informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal

128. **AS HU** consideră că proiectul de decizie indică faptul că este posibil ca articolul 34 din RGPD să fi fost încălcat, în plus față de alte dispoziții ale RGPD, în special prin prisma faptului că eroarea s-a menținut pe parcursul anilor și având în vedere natura sa gravă, care afectează securitatea operatorului. În acest sens, se referă la „existența sau inexistența unei încălcări" a RGPD și la faptul că aceasta nu a fost examinată și abordată de proiectul de decizie. Prin urmare, AS HU consideră că, dacă ar fi schimbat, proiectul de decizie ar conduce la concluzia unor încălcări suplimentare ale RGPD.

129. Cu toate acestea, AS HU nu demonstrează clar riscurile considerabile prezentate de proiectul de decizie în ceea ce privește drepturile și libertățile fundamentale ale persoanelor vizate. În consecință, obiecția AS HU privind articolul 34 din RGPD nu îndeplinește cerințele expuse la articolul 4 alineatul (24) din RGPD[137].

6.4.2 Evaluarea fondului chestiunii (chestiunilor) semnificative semnalate de obiecțiile relevante și motivate și concluzia

130. Comitetul trece la analiza obiecțiilor care se constată că sunt relevante și motivate - în special a obiecțiilor AS DE cu privire la articolul 5 alineatul (1) litera (f), articolele 24 și 32 din RGPD - precum și obiecțiile AS IT privind articolul 5 alineatul (2) din RGPD - precum și răspunsul ASP la obiecțiile respective și la observațiile TIC.

131. În conformitate cu articolul 65 alineatul (1) litera (a) din RGPD în contextul unei proceduri de soluționare a litigiilor, CEPD adoptă o decizie obligatorie cu privire la toate chestiunile care fac obiectul obiecțiilor relevante și motivate, în special dacă a fost încălcat RGPD. CEPD poate (și trebuie) să adopte o decizie obligatorie care va ține cont de elementele dosarului și de dreptul respondentului de a fi ascultat, ori de câte ori acest lucru este posibil, va oferi o concluzie finală privind aplicarea RGPD în legătură cu cauza de față. ASP va avea apoi obligația de a pune în aplicare schimbările în decizia sa finală.

132. Comitetul consideră că elementele faptice disponibile, incluse în proiectul de decizie și în obiecții nu sunt suficiente pentru a permite CEPD să stabilească existența unor alte încălcări alternative ale articolului 5 alineatul (1) litera (f), ale articolului 5 alineatul (2), ale articolelor 24 și 32 din RGPD.

133. Comitetul consideră că, în general, domeniul de aplicare limitat al anchetei AS IE - care se concentrează de la bun început numai asupra existenței sau inexistenței unor încălcări ale articolelor 33 alineatele (1) și (5) din RGPD de către TIC - afectează direct misiunea investigației și constatările ulterioare, precum și capacitatea ASV de a prezenta suficiente elemente către CEPD pentru a susține obiecțiile.

[136] În consecință, CEPD nu se pronunță cu privire la fondul niciuneia dintre chestiunile semnificative semnalate de aceste obiecții. CEPD reiterează că decizia sa actuală nu aduce atingere evaluărilor care pot fi solicitate CEPD în alte cauze, inclusiv cu aceleași părți, ținând cont de conținutul proiectului de decizie relevant și de obiecțiile formulate de ASV-uri.

[137] În consecință, CEPD nu se pronunță cu privire la fondul niciuneia dintre chestiunile semnificative semnalate de aceste obiecții. CEPD reiterează că decizia sa actuală nu aduce atingere evaluărilor care pot fi solicitate CEPD în alte cauze, inclusiv cu aceleași părți, ținând cont de conținutul proiectului de decizie relevant și de obiecțiile formulate de ASV-uri.

134. CEPD reamintește datoria ASP de a „depune eforturi pentru ajunge la un consens cu ASV-urile (articolul 60 alineatul (1) din RGPD) și să le ofere acestora, fără întârziere, „informații relevante” cu privire la chestiunea respectivă (articolul 60 alineatul (3) din RGPD). Chiar și în cazul unei anchete din proprie inițiativă, Orientările privind obiecțiile motivate și relevante afirmă că ASP „trebuie să urmărească să ajungă la un consens privind domeniul de aplicare al procedurii (respectiv aspectele prelucrării datelor care face obiectul controlului) înainte de inițierea formală a procedurii”[138], inclusiv în contextul unei eventuale noi proceduri.

135. Deși CEPD consideră că autoritățile de supraveghere se bucură de un anumit grad de libertate pentru a decide cum să își încadreze domeniul de aplicare al anchetelor, CEPD reamintește că unul dintre principalele obiective ale RGPD este acela de a asigura coerența în întreaga Uniune Europeană, iar cooperarea dintre ASP și ASV-uri constituie unul dintre mijloacele prin care se poate realiza acest lucru. De asemenea, CEPD reamintește de existența unei game complete de instrumente de cooperare prevăzute de RGPD (inclusiv articolele 61 și 62 din RGPD), ținând cont de obiectivul de a ajunge la un consens în cadrul mecanismului de cooperare și de necesitatea de comunica toate informațiile relevante, cu scopul de a asigura protecția drepturilor și libertăților fundamentale ale persoanelor vizate.

136. CEPD consideră că, atunci când stabilește domeniul de aplicare al anchetei, deși acesta poate fi limitat, o ASP trebuie să-l încadreze astfel încât să permită ASV să își îndeplinească rolul în mod eficace, alături de ASP, atunci când stabilește dacă a existat o încălcare a RGPD.

7 DESPRE ACȚIUNILE CORECTIVE DECISE DE ASP - ÎN SPECIAL IMPUNEREA UNEI MUSTRĂRI

7.1 Analiza efectuată de ASP în cadrul proiectului de decizie

137. Proiectul de decizie explică faptul că, dacă în proiectul preliminar de decizie, competențele corective propuse în vederea impunerii erau atât o mustrare, conform articolului 58 alineatul (2) litera (b) din RGPD, cât și o amendă administrativă, conform articolului 58 alineatul (2) litera (i) din RGPD, proiectul de decizie final constă în impunerea numai a unei amenzi administrative în ceea ce privește TIC, în calitate de operator[139].

138. În observațiile sale privind proiectul preliminar de decizie, TIC a înaintat o obiecție la decizia de a emite o mustrare, susținând că încălcările articolului 33 alineatele (1) și (5) din RGPD nu cuprind „operațiuni de prelucrare”, în timp ce articolul 58 alineatul (2) alineatul (b) din RGPD le oferă autorităților de supraveghere competența de a emite mustrări în cazul în care operațiunile de prelucrare au încălcat dispozițiile RGPD[140]. Principalul argument al TIC se baza în principal pe faptul că nici întârzierea în notificarea autorității de supravegherea, nici lipsa păstrării evidențelor adecvate nu constituie o operațiune de prelucrare în sine[141].

139. În proiectul său de decizie, AS IE și-a explicat decizia de a nu emite o mustrare, reamintind argumentul oferit de TIC în observațiile sale referitoare la proiectul preliminar de decizie, susținând că încălcările

[138] Orientările privind ORM, punctul 28.
[139] Proiectul de decizie, punctul 12.1.
[140] Observațiile TIC în ceea ce privește proiectul preliminar de decizie, punctul 11.1.
[141] Proiectul de decizie, punctul 12.4.

articolului 33 alineatele (1) și (5) din RGPD nu cuprind „operațiuni de prelucrare”, în timp ce articolul 58 alineatul (2) alineatul (b) din RGPD le oferă autorităților de supraveghere competența de a emite mustrări în cazul în care operațiunile de prelucrare au încălcat dispozițiile RGPD[142]. AS IE a considerat că termenul „operațiune (operațiuni) de prelucrare” apare de 50 de ori în RGPD și pare să fie utilizat pentru a desemna tratamentul sau utilizarea, sau, altfel spus, lucruri care se aplică datelor cu caracter personal controlate de un operator, dar că, în același timp, definiția cuvântului „prelucrare” oferită de RGPD este foarte amplă, ceea ce face să fie discutabil că, având în vedere faptul că o încălcare a securității este un lucru care afectează datele cu caracter personal sau care se aplică acestora, rezultă că obligația de notificare (în măsura în care, inerent, aceasta trebuie să implice o examinare a ceea ce s-a întâmplat datelor cu caracter personal sau a modului în care acestea au fost afectate) este legată intrinsec de una sau de mai multe operațiuni de prelucrare[143]. AS IE nu a considerat necesar să formuleze o concluzie finală privind sensul și efectul termenului „operațiuni de prelucrare” în proiectul de decizie ci, „în ansamblu”, a considerat că argumentul juridic prezentat de TIC a fost „unul stabil”, hotărând să nu continue prin emiterea unei mustrări adresate societății TIC[144].

7.2 Rezumatul obiecțiilor formulate de ASV-uri

140. **AS DE** a formulat o obiecție privind faptul că, deși în proiectul preliminar de decizie s-a avut în vedere atât o mustrare, cât și o amendă, în proiectul de decizie s-a inclus doar o amendă. AS DE nu a fost de acord cu motivarea prezentată de AS IE cu privire la decizia de a nu impune o mustrare. Potrivit AS DE, motivarea juridică acceptată de ASP ca fiind „stabilă” nu este convingătoare, deoarece interpretarea juridică impune nu doar o examinare a formulării dispoziției, ci și a sensului și a scopului acesteia, a istoricului elaborării sale și a integrării sale sistematice în întregul complex de reglementare.

7.3 Poziția ASP cu privire la obiecții

141. În Memorandumul său compus, AS IE a considerat că, deși obiecția AS DE face referire la „conformitatea [cu RGPD a] măsurii preconizate în raport cu un operator sau cu o persoană împuternicită de operator”, aceasta nu demonstrează în ce mod lipsa emiterii unei mustrări către TIC ar putea genera riscuri considerabile pentru persoanele vizate[145] privind decizia de a nu emite o mustrare nu a fost relevantă și motivată în conformitate cu articolul 4 alineatul (24) din RGPD.

142. Cu toate acestea, abordând fondul chestiunii (chestiunilor) semnificative semnalate de obiecții, ASP a explicat că a luat în considerare termenul „operațiuni de prelucrare” în conformitate cu sensul și aplicarea sa din întregul RGPD, remarcând că acest termen este utilizat numai pentru competențele autorităților de supraveghere în temeiul articolului 58 din RGPD. În urma observațiilor transmise de TIC ca răspuns la obiecțiile ASV cu privire la acest aspect, ASP a decis, luând în considerare domeniul de aplicare al anchetei care viza obligațiile operatorului în ceea ce privește notificarea încălcării securității, că ancheta sa *„nu implica o constatare potrivit căreia operațiunile de prelucrare de bază*

[142] Observațiile TIC în ceea ce privește proiectul preliminar de decizie, punctul 11.1.
[143] Proiectul de decizie, punctul 12.5.
[144] Proiectul de decizie, punctul 12.5. Celelalte argumente separate aduse de TIC cu privire la motivele pentru care impunerea unei mustrări nu era considerată adecvată (observațiile TIC în ceea ce privește proiectul preliminar de decizie, punctele 11.2-11.4) nu au fost luate în considerare separat, ținând cont de decizia sus-menționată (Proiectul de decizie, punctul 12.6).
[145] Memorandumul compus, punctul 5.79.

referitoare la încălcarea securității au încălcat [...] RGPD"[146]. Prin urmare, ASP a considerat că nu există niciun motiv pentru a-și revizui decizia de a nu emite o mustrare, prin prisma obiecției AS DE.

143. ASP a remarcat că poziția sa din proiectul de decizie de a nu emite o mustrare se aplică numai circumstanțelor specifice ale acestei cauze; prin urmare, aceasta nu aduce atingere deciziilor viitoare privind mustrările, care ar putea fi adoptate de ASP sau de orice altă ASV[147].

7.4 Analiza CEPD

7.4.1 Evaluarea caracterului relevant și motivat al obiecțiilor

144. Obiecția **AS DE** se referă la conformitatea măsurii preconizate cu RGPD, întrucât aceasta indică acțiunea corectivă a cărei includere de către ASP în decizia finală ar fi adecvată, în opinia sa: prin urmare, este o obiecție relevantă, care prezintă în mod adecvat concluzia diferită propusă. În plus, include motivarea juridică ce-i susține opinia și propune o interpretare juridică alternativă. Totuși, obiecția nu demonstrează clar importanța riscului pe care îl prezintă proiectul de decizie în ceea ce privește drepturile și libertățile persoanelor vizate și/sau libera circulație a datelor cu caracter personal. În special, nu oferă o motivație privind modul în care lipsa impunerii unei mustrări în acest caz specific - în care se impune și o amendă - poate să declanșeze riscuri pentru drepturile și libertățile fundamentale ale persoanelor vizate.

7.4.2 Concluzie

145. CEPD consideră că această obiecție nu îndeplinește cerințele articolului 4 alineatul (24) din RGPD.

146. CEPD ia notă de poziția ASP potrivit căreia poziția sa de a nu emite o mustrare se aplică numai circumstanțelor specifice acestei cauze; prin urmare, aceasta nu aduce atingere deciziilor viitoare privind mustrările, care ar putea fi adoptate de ASP sau de orice altă ASV[148].

147. Astfel cum s-a indicat mai sus, decizia CEPD de a nu evalua fondul sau substanța obiecției formulate nu aduce atingere deciziilor viitoare ale CEPD privind aceleași chestiuni sau privind chestiuni similare.

8 PRIVIND ACȚIUNILE CORECTIVE - ÎN SPECIAL CALCULUL AMENZII ADMINISTRATIVE

8.1 Analiza efectuată de ASP în cadrul proiectului de decizie

148. Proiectul de decizie explică modul în care AS IE a luat în considerare criteriile din articolul 83 alineatul (2) din RGPD atunci când a decis dacă să impună sau nu o amendă administrativă și modul în care să stabilească valoarea acesteia[149].

149. În ceea ce privește calculul amenzii, proiectul de decizie a analizat în primul rând **natura, gravitatea și durata încălcării**, conform articolului 83 alineatul (2) litera (a) din RGPD[150]. Proiectul de decizie a luat

[146] Memorandumul compus, punctul 5.78.
[147] Memorandumul compus, punctul 5.78.
[148] Memorandumul compus, punctul 5.78.
[149] Proiectul de decizie, punctele 14.1-14.62.
[150] Articolul 83 alineatul (2) litera (a) din RGPD se referă la *„natura, gravitatea și durata încălcării, ținându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum și de numărul persoanelor vizate afectate și de nivelul prejudiciilor suferite de acestea".*

în considerare „natura, domeniul de aplicare sau scopul prelucrării", făcând referire la natura operațiunilor de prelucrare efectuate de Twitter (o platformă de „microblogging" și de comunicare socială, pe care utilizatorii au posibilitatea de a-și documenta gândurile în mesaje „tweet"), la natura prelucrării, care a dat naștere încălcării securității (determinată de o eroare ce a făcut ca mesajele tweet anterior „protejate" să devină „neprotejate" și accesibile publicului - în cazurile în care utilizatorii de Android și-au schimbat adresa de e-mail) și la domeniul de aplicare al prelucrării (eroarea a afectat cel puțin 88 726 de utilizatori din UE/SEE, deoarece și alte persoane au fost afectate între data erorii, respectiv 4 noiembrie 2014, și remedierea integrală a acesteia, de la data de 14 ianuarie 2019, însă nu a fost posibilă identificarea tuturor)[151].

150. De asemenea, proiectul de decizie a ținut seama **de numărul persoanelor vizate afectate și de nivelul prejudiciilor suferite de acestea**[152] concluzionând că numărul de persoane vizate care ar fi putut să fie afectate de notificarea transmisă cu întârziere și potențialul de a cauza prejudicii persoanelor vizate, determinat de evaluarea care, în consecință, a fost efectuată de AS cu întârziere, au fost factori relevanți de luat în considerare [153]. S-a reamintit faptul că impactul asupra utilizatorilor individuali și posibilitatea de generare a daunelor din această cauză va afecta nivelul și natura datelor cu caracter personal devenite publice și că exista cel puțin potențial de a genera prejudicii persoanelor vizate, legat de întârzierea acțiunilor de remediere[154]. Poziția AS IE în proiectul preliminar a fost că, *„deși TIC nu a confirmat natura specifică a datelor care au devenit publice în cadrul încălcării securității, s-a dedus în mod rezonabil că, având în vedere numărul de utilizatori afectați și natura serviciilor oferite de TIC, unele date cu caracter personal eliberate cel puțin în cea ce privește <u>unii</u> utilizatori ar fi inclus categorii sensibile de date și alte materiale cu un caracter deosebit de privat"*[155]. Această poziție a fost nuanțată suplimentar în proiectul de decizie, prin prisma observațiilor transmise de TIC, întrucât AS IE a decis că *„ar trebui să se acorde mai puțină importanță acestui factor"* în temeiul faptului că, *„deși nu se poate spune sigur că niciun utilizator afectat de încălcarea securității nu a fost afectat de notificarea efectuată cu întârziere, nu au existat dovezi directe privind prejudiciile aduse acestora, rezultate în urma notificării transmise cu întârziere"*[156].

151. În ceea ce privește **natura încălcării**, proiectul de decizie a subliniat că încălcarea articolului 33 alineatele (1) și (5) din RGPD nu se referă la elementele materiale ale încălcării securității[157]. De asemenea, AS IE a luat în considerare că natura obligațiilor în temeiul articolului 33 alineatele (1) și (5) din RGPD conferă conformității un rol central pentru funcționarea în ansamblu a regimului de supraveghere și de punere în aplicare implementat de autoritățile de supraveghere în ceea ce privește atât chestiunea specifică a situațiilor de încălcare a securității datelor cu caracter personal, cât și identificarea și evaluarea chestiunilor mai ample de nerespectare a acestor obligații de către operatori și că nerespectarea acestor obligații are consecințe grave prin faptul că riscă să pună în pericol exercitarea eficace de către autoritățile de supraveghere a funcțiilor lor în temeiul RGPD[158].

[151] Proiectul de decizie, punctul 14.2.
[152] Proiectul de decizie, punctele 14.3-14.5.
[153] Proiectul de decizie, punctul 14.5.
[154] Proiectul de decizie, punctul 14.5 (Proiectul de decizie reține că „În mod clar, impactul asupra utilizatorilor individuali și posibilitatea apariției unor prejudicii rezultate în urma acestuia va depinde de măsura în care datele cu caracter personal au devenit publice și, de asemenea, de natura datelor cu caracter personal").
[155] Proiectul de decizie, punctul 14.5.
[156] Proiectul de decizie, punctul 14.5.
[157] Proiectul de decizie, punctul 14.6.
[158] Proiectul de decizie, punctul 14.11.

152. În ceea ce privește **gravitatea încălcării** articolului 33 alineatul (1) din RGPD, proiectul de decizie a ținut cont de modul în care aceasta a afectat scopul în ansamblu de a notifica o încălcare a securității datelor cu caracter personal autorității de supraveghere, de faptul că nu s-au demonstrat daune materiale aduse persoanelor vizate, de faptul că măsurile de remediere luate de TIC s-au limitat la acțiuni orientate spre viitor de oprire a erorii (și nu s-au concretizat într-o analiză retrospectivă de identificare a riscurilor la adresa persoanelor vizate, generate de încălcarea securității) și de aparenta neefectuare de către TIC a unei evaluări formale a riscurilor[159]. Proiectul de decizie nu a considerat că afirmația TIC potrivit căreia încălcarea securității s-a datorat unei erori izolate (care a determinat întârzierea în notificarea RPD) are suficientă forță încât să reducă gravitatea încălcării (dar a ținut cont de natura izolată a incidentului, depărtându-se de opinia provizorie din proiectul preliminar potrivit căreia încălcarea securității indica o problemă mai amplă, sistemică)[160]. În ceea ce privește gravitatea încălcării articolului 33 alineatul (5) din RGPD, proiectul de decizie a evidențiat că este necesară documentarea adecvată a încălcărilor pentru a oferi autorității de supraveghere posibilitatea de a verifica respectarea articolului 33 din RGPD de către operator[161] și că AS IE avea obligația de a adresa numeroase întrebări pentru a dobândi claritate în ceea ce privește faptele asociate notificării încălcării securității[162], dar a recunoscut că deficiențele în documentare au provenit dintr-o neînțelegere cu bună credință a cerințelor (care sunt, totuși, clare în formularea dispoziției)[163]. Proiectul de decizie a concluzionat că încălcarea s-a situat *„la un nivel de gravitate scăzut-moderat”*[164].

153. În ceea ce privește **durata încălcării** articolului 33 alineatul (1) din RGPD, proiectul de decizie a considerat că aceasta a fost o perioadă de două zile și a evaluat-o prin prisma intervalului total permis în general pentru notificarea situațiilor de încălcare a securității (72 de ore), remarcând că aceasta nu este neînsemnată sau neimportantă[165]. În ceea ce privește durata încălcării articolului 33 alineatul (5) din RGPD, proiectul de decizie a concluzionat că aceasta continua să existe[166].

154. În ceea ce privește **articolul 83 alineatul (2) litera (b) din RGPD** (caracterul intenționat sau neglijent al încălcării), AS IE a concluzionat în proiectul său de decizie că a existat un **caracter neglijent** asociat încălcării de către TIC a articolului 33 alineatul (1) din RGPD[167], evidențiind că întârzierea în notificarea RPD de la nivel global s-a produs din cauză că o parte a protocolului intern al Grupului Twitter nu a fost finalizată potrivit instrucțiunilor, iar protocolul nu a fost cât se poate de clar.[168] Acest lucru a dus la concluzia că întârzierea s-a produs ca urmare a unei neglijențe a operatorului, însă observația TIC, potrivit căreia notificarea transmisă cu întârziere nu indica o problemă sistemică mai amplă și a reprezentat un eveniment izolat, a fost acceptată[169]. AS IE nu a identificat nicio dovadă de fapte săvârșite cu intenție în ceea ce privește încălcarea articolului 33 alineatul (1) din RGPD[170]. De asemenea, proiectul de decizie a identificat existența unui caracter neglijent în ceea ce privește

[159] Proiectul de decizie, punctele 14.16-14.18.
[160] Proiectul de decizie, punctul 14.19.
[161] Proiectul de decizie, punctul 14.20.
[162] Proiectul de decizie, punctul 14.21.
[163] Proiectul de decizie, punctul 14.24.
[164] Proiectul de decizie, punctul 14.24.
[165] Proiectul de decizie, punctul 14.26 (a început la expirarea celor 72 de ore de la 3 ianuarie 2019 (respectiv la 6 ianuarie 2019) și s-a încheiat în momentul în care TIC a notificat încălcarea securității la 8 ianuarie 2019).
[166] Proiectul de decizie, punctul 14.29.
[167] Proiectul de decizie, punctul 14.34.
[168] Proiectul de decizie, punctele 14.33-14.34.
[169] Proiectul de decizie, punctul 14.34.
[170] Proiectul de decizie, punctul 14.35.

încălcarea articolului 33 alineatul (5) din RGPD de către TIC[171], deoarece nu au existat cunoștințele și premeditarea pentru a cauza o încălcare (care ar fi echivalat cu intenția), ci documentarea nu a fost suficientă pentru a permite verificarea conformității cu articolul 33[172].

155. În ceea ce privește **articolul 83 alineatul (2) litera (c) din RGPD**, respectiv acțiunile întreprinse de operator pentru **a reduce prejudiciul suferit de persoanele vizate,** proiectul de decizie a considerat că s-au luat măsuri de remediere pentru a evita repetarea problemei și pentru a remedia eroarea, acestea fiind considerate singura circumstanță atenuantă în evaluarea valorii amenzii care urma să fie impusă[173].

156. Proiectul de decizie a luat în considerare **articolul 83 alineatul (2) litera (d) din RGPD**, respectiv **gradul de responsabilitate** al operatorului sau al persoanei împuternicite de operator, ținându-se seama de măsurile tehnice și organizatorice sporite implementate de TIC în calitate de operator, inclusiv de modificarea protocolului intern al Grupului Twitter (care, potrivit constatărilor AS IE, nu era cât se poate de clar) și de măsurile de formare a personalului adoptate ulterior de Twitter, Inc. (s-a asigurat formare suplimentară pe plan intern, evidențiindu-se importanța menționării echipei RPD - și prin urmare a TIC în calitate de operator - în sistemul intern de tichete), precum și de existența structurilor și garanțiilor interne privind responsabilitatea pentru problemele legate de securitatea informațiilor și de existența unui audit de specialitate recurent extern, efectuat de o parte terță, asupra Programului de securitate a informațiilor al Twitter[174]. Deși nu s-a constatat că problemele apărute indică o problemă sistemică mai amplă[175], iar TIC a dat dovadă de o abordare în general responsabilă în ceea ce privește securitatea datelor[176], s-a considerat că operatorul a demonstrat un nivel de responsabilitate moderat-ridicat, întrucât modificarea ulterioară a protocolului a demonstrat și lipsa clarității acestuia[177].

157. A fost evaluat **gradul de cooperare** cu autoritatea de supraveghere, conform **articolului 83 alineatul (2) litera (f) din RGPD** și s-a constatat că aceasta nu a reprezentat o circumstanță atenuantă[178]. AS IE a recunoscut că TIC a colaborat pe deplin, dar a remarcat că era o obligație statutară, iar TIC nu a depășit limitele acestei îndatoriri[179].

158. În ceea ce privește **articolul 83 alineatul (2) litera (g) din RGPD,** cu privire la **categoriile de date cu caracter personal afectate**, proiectul de decizie a concluzionat că orice categorie de date cu caracter personal ar fi putut fi afectată de notificarea efectuată cu întârziere și că nu se poate spune cu siguranță că nu s-au adus daune persoanelor vizate și că nu au existat categorii de date cu caracter personal afectate[180].

159. Modul în care încălcarea a devenit cunoscută de AS IE a fost considerat factor relevant în stabilirea valorii amenzii (conform articolului 83 alineatul (2) litera (h) din RGPD), deoarece, deși TIC a fost deschisă în furnizarea tuturor documentelor disponibile, evidențele nu au permis AS IE să verifice

[171] Proiectul de decizie, punctul 14.38.
[172] Proiectul de decizie, punctele 14.36, 14.38.
[173] Proiectul de decizie, punctele 14.39-14.42.
[174] Proiectul de decizie, punctele 14.43-14.47.
[175] Proiectul de decizie, punctul 14.45.
[176] Proiectul de decizie, punctul 14.47.
[177] Proiectul de decizie, punctul 14.47.
[178] Proiectul de decizie, punctul 14.50.
[179] Proiectul de decizie, punctul 14.49.
[180] Proiectul de decizie, punctul 14.54.

conformitatea cu articolul 33 din RGPD, iar informațiile furnizate inițial în notificarea transmisă către AS IE au avut un caracter imprecis[181].

160. S-a constatat că **criteriile din articolul 83 alineatul (2) literele (e), (i) și (j) din RGPD** nu sunt aplicabile și nu s-au identificat alte elemente în ceea ce privește **articolul 83 alineatul (2) litera (k) din RGPD**[182].

161. AS IE a subliniat în proiectul de decizie că, în absența unor orientări specifice la nivelul UE privind calculul amenzilor, nu avea obligația de a aplica o metodologie specifică sau de a utiliza un punct de pornire fix[183] și că expresia „atenția cuvenită" le oferă autorităților de supraveghere o largă putere de apreciere a modului în care trebuie evaluați factorii din articolul 83 alineatul (2) din RGPD[184].

162. În ceea ce privește identificarea întreprinderii relevante pentru calculul limitei amenzii stabilite la **articolul 83 alineatul (4) din RGPD**, AS IE a subliniat că, chiar dacă TIC se bucură de autonomie în ceea ce privește controlul asupra prelucrării datelor, nu înseamnă că aceasta încetează să facă parte **dintr-o singură entitate economică** împreună cu societatea-mamă și a remarcat că, în plus față de faptul că TIC este deținută de Twitter, Inc., jurisconsultul Twitter, Inc. pare să fie unul dintre cei trei administratori ai TIC[185].

163. Din aceste motive, limita pentru valoarea oricărei amenzi impuse a fost calculată de ASP în raport cu cifra de afaceri a Twitter, Inc[186]. Întrucât cifra de afaceri anuală a Twitter, Inc. în anul 2018 a fost de 3 miliarde USD, s-a considerat că limita este de 60 de milioane USD (2 % din 3 miliarde USD)[187].

164. În aplicarea principiilor **eficacității, proporționalității și disuasiunii [articolul 83 alineatul (1) din RGPD]**, proiectul de decizie a considerat că o amendă nu poate fi eficace dacă nu are o semnificație în raport cu venitul operatorului, că încălcarea nu trebuie să fie luată în considerare în mod abstract, indiferent de impactul asupra operatorului și că viitoarele încălcări trebuie să fie descurajate[188].

165. AS IE a propus impunerea unei amenzi administrative în intervalul de 150 000-300 000 USD, respectiv între 0,005 % și 0,01 % din cifra de afaceri anuală sau între 0,25 % și 0,5 % din valoarea maximă a amenzii care poate fi aplicată în ceea ce privește aceste încălcări. Aceasta echivalează cu o amendă în euro între 135 000 și 275 000[189].

8.2 Rezumatul obiecțiilor formulate de ASV-uri

166. **AS AT** a formulat o obiecție cu privire la valoarea amenzii propuse și cu privire la faptul că ASP a propus un interval de valori în locul unei sume fixe. În ceea ce privește articolul 83 alineatul (2) litera (a) din RGPD, AS AT a subliniat că cel puțin 88 726 de persoane (însă probabil mai multe) au fost afectate de încălcarea securității și *„este foarte probabil ca date sensibile să fi fost divulgate publicului larg"*.

[181] Proiectul de decizie, punctul 14.58.
[182] Proiectul de decizie, punctele 14.48, 14.59, 14.60, 14.61.
[183] Proiectul de decizie, punctul 15.2.
[184] Proiectul de decizie, punctul 15.1.
[185] Proiectul de decizie, punctul 15.13.
[186] Proiectul de decizie, punctul 15.14.
[187] Proiectul de decizie, punctul 15.19.
[188] Proiectul de decizie, punctul 15.18.
[189] Proiectul de decizie, punctul 15.20 (limita superioară propusă în proiectul de decizie este mai mică decât proiectul preliminar de decizie, pentru a reflecta schimbările în ceea ce privește opiniile referitoare la gravitat, gradul de responsabilitate a operatorului și caracterul sistemic sau nu al încălcărilor). La punctul 15.21, proiectul de decizie a subliniat că, pentru a proteja drepturile procedurale ale TIC, s-a propus un interval pentru amendă, nu o valoare fixă, și s-a recunoscut posibilitatea ca ASV-urile să prezinte observații cu privire la valoarea necesară a penalității în cadrul intervalului respectiv.

167. Obiecția formulată de AS AT a exprimat un dezacord cu privire la modul în care proiectul de decizie a analizat*momentul în care trebuie să se considere că operatorul a avut cunoștință de încălcarea securității datelor*. Mai precis, AS AT a susținut în obiecția sa că TIC ar fi trebuit să transmită notificarea încălcării securității datelor în termen de 72 de ore de la momentul în care persoana împuternicită de operator a primit raportul privind eroarea și astfel a luat cunoștință de încălcarea securității. AS AT a evidențiat că TIC răspunde de supravegherea operațiunilor de prelucrare efectuate de persoana împuternicită și că un operator nu trebuie să urmărească să ascundă o eroare a persoanei împuternicite, cu care are o relație contractuală și care a fost aleasă chiar de operator. Acest lucru contribuie la evaluarea încălcării articolului 33 alineatul (1) din RGPD de către AS AT ca fiind „gravă".

168. În ceea ce privește *„dacă încălcarea a fost comisă intenționat sau din neglijență"* [articolul 83 alineatul (2) litera (b) din RGPD], AS AT a susținut că comportamentul TIC trebuie să fie etichetat ca fiind „intenționat" în baza criteriilor de cunoștințe și premeditare stabilite în Orientările privind aplicarea și stabilirea unor amenzi administrative („WP253") ale Grupului de lucru „Articolul 29", avizate de CEPD.[190] Întrucât criteriul care se referă la acțiunile *întreprinse pentru a reduce prejudiciul* suferit de persoanele vizate [articolul 83 alineatul (2) litera (c) din RGPD], AS AT a evidențiat că *„inițial TIC nu a avut intenția de a notifica utilizatorii care au fost afectați de încălcarea securității" și că „măsurile luate de Twitter Inc. pentru a rectifica eroarea constituie singura circumstanță atenuantă".* În final, AS AT consideră că intervalul pentru amendă propus de AS IE nu este nici eficace, nici proporțional, nici disuasiv, având în vedere criteriile enumerate la articolul 83 alineatul (2) literele (a) - (k) din RGPD. În concluzie, AS AT a propus impunerea unei amenzi administrative mai mari, care ar putea să îndeplinească cerința de eficacitate, proporționalitate și disuasiune (respectiv *„o sumă minimă de 1 % din cifra de afaceri anuală a întreprinderii"*).

169. **AS DE** a formulat o obiecție, susținând că amenda propusă de ASP este „prea mică" și „nu respectă dispozițiile din articolul 83 alineatul (1) din RGPD". Mai precis, AS DE a susținut că amenda nu este disuasivă. Obiecția a reamintit că o sancțiune poate fi considerată eficace și disuasivă dacă este adecvată atât ca măsură preventivă generală - pentru a descuraja publicul larg să comită încălcări și pentru a consolida încrederea publicului larg în validitatea dreptului Uniunii - cât și ca măsură preventivă specială - pentru a descuraja infractorii să comită alte încălcări. AS DE continuă, prin a susține că un indiciu important privind sumele necesare pentru a obține disuasivitatea poate fi oferit de capacitatea unei întreprinderi (în ceea ce privește cifra de afaceri): aceasta poate să implice luarea în considerare a părții din cifra de afaceri generată de produsele cu privire la care s-a comis încălcarea, care pot oferi un indiciu al nivelului încălcărilor. De asemenea, AS DE susține că efectul disuasiv al amenzilor mari se poate obține numai dacă sumele impuse nu pot fi achitate cu ușurință din cauza activelor sau a veniturilor mari, evidențiind că amenda trebuie să aibă un efect disuasiv, în special în ceea ce privește prelucrarea specifică a datelor. În consecință, amenda care amenință trebuie să fie suficient de mare încât să facă prelucrarea datelor neeconomică și obiectiv ineficientă. Întrucât modelul de afaceri al Twitter se bazează pe prelucrarea datelor și întrucât Twitter generează cifra de afaceri în principal prin prelucrarea datelor, AS DE consideră că o amendă disuasivă în acest caz specific ar trebui să fie, în consecință, atât de mare, încât să facă prelucrarea ilegală a datelor neprofitabilă. În baza conceptului amenzilor aplicabile autorităților de supraveghere din Germania, amenda pentru încălcarea descrisă în proiectul de decizie s-ar situa aproximativ în intervalul 7.348.035,00 EUR - 22.044.105,00 EUR.

[190] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

170. **AS HU** a susținut că, deși *„amenzile sunt justificate pentru încălcările comise”, „amenda prezentată în proiect este nerezonabil de mică, neproporțională și, prin urmare, nu este disuasivă, având în vedere gravitatea încălcării comise și puterea operatorului pe piața de la nivel mondial”.*

171. **AS IT** a solicitat ASP să *„revizuiască proiectul de decizie și în ceea ce privește valoarea amenzii administrative, ținând cont și de elementele agravante specifice ale cazului în ceea ce privește natura operatorului de date și gravitatea și durata încălcării securității datelor”.*

8.3 Poziția ASP cu privire la obiecții

172. AS IE a evaluat obiecțiile formulate de AS AT, AS DE și AS HU în ceea ce privește caracterul „relevant și motivat” al amenzii administrative, în sensul articolului 4 alineatul (24) din RGPD. În același timp, AS IE nu a dat curs acestor obiecții, din motivele prezentate în Memorandumul compus[191].

173. În special, în ceea ce privește obiecțiile AS AT și DE, AS IE consideră că evaluarea și aplicarea factorilor la articolele 83 alineatul (2) literele (a) și (b) din RGPD, astfel cum acestea sunt elaborate în proiectul de decizie, sunt adecvate. În ceea ce privește obiecția AS AT, AS IE susține că încălcarea de către TIC a articolului 33 alineatele (1) și (5) din RGPD a fost rezultatul neglijenței TIC, iar nu al unei omisiuni intenționate[192]. Prin urmare, AS IE consideră că amenda propusă de AS AT nu este proporțională[193]. În plus, AS IE susține că preocuparea AS IT în ceea ce privește intervalul amenzii propus în proiectul de decizie, spre deosebire de o sumă fixă, nu a fost bine elaborat și clarificat de această ASV[194]. În ceea ce privește obiecția AS DE, AS IE a luat act de obiecția AS DE cu privire la necesitatea ca amenda să respecte cerința disuasiunii, dar este de părere că nivelul amenzii propuse de AS DE nu este proporțional în acest caz[195]. Din motivele prezentate mai sus, AS IE consideră că aceste obiecții sunt motivate și relevante, însă propune să nu li se dea curs[196].

174. AS IE a luat în considerare în mod corespunzător perspectiva AS AT în ceea ce privește momentul la care TIC a luat cunoștință de încălcarea securității și a transmis notificarea cu privire la aceasta, însă a concluzionat că, fără a ține seama de „conștientizarea” efectivă a încălcării securității de către TIC la 7 ianuarie 2019, TIC ar fi trebuit să aibă cunoștință de încălcarea securității cel târziu la 3 ianuarie 2019[197]. Pentru identificarea datei de 3 ianuarie 2019 ca fiind data la care TIC ar fi trebuit să aibă cunoștință de încălcarea securității, AS IE a luat în considerare faptul că se produsese o întârziere și înainte, în perioada de la data la care incidentul a fost notificat pentru prima oară de un contractant către Twitter, Inc. până când Twitter, Inc. a început examinarea acestuia[198]. În plus, AS IE clarifică faptul că nu sugerează că *„în general, trebuie să se considere automat că operatorii de date au cunoștință de situațiile de încălcare a securității datelor, în același moment în care persoana împuternicită ia cunoștință de încălcarea securității”*[199]. De asemenea, AS IE afirmă că *„se întâmplă de obicei ca o persoană împuternicită de operator să ia cunoștință de incident mai devreme decât operatorul și că, având în vedere că procesul convenit de către operator și persoana împuternicită de acesta este eficace*

[191] Memorandumul compus, punctele 5.60- 5.72.
[192] Memorandumul compus, punctul 5.62.
[193] Memorandumul compus, punctul 5.63.
[194] Memorandumul compus, punctul 5.64.
[195] Memorandumul compus, punctul 5.68.
[196] Memorandumul compus, punctele 5.65, 5.68.
[197] Memorandumul compus, punctul 5.48.
[198] Memorandumul compus, punctul 5.50.
[199] Memorandumul compus, punctul 5.50.

și/sau este respectat, operatorului i se va aduce la „cunoștință" încălcarea securității [...] într-un mod care îi permite să își respecte obligația de a o notifica"[200].

8.4 Analiza CEPD

8.4.1 Evaluarea caracterului relevant și motivat al obiecțiilor

175. În ceea ce privește posibilitatea ca anumite obiecții relevante și motivate cu privire la conformitatea cu RGPD a măsurii preconizate în raport cu operatorul sau cu persoana împuternicită de operator[201] să conteste valoarea amenzilor propuse, CEPD a clarificat de curând că *„este posibil ca obiecția să conteste elementele care stau la baza calculului valorii amenzii"*[202]. Aceasta poate să reprezinte un exemplu de obiecție referitor la conformitatea cu RGPD a măsurii preconizate în raport cu operatorul sau cu persoana împuternicită de operator.

176. În cauza de față, obiecția **AS AT** contestă elementele pe care se bazează AS IE în calculul valorii amenzii și vizează astfel conformitatea a măsurii propuse cu RGPD în raport cu operatorul. AS AT a clarificat legătura dintre obiecția sa și proiectul de decizie și a demonstrat modul în care schimbările produse ar genera o concluzie diferită. În plus, aceasta a oferit argumente referitoare la motivul pentru care se propune modificarea deciziei, oferind o interpretare alternativă a criteriilor enumerate de articolul 83 din RGPD și făcând trimitere la argumente faptice și juridice. AS AT demonstrează clar importanța riscurilor pe care le prezintă proiectul de decizie în primul rând prin faptul că susține că amenda propusă nu este eficace și disuasivă în mod adecvat și reamintind că, în acest scop, trebuie să prezinte probabilitatea de a descuraja publicul larg de la comiterea unei încălcări similare și să confirme încrederea publicului în aplicarea dreptului Uniunii, precum și să descurajeze operatorul să comită alte încălcări. În plus, în evaluarea gravității încălcării, obiecția se referă și la măsura în care persoanele vizate (într-un număr care probabil este mai mare decât cel identificat) au fost afectate de încălcarea securității (de exemplu prin expunerea mesajelor tweet care anterior fuseseră protejate și care prezentau probabilitatea de a conține date sensibile la publicul larg. Presupusul caracter intenționat al încălcării, conform AS AT, implică un impact mai mare asupra capacității de a diferenția binele și răul față de o faptă comisă din neglijență. Prin prisma evaluării de mai sus, CEPD consideră că obiecția AS AT este relevantă și motivată în conformitate cu articolul 4 alineatul (24) din RGPD. În consecință, CEPD evaluează fondul chestiunilor semnificative semnalate de această obiecție (vezi secțiunea 8.4.2de mai jos).

177. De asemenea, obiecția **AS DE** trebuie să fie considerată relevantă, deoarece se referă la conformitatea măsurii preconizate cu RGPD, contestând elementele care au stat la baza calculării valorii amenzii. Mai precis, susține că amenda impusă de AS IE nu este disuasivă și, prin urmare, calculul efectuat nu se conformează articolului 83 alineatul (1) din RGPD. AS DE a clarificat că sancțiunea trebuie să fie considerată eficace și disuasivă atunci când reprezintă o măsură preventivă generală pentru a descuraja publicul larg să comită încălcări, precum și pentru a-și afirma încrederea în validitatea dreptului Uniunii, dar și atunci când descurajează infractorul să comită alte încălcări. În plus, AS DE demonstrează clar importanța riscurilor pe care le prezintă proiectul de decizie în ceea ce privește drepturile și libertățile persoanelor vizate, întrucât este posibil ca neimpunerea unei sancțiuni disuasive și eficace să nu descurajeze operatorul să comită alte încălcări.

[200] Memorandumul compus, punctul 5.50.
[201] RGPD, articolul 4 alineatul (24).
[202] Orientările privind ORM, punctul 34.

178. Un alt argument oferit de AS DE pentru a demonstra importanța riscurilor constă în faptul că lipsa unei gestionări adecvate a încălcării securității sugerează o „eroare sistemică", iar aceasta ar fi impus supunerea operatorului la un control mai aprofundat, dincolo de incidentul specific unic. De asemenea, AS DE a reamintit că era vizat un număr mai mare de persoane și că perioada de timp era la fel de importantă și a concluzionat că competențele corective impuse în temeiul articolului 58 alineatul (2) din RGPD trebuie să fie examinate prin prisma elementelor respective. În concluzie, CEPD consideră că obiecția AS DE este motivată și relevantă în sensul definiției articolului 4 alineatul (24) din RGPD. În consecință, CEPD evaluează fondul chestiunilor semnificative semnalate de această obiecție (vezi secțiunea 8.4.2 de mai jos).

179. Obiecția **AS HU** este relevantă, deoarece vizează conformitatea cu RGPD a măsurii preconizate, afirmând că amenda propusă este *„nerezonabil de mică, neproporțională și, prin urmare, nu este disuasivă"*. Cu toate acestea, deși obiecția face referire la *„«eroarea» care a existat în aplicația operatorului de-a lungul anilor"* și la *„natura sa gravă, care afectează securitatea datelor"*, precum și la *„gravitatea încălcării comise"* și la *„puterea operatorului de pe piața de la nivel mondial"*, aceasta nu demonstrează în mod clar importanța riscurilor în ceea ce privește drepturile și libertățile persoanelor vizate pe care o prezintă valoarea amenzii propusă de AS IE. În consecință, CEPD consideră că această obiecție nu îndeplinește cerințele articolului 4 alineatul (24) din RGPD[203].

180. În final, relevanța obiecției formulate de **AS IT** este demonstrată și de faptul că aceasta face referire la conformitatea cu GDPR a măsurii propuse, întrucât aceasta susține că AS IE trebuie să revizuiască proiectul de decizie în ceea ce privește stabilirea valorii amenzii administrative. Făcând referire la *„obiecțiile de mai sus"* și, astfel, la faptul că aspectele menționate sunt *„de natură structurală în ceea ce privește organizația operatorului" și „sigur produc efecte nu numai asupra cazului în discuție, ci și asupra oricărei încălcări a securității datelor care poate să apară în viitor",* obiecția AS IT demonstrează în mod clar importanța riscurilor pentru drepturile și libertățile persoanelor vizate în ceea ce privește stabilirea valorii amenzii.

181. În concluzie, CEPD consideră că obiecția AS IT este motivată și relevantă, îndeplinind cerințele articolului 4 alineatul (24) din RGPD. În consecință, CEPD va evalua fondul chestiunilor semnificative semnalate de această obiecție.

8.4.2 Evaluarea fondului chestiunii (chestiunilor) semnificative formulate de obiecțiile relevante și motivate

182. CEPD consideră că obiecțiile care s-au constatat a fi relevante și motivate în această subsecțiune[204] impun să se evalueze dacă proiectul de decizie propune o amendă care corespunde criteriilor stabilite de articolul 83 din RGPD și de Orientările Grupului de lucru „Articolul 29" privind aplicarea și stabilirea unor amenzi administrative în sensul Regulamentului nr. 2016/679 („WP253") (avizate de CEPD)[205].

[203] În consecință, CEPD nu se pronunță cu privire la fondul niciuneia dintre chestiunile semnificative semnalate de aceste obiecții. CEPD reiterează că decizia sa actuală nu aduce atingere evaluărilor care pot fi solicitate CEPD în alte cauze, inclusiv cu aceleași părți, ținând cont de conținutul proiectului de decizie relevant și de obiecțiile formulate de ASV-uri.
[204] Aceste obiecții sunt cele ale AS AT, AS DE și AS IT.
[205] Orientările Grupului de lucru „Articolul 29" privind aplicarea și stabilirea unor amenzi administrative în sensul Regulamentului nr. 2016/679, WP253, adoptate la 3 octombrie 2017 (avizate de CEPD la 25 mai 2020).

183. Într-adevăr, mecanismul pentru asigurarea coerenței poate fi, de asemenea, utilizat pentru a promova aplicarea consecventă a amenzilor administrative[206]: în cazul în care o obiecție relevantă și motivată contestă elementele pe care se bazează ASP pentru a calcula valoarea amenzii, CEPD poate instrui ASP să efectueze un nou calcul al amenzii propuse, eliminând deficiențele în stabilirea legăturilor de cauzalitate între faptele în discuție și modul în care s-a calculat amenda propusă în temeiul criteriilor din articolul 83 din RGPD și al standardelor comune stabilite de CEPD[207]. O amendă trebuie să fie eficace, proporțională și disuasivă, astfel cum stipulează articolul 83 alineatul (1) din RGPD, ținând cont de faptele cauzei[208]. În plus, atunci când decide cu privire la valoarea amenzii, ASP ia în considerare criteriile enumerate la articolul 83 alineatul (2) din RGPD.

184. În ceea ce privește natura, gravitatea și durata încălcării constatate la articolele 33 alineatele (1) și (5) din RGPD, **articolul 83 alineatul (2) litera (a) din RGPD** impune să se țină seama, printre altele, **de natura, de domeniul de aplicare sau scopul prelucrării în cauză**, precum și **de numărul persoanelor vizate afectate** și de **nivelul prejudiciilor** suferite de acestea

185. CEPD este de acord cu AS IE că încălcarea care trebuie luată în considerare nu este încălcarea securității în sine, ci conformitatea cu articolul 33 alineatele (1) și (5) din RGPD, pentru a notifica respectiva încălcare a securității la AS competentă și pentru a documenta respectiva încălcare a securității.

186. CEPD ia act de faptul că AS IE ține cont de natura prelucrării, precum și de numărul de persoane vizate afectate. În ceea ce privește **natura prelucrării**, AS IE o descrie drept o platformă de „microblogging" și de comunicare socială, pe care utilizatorii au posibilitatea de a-și documenta gândurile în mesaje tweet. CEPD consideră că, atunci când se evaluează natura prelucrării, trebuie să se ia în considerare și faptul că „prelucrarea în cauză" cuprindea comunicări ale persoanelor vizate, care alegeau în mod deliberat să restrângă publicul comunicărilor respective. CEPD ia act de faptul că proiectul de decizie al AS IE a considerat că: *„impactul asupra utilizatorilor individuali și posibilitatea apariției unor prejudicii rezultate în urma acestuia va depinde de măsura în care datele cu caracter personal au devenit publice și, de asemenea, de natura datelor cu caracter personal. În acest sens, AS IE a indicat în proiectul preliminat că, deși TIC nu a confirmat natura specifică a datelor care au devenit publice în cadrul încălcării securității, s-a dedus în mod rezonabil că, având în vedere numărul de utilizatori afectați și natura serviciilor oferite de TIC, unele date cu caracter personal eliberate cel puțin în cea ce privește unii utilizatori ar fi inclus categorii sensibile de date și alte materiale cu un caracter deosebit de privat"*[209]. Cu toate acestea, AS IE, în baza observațiilor TIC, a acordat mai puțină importanță acestui factor decât în proiectul preliminar, întrucât nu a existat nicio dovadă directă în ceea ce privește prejudiciul[210]. Cu toate acestea, CEPD consideră că AS IE ar trebui totuși să acorde importanță deosebită faptului că „prelucrarea în cauză" cuprinde comunicări ale persoanelor vizate, care au ales în mod deliberat să restrângă publicul comunicărilor respective, la evaluarea naturii prelucrării în cauză. În special, AS IE ar fi trebuit să acorde *importanță acestui fapt, având în vedere faptul că AS IE a reamintit de el în proiectul de decizie, în care AS IE a considerat că „amploarea segmentului de utilizatori afectați dă naștere posibilității unui spectru mult mai amplu de prejudicii rezultate în urma încălcării securității, în special având în vedere natura serviciului oferit de TIC" și „probabilitatea ca numeroși utilizatori să se fi bazat pe funcția de păstrare a caracterului „privat" al mesajelor tweet*

[206] RGPD, considerentul 150.
[207] Orientările privind ORM, punctul 34.
[208] Orientările CEPD privind amenzile administrative, p. 7.
[209] Proiectul de decizie, punctul 14.51.
[210] Vezi punctul 150 de mai sus.

pentru a comunica informații sau opinii (în confortul a ceea ce considerau ei că este un mediu privat și controlat) pe care nu le-ar transmite în mod normal în domeniul public"[211].

187. În plus, în ceea ce privește domeniul de aplicare al prelucrării în cauză ca atare, AS IE pare să înlocuiască domeniul de aplicare al prelucrării cu numărul de persoane vizate afectate. CEPD consideră că **natura și domeniul de aplicare al „prelucrării"** de care trebuie să se țină cont în stabilirea amenzii nu este operațiunea de prelucrare ce constă în divulgarea (accidentală) (încălcarea securității datelor cu caracter personal) sau cauza acesteia, ci, mai degrabă, domeniul de aplicare al prelucrării care stă la baza acesteia, efectuată de TIC, potrivit celor descrise la punctul anterior.

188. Conform AS AT, **momentul în care operatorul a luat cunoștință de impactul încălcării afectează gravitatea încălcării** articolului 33 alineatul (1) din RGPD. Obiecția formulată de AS AT a exprimat un dezacord cu privire la modul în care a fost stabilit sau evaluat momentul în care trebuie să se considere că operatorul a avut cunoștință de încălcarea securității datelor. Mai precis, AS AT a susținut în obiecția sa că TIC ar fi trebuit să transmită notificarea încălcării securității datelor în termen de 72 de ore de la momentul în care persoana împuternicită de operator a luat cunoștință de eroare. Acest lucru contribuie la evaluarea încălcării articolului 33 alineatul (1) din RGPD de către AS AT ca fiind „gravă".

189. În acest sens, CEPD reamintește că Orientările privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679 („WP250")[212], care au fost avizate de CEPD, afirmă că *„[p]lanul de răspuns la încălcări ar trebui să se concentreze pe protejarea persoanelor și a datelor lor cu caracter personal. În consecință, notificarea încălcării securității ar trebui considerată drept un instrument de îmbunătățire a conformității în ceea ce privește protecția datelor cu caracter personal"*[213].

190. Conform Orientărilor privind notificarea încălcării securității datelor cu caracter personal, ar trebui considerat că un operator „a luat cunoștință" atunci când operatorul respectiv are un grad rezonabil de certitudine că s-a produs un incident de securitate care a condus la compromiterea datelor cu caracter personal[214]. Operatorul se bazează pe persoana împuternicită de acesta pentru a-și atinge obiectivele; prin urmare, în principiu, ar trebui considerat că operatorul are „cunoștință" odată ce persoana împuternicită de acesta l-a informat despre încălcare.[215] Cu toate acestea, RGPD impune operatorului obligația de a se asigura că va lua „cunoștință" de orice încălcare în timp util" astfel încât să poată lua măsurile corespunzătoare[216] și arată că *„operatorul poate întreprinde o <u>scurtă</u> investigație pentru a stabili dacă o încălcare a avut loc sau nu de fapt. În această perioadă de investigație, operatorul nu poate fi considerat ca având „cunoștință" de încălcare.*[217] Cu toate acestea, Orientările clarifică faptul că investigația inițială trebuie să înceapă cât mai curând posibil, iar ulterior poate urma o investigație mai detaliată.[218]

191. Astfel, Orientările clarifică faptul că operatorul și, prin extensie, persoana împuternicită de operator, trebuie să acționeze rapid. În cele mai multe cazuri, aceste acțiuni preliminare ar trebui să fie finalizate

[211] Proiectul de decizie, punctul 14.51.
[212] Orientările Grupului de lucru „Articolul 29" privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679, WP 250 rev. 01, avizate de CEPD (denumite în continuare "Orientările privind notificarea încălcării securității datelor cu caracter personal").
[213] Orientări privind notificarea încălcării securității datelor cu caracter personal, pag. 5.
[214] Orientări privind notificarea încălcării securității datelor cu caracter personal, pag. 11.
[215] Orientări privind notificarea încălcării securității datelor cu caracter personal, pag. 14.
[216] Orientări privind notificarea încălcării securității datelor cu caracter personal, pag. 11.
[217] Orientări privind notificarea încălcării securității datelor cu caracter personal, pag. 12 (sublinierea noastră).
[218] Orientări privind notificarea încălcării securității datelor cu caracter personal, pag. 12.

imediat după alerta inițială (și anume, *atunci când operatorul sau persoana împuternicită de operator suspectează că a avut loc un incident de securitate care poate implica date cu caracter personal*) – doar în cazuri excepționale ar trebui acestea să dureze mai mult.[219]

192. Ținând cont de cele de mai sus, CEPD este de acord cu poziția din evaluarea AS IE, potrivit căreia nu ne putem aștepta ca operatorul să fi luat cunoștință în momentul în care persoana împuternicită de operator și-a dat seama că s-a produs un incident de securitate. Conform celor prevăzute în WP29 Orientări privind încălcarea securității datelor, care au fost avizate de CEPD, trebuie să existe un grad de certitudine că s-a produs o încălcare a securității datelor cu caracter personal înainte să se poate specifica cunoștința. Faptele în discuție nu indică în mod clar, potrivit celor reflectate în proiectul de decizie, că așa s-a întâmplat înainte de 3 ianuarie 2019. În acest caz, AS AT nu a dovedit că TIC a atins gradul de certitudine necesar în ceea ce privește producerea unei încălcări a securității datelor mai devreme, când AS IE a constatat că TIC are „cunoștință" de încălcare. Prin urmare, CEPD consideră că evaluarea gravității încălcării nu trebuie să fie ajustată prin prisma unei determinări diferite a momentului în care operatorul a luat cunoștință de încălcarea securității datelor.

193. În plus, în ceea ce privește **gravitatea încălcării,** CEPD este de acord cu AS IE că respectarea articolului 33 alineatele (1) și (5) din RGPD este esențială pentru funcționarea în ansamblu a regimului de supraveghere și de punere în aplicare.

194. În ceea ce privește obiecția formulată de AS AT în ceea ce privește **caracterul intenționat al încălcării**, CEPD consideră că obiecția nu a demonstrat suficient că, din momentul în care operatorul a luat cunoștință, acesta nu a ținut seama în mod intenționat de obligația sa de diligență.

195. Cu toate acestea, în ceea ce privește caracterul neglijent al încălcării, CEPD consideră că o societate pentru care prelucrarea datelor cu caracter personal se află în centrul activităților sale comerciale ar trebui să dețină suficiente proceduri pentru documentarea situațiilor de încălcare a securității datelor cu caracter personal, inclusiv măsuri de remediere, care îi vor oferi, de asemenea, posibilitatea de a respecta obligația de notificare în temeiul articolului 33 alineatul (1) din RGPD. Acest element implică un element suplimentar de luat în considerare în analiza gravității încălcării.

196. CEPD reamintește că CJUE a susținut în mod constat că o sancțiune disuasivă este una care are **un real efect descurajator**[220]. În acest sens, se poate face o distincție între descurajarea generală (descurajarea altor persoane să comită aceeași încălcare în viitor) și descurajarea specifică (descurajarea destinatarului amenzii să comită aceeași încălcare din nou)[221]. În plus, gravitatea amenzilor trebuie să fie pe măsura gravității încălcărilor pentru care sunt impuse acestea[222]. Prin urmare, amenzile nu trebuie să fie disproporționate în raport cu obiectivele urmărite, respectiv cu conformitatea cu normele de protecție a datelor, iar valoarea amenzilor impuse unei întreprinderi trebuie să fie proporțională cu încălcarea privită în ansamblu, ținându-se cont în special de gravitatea încălcării[223].

197. Deși ASP a făcut trimitere în decizia sa la cerința ca amenda să fie **disuasivă și proporțională**, CEPD consideră că ASP nu a justificat suficient modul în care amenda propusă răspunde acestor cerințe. În mod special, CEPD remarcă faptul că ASP trece de la calculul valorii maxime a amenzii (stabilită la 60

[219] Orientări privind notificarea încălcării securității datelor cu caracter personal, pag. 12-13 (sublinierea noastră).
[220] Vezi Avizul avocatului general Geelhoed din 29 aprilie 2004 privind Hotărârea din data de 12 iulie 2005, Comisia împotriva Franței, C-304/02, EU:C:2005:444, punctul 39.
[221] Vezi, printre altele, Hotărârea din 13 iunie 2013, Versalis Spa împotriva Comisiei, C-511/11, ECLI:EU:C:2013:386, punctul 94.
[222] Hotărârea CJUE din 25 aprilie 2013, Asociația Accept, C-81/12.
[223] Hotărârea Tribunalului din 26 octombrie 2017, Marine Harvest împotriva Comisiei Europene, T-704/14.

de milioane USD) la specificarea intervalului propus al amenzii (stabilit între 150 000 USD și 300 000 USD), fără a oferi explicații suplimentare referitoare la elementele specifice care au determinat ASP să identifice acest interval specific[224]. Dincolo de trimiterile generale la factorii relevanți din articolul 83 alineatul (2) din RGPD, nu există o motivație clară pentru alegerea procentului propus (între 0,25 % și 0,5 %) din amenda maximă aplicabilă în temeiul articolului 83 alineatul (4) din RGPD.

198. În acest sens, CEPD a detaliat mai sus motivele pentru care ASP, în proiectul său de decizie, ar fi trebuit să acorde mai multă importanță elementului legat de natura, domeniul de aplicare și caracterul neglijent al încălcării și, prin urmare, consideră că intervalul propus pentru amendă trebuie să fie adaptat în consecință.

8.4.3 Concluzie

199. În urma acestei evaluări, CEPD consideră că amenda propusă în proiectul de decizie este prea mică și, prin urmare, nu își îndeplinește scopul ca măsură de corecție, în special nu îndeplinește cerințele din articolul 83 alineatul (1) din RGPD de a fi eficace, disuasivă și proporțională.

200. Astfel, CEPD solicită AS IE să reevalueze elementele pe care se bazează pentru a calcula valoarea amenzii fixe[225] care urmează să fie impusă TIC, pentru a se asigura că este adecvată faptelor cauzei.

201. CEPD remarcă faptul că analiza obiecțiilor se limitează la substanța obiecțiilor care trebuie să fie considerate relevante și motivate. Prin urmare, domeniul de aplicare al analizei CEPD privind calculul amenzii se limitează la o analiză a metodei de calcul al amenzilor ca atare. Aceasta nu constituie o validare implicită sau explicită de către CEPD, privind analiza efectuată de ASP cu privire la încălcarea articolului 33 alineatul (1) sau a articolului 33 alineatul (5) din RGPD sau cu privire la calificarea juridică a Twitter, Inc. și respectiv TIC. CEPD reiterează că decizia sa actuală nu aduce atingere evaluărilor care pot fi solicitate CEPD în alte cauze, inclusiv cu aceleași părți, ținând cont de conținutul proiectului de decizie relevant și de obiecțiile formulate de ASV-uri.

9 DECIZIE OBLIGATORIE

202. Prin prisma celor prezentate mai sus și în conformitate cu sarcina CEPD în temeiul articolului 70 alineatul (1) litera (t) din RGPD, de a emite decizii obligatorii în temeiul articolului 65 din RGPD, Comitetul emite următoarea decizie obligatorie, în conformitate cu articolul 65 alineatul (1) litera (a) din RGPD.

203. <u>Cu privire la obiecțiile privind calificarea operatorului și a persoanei împuternicite de operator și competența ASP:</u>

- CEPD decide că AS IE nu trebuie să își modifice proiectul de decizie în baza obiecțiilor formulate, întrucât acestea nu îndeplinesc cerințele din articolul 4 alineatul (24) din RGPD.

204. <u>Cu privire la obiecțiile referitoare la încălcarea articolului 33 alineatele (1) și (5) din RGPD, constatate de ASP:</u>

- În ceea ce privește obiecția AS FR privind absența unei încălcări a articolului 33 alineatul (1) din RGPD, obiecția AS DE privind stabilirea *dies a quo* pentru încălcarea articolului 33 alineatul (1) din

[224] Proiectul de decizie, punctele 15.19 și 15.20.
[225] Este de preferat ca aceasta să fie deja prevăzută în proiectul de decizie întocmit în temeiul articolului 60 din RGPD.

RGPD și obiecția AS IT referitoare la încălcarea articolului 33 alineatul (5) din RGPD, CEPD decide că AS IE nu trebuie să își modifice proiectul de decizie în baza obiecțiilor formulate, întrucât acestea nu îndeplinesc cerințele din articolul 4 alineatul (24) din RGPD.

205. Cu privire la obiecțiile referitoare la încălcările posibile suplimentare (sau alternative) ale RGPD, identificate de ASV-uri:

- În ceea ce privește obiecția AS DE privind posibilele încălcări ale articolului 5 alineatul (1) litera (f), ale articolelor 24 și 32 din RGPD, precum și în ceea ce privește obiecția AS IT privind posibila încălcare a articolului 5 alineatul (2) din RGPD, CEPD decide că, deși acestea îndeplinesc cerințele articolului 4 alineatul 24) din RGPD, AS IE nu trebuie să își modifice proiectul de decizie, deoarece elementele faptice incluse în proiectul de decizie și în obiecții nu sunt suficiente pentru a oferi CEPD posibilitatea de a stabili existența încălcării articolului 5 alineatul (1) litera (f), a articolului 5 alineatul (2), a articolelor 24 și 32 din RGPD.
- În ceea ce privește obiecția AS DE privind posibila încălcare a articolului 33 alineatul (3) din RGPD, obiecția AS FR privind posibila încălcare a articolelor 28 și 32 din RGPD, obiecția AS HU privind posibila încălcare a articolului 5 alineatul (1) litera (f), a articolelor 32 și 34 din RGPD și obiecția AS IT referitoare la încălcarea articolului 28 din RGPD, CEPD decide că AS IE nu trebuie să își modifice proiectul de decizie în baza obiecțiilor formulate, întrucât acestea nu îndeplinesc cerințele din articolul 4 alineatul (24) din RGPD.

206. Cu privire la obiecția referitoare la decizia ASP de a nu emite o mustrare:

- În ceea ce privește obiecția AS DE referitoare la decizia AS IE de a nu emite o mustrare, CEPD decide că AS IE nu trebuie să își modifice proiectul de decizie în baza obiecției formulate întrucât aceasta nu îndeplinește cerințele din articolul 4 alineatul (24) din RGPD.

207. Cu privire la obiecția privind calculul amenzii sugerată de ASP:

- În ceea ce privește obiecția AS HU privind natura insuficient de disuasivă a amenzii, CEPD decide că AS IE nu trebuie să își modifice proiectul de decizie în baza obiecției formulate întrucât aceasta nu îndeplinește cerințele din articolul 4 alineatul (24) din RGPD.
- În ceea ce privește obiecția AS AT, obiecția AS DE și obiecția AS IT privind natura insuficient de disuasivă a amenzii, CEPD decide că acestea îndeplinesc cerințele articolului 4 alineatul (24) din RGPD și că AS IE trebuie să reevalueze **elementele pe care se bazează pentru a calcula valoarea amenzii fixe** care urmează să fie impusă TIC și pentru a-și modifica proiectul de decizie, crescând nivelul amenzii, pentru a se asigura că aceasta își îndeplinește scopul ca măsură de corecție și îndeplinește cerințele de eficacitate, disuasivitate și proporționalitate stabilite de articolul 83 alineatul (1) din RGPD și ținând cont de criteriile articolului 83 alineatul (2) din RGPD.

10 OBSERVAȚII FINALE

208. Prezenta decizie obligatorie se adresează AS IE și ASV-urilor. AS IE își adoptă decizia finală în baza prezentei decizii obligatorii în temeiul articolului 65 alineatul (6) din RGPD.

209. În ceea ce privește obiecțiile care se consideră că nu îndeplinesc cerințele articolului 4 alineatul (24) din RGPD, CEPD nu se pronunță cu privire la fondul chestiunilor semnificative semnalate de aceste obiecții. CEPD reiterează că decizia sa actuală nu aduce atingere evaluărilor care pot fi solicitate CEPD

în alte cauze, inclusiv cu aceleași părți, ținând cont de conținutul proiectului de decizie relevant și de obiecțiile formulate de ASV-uri.

210. Conform articolului 65 alineatul (6) din RGPD, AS IE comunică decizia sa finală președintelui în termen de o lună de la primirea deciziei obligatorii.

211. După ce AS IE efectuează comunicarea respectivă, decizia obligatorie va deveni publică în temeiul articolului 65 alineatul (5) din RGPD.

212. În temeiul articolului 70 alineatul (1) litera (y) din RGPD, decizia finală a AS IE comunicată CEPD va fi inclusă în registrul deciziilor care au făcut obiectul mecanismului pentru asigurarea coerenței.

Formatted: Romanian

Pentru Comitetul european pentru protecția datelor

Președinte

(Andrea Jelinek)