Repertoriul jurisprudenței

CONCLUZIILE AVOCATULUI GENERAL
DOMNUL NICHOLAS EMILIOU
prezentate la 4 mai 2023 [1]

Cauza C-683/21

Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos
împotriva
Valstybinė duomenų apsaugos inspekcija,
intervenienți:
„IT sprendimai sėkmei” UAB,
Lietuvos Respublikos sveikatos apsaugos ministerija

[cerere de decizie preliminară formulată de Vilniaus apygardos administracinis teismas (Tribunalul Administrativ Regional din Vilnius, Lituania)]

„Trimitere preliminară – Protecția datelor cu caracter personal – Regulamentul (UE) 2016/679 – Articolul 4 alineatul (7) – Noțiunea de «operator» – Dezvoltarea unei aplicații mobile în cadrul pandemiei de COVID-19 – Răspunderea autorității publice însărcinate cu organizarea procedurii de cerere de ofertă pentru achiziționarea aplicației mobile – Articolul 4 alineatul (2) – Noțiunea de «prelucrare» – Utilizarea datelor cu caracter personal în cursul fazei de testare a unei aplicații mobile – Articolul 26 alineatul (1) – Luare în comun a deciziilor – Articolul 83 – Aplicarea unor amenzi administrative – Condiții – Necesitatea ca încălcarea să fie cu intenție sau din neglijență – Răspunderea operatorului pentru prelucrarea datelor cu caracter personal efectuată de o persoană împuternicită de operator”

I. Introducere

1. Într-o lume în care datele cu caracter personal au devenit o monedă de schimb și constituie pentru întreprinderi o mină de aur nou descoperită, în ce condiții pot fi aplicate amenzi administrative operatorilor sau persoanelor împuternicite de operatori pentru încălcarea normelor privind protecția datelor prevăzute în Regulamentul (UE) 2016/679 [2]? Mai exact, este necesar să existe un element de „vinovăție” înainte să le poată fi aplicate astfel de amenzi? Aceasta este problema centrală ridicată de Vilniaus apygardos administracinis teismas (Tribunalul Administrativ Regional din Vilnius, Lituania) în prezenta cauză.

[1] Limba originală: engleza.

[2] 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) (JO 2016, L 119, p. 1) (denumit în continuare „RGPD”).

2. Litigiul aflat pe rolul acestei instanțe între Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (Centrul Național de Sănătate Publică din cadrul Ministerului Sănătății, Lituania, denumit în continuare „NVSC”), pe de o parte, și Valstybinė duomenų apsaugos inspekcija (Inspectoratul de Stat pentru Protecția Datelor, Lituania, denumit în continuare „inspectoratul”), pe de altă parte, privește în esență rolul jucat de NVSC în dezvoltarea și punerea la dispoziția publicului a unei aplicații mobile care a colectat, în lunile aprilie și mai 2020, datele cu caracter personal ale persoanelor care au fost în contact cu pacienți infectați cu COVID-19.

3. În acest context, prezenta cauză oferă Curții ocazia de a furniza clarificări suplimentare cu privire la noțiunile de „operator”, „operatori asociați” și „prelucrare”, definite la articolul 4 punctul 7, la articolul 26 alineatul (1) și, respectiv, la articolul 4 punctul 2 din RGPD, și de a aprecia pentru prima dată dacă este posibil, în conformitate cu articolul 83 din acest regulament, să se aplice o amendă administrativă unui operator care nu a săvârșit în mod intenționat sau din neglijență nicio încălcare a normelor cuprinse în RGPD. Această întrebare impune Curții să clarifice dacă această dispoziție permite aplicarea de amenzi în absența oricărei culpe, pe baza unei răspunderi strict obiective.

II. Cadrul juridic

A. Dreptul Uniunii Europene

4. Considerentul (148) al RGPD afirmă:

„Pentru a consolida respectarea aplicării normelor prevăzute în prezentul regulament, ar trebui impuse sancțiuni, inclusiv amenzi administrative, pentru orice încălcare a prezentului regulament […]. În cazul unei încălcări minore sau în cazul în care amenda susceptibilă de a fi impusă ar constitui o sarcină disproporționată pentru o persoană fizică, poate fi emis un avertisment în locul unei amenzi. Cu toate acestea, ar trebui să se ia în considerare în mod corespunzător natura, gravitatea și durata încălcării, caracterul deliberat al încălcării, acțiunile întreprinse pentru a reduce prejudiciul cauzat, gradul de răspundere sau orice încălcări anterioare relevante, modul în care încălcarea a fost adusă la cunoștința autorității de supraveghere, conformitatea cu măsurile adoptate împotriva operatorului sau a persoanei împuternicite de operator, aderarea la un cod de conduită și orice alt factor agravant sau atenuant. Impunerea de sancțiuni, inclusiv de amenzi administrative, ar trebui să facă obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu carta, inclusiv o protecție judiciară eficientă și un proces echitabil.”

5. În conformitate cu considerentul (150) al acestui regulament:

„Pentru consolidarea și armonizarea sancțiunilor administrative în cazul încălcării prezentului regulament, fiecare autoritate de supraveghere ar trebui să aibă competența de a impune amenzi administrative. Prezentul regulament ar trebui să indice încălcările, limita maximă și criteriile pentru stabilirea amenzilor administrative aferente, care ar trebui să fie stabilite de autoritatea de supraveghere competentă în fiecare caz în parte, ținând seama de toate circumstanțele relevante ale situației specifice, luându-se în considerare în mod corespunzător, în special, natura, gravitatea și durata încălcării, precum și consecințele acesteia și măsurile luate pentru a se asigura respectarea obligațiilor în temeiul prezentului regulament și pentru a se preveni sau

atenua consecințele încălcării. […] Impunerea unei amenzi administrative sau transmiterea unei avertizări nu afectează aplicarea altor competențe ale autorităților de supraveghere sau a altor sancțiuni în temeiul prezentului regulament.”

6. Articolul 4 punctul 7 din RGPD definește conceptul de „operator” ca fiind „persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal […]”.

7. Articolul 26 din acest regulament, intitulat „Operatori asociați”, prevede în partea relevantă:

„(1) În cazul în care doi sau mai mulți operatori stabilesc în comun scopurile și mijloacele de prelucrare, aceștia sunt operatori asociați. […]

[…]”

8. Articolul 83 din acest regulament, intitulat „Condiții generale pentru impunerea amenzilor administrative”, prevede:

„(1) Fiecare autoritate de supraveghere asigură faptul că impunerea unor amenzi administrative în conformitate cu prezentul articol pentru încălcările prezentului regulament menționate la alineatele (4), (5) și, (6) este, în fiecare caz, eficace, proporțională și disuasivă.

(2) În funcție de circumstanțele fiecărui caz în parte, amenzile administrative sunt impuse în completarea sau în locul măsurilor menționate la articolul 58 alineatul (2) literele (a)-(h) și (j). Atunci când se ia decizia dacă să se impună o amendă administrativă și decizia cu privire la valoarea amenzii administrative în fiecare caz în parte, se acordă atenția cuvenită următoarelor aspecte:

(a) 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;

(b) dacă încălcarea a fost comisă intenționat sau din neglijență;

[…]

(k) orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării.

(3) În cazul în care un operator sau o persoană împuternicită de operator încalcă în mod intenționat sau din neglijență, pentru aceeași operațiune de prelucrare sau pentru operațiuni de prelucrare conexe, mai multe dispoziții din prezentul regulament, cuantumul total al amenzii administrative nu poate depăși suma prevăzută pentru cea mai gravă încălcare.

[…]”

B. Dreptul lituanian

9. Articolul 72 alineatul (2) din Viešųjų pirkimų įstatymas (Legea privind achizițiile publice) prevede:

„Autoritatea contractantă desfășoară o procedură negociată fără publicarea unui anunț de participare având următoarele etape:

(1) invitația scrisă adresată operatorilor economici selectați în vederea prezentării de oferte;

(2) verificarea existenței unor motive de excludere a operatorilor economici, astfel cum sunt acestea prevăzute în documentația privind achiziția, și verificarea îndeplinirii de către operatorii economici a cerințelor de calificare impuse și, dacă este cazul, a standardelor impuse de asigurare a calității și/sau a standardelor de management al mediului;

(3) desfășurarea de negocieri cu ofertanții în conformitate cu procedura prevăzută la articolul 66 din prezenta lege și solicitarea adresată acestora de a depune oferte finale. Autoritatea contractantă nu este obligată să solicite depunerea unei oferte finale în cazul în care la procedura de negociere fără publicarea unui anunț prealabil participă un singur operator economic;

(4) evaluarea ofertelor finale și stabilirea candidatului câștigător."

III. Situația de fapt, procedura națională și întrebările preliminare

10. Pentru a răspunde situației survenite prin răspândirea COVID-19, ministrul sănătății al Republicii Lituania (denumit în continuare „ministrul sănătății") l-a însărcinat, prin decizia din 24 martie 2020, pe directorul NVSC să organizeze dezvoltarea și achiziționarea unei aplicații mobile, și anume KARANTINAS. Această aplicație mobilă a fost concepută pentru a colecta și monitoriza datele cu caracter personal ale persoanelor care au fost în contact cu pacienți infectați cu COVID-19[3].

11. La 27 martie 2020, o persoană care susținea că este un agent care reprezintă NVSC a informat societatea „IT sprendimai sėkmei" UAB (denumită în continuare „ITSS"), că a fost selectată ca dezvoltator al aplicației mobile KARANTINAS. Au avut loc schimburi de e-mailuri între ITSS și persoana respectivă, precum și între ITSS și o serie de salariați și directorul NVSC în legătură cu dezvoltarea aplicației respective. De asemenea, în etapa respectivă a fost redactat un acord de confidențialitate, în care erau indicați ca operatori atât ITSS, cât și NVSC.

12. Aplicația mobilă care a fost dezvoltată în cele din urmă a fost pusă la dispoziția publicului pentru a fi descărcată din Google Play Store la 4 aprilie 2020 și din Apple App Store la 6 aprilie 2020. Atât ITSS, cât și NVSC au fost din nou menționați ca operatori în versiunea aplicației KARANTINAS care a fost pusă la dispoziția publicului pentru a fi descărcată. La momentul respectiv, această aplicație mobilă nu fusese încă achiziționată de NVSC.

[3] Printre datele cu caracter personal colectate prin KARANTINAS de la utilizatorii săi se numără următoarele: numărul de identitate, coordonatele de latitudine și longitudine, țara, orașul, municipalitatea, adresa de reședință, prenumele, numele, numărul de identificare personal, numărul de telefon, faptul dacă persoana a fost obligată să se autoizoleze, dacă aceasta s-a înregistrat etc. Aceste date au fost colectate nu doar în Lituania, ci și în străinătate.

13. Prin decizia din 10 aprilie 2020, ministrul sănătății l-a însărcinat pe directorul NVSC să achiziționeze aplicația mobilă KARANTINAS printr-o procedură de negociere fără publicarea unui anunț de participare, în conformitate cu articolul 72 alineatul (2) din Legea privind achizițiile publice.

14. Această procedură a fost inițiată, însă NVSC a închis-o, deoarece nu a primit finanțarea necesară. Astfel, nu a fost încheiat niciun contract de achiziție publică. Cu toate acestea, aplicația KARANTINAS a continuat să fie disponibilă publicului pentru a fi descărcată.

15. La 15 mai 2020, NVSC a solicitat ITSS să nu utilizeze niciun detaliu aparținând NVSC și să nu stabilească link-uri cu NVSC în aplicația mobilă. La 18 mai 2020, inspectoratul a început o investigație cu privire atât la ITSS, cât și la NVSC, în legătură cu încălcarea normelor prevăzute în RGPD. Operațiunile KARANTINAS au fost suspendate la cererea inspectoratului la 26 mai 2020. Potrivit ITSS, 3 802 utilizatori au furnizat datele lor cu caracter personal prin intermediul aplicației între 4 aprilie și 26 mai 2020.

16. Prin decizia din 24 februarie 2021, inspectoratul a aplicat amenzi administrative atât NVSC, cât și ITSS, în calitatea lor de operatori asociați, pentru încălcarea articolelor 5, 13, 24, 32 și 35 din RGPD [4].

17. Această decizie a fost contestată de NVSC la Vilniaus apygardos administracinis teismas (Tribunalul Administrativ Regional, Vilnius). Această instanță se întreabă în esență dacă noțiunea de „operator”, în sensul articolului 4 punctul 7 din RGPD, trebuie interpretată în sens larg, astfel încât să includă orice persoană fizică sau juridică sau orice organism precum NVSC, care nu este dezvoltatorul unei aplicații mobile, dar care, pentru a achiziționa o astfel de aplicație mobilă prin intermediul unei proceduri de licitație, a stabilit „scopurile și mijloacele de prelucrare a datelor cu caracter personal”, sau dacă această noțiune trebuie interpretată mai strict, luând în considerare procedura de atribuire a contractelor de achiziții publice și rezultatul acesteia.

18. În special, aceasta se întreabă dacă are relevanță în această privință faptul că procedura de cerere de ofertă a fost în cele din urmă abandonată, iar KARANTINAS nu a fost niciodată achiziționată de NVSC. Instanța se întreabă de asemenea dacă faptul că NVSC nu și-a dat în mod oficial consimțământul sau nu a autorizat punerea la dispoziția publicului a acestei aplicații mobile are vreun impact asupra acestei evaluări.

19. În plus, instanța de trimitere pune sub semnul întrebării relația dintre NVSC și ITSS. În această privință, aceasta se întreabă în ce împrejurări entitatea și societatea respective ar trebui considerate „operatori asociați” în sensul articolului 4 punctul 7 și al articolului 26 alineatul (1) din RGPD. În mod alternativ, în cazul în care NVSC și ITSS nu ar trebui considerate „operatori asociați”, ci „operator” și, respectiv, „persoană împuternicită de operator” [5] în sensul RGPD, aceasta dorește să știe când ar putea acțiunile ITSS să determine angajarea răspunderii NVSC.

[4] Articolul 5 din RGPD conține o listă de principii generale a căror respectare trebuie asigurată de operatori atunci când sunt prelucrate date cu caracter personal. Articolul 13 din acest regulament enumeră informațiile pe care operatorii trebuie să le furnizeze persoanelor vizate atunci când sunt colectate datele cu caracter personal de la acestea. Articolul 24 din regulamentul respectiv prevede că operatorii trebuie, *inter alia*, să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta (și a fi în măsură să demonstreze) că prelucrarea se efectuează în conformitate cu normele aplicabile în materie de protecție a datelor. Articolul 32 din RGPD se referă la securitatea prelucrării și creează obligații în această privință atât pentru operatori, cât și pentru persoanele împuternicite de operatori, în timp ce articolul 35 din acesta se referă la obligația operatorilor de a efectua evaluări ale impactului asupra protecției datelor înainte de a întreprinde anumite tipuri de prelucrare.

[5] În conformitate cu articolul 29 din RGPD, „[p]ersoana împuternicită de operator și orice persoană care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care dreptul Uniunii sau dreptul intern îl obligă să facă acest lucru”.

Referitor la acest aspect, ridică problema dacă articolul 83 din RGPD trebuie interpretat în sensul că o amendă administrativă poate fi aplicată unui operator precum NVSC, care nu a săvârșit el însuși, cu intenție sau din neglijență, nicio încălcare a acestui regulament.

20. În aceste condiții, Vilniaus apygardos administracinis teismas (Tribunalul Administrativ Regional, Vilnius), a decis să suspende judecarea cauzei și să adreseze Curții de Justiție următoarele întrebări preliminare:

„1) Noțiunea de «operator» de la articolul 4 punctul 7 din RGPD poate fi interpretată în sensul că o persoană care intenționează să achiziționeze un instrument de colectare a datelor (aplicație mobilă) prin intermediul unei achiziții publice trebuie considerată de asemenea ca fiind un operator chiar dacă nu a fost încheiat un contract de achiziții publice și nu a fost transferat produsul creat (aplicația mobilă) pentru achiziționarea căruia a fost utilizată o procedură de achiziții publice?

2) Noțiunea de «operator» de la articolul 4 punctul 7 din RGPD poate fi interpretată în sensul că o autoritate contractantă care nu a dobândit dreptul de proprietate asupra produsului informatic creat și care nu s-a aflat în posesia acestuia trebuie considerată de asemenea ca fiind un operator în cazul în care versiunea finală a aplicației create furnizează linkuri către sau interfețe ale acestei entități publice și/sau [în cazul în care] politica de confidențialitate, care nu a fost aprobată oficial sau recunoscută de entitatea publică în discuție, preciza că entitatea publică respectivă este ea însăși operator?

3) Noțiunea de «operator» de la articolul 4 punctul 7 din RGPD poate fi interpretată în sensul că o persoană care nu a realizat nicio operațiune efectivă de prelucrare a datelor, astfel cum a fost definită la articolul 4 alineatul (2) din RGPD, și/sau care nu a dat o permisiune/un consimțământ clar pentru realizarea unor astfel de operațiuni trebuie considerată de asemenea ca fiind un operator? Faptul că produsul informatic utilizat pentru prelucrarea datelor cu caracter personal a fost creat în conformitate cu sarcina trasată de autoritatea contractantă este semnificativ pentru interpretarea noțiunii de «operator»?

4) În cazul în care stabilirea operațiunilor efective de prelucrare a datelor este pertinentă pentru interpretarea noțiunii de «operator», definiția «prelucrării» datelor cu caracter personal de la articolul 4 punctul 2 din RGPD trebuie interpretată în sensul că se referă și la situațiile în care, la testarea sistemelor informatice în procesul de achiziționare a unei aplicații mobile, au fost utilizate copii ale unor date cu caracter personal?

5) O prelucrare în comun a datelor în conformitate cu articolul 4 punctul 7 și cu articolul 26 alineatul (1) din RGPD poate fi interpretată exclusiv în sensul că presupune acțiuni coordonate în mod intenționat în ceea ce privește stabilirea scopurilor și a mijloacelor de prelucrare a datelor sau această noțiune poate fi interpretată și în sensul în care luarea în comun a deciziilor include și situațiile în care nu există un «acord» clar cu privire la scopurile și mijloacele de prelucrare a datelor și/sau acțiunile nu sunt coordonate între entități? Împrejurarea referitoare la stadiul la care, în cursul creării mijloacelor de prelucrare a datelor cu caracter personal (aplicația informatică), au fost prelucrate date cu caracter personal și la scopul creării aplicației este importantă din punct de vedere juridic pentru interpretarea noțiunii de prelucrare în comun a datelor? Un «acord» între operatorii asociați poate fi înțeles exclusiv ca o fiind o stabilire clară și definită a condițiilor care reglementează prelucrarea în comun a datelor?

6) Dispoziția cuprinsă la articolul 83 alineatul (1) din RGPD, potrivit căreia «[impunerea unor] amenzi administrative […] este […] eficace, proporțională și disuasivă», trebuie interpretată în sensul că include și cazurile care atrag răspunderea «operatorului» atunci când, în procesul de creare a unui produs informatic, dezvoltatorul realizează și acțiuni de prelucrare a datelor cu caracter personal, iar acțiunile inadecvate de prelucrare a datelor cu caracter personal efectuate de persoana împuternicită de operator determină întotdeauna în mod automat răspunderea juridică a operatorului? Această dispoziție trebuie interpretată în sensul că include și cazurile de răspundere obiectivă a operatorului?”

21. Cererea de decizie preliminară din data de 22 octombrie 2021 a fost înregistrată la Curte la 12 noiembrie 2021. NVSC, Inspectoratul, guvernul lituanian și Comisia Europeană au prezentat observații scrise.

22. Guvernele lituanian și neerlandez, Comisia și Consiliul au fost reprezentate în ședința care a avut loc la 17 ianuarie 2023.

IV. Analiză

23. În timpul pandemiei COVID-19, în multe state membre au fost puse la dispoziția publicului, pentru a fi descărcate, aplicații mobile concepute pentru „urmărirea și localizarea” persoanelor infectate cu virusul și/sau a celor care au intrat în contact cu cineva infectat cu virusul. Astfel de aplicații mobile au fost dezvoltate în efortul de a răspunde urgenței situației, adesea cu participarea mai multor entități publice și private (cum ar fi ministerele și alte entități publice, precum și societăți private). Utilizatorilor li s-a cerut să își încarce datele cu caracter personal în aplicațiile mobile, în special datele referitoare la sănătatea lor [6].

24. Procedura principală privește tocmai o astfel de aplicație mobilă, și anume KARANTINAS, care a fost dezvoltată de ITSS (o societate privată), la inițiativa NVSC (o autoritate publică), în urma unei decizii a ministrului sănătății. Nu reiese în mod clar din informațiile din dosarul cauzei, nici din cele furnizate în ședință ce alte entități publice din Lituania au fost implicate, în cazul în care a fost vreuna, în dezvoltarea aplicației [7]. Există de asemenea unele îndoieli dacă NVSC a consimțit ca aplicația KARANTINAS să fie pusă la dispoziția publicului în perioada în care a avut loc prelucrarea datelor cu caracter personal (lunile aprilie și mai 2020). Cu toate acestea, în întrebările adresate Curții, Vilniaus apygardos administracinis teismas (Tribunalul Administrativ Regional, Vilnius) a identificat următoarele împrejurări ca fiind relevante.

– NVSC a intenționat să achiziționeze KARANTINAS în conformitate cu articolul 72 alineatul (2) din Legea privind achizițiile publice, însă procedura nu a fost niciodată finalizată și achiziția nu a avut loc vreodată. Prin urmare, proprietatea asupra KARANTINAS nu a fost niciodată transferată de la ITSS la NVSC;

[6] Observăm că datele cu caracter personal privind sănătatea constituie o „categorie specială de date cu caracter personal”, a căror prelucrare este interzisă de articolul 9 din RGPD, cu excepția cazului în care se aplică unul dintre motivele enumerate la alineatul (2) din dispoziția respectivă (de exemplu, faptul că prelucrarea este necesară din motive de interes public în domeniul sănătății publice [litera (i)] sau în scopuri legate de medicina preventivă sau a muncii [litera (h)]). Observăm însă că întrebările adresate Curții în prezenta cauză nu privesc legalitatea unei astfel de prelucrări, ci mai degrabă condițiile în care o entitate precum NVSC poate fi făcută responsabilă pentru prelucrarea efectuată de dezvoltatorul unei astfel de aplicații mobile (*in casu*, ITSS).

[7] Pe baza informațiilor furnizate în dosarul cauzei și în ședință, nu este clar dacă orașul Vilnius a participat la dezvoltarea aplicației KARANTINAS.

– NVSC a fost menționat ca operator în politica de confidențialitate a KARANTINAS, care a fost pusă la dispoziția publicului. De asemenea, în ultima versiune a aplicației au fost incluse linkuri către NVSC, care nu a fost însă niciodată aprobată în mod oficial de această entitate;

– NVSC nu a prelucrat niciodată el însuși date cu caracter personal și nici nu și-a dat în mod formal consimțământul pentru operațiunile de prelucrare întreprinse, dar a furnizat instrucțiuni privind dezvoltarea KARANTINAS, iar aceste instrucțiuni au fost urmate de ITSS;

– ITSS și NVSC nu au ajuns în mod formal la vreun acord cu privire la scopurile și mijloacele de prelucrare a datelor cu caracter personal care a avut loc.

25. În acest context, întrebările adresate Curții privesc interpretarea mai multor dispoziții din RGPD. Primele trei întrebări, precum și a cincea întrebare fac apel la o interpretare a noțiunii de „operator”, în sensul articolului 4 punctul 7 din acest regulament, și necesită o clarificare a împrejurărilor în care două sau mai multe entități pot fi considerate „operatori asociați” în conformitate cu această dispoziție și cu articolul 26 alineatul (1) din regulamentul menționat. Vom analiza mai întâi aceste întrebări împreună (A), înainte de a trece la a patra întrebare, care privește conceptul de „prelucrare”, în sensul articolului 4 punctul 2 din RGPD, și aplicarea lui în contextul fazei de testare a unei aplicații mobile (B)[8]. Vom aprofunda ulterior chestiunea care se află în centrul prezentei cauze, și anume a șasea întrebare, care are un caracter transversal, întrucât privește condițiile în care pot fi aplicate amenzi administrative operatorilor, în conformitate cu articolul 83 din RGPD (C).

A. Cu privire la noțiunea de „operator” și situațiile de prelucrare în comun (primele trei întrebări și întrebarea a cincea)

26. Prin intermediul primelor trei întrebări, instanța de trimitere solicită să se stabilească în esență dacă, având în vedere împrejurările detaliate la punctul 24 de mai sus, o entitate precum NVSC trebuie considerată „operator”, în sensul articolului 4 punctul 7 din GDPR. În plus, prin intermediul celei de a cincea întrebări, instanța de trimitere solicită să se clarifice dacă, în astfel de împrejurări, două entități precum NVSC și ITSS trebuie considerate „operatori asociați”, în conformitate cu această dispoziție și cu articolul 26 alineatul (1) din regulamentul menționat, chiar dacă acestea nu au ajuns în mod oficial la vreun acord cu privire la scopurile și mijloacele de prelucrare și/sau nu par să își fi coordonat în alt mod acțiunile.

1. Ce este un operator? (primele trei întrebări)

27. Reamintim că, în conformitate cu articolul 4 punctul 7 din RGPD, un „operator” este definit ca fiind persoana sau entitatea care, „singur[ă] sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal”. În termeni mai simpli, un operator nu trebuie să prelucreze el însuși datele cu caracter personal, dar trebuie să stabilească „de ce și cum” se efectuează operațiunile de prelucrare relevante[9]. Curtea a sugerat că, pentru a îndeplini

[8] După cum vom explica la punctul 46 de mai jos, deducem din cererea de decizie preliminară că aplicația KARANTINAS a fost supusă unei faze de testare înainte de a fi pusă la dispoziția publicului pentru a fi descărcată. Din înțelegerea noastră, a patra întrebare privește, așadar, utilizarea datelor cu caracter personal care a avut loc în timpul acestei faze de testare, spre deosebire de cele utilizate într-o etapă ulterioară, când KARANTINAS a fost pusă la dispoziția publicului pentru a fi descărcată.

[9] A se vedea Rücker, D., și Kugler, T., *New European General Data Protection Regulation: A Practitioner's Guide*, C.H. Beck, Hart and Nomos, Oxford, 2018, p. 27. Potrivit autorilor, cea mai importantă caracteristică a unui operator este că determină mai curând rezultatele care trebuie obținute decât mijloacele sau „modul” de prelucrare care pot fi delegate, cel puțin în aspectele lor neesențiale, unei persoane împuternicite de operator, fără a pierde calitatea de operator.

acest criteriu, o persoană sau o entitate trebuie să „[influențeze] prelucrarea datelor cu caracter personal”[10]. Cu toate acestea, nu este necesar ca scopurile și mijloacele de prelucrare să fie stabilite în conformitate cu orientările sau instrucțiunile scrise ale operatorului[11]. Într-adevăr, articolul 4 punctul 7 din RGPD impune mai degrabă o analiză factuală decât una formală.

28. În legătură cu aceasta, Comitetul European pentru Protecția Datelor (EDPB) a sugerat că este de asemenea posibil ca cineva să fie operator, indiferent de conferirea prin lege a unei competențe sau a unei puteri specifice de a controla datele. Într-adevăr, capacitatea de a determina scopurile și mijloacele de prelucrare depinde, înainte de toate, de influența exercitată care poate fi dedusă din circumstanțele de fapt. O entitate care este de fapt în măsură să determine scopurile și mijloacele de prelucrare va fi, așadar, considerată „operator”, independent de desemnarea ca atare în mod formal (prin lege, printr-un contract sau în alt mod)[12].

29. Odată făcute aceste precizări, constatăm că unele dintre împrejurările descrise de instanța de trimitere în cadrul primelor trei întrebări sunt de natură pur formală; de exemplu, faptul că NVCS nu deține din punct de vedere juridic KARANTINAS sau că procedura de achiziție a acestei aplicații mobile nu a fost niciodată finalizată ori faptul că NVSC nu a autorizat în mod oficial punerea la dispoziția publicului larg a aplicației sau nu a aprobat ultima versiune a acesteia. În opinia noastră, niciuna dintre aceste împrejurări nu poate în sine împiedica constatarea că NVSC a acționat în calitate de „operator”, în sensul articolului 4 punctul 7 din RGPD, în contextul procedurii principale. Într-adevăr, acestea nu sunt suficiente pentru a infirma concluzia că NVSC a fost de fapt în măsură să determine scopurile și mijloacele prelucrării datelor cu caracter personal care a avut loc. De altfel, considerăm că faptul că NVSC a fost menționat ca operator în politica de confidențialitate a versiunii KARANTINAS care a fost pusă la dispoziția publicului pentru a fi descărcată sau că în această versiune a aplicației mobile au fost incluse linkuri către această entitate este relevant, dar neconcludent în ceea ce privește influența exercitată efectiv de această entitate.

30. În schimb, dovezile de care dispune instanța de trimitere care arată că NVSC a decis ce tip de date cu caracter personal ar trebui colectate de KARANTINAS și de la ce persoane vizate și/sau alte aspecte esențiale ale prelucrării sunt suficiente, în opinia noastră, pentru a demonstra că această entitate a stabilit „mijloacele” prelucrării. De asemenea, considerăm că faptul că aplicația KARANTINAS a fost creată pentru a îndeplini obiectivul definit de NVSC, și anume pentru a oferi suport în pandemia COVID-19, și că funcționarea sa a fost modificată în mod regulat de ITSS pentru a răspunde nevoilor stabilite de NVSC, în conformitate cu instrucțiunile furnizate de această entitate, este îndeajuns pentru a concluziona că entitatea amintită a stabilit „scopurile” acestei prelucrări.

[10] A se vedea Hotărârea din 10 iulie 2018, Jehovan todistajat (C-25/17, EU:C:2018:551, punctul 68). Acea hotărâre privea interpretarea noțiunii de „operator”, astfel cum a fost definită la articolul 2 litera (d) din Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (JO 1995, L 281, p. 31, Ediție specială, 13/vol. 17, p. 10). Chiar dacă această directivă nu mai este în vigoare și a fost înlocuită prin RGPD, interpretarea dată de Curte cu privire la dispoziția amintită rămâne relevantă în contextul aplicării RGPD, având în vedere că definiția acestei noțiuni rămâne identică în ambele instrumente legislative, cu excepția unor modificări formale minore. De aceea, vom face referire la hotărâri referitoare la un instrument sau altul, fără distincție.

[11] A se vedea Hotărârea din 10 iulie 2018, Jehovan todistajat (C-25/17, EU:C:2018:551, punctul 67).

[12] A se vedea „Orientările 07/2020 privind noțiunile de operator și persoană împuternicită de operator în cadrul RGPD” ale EDPB, versiunea 2.1, adoptate la 7 iulie 2021 (denumite în continuare „Orientările 07/2020”, disponibile în limba engleză la următoarea adresă electronică: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf), p. 3 și punctele 21 și 25-27.

31. Acestea fiind spuse, considerăm că, pentru a stabili dacă o entitate precum NVSC poate fi considerată un „operator” în sensul articolului 4 punctul 7 din RGPD, instanța de trimitere trebuie să stabilească de asemenea dacă, în pofida influenței exercitate de NVSC în etapa de dezvoltare a KARANTINAS, decizia de a pune la dispoziția publicului această aplicație mobilă și, prin urmare, de a se angaja în prelucrarea datelor cu caracter personal a fost adoptată în realitate cu consimțământul (expres sau tacit) al acestei entități (independent de faptul că acest consimțământ nu a fost furnizat în mod oficial sau formal).

32. Într-adevăr, după cum arată în mod clar definiția noțiunii de „operator” de la articolul 4 punctul 7 din RGPD, influența exercitată de un operator trebuie să vizeze prelucrarea în sine a datelor cu caracter personal, iar nu doar oricare etapă anterioară. O persoană fizică sau juridică ori o entitate nu devine „operator” prin simplul fapt că inițiază dezvoltarea unei aplicații mobile sau definește parametrii acestei aplicații (sau ai unui alt instrument de colectare a datelor). Acțiunile sale trebuie să fie efectiv legate de prelucrarea datelor cu caracter personal și, prin urmare, trebuie să fi consimțit în mod expres sau tacit ca instrumentul relevant să fie utilizat pentru a efectua o astfel de prelucrare.

33. Curtea a insistat asupra acestei cerințe în Hotărârea Fashion ID [13], în care a declarat expres că răspunderea unui operator este limitată la operațiunea sau la ansamblul operațiunilor de prelucrare de date cu caracter personal ale căror scopuri și mijloace le stabilește *efectiv* [14]. Reiese deci că stabilirea scopurilor și a mijloacelor trebuie să fie direct legată de operațiunea relevantă sau de ansamblul operațiunilor ce implică prelucrarea datelor cu caracter personal.

34. În opinia noastră, din aceste constatări rezultă că o entitate precum NVSC, care inițiază dezvoltarea unei aplicații mobile, poate fi considerată „operator” în sensul articolului 4 punctul 7 din RGPD numai în situația în care există suficiente elemente de natură mai degrabă factuală decât formală din care instanțele naționale pot deduce că o astfel de entitate a exercitat o influență reală asupra „scopurilor și mijloacelor” acestei prelucrări și că a consimțit efectiv la punerea la dispoziția publicului a aplicației mobile și, în consecință, la prelucrarea datelor cu caracter personal. Sub rezerva verificărilor care urmează să fie efectuate de instanța de trimitere, considerăm că NVSC îndeplinește aceste cerințe.

2. Când pot fi două entități considerate operatori asociați? (a cincea întrebare)

35. A cincea întrebare privește condițiile care trebuie îndeplinite pentru ca două (sau mai multe) entități să fie considerate operatori asociați. Înțelegem că instanța de trimitere solicită clarificări cu privire la interpretarea acestei noțiuni, întrucât bănuiește că, în situația în discuție în procedura principală, NVSC și ITSS ar putea fi considerate „operatori asociați” și, în această calitate, ar putea fi răspunzătoare în solidar pentru prejudiciile cauzate [15] și/sau ar putea fi sancționate în solidar cu amendă pentru încălcări ale normelor privind protecția datelor săvârșite cu ocazia punerii la dispoziția publicului a aplicației KARANTINAS pentru a fi descărcată. Constatăm în această privință că, după cum am arătat la punctul 16 de mai sus, această entitate și această societate au fost în fapt deopotrivă considerate responsabile și sancționate cu amendă de către inspectorat în temeiul articolului 83 din RGPD pentru încălcările săvârșite în calitatea lor de operatori asociați.

[13] Hotărârea din 29 iulie 2019 (C-40/17, EU:C:2019:629, punctul 85).

[14] A se vedea de asemenea Orientările 07/2020, punctul 42.

[15] A se vedea articolul 26 alineatul (3) din RGPD, în temeiul căruia „persoana vizată își poate exercita drepturile în temeiul [RGPD] cu privire la și în raport cu fiecare dintre operatori”. A se vedea de asemenea articolul 82 alineatele (4) și (5) din acest regulament.

36. În conformitate cu articolul 26 alineatul (1) din RGPD, există „operatori asociați” în cazul în care doi sau mai mulți operatori stabilesc în comun scopurile și mijloacele de prelucrare. În consecință, fiecare operator asociat trebuie să îndeplinească în mod independent criteriile enumerate în definiția „operatorului” prevăzută la articolul 4 punctul 7 din acest regulament [16]. În plus, operatorii asociați trebuie să aibă o anumită relație între ei, având în vedere că influența lor asupra prelucrării trebuie să fie exercitată în comun.

37. Curtea a arătat că existența unei luări în comun a deciziilor nu implică în mod necesar o responsabilitate sau o participare egală a diferitelor persoane sau entități implicate. Dimpotrivă, operatorii asociați pot fi implicați în diferite stadii ale acestei prelucrări, astfel încât nivelul de răspundere al fiecăruia dintre ei trebuie să fie evaluat ținând seama de toate împrejurările pertinente ale speței [17]. În plus, responsabilitatea comună a mai multor entități pentru aceeași prelucrare nu presupune ca fiecare dintre acestea să aibă acces la datele cu caracter personal vizate [18]. Ceea ce contează însă este faptul că aceste entități *participă în comun* la stabilirea „scopurilor și mijloacelor” prelucrării.

38. În această privință, observăm că, așa cum se precizează în Orientările 07/2020, o astfel de participare în comun se poate regăsi sub diferite forme. Aceasta poate rezulta dintr-o decizie comună luată de două sau mai multe entități ori poate rezulta pur și simplu din decizii convergente ale acestor entități. În acest ultim caz, contează numai faptul că deciziile se completează reciproc și sunt necesare pentru ca prelucrarea să aibă loc, în așa fel încât acestea au un impact concret asupra stabilirii scopurilor și mijloacelor de prelucrare, ceea ce înseamnă în esență că prelucrarea nu ar fi posibilă fără participarea ambelor părți [19].

39. În acest context, instanța de trimitere se întreabă dacă faptul că doi operatori (*in casu*, NVSC și ITSS), nu au ajuns la niciun acord formal cu privire la scopurile și mijloacele de prelucrare și/sau nu par să își fi coordonat în alt mod acțiunile nu permite ca aceștia să fie considerați „operatori asociați”.

40. Înțelegem că îndoielile instanței de trimitere în această privință decurg din faptul că, în conformitate cu articolul 26 alineatul (1) din RGPD, operatorii asociați trebuie să stabilească în mod transparent, prin intermediul unui acord, responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor prevăzute de acest regulament. În plus, considerentul (79) al regulamentului respectiv precizează că este necesară „o atribuire clară a responsabilităților”, inclusiv în cazul în care un operator stabilește scopurile și mijloacele prelucrării împreună cu alți operatori. În opinia noastră însă, aceste obligații și cerințe se aplică operatorilor asociați *numai* din momentul în care ei pot fi considerați astfel. Obligațiile și cerințele respective nu fac parte din criteriile care trebuie îndeplinite pentru ca aceștia să fie calificați ca atare.

41. După cum am afirmat la punctul 36 de mai sus, luarea în comun a deciziilor depinde doar de îndeplinirea a două condiții obiective. Prima, fiecare operator asociat trebuie să îndeplinească criteriile enumerate în definiția „operatorului” prevăzută la articolul 4 punctul 7 din RGPD. La dosarul cauzei nu există suficiente informații pe baza cărora să se poată stabili dacă, în situația din cauza principală, ITSS trebuie considerat „operator” în sensul acestei dispoziții. Totuși, în opinia noastră, în lumina constatărilor pe care le-am făcut în secțiunea anterioară și sub rezerva verificărilor care urmează a fi efectuate de instanța de trimitere, cel puțin NVSC – dacă nu

16 A se vedea în această privință Hotărârea din 29 iulie 2019, Fashion ID (C-40/17, EU:C:2019:629, punctul 67 și jurisprudența citată).

17 A se vedea în acest sens Hotărârea din 5 iunie 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388, punctul 43).

18 A se vedea Hotărârea din 10 iulie 2018, Jehovan todistajat (C-25/17, EU:C:2018:551, punctul 69 și jurisprudența citată).

19 A se vedea Orientările 07/2020, p. 3 și punctele 54 și 55.

ambele, atât această entitate, cât și ITSS – îndeplinește condițiile pentru a fi considerat „operator” în sensul acestei dispoziții. A doua, influența operatorilor asupra prelucrării trebuie să fie exercitată în comun (ceea ce înseamnă că aceasta trebuie să fie exercitată în conformitate cu criteriile legale și cu jurisprudența amintite la punctele 37 și 38 de mai sus). În această privință, am explicat că participarea în comun la prelucrare poate avea loc sub diferite forme și nici măcar nu trebuie să provină dintr-o decizie comună a părților implicate. Ca atare, abordarea materială și funcțională necesară pentru a stabili dacă o persoană sau o entitate trebuie să fie considerată „operator”, în sensul articolului 4 punctul 7 din RGPD, se aplică de asemenea, în opinia noastră, în cazul luării în comun a deciziilor [20].

42. Având în vedere aceste elemente, considerăm, în primul rând, că absența oricărui acord sau înțelegere ori chiar a unei decizii comune între doi sau mai mulți operatori, cum sunt NVSC și ITSS, nu poate exclude, în sine, constatarea că sunt „operatori asociați” în sensul articolului 4 punctul 7 coroborat cu articolul 26 alineatul (1) din RGPD. În această privință, adăugăm că EDPB a sugerat că înțelegerile contractuale, deși pot fi utile în evaluarea luării în comun a deciziilor, ar trebui întotdeauna verificate în raport cu împrejurările de fapt ale relației dintre părți [21].

43. În al doilea rând, considerăm de asemenea că doar pentru că NVSC și ITSS nu par, dincolo de faptul că nu au ajuns la un acord, la o înțelegere sau la o decizie comună, să își fi coordonat acțiunile sau să fi cooperat în alt mod una cu cealaltă nu înseamnă că nu pot fi considerate „operatori asociați”. Chiar dacă există o astfel de coordonare sau cooperare, aceasta nu are nicio relevanță în ceea ce privește chestiunea dacă relația dintre aceste două entități este sau nu una de control în comun. Într-adevăr, se poate imagina cu ușurință că ar putea exista cooperare sau coordonare între două sau mai multe entități, fără ca acestea să fie deloc operatori asociați. De exemplu, doi operatori diferiți ar putea să își coordoneze acțiunile sau să coopereze reciproc cu intenția de a transfera date cu caracter personal între ei. Totuși, acest lucru nu i-ar transforma în „operatori asociați” în sensul articolului 4 punctul 7 și al articolului 26 alineatul (1) din RGPD [22]. Ceea ce contează, după cum am explicat la punctul 38 de mai sus, este faptul că prelucrarea nu ar fi posibilă fără participarea ambelor părți, întrucât ambele au un impact tangibil asupra stabilirii scopurilor și mijloacelor respectivei prelucrări.

3. Concluzie privind interpretarea noțiunii de „operator” și situațiile de luare în comun a deciziilor

44. Având în vedere cele menționate anterior, considerăm că, pe de o parte, sub rezerva verificărilor care urmează să fie efectuate de instanța de trimitere, o entitate precum NVSC îndeplinește condițiile enumerate la articolul 4 punctul 7 din RGPD pentru a fi considerată „operator”. Pe de altă parte, faptul dacă NVSC și ITSS pot fi considerați „operatori asociați”, în conformitate cu criteriile pe care le-am prezentat în secțiunea anterioară, sau dacă pot fi considerați „operator” și, respectiv, „persoană împuternicită de operator” depinde de natura relației lor, aspect a cărui verificare revine instanței de trimitere.

45. În această privință, adăugăm că natura relației dintre NVSC și ITSS (și anume dacă sunt „operatori asociați” sau „operator” și, respectiv, „persoană împuternicită de operator”) este relevantă pentru a șasea întrebare. Prin urmare, vom reveni la constatările pe care le-am făcut cu privire la a cincea întrebare atunci când vom aborda problemele ridicate prin a șasea întrebare.

[20] Într-adevăr, ar fi ușor contradictoriu dacă ar fi posibil să se elimine cerințele formale pentru ca o persoană sau o entitate să fie calificată drept „operator”, dar nu și ca aceeași entitate împreună cu o altă entitate să fie considerate „operatori asociați”.

[21] A se vedea Orientările 07/2020, punctul 52.

[22] A se vedea în această privință Orientările 07/2020, punctul 69.

B. Cu privire la conceptul de „prelucrare” (a patra întrebare)

46. Prin intermediul celei de a patra întrebări, instanța de trimitere solicită să se stabilească în esență dacă definiția noțiunii de „prelucrare” prevăzută la articolul 4 punctul 2 din RGPD acoperă o situație în care datele cu caracter personal sunt utilizate în faza de testare a unei aplicații mobile [23]. Deducem din cererea de decizie preliminară că aplicația KARANTINAS a fost supusă unei faze de testare înainte de a fi pusă la dispoziția publicului pentru a fi descărcată. Din câte înțelegem, a patra întrebare privește o situație care diferă de cea care stă în centrul celeilalte întrebări adresate Curții, toate referindu-se la prelucrarea datelor cu caracter personal după derularea fazei de testare, când KARANTINAS a fost pusă la dispoziția publicului. Mai exact, instanța de trimitere dorește să știe dacă utilizarea datelor cu caracter personal în cursul acestei faze de testare poate fi calificată drept „prelucrare” în sensul articolului 4 punctul 2 din RGPD și, ca atare, ar putea atrage răspunderea potențială a operatorilor și/sau a persoanelor împuternicite de operatori implicate.

47. Articolul 4 punctul 2 din RGPD definește „prelucrarea” ca fiind „*orice* operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate […]” [24].

48. Deducem din această formulare (în special din utilizarea cuvântului „orice” și a unor termeni generici, cum ar fi „operațiune” sau „set de operațiuni”) că dispoziția trebuie să primească o accepțiune largă, astfel încât să acopere cât mai multe situații posibile în care sunt utilizate date cu caracter personal. Lista neexhaustivă a unor astfel de situații prevăzută în această dispoziție confirmă interpretarea noastră, dată fiind varietatea operațiunilor incluse în aceasta [25].

49. În plus, deși din secțiunea de mai sus rezultă că definiția „operatorului”, în sensul articolului 4 punctul 7 din regulamentul menționat, este strâns legată de scopurile prelucrării datelor cu caracter personal (motivele „pentru care” sunt colectate datele cu caracter personal), situația este diferită în cazul definiției de la articolul 4 punctul 2 din regulamentul respectiv. Ca atare, motivele pentru care se efectuează o operațiune sau un set de operațiuni sunt, în principiu, irelevante pentru întrebarea dacă acestea trebuie să fie calificate drept „prelucrare” în sensul acestei dispoziții. Implicit, în opinia noastră, împrejurarea că datele cu caracter personal sunt colectate în vederea testării sistemelor informatice încorporate într-o aplicație mobilă sau în alt scop nu are nicio incidență asupra chestiunii dacă operațiunea în cauză poate fi calificată drept „prelucrare”.

[23] Observăm că, în a patra întrebare, instanța de trimitere menționează mai curând utilizarea de „copii ale unor date cu caracter personal” decât de date cu caracter personal. Trebuie să recunoaștem că nu ne este clar ce înțelege această instanță prin sintagma „copii ale unor date cu caracter personal”, având în vedere că datele cu caracter personal pot exista într-o formă necorporală, și că, astfel cum se arată în mod clar la articolul 4 punctul 1 din RGPD, sintagma „date cu caracter personal” este definită în această dispoziție ca fiind „*orice* informații privind o persoană fizică identificată sau identificabilă” (sublinierea noastră), fără alte cerințe privind „copierea” sau transcrierea datelor personale pe un dispozitiv sau un mediu de comunicare anume. În opinia noastră, obiectul fizic (de exemplu copii pe suport fizic) sau, în măsura în care prezintă interes, dosarele electronice pe care sunt disponibile datele cu caracter personal nu sunt relevante pentru a stabili dacă un anumit set de operațiuni care implică date cu caracter personal poate fi considerat „prelucrare” în sensul articolului 4 punctul 2 din acest regulament. Adăugăm în această privință că „prelucrarea” are loc în prezent adesea într-un mod computerizat în care datele cu caracter personal sunt, în general, utilizate oricum într-o formă necorporală. În consecință, în răspunsul nostru la a patra întrebare, vom face referire mai degrabă la „date cu caracter personal” decât la „copii ale unor date cu caracter personal”.

[24] Sublinierea noastră.

[25] În conformitate cu articolul 4 punctul 2 din RGPD, „prelucrarea” include operațiuni precum „colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea”.

50. În această privință, observăm în continuare că „utilizarea” datelor cu caracter personal (fără nicio altă mențiune și, în consecință, indiferent de scopul utilizării) este enumerată printre operațiunile sau seturile de operațiuni care constituie o „prelucrare” [26]. În plus, articolul 4 punctul 2 din RGPD nu conține nicio excepție, derogare sau excludere expresă pentru operațiunile referitoare la utilizarea datelor cu caracter personal în vederea *testării* sistemelor informatice. În concluzie, nimic nu împiedică să se considere utilizarea datelor cu caracter personal în vederea efectuării unor astfel de teste ca fiind o „prelucrare” în sensul dispoziției respective, ba dimpotrivă.

51. În lumina acestor elemente, apreciem că definiția „prelucrării” prevăzută la articolul 4 punctul 2 din RGPD acoperă situația în care datele cu caracter personal sunt utilizate în timpul fazei de testare a unei aplicații mobile.

52. Concluzia noastră în această privință nu este afectată de simplul fapt că este posibil ca datele cu caracter personal furnizate în scopul testării sistemelor informatice încorporate într-o aplicație mobilă să fi fost supuse pseudonimizării [27]. Singura împrejurare în care RGPD nu ar fi aplicabil este aceea în care informațiile furnizate pe aplicația mobilă constau doar în informații anonime care „nu sunt legate de o persoană fizică identificată sau identificabilă” sau în date cu caracter personal care au fost „anonimizate astfel încât persoana vizată nu este sau nu mai este identificabilă”. Cu toate acestea, constatăm că, în cauza din litigiul principal, datele utilizate pentru faza de testare *nu* par, pe baza informațiilor furnizate în dosarul cauzei, să fi constat în astfel de date anonimizate [28].

53. Având în vedere cele menționate anterior, considerăm că definiția „prelucrării” prevăzută la articolul 4 punctul 2 din RGPD acoperă o situație în care datele cu caracter personal sunt utilizate în cursul fazei de testare a unei aplicații mobile, cu excepția cazului în care astfel de date au fost anonimizate în așa fel încât persoana vizată nu este sau nu mai este identificabilă. Faptul că datele cu caracter personal sunt colectate în vederea testării sistemelor informatice încorporate într-o aplicație mobilă sau într-un alt scop nu are, la rândul său, nicio influență asupra chestiunii dacă operațiunea în discuție poate fi considerată o „prelucrare” [29].

54. Odată făcute aceste clarificări, vom trece în continuare la problema principală din prezenta cauză, referitoare la condițiile în care o amendă administrativă poate fi impusă unui operator sau unei persoane împuternicite de operator, în temeiul articolului 83 din RGPD.

[26] A se vedea nota de subsol anterioară.

[27] Într-adevăr, „datele cu caracter personal”, în sensul articolului 4 punctul 1 din RGPD, interpretat în lumina considerentului (26) al acestuia, includ datele cu caracter personal care au fost supuse pseudonimizării, dar care ar putea fi atribuite unei persoane fizice prin utilizarea de informații personale suplimentare.

[28] În cererea de decizie preliminară, instanța de trimitere menționează că este posibil ca o parte, dar nu toate, din datele cu caracter personal utilizate în scopul etapei de testare să fi fost date „false”. Totuși, aceasta nu detaliază în continuare ce înțelege prin acest termen. Dorim numai să precizăm în această privință că, în opinia noastră, informațiile pot fi calificate ca fiind „date cu caracter personal”, în sensul articolului 4 punctul 1 din RGPD, indiferent dacă ele conțin informații adevărate sau false. Ceea ce contează, după cum am afirmat, este doar faptul că informațiile se referă la o persoană fizică identificată sau identificabilă. În cazul în care datele sunt în întregime inventate, astfel încât nu se poate spune că acestea se referă la o persoană identificată sau identificabilă, atunci, în opinia noastră, ele nu sunt „date cu caracter personal”, iar RGPD nu se aplică prelucrării respectivelor date. Cu toate acestea, regulamentul rămâne aplicabil în privința celorlalte date „care nu sunt false”, colectate în cursul fazei de testare.

[29] Dorim să reamintim că utilizarea datelor cu caracter personal în scopul testării sistemelor informatice încorporate într-o aplicație mobilă constituie o „prelucrare” diferită de cea care are loc atunci când aceeași aplicație mobilă este pusă la dispoziția publicului pentru a fi descărcată. Prin urmare, este necesară o evaluare separată pentru a stabili ce este un „operator”, o „persoană împuternicită de operator” sau un „operator asociat”.

C. Cu privire la amenzile administrative aplicate în temeiul articolului 83 din RGPD (a șasea întrebare)

55. Înainte de adoptarea RGPD, sancțiunile pentru încălcarea normelor de protecție a datelor erau în mare parte lăsate la aprecierea statelor membre, în conformitate cu autonomia lor procedurală și procesuală [30]. Amenzile administrative introduse prin articolul 83 din regulamentul menționat sunt, în consecință, o „evoluție" relativ nouă în dreptul Uniunii în materie de protecție a datelor. Acestea au fost descrise de Grupul de lucru „Articolul 29" ca fiind un „element central în cadrul noului sistem de punere în aplicare" [31]. Chiar dacă această dispoziție nu a fost interpretată încă de Curte, ea a fost deja aplicată de autoritățile de supraveghere, uneori pentru a impune amenzi ridicate operatorilor sau persoanelor împuternicite de operatori [32].

56. Articolul 83 din RGPD prevede un sistem de sancțiuni pe două niveluri, în funcție de tipul specific de dispoziție încălcată. În timp ce primul nivel, definit la articolul 83 alineatul (4) din acest regulament, se aplică situațiilor în care un operator sau o persoană împuternicită de operator încalcă obligațiile generale care îi revin, precum și anumite obligații specifice, cel de al doilea nivel este rezervat, după cum indică articolul 83 alineatul (5) din RGPD, unor încălcări mai grave, cum ar fi încălcarea printre altele a principiilor de bază pentru prelucrare, a drepturilor persoanelor vizate și a normelor referitoare la transferul de date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională.

57. În cazul ambelor niveluri, autoritățile naționale competente, după ce au stabilit că o anumită dispoziție din RGPD a fost încălcată, trebuie să efectueze două evaluări. În primul rând, trebuie să stabilească dacă s-ar impune să se aplice o amendă și, în al doilea rând, în cazul în care au stabilit că se impune, trebuie să determine cuantumul amenzii respective. Aceste evaluări trebuie efectuate *în fiecare caz individual*, având în vedere diferiții factori enumerați la articolul 83 alineatul (2) din GDPR. Printre acești factori se numără „dacă încălcarea a fost comisă intenționat sau din neglijență" [articolul 83 alineatul (2) litera (b) din acesta].

58. Prin intermediul celei de a șasea întrebări, instanța de trimitere solicită să se stabilească în esență dacă o amendă administrativă poate fi impusă unui operator atunci când acesta nu a încălcat în mod intenționat sau din neglijență normele privind protecția datelor, iar prelucrarea ilegală a datelor cu caracter personal nu a fost efectuată de operatorul însuși, ci de o persoană împuternicită de operator. Revenind la constatările făcute anterior cu privire la a cincea întrebare, considerăm că a șasea întrebare este adresată în cazul în care, în litigiul principal, NVSC și ITSS ar putea să nu fie considerați „operatori asociați", în sensul articolului 4 punctul 7 coroborat cu articolul 26 alineatul (1) din RGPD, și ar trebui să fie considerați „operator" și, respectiv, „persoană împuternicită de operator". În acest cadru special, instanța de trimitere ar dori să se clarifice în ce împrejurări NVSC poate fi sancționat cu amendă în temeiul articolului 83 din RGPD.

59. Remarcăm încă faptul că a șasea întrebare menționează numai articolul 83 alineatul (1) din RGPD ca fiind dispoziția relevantă. Cu toate acestea, în opinia noastră, problemele ridicate de această întrebare impun luarea în considerare a articolului 83 din acest regulament în ansamblul

[30] A se vedea articolul 24 din Directiva 95/46.

[31] A se vedea „Orientările privind aplicarea și stabilirea unor amenzi administrative în sensul [RGPD]" ale Grupului de lucru „Articolul 29" pentru protecția datelor, adoptate la 3 octombrie 2017, p. 4. Acest grup de lucru a fost înlocuit ulterior de EDPB. Totuși, „Orientările privind aplicarea și stabilirea unor amenzi administrative" ale acestuia rămân valabile.

[32] A se vedea de exemplu amenda de mai multe milioane de euro aplicată în cazul Google de autoritatea franceză pentru protecția datelor în ianuarie 2019 (https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en).

său și în special după cum am explicat la punctul 57 de mai sus, luarea în considerare a articolului 83 alineatul (2) litera (b) din acesta, având în vedere că această dispoziție vizează „dacă încălcarea a fost comisă intenționat sau din neglijență”. Astfel, vom considera că a șasea întrebare privește interpretarea articolului 83 din RGPD în ansamblul său, iar nu doar a articolului 83 alineatul (1) din acesta.

60. În opinia noastră, această întrebare conține două părți. În primul rând, se solicită Curții să stabilească dacă articolul 83 din RGPD permite ca amenzile administrative în general să fie impuse operatorilor sau persoanelor împuternicite de operatori în absența *mens rea* (element mental – culpă). În esență, instanța de trimitere ar dori să se stabilească dacă NVSC ar putea fi amendat pentru simplul motiv că a încălcat obligațiile care îi sunt impuse în virtutea calității de operator (răspundere strict obiectivă) sau dacă este necesar un element de vinovăție în comiterea încălcării/încălcărilor relevante. În al doilea rând, aceasta solicită să se clarifice dacă faptul că prelucrarea ilegală a datelor cu caracter personal nu a fost efectuată de operatorul însuși, ci de o persoană împuternicită de operator afectează în vreun fel capacitatea autorităților de supraveghere de a-i impune o amendă operatorului.

61. Vom analiza pe rând fiecare dintre aceste două părți.

1. Primul aspect: necesitatea de a stabili existența vinovăției

62. Articolul 83 din RGPD prevede că orice amendă administrativă impusă pentru încălcarea normelor privind protecția datelor trebuie să fie „eficace, proporțională și disuasivă”. Acest lucru este indicat la alineatul (1) din dispoziția respectivă. Acest alineat nu precizează însă dacă o astfel de amendă poate fi impusă numai dacă se stabilește și existenta vinovăției, cu alte cuvinte, dacă „vinovăția” este o condiție prealabilă pentru aplicarea unei amenzi administrative.

63. Pe de altă parte, alineatul (2) litera (b) al acestei dispoziții menționează „dacă încălcarea a fost comisă intenționat sau din neglijență” printre elementele[33] cărora autoritățile de supraveghere trebuie să le acorde „atenția cuvenită” în fiecare caz în parte. Potrivit articolului 83 alineatul (2) litera (k) din regulamentul menționat, aceste elemente trebuie înțelese ca „factor[i] agravan[ți] sau atenuan[ți]” și nu sunt exhaustive.

64. În acest context, există, în opinia noastră, două modalități posibile de a înțelege articolul 83 din RGPD.

65. Pe de o parte, s-ar putea considera că, deși decizia de a impune o amendă și cuantumul acesteia trebuie stabilite ținând seama în mod corespunzător de gradul de vinovăție existent (astfel încât, de exemplu, o amendă mai mare ar trebui impusă în principiu dacă încălcarea a fost rezultatul unui comportament intenționat și, dimpotrivă, un comportament neglijent ar trebui să conducă la o amendă mai mică), nimic nu împiedică impunerea unei amenzi și *în absența oricărei forme de vinovăție*, atât timp cât persoana împuternicită de operator sau operatorul poate fi

[33] Mai exact, la articolul 83 alineatul (2) litera (b) din acest regulament. Celelalte elemente enumerate la articolul 83 alineatul (2) literele (a)-(k) sunt legate fie de *încălcarea propriu-zisă* [de exemplu natura, gravitatea și durata acesteia (a) sau categoriile de date cu caracter personal vizate (g)], fie de *operatorul* sau de *persoana împuternicită de operator* căreia i se va aplica amenda [și anume gradul de responsabilitate a acestora (d), conduita lor *ex ante*, cum ar fi încălcările anterioare relevante (e), și măsurile anterioare dispuse împotriva acestora (i), precum și comportamentul lor *ex post*, inclusiv dacă au notificat sau nu încălcarea (h), acțiunile pe care le-au întreprins pentru a reduce prejudiciul (c) și gradul de cooperare cu autoritatea de supraveghere pentru a remedia încălcarea și a atenua posibilele efecte negative ale acesteia (f)]. În plus, trebuie să se acorde atenția cuvenită „oric[ărui] alt factor agravant sau atenuant aplicabil circumstanțelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării” (k).

considerat responsabil pentru încălcare. Această interpretare ar fi susținută de o lectură a articolului 83 alineatul (2) literele (b) și (k), în sensul că, prin menționarea unor forme diferite de vinovăție (intenție sau neglijență) ca „factor[i] agravan[ți] sau atenuan[ți]”, aceste dispoziții ar putea să implice faptul că, în general, vinovăția nu este o condiție prealabilă pentru impunerea unei amenzi.

66. Pe de altă parte, s-ar mai putea argumenta, asemenea Comisiei în prezenta cauză, că neglijența persoanei sau a entității care a săvârșit încălcarea trebuie, *ca cerință minimă*, să fie stabilită înainte de a se putea impune o amendă. Această abordare ar fi susținută de o interpretare diferită, mai prudentă, a articolului 83 alineatul (2) literele (b) și (k) din RGPD, și anume că aceste dispoziții obligă autoritățile de supraveghere să facă distincție între un factor atenuant (neglijența) și unul agravant (intenția), dar nu indică faptul că o amendă ar putea fi impusă *în lipsa oricărei forme de vinovăție*.

67. Comisia a optat în mod expres pentru această interpretare în propunerea sa inițială care a condus la adoptarea RGPD [34], în care sugera organizarea sistemului de amenzi ca un sistem cu trei niveluri. Pentru fiecare nivel, Comisia a propus ca amenzile să poată fi exclusiv aplicate „oricărei persoane care, cu intenție sau din neglijență” [35], a săvârșit una sau mai multe dintre încălcările presupuse. Astfel, Comisia a avut în vedere în mod clar vinovăția drept condiție prealabilă pentru impunerea unei astfel de amenzi [36].

68. Chiar dacă ambele abordări pot fi, în opinia noastră, susținute printr-o interpretare literală a articolului 83 alineatul (2) din RGPD, întrucât fiecare dintre ele corespunde unei înțelegeri a formulării „dacă încălcarea a fost comisă intenționat sau din neglijență” drept factor „agravant” sau „atenuant”, considerăm că numai a doua abordare reflectă în mod corect intenția legiuitorului Uniunii. Există mai multe motive care ne ghidează spre această concluzie.

a) Motivele pentru care este necesară vinovăția

69. În primul rând, observăm că mai mulți factori dintre cei enumerați la articolul 83 alineatul (2) din RGPD conțin formulări specifice din care se poate deduce că nu este posibil să se aplice astfel de factori în toate cazurile, ci numai în unele. În special, articolul 83 alineatul (2) literele (c), (e) și (k) începe de fiecare dată cu cuvântul „orice” [sau un echivalent al acestuia] („orice acțiuni întreprinse de operator sau de persoana împuternicită de operator pentru a reduce prejudiciul […]”; „eventualele încălcări anterioare relevante […]”; „orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului […]”), sugerând astfel că, deși autoritățile de supraveghere trebuie să ia întotdeauna în considerare existența oricărei acțiuni atenuante, a unei încălcări anterioare sau a altui factor agravant sau atenuant relevant, în cazul în care există sau sunt dovedite asemenea elemente, pot în fapt exista situații în care aceleași elemente lipsesc pur și simplu și totuși autoritatea competentă în materie de protecție a datelor poate decide totuși să impună o amendă (sau, dimpotrivă, să nu impună o amendă). În mod similar, observăm că articolul 83 alineatul (2) litera (i) din RGPD este formulat tot într-o manieră nesistematică,

[34] „Propunere de regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulament general privind protecția datelor)”, COM(2012) 11 final (denumită în continuare „Propunerea inițială a Comisiei privind adoptarea unui regulament”).

[35] A se vedea articolul 79 alineatele (4), (5) și (6) din propunerea inițială a Comisiei pentru adoptarea unui regulament. Observăm că natura „*intenționat*[*ă*] sau *din neglijență*” a încălcării a fost inclusă de asemenea în lista de factori cuprinsă la articolul 79 alineatul (2) din această propunere, care trebuiau luați în considerare pentru a stabili cuantumul amenzii; sublinierea noastră.

[36] Formularea respectivă a fost modificată ulterior, iar sintagma „în mod intenționat sau din neglijență” nu mai este inclusă în dispozițiile care definesc cele două niveluri ale sistemului de amenzi instituit prin RGPD.

întrucât impune să se analizeze dacă operatorul sau persoana împuternicită de operator a respectat măsurile menționate la articolul 58 alineatul (2) din regulamentul menționat, dar numai „în cazul în care [astfel de] măsur[i] […] au fost dispuse anterior împotriva operatorului sau persoanei împuternicite de operator”.

70. În schimb, articolul 83 alineatul (2) litera (b) menționează „dacă încălcarea a fost comisă intenționat sau din neglijență”[37]. Ca atare, considerăm că acesta face parte din factorii care trebuie să *se regăsească* în toate cazurile și, figurativ vorbind, care trebuie „bifat” în toate cazurile înainte de a se putea impune o amendă, la fel ca „natura, gravitatea și durata încălcării […]” [articolul 83 alineatul (2) litera (a)], „categoriile de date cu caracter personal afectate de încălcare […]” [articolul 83 alineatul (2) litera (g)], și „modul în care încălcarea a fost adusă la cunoștință[ă] […]” [articolul 83 alineatul (2) litera (h)]. În opinia noastră, acești alți factori trebuie de asemenea să „se regăsească” în toate cazurile: de exemplu, „natura, gravitatea și durata încălcării” pot fi foarte diferite de la un caz la altul (și, în consecință, pot fi considerate fie ca un motiv „pentru”, fie ca un motiv „împotriva” impunerii unei amenzi). Cu toate acestea, în toate cazurile vor exista *natura*, *o anumită* gravitate și *o anumită* durată a încălcării care trebuie luate în considerare. În opinia noastră, acesta constituie primul indiciu că amenzile administrative au fost introduse la articolul 83 din RGPD astfel încât acestea să fie impuse numai în situațiile în care presupusa încălcare a fost săvârșită fie intenționat, fie din neglijență[38].

71. În al doilea rând, observăm că, deși articolul 83 alineatul (2) din RGPD nu prevede în mod expres că încălcarea trebuie să fi avut loc „în mod intenționat sau din neglijență”, nu se poate spune același lucru despre alineatul (3) al acestei dispoziții, care conține o regulă generală ce exclude cumularea amenzilor administrative. Acest alineat menționează *numai* situația în care încălcarea/încălcările relevantă/relevante a/au avut loc „în mod intenționat sau din neglijență”.

72. În opinia noastră, în mod logic rezultă că articolul 83 alineatul (2) din RGPD trebuie interpretat în sensul că o amendă poate fi impusă *numai în cazul în care* presupusa încălcare a avut loc în mod intenționat sau din neglijență. Într-adevăr, dacă domeniul de aplicare al articolului 83 alineatele (2) și (3) din RGPD ar fi diferit, atunci ar fi posibilă impunerea unor amenzi cumulate pentru încălcări mai puțin grave (și anume cele săvârșite *fără nicio formă de vinovăție*), întrucât acestea, deși ar putea încă să determine aplicarea unei amenzi în temeiul primei dintre dispozițiile menționate [articolul 83 alineatul (2)], nu ar intra sub incidența celei de a doua dispoziții [articolul 83 alineatul (3)], dar ar putea totuși să conducă la aplicarea unei amenzi în temeiul primei dispoziții [articolul 83 alineatul (2)]. Cu toate acestea, nu ar fi posibil același lucru în cazul încălcărilor săvârșite din neglijență sau cu intenție, întrucât toate ar face obiectul regulii care nu permite cumulul, prevăzută la articolul 83 alineatul (3) din acest regulament. Un astfel de rezultat ar fi în mod clar contrar principiului de bază al regimului sancționator instituit de RGPD, și anume că încălcările grave ar trebui, în principiu, să fie sancționate mai strict decât cele mai puțin grave, și nu invers.

73. În al treilea rând, remarcăm că amenzile impuse în temeiul articolului 83 din RGPD pot avea ca rezultat o pedepsire severă. Într-adevăr, primul nivel, care este reglementat de articolul 83 alineatul (4) din acest regulament, poate conduce la impunerea unor amenzi de până la 10 000 000 de euro sau, în cazul unei întreprinderi, de până la 2 % din cifra de afaceri mondială

[37] Sublinierea noastră.

[38] Aceeași observație poate fi făcută și dacă privim celelalte versiuni lingvistice ale articolului 83 alineatul (2) din RGPD, în special versiunile în limbile cehă, greacă, spaniolă, franceză și italiană. Cu toate acestea, arătăm că în versiunea în limba italiană se folosește mai curând articolul hotărât „*le*” decât „eventuali” („orice”), în ceea ce privește articolul 83 alineatul (2) litera (c) din acest regulament, care se referă la măsurile luate de operator sau de persoana împuternicită de operator pentru a reduce prejudiciul.

totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare. Al doilea nivel prevede amenzi de până la 20 000 000 de euro sau, în cazul unei întreprinderi, de până la 4 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior (luându-se în calcul, din nou, cea mai mare valoare).

74. În consecință, considerăm că amenzile aplicate în conformitate cu articolul 83 din RGPD urmăresc un scop punitiv, cel puțin în anumite situații [39], și prezintă un grad ridicat de severitate, astfel încât pot fi considerate ca fiind de natură penală [40] și, prin urmare, ca intrând sub incidența articolului 49 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”) [41].

75. În lumina acestor elemente și îndeosebi a naturii penale a amenzilor aplicate în temeiul articolului 83 din RGPD, am putea fi tentați să susținem că ar fi astfel incompatibil cu cerința de la alineatul (1) al aceste dispoziții ca amenzile să fie, în toate cazurile, nu doar „eficiente” și „disuasive”, ci și „proporționale”, pentru a permite ca astfel de amenzi să fie aplicate în lipsa vinovăției. Cu alte cuvinte, ar fi disproporționat să se impună amenzi în cazurile în care nici măcar neglijența nu a fost stabilită. În opinia noastră, acest argument este însă greu de susținut, având în vedere că Curtea a constatat deja că un regim de sancțiuni bazat pe răspunderea strict obiectivă, chiar și unul de natură penală, nu este, în sine, disproporționat în raport cu obiectivele urmărite atunci când acest regim este de natură să stimuleze persoanele în cauză să respecte dispozițiile unui regulament și când obiectivele urmărite prezintă un interes general care poate justifica instituirea unui asemenea regim [42]. În plus, Curtea Europeană a Drepturilor Omului (Curtea EDO) a statuat, în ceea ce privește articolul 7 din Convenția Europeană a Drepturilor Omului (CEDO) (care corespunde articolului 49 din cartă) [43], că, deși pedeapsa în temeiul acestei dispoziții presupune în general existența unei legături mentale prin care să poată fi detectat un element de răspundere în comportamentul persoanei care a săvârșit fizic infracțiunea, această cerință nu exclude existența anumitor forme de răspundere obiectivă [44].

76. Deducem însă din această jurisprudență că, de regulă, pentru a impune o sancțiune penală este necesar să existe *mens rea* și că răspunderea obiectivă constituie astfel un fel de „excepție” de la această regulă generală, încât trebuie să își găsească justificare în lumina obiectivelor urmărite de regulament.

[39] Potrivit Grupului de lucru „Articolul 29”, amenzile administrative sunt „măsuri corective” al căror obiectiv poate fi „fie restabilirea conformității cu normele, fie *sancționarea* unui comportament ilicit (sau ambele)” (sublinierea noastră) (a se vedea „Orientările privind aplicarea și stabilirea unor amenzi administrative în sensul [RGPD]” ale Grupului de lucru „Articolul 29” pentru protecția datelor, adoptate la 3 octombrie 2017, p. 6).

[40] A se vedea prin analogie Hotărârea din 2 februarie 2021, Consob (C-481/19, EU:C:2021:84, punctul 43). Reamintim că pentru a aprecia dacă sancțiunile sunt de natură penală sunt relevante trei criterii: primul criteriu este calificarea juridică a faptei ilicite în dreptul intern, al doilea privește natura intrinsecă a faptei ilicite, iar al treilea se referă la gradul de severitate a sancțiunii pe care persoana în cauză riscă să o suporte (a se vedea punctul 42 din acea hotărâre, precum și Hotărârea din 5 iunie 2012, Bonda, C-489/10, EU:C:2012:319, punctul 37; a se vedea de asemenea Curtea EDO, 8 iunie 1976, Engel și alții împotriva Țărilor de Jos, CE:ECHR:1976:0608JUD000510071, § 82). Nu trebuie îndeplinite toate criteriile pentru ca o amendă să fie considerată ca fiind penală (a se vedea în această privință Concluziile avocatului general Bot prezentate în cauza ThyssenKrupp Nirosta/Comisia (C-352/09 P, EU:C:2010:635, punctul 50 și jurisprudența citată).

[41] Articolul 49 din cartă, intitulat „Principiile legalității și proporționalității infracțiunilor și pedepselor”, prevede la alineatul (3) că „[p]edepsele nu trebuie să fie disproporționate față de infracțiune”.

[42] A se vedea Hotărârea din 9 februarie 2012, Urbán (C-210/10, EU:C:2012:64, punctul 48), Hotărârea din 13 noiembrie 2014, Reindl (C-443/13, EU:C:2014:2370, punctul 42), Hotărârea din 20 decembrie 2017, Global Starnet (C-322/16, EU:C:2017:985, punctul 63), precum și Hotărârea din 22 martie 2017, Euro-Team și Spirál-Gép (C-497/15 și C-498/15, EU:C:2017:229, punctele 53 și 54). Aceste hotărâri ilustrează faptul că jurisprudența respectivă a fost aplicată în domenii variate ale dreptului Uniunii.

[43] A se vedea „Explicațiile cu privire la Carta drepturilor fundamentale” (JO 2007, C 303, p. 17). În conformitate cu articolul 52 alineatul (3) din cartă, nivelul de protecție acordat de articolul 49 din cartă nu poate fi inferior celui oferit de articolul 7 din CEDO.

[44] A se vedea Curtea EDO (Marea Cameră), 28 iunie 2018, GIEM s.r.l. și alții împotriva Italiei (CE:ECHR:2018:0628JUD000182806, § 242 și 243).

77. În opinia noastră, dacă luăm în considerare RGPD în ansamblul său, amenzile administrative au fost avute în vedere de legiuitorul Uniunii ca fiind *numai unul* dintre instrumentele prevăzute în acest act normativ pentru a asigura respectarea efectivă a acestuia. Într-adevăr, amenzile trebuie să fie impuse „în completarea sau în locul" celorlalte măsuri enumerate la articolul 58 alineatul (2) din acest regulament, care conferă autorităților de supraveghere o serie de competențe corective (precum competența de a emite avertizări, mustrări sau somații)[45]. În plus, în situațiile în care nu este impusă o amendă administrativă în conformitate cu articolul 83 din RGPD, autoritățile de supraveghere au posibilitatea de a impune alte sancțiuni în temeiul articolului 84 din acest regulament[46].

78. În opinia noastră, aceste dispoziții arată în mod clar că, atunci când a adoptat acest regulament, legiuitorul Uniunii nu a avut intenția de a sancționa cu amendă administrativă *fiecare* încălcare a normelor privind protecția datelor. Acesta a urmărit mai degrabă să prevadă un sistem flexibil și diferențiat de penalități și sancțiuni. Acest lucru este confirmat de considerentul (148) al RGPD, care prevede că autoritățile de supraveghere se pot abține de la impunerea unei amenzi administrative și pot emite în schimb un avertisment, în cazul unei „încălcări minore sau în cazul în care amenda susceptibilă de a fi impusă ar constitui o sarcină disproporționată pentru o persoană fizică". În acest context, limitarea aplicării articolului 83 din RGPD la situațiile în care se constată existența neglijenței, ca cerință minimă, se aliniază, în opinia noastră, la aceste obiective și la logica generală a diferitelor dispoziții potrivit cărora aplicarea unor amenzi administrative ar trebui să fie posibilă numai pentru anumite tipuri de încălcări.

79. De asemenea, considerăm că, atunci când legiuitorul Uniunii și-a manifestat dorința de a introduce în RGPD răspunderea obiectivă sau prezumată, a făcut acest lucru folosind o formulare specifică ce nu se regăsește la articolul 83 din acesta. De exemplu, în ceea ce privește răspunderea civilă (și anume răspunderea operatorilor și a persoanelor împuternicite de operatori față de persoanele vizate), reglementată la articolul 82 din RGPD, legiuitorul Uniunii a afirmat că operatorii și persoanele împuternicite de operatori au obligația strictă de a despăgubi prejudiciile pe care le cauzează persoanelor vizate, *cu excepția cazului în care* reușesc să demonstreze că nu sunt răspunzători în niciun fel de evenimentele care au cauzat prejudiciul[47]. „Vinovăția", ca element, nu joacă niciun rol în contextul aplicării acestei dispoziții. În schimb, articolul 83 din acest regulament nu conține o formulare similară cu textul articolului 84 din RGPD. Acest lucru confirmă, în opinia noastră, faptul că legiuitorul Uniunii nu a avut intenția ca această dispoziție să introducă un sistem de amenzi bazat pe răspunderea obiectivă sau prezumată.

80. În al patrulea rând și poate cel mai important, considerăm că, în practică, pragul pentru o încălcare din neglijență a RGPD, în sensul articolului 83 alineatul (2) litera (b) din acest regulament, este, în orice caz, atât de scăzut încât sunt dificil de imaginat situații în care va fi imposibilă aplicarea unei amenzi pentru simplul motiv că elementul respectiv nu există. Ca atare, considerăm că simplul fapt că trebuie să se stabilească intenția sau neglijența înainte de a se putea impune o amendă în conformitate cu articolul 83 din regulamentul amintit nu pune în pericol obiectivul urmărit de legiuitorul Uniunii de a garanta aplicarea efectivă a normelor din regulament privind protecția datelor cuprinse, ci dimpotrivă.

[45] A se vedea articolul 58 alineatul (2) litera (i) și articolul 83 alineatul (2) din RGPD.

[46] În conformitate cu articolul 84 alineatul (1) din RGPD, „[s]tatele membre stabilesc normele privind alte sancțiunile aplicabile în caz de încălcare […], în special pentru încălcări care nu fac obiectul unor amenzi administrative în temeiul articolului 83, și iau toate măsurile necesare pentru a garanta faptul că acestea sunt puse în aplicare". Considerentul (152) al acestui regulament explică faptul că articolul 84 este aplicabil în cazul în care RGPD „nu armonizează sancțiunile administrative sau în alte cazuri, acolo unde este necesar, de exemplu în cazul unor încălcări grave".

[47] A se vedea în această privință Chamberlain, J., și Reichel, J., „The Relationship Between Damages and Administrative Fines in the EU General Data Protection Regulation", vol. 89, nr. 4, *Mississippi Law Journal*, 2020, p. 677-679.

81. În această privință, s-a susținut că simpla neluare a niciunei măsuri într-o situație în care operatorul sau persoana împuternicită de operator are oarecare îndoieli cu privire la legalitatea prelucrării întreprinse constituie deja o acceptare deliberată a unei posibile încălcări a RGPD și, prin urmare, o neglijență gravă [48]. În plus, Grupul de lucru „Articolul 29” a sugerat că o încălcare din neglijență echivalează, în multe privințe, cu o încălcare „neintenționată”, întrucât, în opinia sa, o astfel de încălcare poate exista acolo unde nu a existat nicio intenție de a săvârși încălcarea, iar operatorul sau persoana împuternicită de operator și-a încălcat obligația de diligență [49]. În special, aceasta a declarat că inclusiv simple „erori umane” [50] pot fi un indiciu privind neglijența.

82. Avem în vedere două concluzii. În primul rând, linia de demarcație dintre o încălcare fără vinovăție și una din neglijență este, de fapt, foarte subțire. Considerăm că autoritățile de supraveghere vor avea rareori dificultăți în a găsi suficiente elemente care să ateste că presupusa încălcare s-a produs cel puțin din neglijență. În această privință, observăm că în literatura de specialitate s-a afirmat că, „având în vedere deja numeroasele acțiuni de conștientizare […] pentru a asigura conformitatea cu RGPD […], este greu de imaginat […] existența unor încălcări ale RGPD fără a fi cel puțin în prezența unei neglijențe” [51]. Suntem întru totul de acord și reamintim că RGPD urmărește în mod specific garantarea că operatorii și persoanele împuternicite de operatori sunt conștienți de normele privind protecția datelor, ceea ce face și mai dificil, în opinia noastră, să se considere că ar putea avea loc o încălcare fără nicio formă de vinovăție (nici măcar neglijență) [52].

83. În al doilea rând, acest rezultat pare perfect coerent cu obiectivul principal al RGPD, care este acela de a garanta un nivel coerent și ridicat de protecție a persoanelor fizice în cadrul Uniunii Europene [53]. Într-adevăr, amenzile au un efect disuasiv [54]. Datorită stimulentului pe care îl creează pentru operatori și pentru persoanele împuternicite de operatori să se conformeze RGPD, acestea contribuie în general la consolidarea protecției persoanelor vizate și, în consecință, reprezintă un element-cheie în asigurarea respectării drepturilor acestora [55]. În opinia noastră, rezultă că, deși nu se poate renunța la „vinovăție”, gradul de vinovăție, impus de articolul 83 din acest regulament, care trebuie să existe este suficient de scăzut, astfel încât să se asigure un nivel adecvat de protecție a persoanelor vizate.

84. În plus, dorim să subliniem că această abordare pe care o propunem Curții spre adoptare ar confirma de asemenea alinierea sistemului de amenzi instituit prin această dispoziție cu cel prevăzut la articolul 23 alineatul (1) din Regulamentul (CE) nr. 1/2003 [56], pentru încălcările

[48] A se vedea Nemitz, P., „Fines under the GDPR”, în Leenes, R., van Brakel, R., Gutwirth, S., și De Hert, P., *Data Protection and Privacy: The Internet of Bodies*, Hart Publishing, Oxford, 2019, p. 241.

[49] În schimb, acesta a definit noțiunea de „intenție” ca incluzând atât cunoștințe, cât și premeditare în raport cu caracteristicile unei infracțiuni (a se vedea „Orientări privind aplicarea și stabilirea unor amenzi administrative în sensul [RGPD]” ale Grupului de lucru „Articolul 29” pentru protecția datelor, adoptate la 3 octombrie 2017, p. 11).

[50] *Ibidem*, p. 12. Alte circumstanțe menționate includ simpla neluare la cunoștință și nerespectare a politicilor existente, neverificarea datelor cu caracter personal în informațiile publicate, neaplicarea actualizărilor tehnice în timp util sau neadoptarea de politici.

[51] A se vedea Nemitz, P., „Fines under the GDPR”, în Leenes, R., van Brakel, R., Gutwirth, S., și De Hert, P., *Data Protection and Privacy: The Internet of Bodies*, Hart Publishing, Oxford, 2019, p. 240.

[52] A se vedea considerentele (122) și (132) ale RGPD.

[53] A se vedea în special considerentul (1) al RGPD, care reamintește, cu referire la articolul 8 alineatul (1) din cartă și la articolul 16 alineatul (1) TFUE, că protecția datelor cu caracter personal este un drept fundamental. A se vedea de asemenea considerentele (10), (11) și (13) ale RGPD și Hotărârea din 24 septembrie 2019, Google (Întinderea teritorială a dezindexării) (C-507/17, EU:C:2019:772, punctul 54).

[54] A se vedea considerentul (148) al RGPD.

[55] A se vedea Chamberlain, J., și Reichel, J., „The Relationship Between Damages and Administrative Fines in the EU General Data Protection Regulation”, vol. 89, nr. 4, *Mississippi Law Journal*, 2020, p. 685.

[56] Regulamentul Consiliului din 16 decembrie 2002 privind punerea în aplicare a normelor de concurență prevăzute la articolele [101 și 102] TFUE (JO 2003, L 1, p. 1, Ediție specială, 08/vol. 1, p. 167).

dreptului concurenței, care este de asemenea aplicabil numai dacă se stabilește intenția sau neglijența. Faptul că acest alt sistem de amenzi a inspirat formularea articolului 83 din RGPD este susținut de considerentul (150) al acestuia, care prevede că, „[î]n cazul în care amenzile administrative sunt impuse unei întreprinderi, o întreprindere ar trebui înțeleasă ca fiind o întreprindere în conformitate cu articolele 101 și 102 TFUE în aceste scopuri”, precum și de alte similitudini între aceste două sisteme de amenzi, cum este faptul că în ambele sisteme valoarea amenzilor se poate baza, în cazul întreprinderilor, pe cifra de afaceri a acestora. Remarcăm totodată că mai mulți factori dintre cei enumerați la articolul 83 alineatul (2) din RGPD reflectă factorii care sunt relevanți la stabilirea cuantumului unei amenzi pentru încălcări ale dreptului concurenței [57].

85. Odată ce am subliniat motivele pentru care considerăm că trebuie să se stabilească vinovăția înainte de a se putea impune o amendă unui operator sau unei persoane împuternicite de operator în temeiul articolului 83 alineatul (2) din RGPD, ne rămâne să spunem câteva cuvinte despre raționamentul prezentat de Consiliu și de guvernul lituanian. Potrivit acestor părți, este de competența statelor membre să decidă dacă este necesară sau nu stabilirea vinovăției înainte de a se putea impune o amendă administrativă.

86. În ceea ce ne privește, pur și simplu nu suntem de acord cu această sugestie.

b) De ce statele membre nu dispun de nicio marjă de apreciere cu privire la necesitatea existenței vinovăției

87. Este clar, în opinia noastră, că unul dintre obiectivele de bază ale RGPD și în special ale articolului 83 din acesta este acela de a atinge un nivel mai mare de *armonizare* în întreaga Uniune Europeană în ceea ce privește îndeosebi impunerea de amenzi [58]. Ca atare, considerăm, contrar celor susținute de Consiliu și de guvernul lituanian, că legiuitorul Uniunii *nu* a urmărit ca statele membre să dispună de o marjă de apreciere cu privire la necesitatea existenței sau inexistenței vinovăției.

88. Este adevărat că în legislația națională pot fi prevăzute cerințe suplimentare privind *procedura* care trebuie respectată de autoritățile de supraveghere la impunerea unei amenzi (în ceea ce privește aspecte precum notificarea amenzii și termenele pentru depunerea observațiilor, pentru formularea căii de atac, pentru punerea în aplicare și pentru a efectua plata) [59]. Acest lucru reiese clar din articolul 83 alineatul (8) din RGPD, care prevede că exercitarea de către autoritățile de supraveghere a competențelor lor de a aplica amenzi are loc „cu condiția existenței unor garanții procedurale adecvate”, care trebuie prevăzute în dreptul intern, dar cu garantarea respectării dreptului Uniunii (și în special a dreptului la o cale de atac judiciară eficientă și la un proces echitabil).

[57] A se vedea Hotărârea din 8 decembrie 2011, Chalkor/Comisia (C-386/10 P, EU:C:2011:815, punctele 56 și 57 și jurisprudența citată). În această privință, subliniem că, deși trebuie să se stabilească intenția sau neglijența înainte de a se impune o amendă pentru încălcarea normelor de drept al concurenței, această cerință este în același timp foarte redusă în practică. Într-adevăr, Curtea a statuat că această condiție este îndeplinită atunci când întreprinderea în cauză nu poate ignora caracterul anticoncurențial al comportamentului său, indiferent dacă are sau nu cunoștință de încălcarea normelor de concurență [a se vedea Hotărârea din 10 iulie 2014, Telefónica și Telefónica de España/Comisia (C-295/12 P, EU:C:2014:2062, punctul 156 și jurisprudența citată)].

[58] A se vedea de exemplu considerentul (9) al RGPD, care precizează că diferențele existente între statele membre în ceea ce privește nivelul de protecție a drepturilor și libertăților persoanelor fizice „împiedic[ă] libera circulație a datelor cu caracter personal” și „constitui[e] un obstacol în desfășurarea de activități economice la nivelul Uniunii”.

[59] A se vedea considerentul (129) [„[a]cest lucru nu ar trebui să excludă cerințe suplimentare în conformitate cu dreptul *procedural* național” (sublinierea noastră)] și considerentul (150) ale RGPD. A se vedea în această privință și „Orientările privind aplicarea și stabilirea unor amenzi administrative în sensul [RGPD]” ale Grupului de lucru „Articolul 29” pentru protecția datelor, adoptate la 3 octombrie 2017, p. 6.

89. Această putere de apreciere nu se poate extinde însă la cerințele *de fond* care se aplică pentru impunerea unei amenzi, cum ar fi gradul de vinovăție. În opinia noastră, această concluzie izvorăște în mod direct din mai multe considerente ale acestui regulament [60], care prevăd că sistemul de amenzi administrative instituit prin articolul 83 din RGPD a fost conceput de legiuitorul Uniunii pentru a produce rezultate coerente pe întreg teritoriul Uniunii Europene.

90. Din motive de exhaustivitate, adăugăm că, având în vedere că amenzile au un impact puternic asupra concurenței între întreprinderi și au repercusiuni semnificative pe piață, este esențial, în opinia noastră, ca articolul 83 din RGPD să fie aplicat în mod coerent, în caz contrar putând contribui de fapt la introducerea unor denaturări ale concurenței între întreprinderi [61].

2. Al doilea aspect: poate fi amendat un operator pentru o încălcare săvârșită într-un context în care prelucrarea ilegală nu a fost efectuată de acesta, ci de o persoană împuternicită de operator?

91. Prin intermediul celei de a doua părți a celei de a șasea întrebări, instanța de trimitere solicită să se stabilească în esență dacă un operator poate fi sancționat în conformitate cu articolul 83 din RGPD într-un context în care prelucrarea ilicită a datelor cu caracter personal *nu* a fost efectuată de operatorul însuși, ci de o persoană împuternicită de operator (*in casu*, de ITSS).

92. În opinia noastră, răspunsul la această întrebare trebuie să fie unul afirmativ.

93. În această privință, reamintim că, astfel cum am arătat la punctul 27 de mai sus, un operator nu trebuie să prelucreze el însuși vreuna din datele cu caracter personal, atât timp cât stabilește „de ce și cum” se efectuează operațiunile de prelucrare relevante. Remarcăm de asemenea că articolul 4 punctul 8 din RGPD definește „persoana împuternicită de operator” ca fiind „persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal *în numele* operatorului” [62].

94. Aceste definiții confirmă, în opinia noastră, faptul că, în contextul aplicării RGPD, un operator poate fi tras la răspundere și, în consecință, poate fi amendat în temeiul articolului 83 din acest regulament într-o situație în care datele cu caracter personal sunt prelucrate în mod ilegal, iar această prelucrare ilegală nu a fost efectuată de operatorul însuși, ci de o persoană împuternicită de operator. Această posibilitate rămâne în vigoare atât timp cât o astfel de persoană împuternicită de operator prelucrează date cu caracter personal *în numele* operatorului.

95. Acest lucru este valabil atât timp cât persoana împuternicită de operator acționează în limitele mandatului încredințat de operator și prelucrează datele în conformitate cu instrucțiunile legale primite de la operator [63]. Cu toate acestea, în cazul în care persoana împuternicită de operator depășește întinderea acestui mandat și utilizează datele primite în calitate de persoană

[60] În această privință, observăm că considerentul (10) al RGPD enunță că „nivelul protecției […] ar trebui să fie echivalent în toate statele membre”, în timp ce considerentele (11), (13) și (129) ale acestui regulament fac apel la competențe echivalente pentru monitorizarea și asigurarea conformității și la sancțiuni echivalente pentru încălcări în statele membre. La rândul său, considerentul (152) al aceluiași regulament precizează că numai în măsura în care regulamentul respectiv nu armonizează sancțiunile administrative (sau acolo unde este *necesar* în alt mod), statele membre ar trebui să pună în aplicare un sistem care să prevadă astfel de sancțiuni [a se vedea de asemenea considerentul (150) al RGPD].

[61] A se vedea în această privință Voss, W. G., și Bouthinon-Dumas, H., „EU General Data Protection Regulation Sanctions in Theory and in Practice”, vol. 37, *Santa Clara High Tech*, 2020, p. 44.

[62] Sublinierea noastră.

[63] În conformitate cu articolul 29 din RGPD, „[p]ersoana împuternicită de operator și orice persoană care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care dreptul Uniunii sau dreptul intern îl obligă să facă acest lucru”.

împuternicită de operator în scopuri proprii și este clar că părțile nu sunt „operatori asociați” în sensul articolului 4 punctul 7 și al articolului 21 alineatul (6) din RGPD, atunci operatorul nu poate, după părerea noastră, să fie amendat în temeiul articolului 83 din acest regulament, în legătură cu prelucrarea ilegală care a avut loc [64].

96. Rezultă că, într-un caz precum cel din litigiul principal, NVSC poate fi amendat în temeiul articolului 83 din RGPD, chiar dacă datele cu caracter personal au fost prelucrate în mod ilegal *numai* de ITSS, iar NVSC nu a participat la prelucrare. Există această posibilitate atât timp cât se poate considera că respectiva societate a prelucrat date cu caracter personal în numele NVSC, ceea ce nu va fi cazul dacă ITSS a acționat în afara sau contrar instrucțiunilor legale date de NVSC și a utilizat datele cu caracter personal în scopuri proprii și este clar că NVSC și ITSS nu au acționat în calitate de operatori asociați.

V. Concluzie

97. Având în vedere cele menționate anterior, propunem Curții să răspundă la întrebările preliminare adresate de Vilniaus apygardos administracinis teismas (Tribunalul Administrativ Regional din Vilnius, Lituania) după cum urmează:

1) Articolul 4 punctul 7 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)

   trebuie interpretat în sensul că o entitate care inițiază dezvoltarea unei aplicații mobile poate fi considerată „operator” în sensul acestei dispoziții numai în situația în care există suficiente elemente mai curând de natură factuală decât formală, din care instanțele naționale pot trage concluzia că o astfel de entitate a exercitat o influență reală atât asupra „scopurilor”, cât și a „mijloacelor” acestei prelucrări și că a consimțit în fapt la punerea la dispoziția publicului a aplicației mobile și, în consecință, la prelucrarea datelor cu caracter personal.

2) Această dispoziție coroborată cu articolul 26 alineatul (1) din acest regulament

   trebuie interpretată în sensul că, pentru ca doi sau mai mulți operatori să fie considerați „operatori asociați”, este necesar să fie îndeplinite două condiții: prima, fiecare operator asociat să îndeplinească în mod independent criteriile enumerate în definiția noțiunii de „operator” prevăzute la articolul 4 punctul 7 din regulamentul menționat și, a doua, influența operatorilor asupra „scopurilor și mijloacelor” prelucrării să fie exercitată în comun. În plus, lipsa oricărui acord sau chiar a oricărei coordonări între operatori nu poate în sine exclude constatarea că operatorii sunt „operatori asociați” în sensul acestor dispoziții.

3) Articolul 4 alineatul (2) din acest regulament

   trebuie interpretat în sensul că noțiunea de „prelucrare” acoperă o situație în care datele cu caracter personal sunt utilizate în cursul fazei de testare a unei aplicații mobile, cu excepția cazului în care aceste date au fost anonimizate astfel încât persoana vizată nu este sau nu mai este identificabilă. Faptul că datele cu caracter personal sunt colectate în vederea testării

[64] În conformitate cu articolul 28 alineatul (10) din RGPD, persoana împuternicită de operator este considerată a fi operator în ceea ce privește prelucrarea unor astfel de date. A se vedea în această privință și Rücker, D., și Kugler, T., *New European General Data Protection Regulation: A Practitioner's Guide*, C. H. Beck, Hart and Nomos, Oxford, 2018, p. 30.

sistemelor informatice încorporate într-o aplicație mobilă sau într-un alt scop nu are, la rândul său, nicio influență asupra chestiunii dacă operațiunea în cauză poate fi considerată a fi o „prelucrare”.

4) Articolul 83 din Regulamentul 2016/679

trebuie interpretat în sensul că o amendă poate fi aplicată numai pentru a sancționa o încălcare a normelor din regulamentul menționat care a fost săvârșită „în mod intenționat sau din neglijență”. În plus, un operator poate fi sancționat cu amendă în conformitate cu această dispoziție chiar dacă prelucrarea ilegală este efectuată de o persoană împuternicită de operator. Există această posibilitate atât timp cât se stabilește că persoana împuternicită de operator acționează în numele operatorului. Cu toate acestea, în cazul în care persoana împuternicită de operator prelucrează datele cu caracter personal în afara sau contrar instrucțiunilor legale date de operator și utilizează datele cu caracter personal primite în scopuri proprii și este clar că părțile nu sunt „operatori asociați” în sensul articolului 4 punctul 7 și al articolului 21 alineatul (6) din Regulamentul 2016/679, atunci operatorul nu poate fi amendat în conformitate cu articolul 83 din regulamentul menționat în legătură cu prelucrarea ilegală care a avut loc.