Repertoriul jurisprudenței

CONCLUZIILE AVOCATULUI GENERAL
DOMNUL PRIIT PIKAMÄE
prezentate la 16 martie 2023 [1]

Cauzele conexate C-26/22 și C-64/22

UF (C-26/22)
AB (C-64/22)
împotriva
Land Hessen,
cu participarea
SCHUFA Holding AG

[cerere de decizie preliminară formulată de Verwaltungsgericht Wiesbaden (Tribunalul Administrativ din Wiesbaden, Germania)]

„Trimitere preliminară – Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal – Regulamentul (UE) 2016/679 – Articolul 6 alineatul (1) primul paragraf litera (f) – Legalitatea prelucrării – Articolul 17 alineatul (1) litera (d) – Dreptul la ștergere în cazul prelucrării ilegale a datelor cu caracter personal – Articolul 40 – Coduri de conduită – Articolul 77 alineatul (1) – Dreptul de a depune o plângere – Articolul 78 alineatul (1) – Dreptul la o cale de atac judiciară eficientă împotriva unei autorități de supraveghere – Articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene – Decizie luată de autoritatea de supraveghere cu privire la o plângere – Întinderea controlului jurisdicțional asupra acestei decizii – Societăți private care furnizează informații comerciale – Stocare a datelor provenite dintr-un registru public – Interes legitim – Durata stocării”

I. Introducere

1. Cererile de decizie preliminară de față adresate în temeiul articolului 267 TFUE de Verwaltungsgericht Wiesbaden (Tribunalul Administrativ din Wiesbaden, Germania), au ca obiect interpretarea articolelor 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”), precum și a articolului 6 alineatul (1) primul paragraf litera (f), a articolului 17 alineatul (1) litera (d), a articolului 40, a articolului 77 alineatul (1) și a articolului 78 alineatul (1) 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) [2] (denumit în continuare „RGPD”).

[1] Limba originală: franceza.

[2] JO 2016, L 119, p. 1.

2. Aceste cereri se înscriu în cadrul a două litigii între, în primul, UF (cauza C-26/22) și, în al doilea, AB (cauza C-64/22), pe de o parte, și Land Hessen (landul Hessen, Germania), reprezentat de Hessischer Beauftragte für Datenschutz und Informationsfreiheit (Comisarul landului Hessen pentru Protecția Datelor și Libertatea de Informare, denumit în continuare „HBDI”), pe de altă parte, cu privire la cererile depuse de UF și, respectiv, de AB la HBDI în sensul de a se acționa în vederea ștergerii unei înregistrări la SCHUFA Holding AG (denumită în continuare „SCHUFA”), referitoare la o liberare de restul de datorie.

3. Cele două cauze ridică o varietate de probleme juridice inedite, referitoare printre altele la natura juridică a deciziei luate de autoritatea de supraveghere sesizată cu o plângere, precum și la întinderea controlului jurisdicțional pe care instanța îl poate exercita în cadrul unei acțiuni introduse împotriva unei astfel de decizii. Aceste cauze privesc de asemenea problema legalității stocării datelor cu caracter personal provenite din registrele publice la societățile de informații comerciale.

II. Cadrul juridic

A. Dreptul Uniunii

1. Regulamentul (UE) 2015/848

4. Potrivit articolului 79 alineatele (4) și (5) din Regulamentul (UE) 2015/848 al Parlamentului European și al Consiliului din 20 mai 2015 privind procedurile de insolvență [3]:

„(4) Statele membre răspund, în conformitate cu 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)], de colectarea și stocarea datelor în bazele de date naționale, precum și de deciziile luate cu privire la punerea acestor date la dispoziție în registrul interconectat care poate fi consultat prin intermediul portalului european e-justiție.

(5) Ca parte a informațiilor care ar trebui furnizate persoanelor vizate astfel încât să li se permită să își exercite drepturile, în special dreptul la ștergerea datelor, statele membre informează persoanele vizate în legătură cu perioada de accesibilitate stabilită pentru datele cu caracter personal stocate în registrele de insolvență.”

2. RGPD

5. Articolul 5 din GDPR prevede la alineatul (1):

„Datele cu caracter personal sunt:

[…]

(b) colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; […] («limitări legate de scop»);

[3] JO 2015, L 141, p. 19.

[…]”

6. Articolul 6 din acest regulament prevede la alineatul (1):

„Prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

[…]

(f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal […]

[…]”

7. Articolul 17 din RGPD prevede la alineatul (1):

„Persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligația de a șterge datele cu caracter personal fără întârzieri nejustificate în cazul în care se aplică unul dintre următoarele motive:

[…]

(c) persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (1) și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea sau persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (2);

(d) datele cu caracter personal au fost prelucrate ilegal;

[…]”

8. Articolul 21 din acest regulament dispune la alineatul (1):

„În orice moment, persoana vizată are dreptul de a se opune, din motive legate de situația particulară în care se află, prelucrării în temeiul articolului 6 alineatul (1) litera (e) sau (f) sau al articolului 6 alineatul (1) a datelor cu caracter personal care o privesc, inclusiv creării de profiluri pe baza respectivelor dispoziții. Operatorul nu mai prelucrează datele cu caracter personal, cu excepția cazului în care operatorul demonstrează că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanță.”

9. Articolul 40 din regulamentul menționat prevede:

„(1) Statele membre, autoritățile de supraveghere, comitetul și Comisia încurajează elaborarea de coduri de conduită menite să contribuie la buna aplicare a prezentului regulament, ținând seama de caracteristicile specifice ale diverselor sectoare de prelucrare și de nevoile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii.

(2) Asociațiile și alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot pregăti coduri de conduită sau le pot modifica sau extinde pe cele existente, în scopul de a specifica modul de aplicare a prezentului regulament, cum ar fi în ceea ce privește:

(a) prelucrarea în mod echitabil și transparent;

(b) interesele legitime urmărite de operatori în contexte specifice;

(c) colectarea datelor cu caracter personal;

[…]

(5) Asociațiile și alte organisme menționate la alineatul (2) din prezentul articol care intenționează să pregătească un cod de conduită sau să modifice sau să extindă un cod existent transmit proiectul de cod, de modificare sau de extindere autorității de supraveghere care este competentă în temeiul articolului 55. Autoritatea de supraveghere emite un aviz cu privire la conformitatea cu prezentul regulament a proiectului de cod, de modificare sau de extindere și îl aprobă în cazul în care se constată că acesta oferă garanții adecvate suficiente.

[…]”

10. Articolul 77 din RGPD prevede la alineatul (1):

„Fără a aduce atingere oricăror alte căi de atac administrative sau judiciare, orice persoană vizată are dreptul de a depune o plângere la o autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, în care se află locul său de muncă sau în care a avut loc presupusa încălcare, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încalcă prezentul regulament.”

11. Articolul 78 din acest regulament dispune:

„(1) Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană fizică sau juridică are dreptul de a exercita o cale de atac judiciară eficientă [a se citi «jurisdicțională efectivă»] împotriva unei decizii obligatorii din punct de vedere juridic a unei autorități de supraveghere care o vizează.

(2) Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care autoritatea de supraveghere care este competentă în temeiul articolelor 55 și 56 nu tratează o plângere sau nu informează persoana vizată în termen de trei luni cu privire la progresele sau la soluționarea plângerii depuse în temeiul articolului 77.

[…]”

B. Dreptul german

12. Alineatul 9 din Insolvenzordnung (Codul insolvenței), în versiunea în vigoare la data faptelor din litigiile principale, dispune la alineatul (1):

„Publicitatea oficială se realizează prin intermediul unei publicări pe internet la nivel central și al Länder; aceasta poate fi efectuată în extras. În acest scop, debitorul trebuie identificat cu precizie, în special prin indicarea adresei și a domeniului său comercial. Se consideră că publicitatea este efectivă la două zile de la data publicării."

13. Articolul 3 din Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet (Regulamentul privind publicitatea oficială difuzată pe internet în cadrul procedurilor de insolvență, denumit în continuare „InsBekV") prevede la alineatele (1) și (2):

„(1) Publicarea într-un sistem electronic de informare și de comunicare a datelor provenite dintr-o procedură de insolvență, inclusiv din procedura de deschidere, este ștearsă în termen de cel mult șase luni de la anularea procedurii de insolvență sau de la data la care închiderea acestei proceduri a rămas definitivă. În cazul nedeschiderii procedurii, termenul începe să curgă de la anularea măsurilor asigurătorii publicate.

(2) În ceea ce privește publicările din cadrul procedurii de liberare de restul de datorie, inclusiv ordonanța menționată la articolul 289 din Legea insolvenței, se aplică alineatul (1) prima teză, cu condiția ca termenul să înceapă să curgă de la data la care decizia privind liberarea de restul de datorie devine definitivă."

III. Situația de fapt care a stat la baza litigiilor, procedurile principale și întrebările preliminare

14. Lui UF și lui AB le-a fost acordată, în contextul procedurilor de insolvență care îi vizează, o liberare anticipată de restul de datorie prin deciziile judiciare pronunțate la 17 decembrie 2020 și, respectiv, la 23 martie 2021. În conformitate cu articolul 9 alineatul (1) din Legea insolvenței și cu articolul 3 alineatele (1) și (2) din InsBekV, această împrejurare a făcut obiectul unei publicări oficiale pe internet, care a fost suprimată după șase luni.

15. SCHUFA, o societate privată care furnizează informații comerciale, înregistrează în propriile baze de date informațiile publicate privind liberarea anticipată de restul de datorie, dar nu le suprimă decât după trei ani de la înregistrare.

16. Interpelată de UF și, respectiv, de AB cu solicitarea de a șterge înregistrările care îi privesc, SCHUFA le-a indicat că activitatea sa respectă RGPD și că termenul de ștergere de șase luni prevăzut la articolul 3 alineatul (1) din InsBekV nu îi este aplicabil. UF și AB au depus ulterior câte o plângere la HBDI, care este autoritatea de supraveghere competentă.

17. HBDI s-a pronunțat cu privire la aceste plângeri prin intermediul a două avize emise la 1 martie 2021 și, respectiv, la 9 iulie 2021. Potrivit acestuia, SCHUFA are dreptul de a stoca înscrisuri negative referitoare la o liberare de restul de datorie dincolo de perioada de îndestulare a unei creanțe.

18. Împotriva avizului HBDI, UF și AB au introdus fiecare o acțiune la Verwaltungsgericht Wiesbaden (Tribunalul Administrativ din Wiesbaden), instanța de trimitere. În această privință, reclamanții susțin că HBDI este obligat, în cadrul sarcinilor și al competențelor sale, să adopte împotriva SCHUFA măsuri de asigurare a ștergerii înregistrărilor care îi privesc.

19. În această privință, instanța de trimitere consideră necesar, în primul rând, să clarifice natura juridică a deciziei pe care autoritatea de supraveghere o adoptă cu privire la o plângere întemeiată pe articolul 77 alineatul (1) din RGPD. Această instanță precizează că, în opinia HBDI, dreptul prevăzut la articolul 77 alineatul (1) este conceput ca un drept de petiționare. Ca atare, acesta ar fi supus doar unui control jurisdicțional limitat, care s-ar limita la verificarea faptului că autoritatea de supraveghere a tratat plângerea și a informat reclamantul cu privire la stadiul și la soluționarea plângerii. În schimb, instanța nu ar trebui să controleze exactitatea pe fond a deciziei adoptate cu privire la plângere.

20. Cu toate acestea, instanța menționată are îndoieli în ceea ce privește conformitatea acestei analize cu RGPD. În opinia sa, articolul 78 alineatul (1) din acest regulament ar impune o cale de atac jurisdicțională efectivă. Având în vedere obiectivul regulamentului menționat, care, în contextul punerii în aplicare a articolelor 7 și 8 din cartă, constă în a asigura o protecție efectivă a drepturilor și libertăților fundamentale ale persoanelor fizice, tratamentul dreptului la plângere nu poate fi interpretat în mod restrictiv. Prin urmare, instanța de trimitere este înclinată să adopte o interpretare potrivit căreia decizia luată pe fond de autoritatea de supraveghere este supusă pe deplin controlului deplin al instanței, ținând totuși seama de faptul că această autoritate dispune atât de o putere de apreciere, cât și de o putere discreționară și că poate fi obligată să acționeze numai atunci când nu pot fi identificate opțiuni legale.

21. În al doilea rând, instanța de trimitere are îndoieli cu privire la legalitatea stocării datelor provenite din registrele publice de către societățile de informații comerciale. În această privință, instanța de trimitere precizează că aceste societăți obțin de la stat toate înregistrările provenite din registrele publice, în speță lista debitorilor și lista de insolvență. Potrivit HBDI, aceste date pot servi la aprecierea bonității și pot fi păstrate atât timp cât este necesar pentru îndeplinirea scopurilor pentru care au fost stocate. În plus, în lipsa unei reglementări din partea legiuitorului național, codurile de conduită ar fi fost adoptate de autoritățile de supraveghere, în consultare cu asociația societăților de informații comerciale, aceste coduri prevăzând ștergerea la exact trei ani de la data înregistrării în sistemul de evidență.

22. Potrivit instanței de trimitere, în lumina articolelor 7 și 8 din cartă, se pune problema dacă înregistrările în registrele publice pot fi transferate în mod identic unor registre private, fără ca datele să fie stocate cu o anumită ocazie. Acest lucru ar echivala, în cele din urmă, cu o păstrare a datelor, mai ales dacă datele au fost deja șterse din registrul național ca urmare a expirării termenului de stocare. În plus, SCHUFA nu ar fi decât o societate care furnizează printre altele informații comerciale, astfel încât datele ar fi stocate în Germania în mai multe moduri, fapt care ar implica o încălcare masivă a dreptului fundamental consacrat la articolul 7 din cartă.

23. Instanța de trimitere adaugă că prelucrarea și, prin urmare, stocarea datelor sunt autorizate numai dacă se aplică una dintre condițiile prevăzute la articolul 6 alineatul (1) din RGPD, precizându-se că în speță numai articolul 6 alineatul (1) primul paragraf litera (f) din acest regulament este relevant. Or, este îndoielnic ca un operator de date precum SCHUFA să aibă un interes legitim în sensul acestei dispoziții. În orice caz, o societate de informații comerciale ar avea mereu posibilitatea de a consulta registrele publice, în cazul în care există un interes legitim, atât timp cât datele sunt stocate în acestea.

24. În plus, legiuitorul german ar prevedea la articolul 3 din InsBekV doar o perioadă de stocare relativ scurtă, de șase luni, a înregistrării în lista de insolvență referitoare la liberarea de restul de datorie. Această reglementare s-ar întemeia, la rândul său, pe articolul 79 alineatul (5) din Regulamentul 2015/848, potrivit căruia statele membre informează persoanele vizate cu privire la perioada de accesibilitate stabilită pentru datele cu caracter personal stocate în registrele de insolvență, astfel încât să li se permită să își exercite drepturile, în special dreptul la ștergerea datelor. Totuși, acest drept nu ar mai exista în cazul stocării într-un număr mare de registre private, în care datele ar fi stocate ulterior pentru o perioadă mai lungă.

25. În fond, chiar dacă se acceptă că stocarea datelor, care provin din registrele publice, de către societățile private care furnizează informații comerciale este legală, ne-am putea întreba dacă codurile de conduită aprobate în conformitate cu articolul 40 din RGPD, care prevăd un termen de ștergere de trei ani pentru înregistrarea referitoare la liberarea de restul de datorie, trebuie luate în considerare în cadrul evaluării comparative pe care o presupune aprecierea în temeiul articolului 6 alineatul (1) primul paragraf litera (f) din RGPD.

26. În aceste condiții, Verwaltungsgericht Wiesbaden (Tribunalul Administrativ din Wiesbaden) a decis să suspende judecata și să adreseze Curții următoarele întrebări preliminare:

„1) Articolul 77 alineatul (1) coroborat cu articolul 78 alineatul (1) din [RGPD] trebuie interpretat în sensul că rezultatul autorității de supraveghere pe care aceasta îl comunică persoanei vizate

a) are caracterul unui răspuns la o petiție?

Aceasta are drept consecință faptul că controlul jurisdicțional al unei decizii privind plângerea adoptate de o autoritate de supraveghere în temeiul articolului 78 alineatul (1) din RGPD este, în principiu, limitat la problema dacă autoritatea a tratat plângerea, a investigat în mod adecvat obiectul plângerii și l-a informat pe petiționar cu privire la rezultatul examinării

sau

b) trebuie interpretat ca fiind o decizie administrativă pe fond?

Aceasta are drept consecință faptul că o decizie privind plângerea adoptată de o autoritate de supraveghere în temeiul articolului 78 alineatul (1) din RGPD trebuie analizată complet de către instanță, într-un caz individual – de exemplu în cazul reducerii la zero a puterii discreționare –, autoritatea de supraveghere putând fi de asemenea obligată de instanță să adopte o măsură concretă în sensul articolului 58 din RGPD?

2) Stocarea datelor la o societate privată care furnizează informații comerciale, stocare în cadrul căreia sunt păstrate, fără un motiv concret, date cu caracter personal provenite dintr-un registru public precum «bazele de date naționale», în sensul articolului 79 alineatele (4) și (5) din [Regulamentul 2015/848], pentru a putea furniza informații în cazul unei cereri, este compatibilă cu articolele 7 și 8 din [cartă]?

3) a) Bazele de date paralele private (în special bazele de date ale unei societăți care furnizează informații comerciale), create în plus față de bazele de date ale statului și în care datele provenite din bazele de date ale statului (în speță, publicitatea referitoare la insolvență) sunt stocate mai mult timp decât este prevăzut în cadrul strict al Regulamentului 2015/848, coroborat cu dreptul național, sunt admisibile în principiu?

b) În cazul unui răspuns afirmativ la a treia întrebare litera a), dreptul de a fi uitat prevăzut la articolul 17 alineatul (1) litera (d) din RGPD implică faptul că aceste date trebuie șterse atunci când perioada de prelucrare prevăzută pentru registrul public a expirat?

4) În măsura în care articolul 6 alineatul (1) primul paragraf litera (f) din RGPD poate fi considerat drept temei juridic unic pentru stocarea datelor la societățile private de informații comerciale în ceea ce privește datele stocate și în registre publice, trebuie să se considere că există un interes legitim al unei societăți care furnizează informații comerciale atunci când această societate de informații preia datele din evidențele publice fără un motiv concret pentru ca aceste date să fie ulterior disponibile în cazul unei cereri?

5) Codurile de conduită aprobate de autoritățile de supraveghere în temeiul articolului 40 din RGPD și care prevăd termene de examinare și de ștergere care depășesc perioadele de stocare ale registrelor publice pot suspenda evaluarea comparativă prevăzută la articolul 6 alineatul (1) primul paragraf litera (f) din RGPD?”

IV. Procedura în fața Curții

27. Decizia de trimitere în cauza C-26/22 din 23 decembrie 2021 a fost primită la grefa Curții la 11 ianuarie 2022. Decizia de trimitere în cauza C-64/22 din 31 ianuarie 2022 a fost primită la grefa Curții la 2 februarie 2022.

28. Prin decizia Curții din 11 februarie 2022, aceste cauze au fost conexate în scopul desfășurării procedurii scrise și orale, precum și al pronunțării hotărârii.

29. Părțile din cauza principală, SCHUFA, guvernele german și portughez, precum și Comisia Europeană au depus observații scrise în termenul prevăzut la articolul 23 din Statutul Curții de Justiție a Uniunii Europene.

30. În ședința din 26 ianuarie 2023, mandatarii *ad litem* ai părților din cauza principală, ai SCHUFA și agenții Comisiei au prezentat observații orale.

V. Analiză juridică

A. Observații preliminare

31. Întrucât încrederea reciprocă constituie baza oricărui angajament contractual într-o economie de piață, este, în principiu, de înțeles dintr-un punct de vedere antreprenorial că furnizorii de servicii și de bunuri doresc să își cunoască clienții, precum și riscurile inerente unui astfel de angajament contractual. Societățile care furnizează informații comerciale pot contribui la stabilirea acestei încrederi reciproce prin metode statistice care permit întreprinderilor să stabilească dacă sunt în speță îndeplinite anumite criterii relevante, inclusiv bonitatea clienților lor. Procedând astfel, ele ajută întreprinderile să se conformeze diferitelor dispoziții de drept al Uniunii care le impun o astfel de obligație în mod specific pentru anumite categorii de contracte,

în special pentru contractele de credit [4]. Totuși, aceste societăți nu sunt singurele care furnizează astfel de servicii. Recunoscând necesitatea de a asigura o anumită transparență și previzibilitate a tranzacțiilor financiare, legiuitorul Uniunii impune statelor membre să instituie și să mențină unul sau mai multe registre în care sunt publicate informații privind procedurile de insolvență.

32. Rezultă că vor exista în paralel mai multe baze de date, și anume, pe de o parte, registrele „oficiale” gestionate de autoritățile publice și, pe de altă parte, bazele de date administrate de societăți private. Acest paralelism poate conduce la o concurență între sisteme și poate chiar suscita conflicte juridice dacă regimurile juridice la care sunt supuse aceste registre diferă în mod semnificativ. Diferențele de reglementare pot deveni deosebit de problematice în cazul în care afectează protecția datelor, întrucât, indiferent de entitatea publică sau privată care gestionează registrul, aceasta trebuie să respecte interesul persoanelor vizate în privința modului în care aceste date sunt gestionate și înregistrate. Într-adevăr, întrucât informațiile referitoare la situația economică a unei persoane se caracterizează prin sensibilitatea lor în ceea ce privește respectarea dreptului la protecția datelor cu caracter personal și a vieții private, este necesară o vigilență deosebită.

33. RGPD, aplicabil de la 25 mai 2018, a creat un cadru juridic care urmărește să țină seama de interesele menționate mai sus în întreaga Uniune, printre altele prin impunerea anumitor condiții privind prelucrarea datelor cu caracter personal. Astfel, articolul 6 alineatul (1) primul paragraf litera (f) din RGPD impune ca prelucrarea să fie necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal. Cu alte cuvinte, legalitatea prelucrării trebuie să rezulte dintr-o evaluare comparativă a diferitelor interese aflate în joc, fiind necesar ca interesele legitime urmărite de operator sau de o parte terță să prevaleze. Este de competența autorității de supraveghere care, în temeiul articolului 77 alineatul (1) din RGPD, va trebui să soluționeze orice eventuală plângere din partea persoanei vizate referitoare la încălcarea drepturilor sale fundamentale să verifice dacă aceste condiții sunt îndeplinite. În sfârșit, în cazul în care persoana vizată decide să exercite o cale de atac împotriva deciziilor autorității de supraveghere, în conformitate cu articolul 78 alineatul (1) din RGPD, va reveni instanțelor naționale sarcina de a asigura un control jurisdicțional efectiv.

34. Punctele precedente din prezentele concluzii redau pe scurt diferitele aspecte juridice ridicate de instanța de trimitere în cererile sale de decizie preliminară. Prima întrebare privește natura juridică a unei decizii luate de autoritatea de supraveghere sesizată cu o plângere, precum și întinderea controlului jurisdicțional pe care instanța îl poate exercita în cadrul unei căi de atac introduse împotriva unei astfel de decizii. Întrebările a doua-a cincea privesc în esență legalitatea stocării datelor cu caracter personal provenite din registrele publice în cadrul societăților de informații comerciale. Întrebările preliminare vor fi examinate în continuare în ordinea în care au fost adresate de instanța de trimitere.

[4] Este vorba în mod concret despre articolele 18 și 21 din Directiva 2014/17/UE a Parlamentului European și a Consiliului din 4 februarie 2014 privind contractele de credit oferite consumatorilor pentru bunuri imobile rezidențiale și de modificare a Directivelor 2008/48/CE și 2013/36/UE și a Regulamentului (UE) nr. 1093/2010 (JO 2014, L 60, p. 34), precum și despre articolele 8 și 9 din Directiva 2008/48/CE a Parlamentului European și a Consiliului din 23 aprilie 2008 privind contractele de credit pentru consumatori și de abrogare a Directivei 87/102/CEE a Consiliului (JO 2008, L 133, p. 66).

B. Cu privire la prima întrebare preliminară

35. Având în vedere că prima întrebare privește cele două etape ale căii de atac administrative, și anume plângerea la autoritatea de supraveghere și calea de atac jurisdicțională la o autoritate judiciară, reglementate de articolele 77 și, respectiv, 78 din RGPD, considerăm că este oportun să descriem pe scurt aceste două etape și, în acest fel, să abordăm aspectele juridice asupra cărora instanța de trimitere are îndoieli.

36. După cum am arătat în observațiile noastre introductive, RGPD urmărește să asigure protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, recunoscută ca un drept fundamental de articolul 8 alineatul (1) din cartă, precum și de articolul 16 alineatul (1) TFUE. Întrucât orice prelucrare a datelor cu caracter personal poate avea un impact asupra vieții private, trebuie menționată de asemenea protecția garantată de articolul 7 din cartă[5]. În plus, rezultă din articolul 1 alineatul (2) din RGPD coroborat cu considerentele (10), (11) și (13) ale acestui regulament că legiuitorul Uniunii încredințează această sarcină organelor, oficiilor și agențiilor Uniunii, dar și autorităților competente din statele membre, printre care se numără autoritățile de supraveghere și instanțele naționale[6].

1. Rolul autorităților de supraveghere, inclusiv obligația de a examina plângeri

37. În această privință, trebuie remarcat că articolul 8 alineatul (3) din cartă prevede că respectarea normelor privind protecția datelor cu caracter personal se supune controlului unei autorități independente. Articolul 57 alineatul (1) litera (a) din RGPD pune în aplicare această obligație derivată din dreptul primar, prevăzând că fiecare autoritate de supraveghere are sarcina de a *monitoriza și de a asigura aplicarea acestui regulament*. Tratarea plângerilor depuse de o persoană vizată face parte din responsabilitățile sale, astfel cum rezultă în mod expres din articolul 57 alineatul (1) litera (f) din RGPD.

38. Curtea a statuat că, în temeiul acestei dispoziții, „fiecare autoritate de supraveghere *este obligată*, pe teritoriul său, *să trateze plângerile* pe care orice persoană are dreptul să le depună în conformitate cu articolul 77 alineatul (1) din RGPD atunci când consideră că prelucrarea datelor cu caracter personal care o privesc constituie o încălcare a regulamentului menționat și să examineze obiectul acestora în măsura în care este necesar”[7]. În acest context, trebuie atrasă atenția asupra faptului că Curtea a subliniat obligația care revine autorității de supraveghere de a „trata o astfel de plângere *cu toată diligența necesară*” pentru a asigura respectarea dispozițiilor din RGPD. În mod similar, trebuie remarcat că în considerentul (141) al RGPD se precizează că „[i]nvestigația în urma unei plângeri ar trebui să fie *efectuată* […] *în măsura în care este necesar, în funcție de caz*” (sublinierea noastră).

39. Toate aceste elemente ne determină să credem că autoritatea de supraveghere are *o obligație imperativă de a trata plângerile* depuse de o persoană vizată cu toată diligența cerută în speță[8]. În măsura în care orice încălcare a RGPD este în principiu susceptibilă să constituie o încălcare a drepturilor fundamentale, ar fi, în opinia noastră, incompatibil cu sistemul instituit prin acest regulament să se acorde autorității de supraveghere o putere discreționară de a trata sau nu

5 A se vedea Concluziile avocatului general Szpunar prezentate în cauza Latvijas Republikas Saeima (Puncte de penalizare) (C-439/19, EU:C:2020:1054, punctul 48).

6 Hotărârea din 15 iunie 2021, Facebook Ireland și alții (C-645/19, EU:C:2021:483, punctele 44 și 45).

7 Hotărârea din 16 iulie 2020, Facebook Ireland și Schrems (C-311/18, EU:C:2020:559, punctul 109).

8 A se vedea în acest sens Kotschy, W., „Article 77. Right to lodge a complaint with a supervisory authority”, *The EU General Data Protection Regulation (GDPR)*, Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L. (editori), Oxford, 2020, p. 1 123.

plângerile. O astfel de abordare ar ignora rolul crucial pe care RGPD îl conferă autorității de supraveghere de a asigura respectarea normelor privind protecția datelor cu caracter personal și, prin urmare, ar fi contrară obiectivelor urmărite de legiuitorul Uniunii [9]. În sfârșit, nu trebuie uitat că plângerile constituie o sursă valoroasă de informații pentru autoritatea de supraveghere, care îi permit acesteia să identifice încălcările [10].

40. Această interpretare este cu atât mai convingătoare cu cât articolul 57 alineatul (1) litera (f) din RGPD impune o serie de cerințe autorității de supraveghere în contextul tratării unei astfel de plângeri, și anume obligația de a investiga într-o măsură adecvată obiectul plângerii și de a informa reclamantul cu privire la evoluția și rezultatul investigației, într-un termen rezonabil, în special dacă este necesară efectuarea unei investigații mai amănunțite sau coordonarea cu o altă autoritate de supraveghere. Acestor cerințe li se adaugă obligația, menționată la articolul 77 alineatul (2) din RGPD, de a informa reclamantul cu privire la evoluția și rezultatul plângerii, inclusiv posibilitatea de a exercita o cale de atac jurisdicțională în temeiul articolului 78 din RGPD. Toate aceste cerințe, care se încadrează în noțiunea de „bună administrare” menționată la articolul 41 din cartă în ceea ce privește în mod specific activitățile instituțiilor și organelor Uniunii [11], au ca scop consolidarea procedurii privind plângerile pentru a face din aceasta *o veritabilă cale de atac administrativă*.

41. Chiar dacă autoritatea de supraveghere, în calitate de garant al respectării dispozițiilor RGPD, este obligată să trateze plângerile care îi sunt adresate, există mai multe elemente care pledează în favoarea unei interpretări în sensul că dispune de *o putere de apreciere cu ocazia examinării acestor plângeri*, precum și de *o anumită marjă de manevră în ceea ce privește alegerea mijloacelor adecvate* pentru îndeplinirea sarcinilor sale. Într-adevăr, domnul avocat general Saugmandsgaard Øe a observat că articolul 58 alineatul (1) din RGPD „atribuie […] autorităților de supraveghere competențe de investigare importante” și că autoritățile de supraveghere dispun, în temeiul articolului 58 alineatul (2) din RGPD, de „o gamă largă de mijloace […] pentru a-și îndeplini sarcina care [le]-a fost atribuită”, făcând referire în acest context la diferitele competențe corective enumerate în această dispoziție [12]. În continuare, acesta a precizat că, deși autoritatea de supraveghere competentă „este obligată să își îndeplinească pe deplin misiunea de supraveghere care i-a fost încredințată”, „alegerea celui mai eficient mijloc ține de aprecierea [sa] având în vedere toate împrejurările […] în cauză” [13]. Nu putem decât să achiesăm la această interpretare.

42. Descrierea detaliată a competenței autorităților de supraveghere de a adopta măsuri corective evidențiază faptul că legiuitorul Uniunii nu a urmărit să facă din procedura privind plângerea o procedură asemănătoare celei privind petiția. Dimpotrivă, obiectivul legislativ pare să fi fost acela de a crea un mecanism capabil să *protejeze în mod eficient drepturile și interesele persoanelor care*

[9] A se vedea în acest sens Härting, N., Flisek, C., Thiess, L., „DSGVO: Der Verwaltungsakt wird zum Normalfall – Das neue Beschwerderecht”, *Computer und Recht*, 5/2018, p. 299, care reamintesc că, în conformitate cu articolul 57 alineatul (1) litera (a) din RGPD, sarcina autorității de supraveghere este de a monitoriza și a asigura aplicarea RGPD în interesul persoanelor vizate. Potrivit autorilor, aceasta nu trebuie să rămână inactivă atunci când drepturile unui cetățean sunt încălcate printr-o prelucrare a datelor cu caracter personal. Dimpotrivă, autoritatea de supraveghere este obligată să remedieze situația și să exercite competențele de care dispune în temeiul articolului 58 alineatul (2) din RGPD.

[10] A se vedea în acest sens Hijmans, H., „Article 55. Tasks”, *The EU General Data Protection Regulation (GDPR)*, Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L. (editori), Oxford 2020, p. 934 și 936.

[11] A se vedea Concluziile noastre prezentate în cauza Parlamentul/UZ (C-894/19 P, EU:C:2021:497, punctul 68), pentru o explicație detaliată a noțiunii de „bună administrare” în dreptul administrativ al Uniunii.

[12] Concluziile avocatului general Saugmandsgaard Øe prezentate în cauza Facebook Ireland și Schrems (C-311/18, EU:C:2019:1145, punctele 146 și 147).

[13] Concluziile avocatului general Saugmandsgaard Øe prezentate în cauza Facebook Ireland și Schrems (C-311/18, EU:C:2019:1145, punctul 148).

depun plângeri. Însă, în opinia noastră, este clar că această marjă de apreciere nu ar trebui interpretată în sensul că autoritatea de supraveghere ar dispune de o putere nelimitată care o abilitează să acționeze în mod arbitrar. Din contră, autoritatea de supraveghere este obligată să exercite marja de manevră menționată în limitele pe care i le impune dreptul Uniunii. Nici din acest motiv nu poate fi exclusă posibilitatea ca autoritatea de supraveghere, în calitate de organ administrativ, să fie obligată să adopte o anumită măsură ca urmare a împrejurărilor specifice ale speței, în special în cazul în care există un risc grav de încălcare a drepturilor fundamentale ale persoanei vizate.

43. Această interpretare, care conferă autorității de supraveghere o anumită marjă de manevră în alegerea mijloacelor, se coroborează cu articolul 58 alineatul (4) din RGPD, care prevede că „[e]xercitarea competențelor conferite autorității de supraveghere în temeiul prezentului articol face obiectul unor garanții adecvate, inclusiv *căi de atac judiciare eficiente*” (sublinierea noastră), în conformitate cu articolul 47 din cartă. Articolul 78 alineatele (1) și (2) din RGPD recunoaște de altfel dreptul fiecărei persoane de a exercita o cale de atac jurisdicțională efectivă împotriva unei decizii care o vizează, obligatorie din punct de vedere juridic, a unei autorități de supraveghere sau în cazul în care autoritatea respectivă omite să trateze plângerea sa.

44. Ajungem astfel la problema *naturii juridice a deciziilor luate de autoritatea de supraveghere*, pe care instanța de trimitere a ridicat-o în cererile sale de decizie preliminară. În această privință, trebuie să se facă trimitere la considerentul (141) al RGPD, din care rezultă că „[o]rice persoană vizată ar trebui să aibă dreptul de a depune o plângere la o […] autoritate de supraveghere […], precum și dreptul la o cale de atac eficientă în conformitate cu articolul 47 din cartă, în cazul în care persoana vizată consideră că drepturile sale în temeiul prezentului regulament sunt încălcate sau în cazul în care autoritatea de supraveghere *nu reacționează la o plângere, respinge sau refuză parțial sau total o plângere sau nu acționează* atunci când o astfel de acțiune este necesară pentru asigurarea protecției drepturilor persoanei vizate” (sublinierea noastră). Acest considerent ține cont de faptul că o decizie a autorității de supraveghere poate cauza prejudicii persoanei vizate, în special în cazul în care concluzionează că plângerea este nefondată, consideră că nu există nicio încălcare a RGPD și nu ia deci măsuri pentru a remedia situația care a dat naștere plângerii. Legiuitorul Uniunii recunoaște *efectul obligatoriu din punct de vedere juridic al unei astfel de decizii* și, în consecință, deschide autorului plângerii posibilitatea de a exercita o cale de atac la o instanță națională.

45. În mod similar, trebuie remarcat că *autoritatea de supraveghere nu are posibilitatea de a nu reacționa*, întrucât din articolul 78 alineatul (2) din RGPD rezultă că „fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care autoritatea de supraveghere care este competentă în temeiul articolelor 55 și 56 nu tratează o plângere sau nu informează persoana vizată în termen de trei luni cu privire la progresele sau la soluționarea plângerii depuse în temeiul articolului 77”. Această împrejurare face imposibil să fie asimilată procedura privind plângerea celei privind o petiție.

46. În prezenta cauză, astfel cum a arătat instanța de trimitere în deciziile sale de trimitere, autoritatea de supraveghere a adoptat decizii obligatorii din punct de vedere juridic în privința reclamanților din cauza principală. Aceasta a constatat în esență că prelucrarea de către SCHUFA a datelor cu caracter personal ale reclamanților era legală în temeiul articolului 6 alineatul (1) primul paragraf literele (b) și (f) din RGPD și, ca atare, a exclus în mod implicit recurgerea la o măsură de investigare sau la una corectivă.

2. Întinderea controlului jurisdicțional al deciziilor luate de autoritatea de supraveghere

47. Calea de atac jurisdicțională prevăzută la articolul 78 din RGPD constituie cea de a doua etapă a căii de atac administrative prevăzute de acest regulament. Trebuie subliniat în acest context că atât „plângerea” la autoritatea de supraveghere, cât și „calea de atac jurisdicțională” sunt concepute ca „drepturi” ale persoanei vizate, ceea ce este întru totul de înțeles dacă se pleacă de la ideea că articolele 77-79 din RGPD vizează *punerea în aplicare a dreptului la o cale de atac efectivă*, consacrat la articolul 47 din cartă. După cum am arătat anterior [14], o interpretare coroborată a articolului 58 alineatul (4) și a articolului 78 din RGPD, în lumina considerentului (141) al acestui regulament, permite identificarea în mod clar a acestui obiectiv [15].

48. În ceea ce privește *întinderea controlului jurisdicțional* asupra deciziilor luate de autoritatea de supraveghere, trebuie reamintit că normele naționale privind procedura administrativă se aplică în general în contextul autonomiei procedurale, sub rezerva principiilor echivalenței și efectivității [16]. Cu toate acestea, considerăm că o cale de atac poate fi „efectivă” în sensul articolului 47 din cartă și al articolului 78 alineatul (1) din RGPD numai dacă instanța națională competentă are puterea și obligația de a supune decizia pe fond a autorității de supraveghere unui *control jurisdicțional complet* pentru a verifica dacă autoritatea de supraveghere a aplicat în mod corect RGPD.

49. Astfel cum a reamintit Curtea în jurisprudența sa, „[o] reglementare care nu prevede nicio posibilitate a justițiabilului de a exercita căi legale pentru a avea acces la date cu caracter personal care îl privesc sau pentru a obține rectificarea sau ștergerea unor astfel de date nu respectă nici substanța dreptului fundamental la o protecție jurisdicțională efectivă, astfel cum este consacrat la articolul 47 din cartă. În realitate, articolul 47 primul paragraf din cartă impune ca orice persoană ale cărei drepturi și libertăți garantate de dreptul Uniunii sunt încălcate să aibă dreptul la o cale de atac efectivă în fața unei instanțe judecătorești, cu respectarea condițiilor stabilite de acest articol. În această privință, existența însăși a unui control jurisdicțional efectiv menit să asigure respectarea dispozițiilor dreptului Uniunii este inerentă existenței unui stat de drept” [17].

50. Pentru a determina întinderea controlului jurisdicțional asupra deciziilor luate de autoritatea de supraveghere, considerăm că este relevant să menționăm mai întâi considerentul (141) al RGPD, din care rezultă că „[i]nvestigația în urma unei plângeri ar trebui să fie efectuată, *sub control ju[risdicțional]*, în măsura în care este necesar, în funcție de caz” (sublinierea noastră). În al doilea rând, trebuie amintit considerentul (143) al RGPD, care precizează că „orice persoană fizică sau juridică ar trebui să aibă dreptul la o cale de atac ju[risdicțională efectivă] în fața instanței naționale competente împotriva unei decizii a unei autorități de supraveghere care produce efecte juridice privind respectiva persoană. *O astfel de decizie se referă în special la exercitarea competențelor de investigare, corective și de autorizare de către autoritatea de supraveghere sau la refuzul sau respingerea plângerilor*” (sublinierea noastră). În opinia noastră, aceste pasaje trebuie interpretate în sensul că controlul jurisdicțional care se impune a fi efectuat de instanța națională în temeiul articolului 78 din RGPD trebuie să fie complet, adică să se extindă

[14] A se vedea punctele 43 și 44 din prezentele concluzii.

[15] A se vedea Hotărârea Curții AELS din 10 decembrie 2020 în cauzele conexate E-11/19 și E-12/19, Adpublisher AG/J și K, punctul 58, în care această instanță a remarcat că articolul 58 alineatul (4) și articolul 78 din RGPD „exprimă dreptul la o cale de atac jurisdicțională efectivă”.

[16] Hotărârea din 7 septembrie 2021, Klaipėdos regiono atliekų tvarkymo centras (C-927/19, EU:C:2021:700, punctul 146).

[17] Hotărârea din 6 octombrie 2015, Schrems (C-362/14, EU:C:2015:650, punctul 95).

la toate aspectele relevante care intră sub incidența puterii de apreciere exercitate de autoritatea de supraveghere la examinarea obiectului unei plângeri, precum și sub incidența marjei discreționare a acesteia de a alege măsurile de investigare și corective.

51. Obiectivul legiuitorului Uniunii de a garanta un control jurisdicțional complet asupra oricărei decizii a unei autorități de supraveghere care produce efecte juridice față de persoana vizată care i-a adresat o plângere devine deosebit de evident dacă se ia în considerare un alt pasaj din considerentul (143) al RGPD, care menționează că „[a]cțiunile împotriva unei autorități de supraveghere ar trebui să fie aduse în fața instanțelor statului membru în care este stabilită autoritatea de supraveghere și ar trebui să se desfășoare în conformitate cu dreptul procesual al statului membru respectiv. *Respectivele instanțe ar trebui să își exercite competența judiciară deplină, care ar trebui să includă competența de a examina toate aspectele de fapt sau de drept care au relevanță pentru litigiul cu care acestea sunt sesizate*” (sublinierea noastră) [18]. Considerăm că numai un control jurisdicțional de această amploare îndeplinește cerințele articolului 47 din cartă [19].

52. În schimb, considerăm că argumentele invocate de SCHUFA și HBDI în favoarea unui control jurisdicțional limitat asupra deciziilor autorităților de supraveghere nu sunt convingătoare. În primul rând, „independența” recunoscută autorității de supraveghere în temeiul articolului 52 din RGPD, care materializează cerința prevăzută la articolul 8 alineatul (3) din cartă, este menită să protejeze această autoritate de orice ingerință nejustificată, dar nu o dispensează de obligația de a-și îndeplini sarcinile și de a-și exercita competențele în deplină conformitate cu dreptul Uniunii și de a supune deciziile sale unui control jurisdicțional efectiv, dar și orice altă autoritate națională. În al doilea rând, existența unui drept la o cale de atac jurisdicțională împotriva operatorului de date, prevăzut la articolul 79 din RGPD, nu exclude dreptul de a introduce o cale de atac împotriva unei decizii luate de autoritatea de supraveghere, în temeiul articolului 78 din RGPD. Aceste căi de atac coexistă în mod autonom, fără ca una să fie subsidiară în raport cu cealaltă, astfel încât acestea pot fi exercitate în paralel [20]. Prin urmare, nu li se poate reproșa reclamanților că au acționat în mod nelegal în apărarea drepturilor lor protejate de RGPD pentru motivul că au favorizat o anumită cale de atac. În consecință, aceste argumente trebuie respinse.

53. Având în vedere considerentele care precedă, este necesar să se răspundă la prima întrebare preliminară că articolul 78 alineatul (1) din RGPD trebuie interpretat în sensul că rezultă din această dispoziție că o decizie obligatorie din punct de vedere juridic a unei autorități de supraveghere este supusă unui control jurisdicțional complet pe fond.

C. Cu privire la întrebările preliminare a doua-a cincea

54. Întrebările preliminare a doua-a cincea privesc în esență legalitatea stocării datelor cu caracter personal provenite din registre publice la societăți care furnizează informații comerciale. Întrebările adresate de instanța de trimitere ridică o serie de probleme juridice legate de această practică, care vor trebui examinate în mod structurat. Pentru claritate, considerăm că este oportună regruparea întrebărilor în funcție de temă și abordarea lor în această ordine.

[18] A se vedea Hotărârea din 12 ianuarie 2023, Nemzeti Adatvédelmi és Információszabadság Hatóság (C-132/21, EU:C:2023:2, punctul 41).

[19] A se vedea în acest sens Kotschy, W., „Article 77. Right to lodge a complaint with a supervisory authority”, *The EU General Data Protection Regulation (GDPR)*, Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L. (editori), Oxford 2020, p. 1 127-1 130.

[20] A se vedea Concluziile avocatului general Richard de la Tour prezentate în cauza Budapesti Elektromos Művek și alții (C-132/21, EU:C:2022:661, punctul 43 și următoarele).

55. Pentru a oferi un răspuns util instanței de trimitere, care să îi permită acesteia să soluționeze cauza cu care este sesizată, Curtea va trebui să interpreteze mai multe dispoziții din RGPD care, deși nu au fost menționate în mod expres în întrebări, par totuși relevante. O astfel de abordare este posibilă având în vedere că, potrivit unei jurisprudențe constante, Curtea poate extrage din ansamblul elementelor furnizate de instanța de trimitere și mai ales din motivarea deciziei de trimitere normele și principiile de drept al Uniunii care necesită o interpretare, având în vedere obiectul litigiului principal [21].

56. Considerăm că o astfel de analiză aprofundată este cu atât mai necesară cu cât instanța de trimitere se referă uneori în întrebările sale exclusiv la articolele 7 și 8 din cartă, deși aceste dispoziții nu trebuie aplicate în mod izolat, după cum a explicat Curtea, ci trebuie luate în considerare în cadrul evaluării comparative prevăzute la articolul 6 alineatul (1) primul paragraf litera (f) din RGPD [22]. În plus, trebuie reamintit în acest context că, în măsura în care dispozițiile RGPD pun în aplicare drepturile fundamentale în cauză, interpretarea dreptului derivat reprezintă, în mod logic, punctul de plecare al oricărei exegeze, fiind necesar ca acesta să fie interpretat în lumina dreptului primar din care carta face parte integrantă [23]. Prin urmare, vom include în analiza care urmează toate dispozițiile pe care le considerăm relevante.

1. Cu privire la conformitatea practicii societăților care furnizează informații comerciale cu principiile, consacrate în RGPD, care guvernează prelucrarea datelor cu caracter personal

57. Capitolul II din RGPD, intitulat „Principii”, stabilește principiile referitoare la prelucrarea datelor cu caracter personal. Vom examina în continuare dacă practica societăților care furnizează informații comerciale de a stoca datele cu caracter personal provenite din registrele publice timp de trei ani este conformă cu principiile pe care le considerăm cele mai relevante în prezentul context, și anume principiile legalității, limitărilor legate de scop și reducerii la minimum a datelor.

58. În scopul analizei, ne vom baza pe informațiile furnizate de instanța de trimitere și de SCHUFA, subliniind totuși că revine acesteia din urmă, în calitate de operator de date, să demonstreze că principiile menționate anterior au fost respectate, în conformitate cu principiul responsabilității prevăzut la articolul 5 alineatul (2) din RGPD.

a) Cu privire la conformitatea cu principiul legalității [articolul 6 alineatul (1) primul paragraf litera (f) din RGPD]

59. Articolul 5 alineatul (1) litera (a) din RGPD impune ca datele cu caracter personal să fie prelucrate în mod legal, echitabil și transparent față de persoana vizată. În conformitate cu articolul 6 alineatul (1) din RGPD, prelucrarea datelor cu caracter personal este legală numai dacă este îndeplinită condiția referitoare la unul dintre motivele pe care acesta le enumeră. Astfel cum a statuat Curtea, este vorba despre o listă exhaustivă și limitativă de cazuri în care o astfel de prelucrare poate fi considerată legală [24]. Instanța de trimitere solicită să se stabilească în esență

[21] Hotărârea din 11 noiembrie 2020, DenizBank (C-287/19, EU:C:2020:897, punctul 59), și Hotărârea din 24 februarie 2022, Glavna direktsia „Pozharna bezopasnost i zashtita na naselenieto” (C-262/20, EU:C:2022:117, punctul 33).

[22] Hotărârea din 11 decembrie 2019, Asociația de Proprietari bloc M5A-ScaraA (C-708/18, EU:C:2019:1064, punctul 32).

[23] Hotărârea din 26 aprilie 2022, Polonia/Parlamentul și Consiliul (C-401/19, EU:C:2022:297, punctul 47).

[24] Hotărârea din 22 iunie 2021, Latvijas Republikas Saeima (Puncte de penalizare) (C-439/19, EU:C:2021:504, punctul 99), și Hotărârea din 1 august 2022, Vyriausioji tarnybinės etikos komisija (C-184/20, EU:C:2022:601, punctul 67).

dacă articolul 6 alineatul (1) primul paragraf litera (f) din GDPR permite unei societăți private care furnizează informații comerciale să stocheze date cu caracter personal provenite din registre publice pentru a pune aceste date, la cerere, la dispoziția unui client.

60. Potrivit jurisprudenței Curții [25], articolul 6 alineatul (1) primul paragraf litera (f) din RGPD prevede trei condiții cumulative pentru ca o prelucrare de date cu caracter personal să fie legală, și anume, în primul rând, urmărirea unui interes legitim de către operator sau de către terțul sau terții cărora le sunt comunicate datele, în al doilea rând, necesitatea prelucrării datelor cu caracter personal pentru realizarea interesului legitim urmărit și, în al treilea rând, condiția ca drepturile și libertățile fundamentale ale persoanei vizate de protecția datelor să nu prevaleze. Chiar dacă este de competența instanței de trimitere să aprecieze dacă aceste condiții sunt îndeplinite, revine totuși Curții sarcina să o ghideze în această apreciere prin clarificarea problemelor de drept ridicate.

1) Existența unui „interes legitim”

61. În primul rând, în ceea ce privește urmărirea unui „interes legitim”, dorim să reamintim că RGPD și jurisprudența recunosc o gamă largă de interese considerate legitime [26], precizând în același timp că, în conformitate cu articolul 13 alineatul (1) litera (d) din RGPD, operatorului îi revine sarcina de a indica interesele legitime urmărite în contextul articolului 6 alineatul (1) primul paragraf litera (f) din RGPD.

62. SCHUFA susține că prelucrarea datelor în cauză servește urmăririi unor interese legitime de o importanță deosebită. Mai exact, societățile care furnizează informații comerciale ar prelucra date necesare evaluării bonității persoanelor sau a întreprinderilor pentru a putea pune aceste informații la dispoziția partenerilor lor contractuali. Acest lucru ar proteja de asemenea interesele economice ale întreprinderilor care doresc să încheie contracte referitoare la un credit. În plus, determinarea bonității și furnizarea de informații privind bonitatea ar constitui baza creditării și a capacității de funcționare a economiei. Activitatea acestor societăți ar contribui totodată la îndeplinirea dezideratelor comerciale ale persoanelor interesate de operațiuni de creditare, întrucât informațiile ar permite o examinare rapidă și nebirocratică.

63. Considerăm că nu există în principiu niciun motiv obiectiv pentru a pune la îndoială legitimitatea interesului SCHUFA de a furniza clienților săi serviciul comercial descris mai sus și nici legitimitatea interesului clienților SCHUFA de a recurge la serviciile sale pentru evaluarea bonității potențialilor parteneri de afaceri în sensul menționat. Chiar dacă este adevărat că prestarea acestui tip de servicii are ca scop obținerea unei remunerații și constituie, prin urmare, modelul de afaceri al unei societăți private, nu este mai puțin adevărat că această împrejurare nu este în sine suficientă pentru a repune în discuție faptul că prima condiție menționată la articolul 6 alineatul (1) primul paragraf litera (f) din RGPD este îndeplinită în speță.

64. Acest lucru este cu atât mai adevărat în cazul în care obiectivul urmărit de serviciul în cauză este în esență similar celui vizat de legiuitorul Uniunii la adoptarea articolului 24 din Regulamentul 2015/848, care impune statelor membre să instituie și să mențină pe teritoriul lor unul sau mai multe registre în care sunt publicate informații privind procedurile de insolvență. După cum rezultă din considerentul (76) al acestui regulament, scopul acestor registre publice

[25] Hotărârea din 17 iunie 2021, M.I.C.M. (C-597/19, EU:C:2021:492, punctul 106).

[26] A se vedea în această privință Concluziile avocatului general Rantos prezentate în cauza Meta Platforms și alții (Condiții generale de utilizare a unei rețele sociale) (C-252/21, EU:C:2022:704, punctul 60).

este „[o] mai bun[ă] inform[are] a creditorilor și a instanțelor relevante și […] preveni[rea] deschider[ii] de proceduri paralele de insolvență”. Apreciem că serviciul oferit de SCHUFA nu are un alt scop. Întrebarea dacă paralelismul sistemelor poate conduce la conflicte juridice va fi examinată mai jos. În acest stadiu al analizei, este suficient să reținem că, având în vedere această identitate de obiective, prelucrarea datelor efectuată de SCHUFA trebuie considerată ca servind un interes legitim în sensul articolului 6 alineatul (1) primul paragraf litera (f) din RGPD.

2) „Necesitatea” prelucrării pentru realizarea interesului legitim

65. În ceea ce privește condiția privind necesitatea prelucrării datelor cu caracter personal pentru realizarea interesului legitim urmărit, potrivit jurisprudenței Curții, derogările de la principiul protecției datelor cu caracter personal și restrângerile aduse acestuia trebuie să fie operate în limitele strictului necesar [27]. Prin urmare, trebuie să existe o legătură strânsă între prelucrare și interesul urmărit, în absența unor alternative care să respecte într-o mai mare măsură protecția datelor cu caracter personal, întrucât nu este suficient ca prelucrarea să aibă o simplă utilitate pentru operator.

66. În prezenta cauză, ar trebui să se demonstreze că recuperarea datelor cu caracter personal privind insolvența provenite din registre publice și stocarea privată a acestora reprezintă singura posibilitate pentru SCHUFA de a oferi aceste informații precise clienților săi în scopuri comerciale. Nu se poate exclude faptul că SCHUFA poate să ofere serviciul comercial și să furnizeze informații privind bonitatea persoanelor utilizând alte date disponibile. Revine instanței de trimitere să verifice dacă această posibilitate ar mai permite SCHUFA să ofere în mod util acest serviciu comercial clienților săi.

67. SCHUFA consideră că prelucrarea datelor este necesară. Potrivit acesteia, în cazul în care o societate care furnizează informații comerciale ar aștepta o cerere concretă înainte de a începe să colecteze datele, ar fi imposibil să furnizeze informații în timp util. SCHUFA estimează că faptul că datele sunt (de asemenea) accesibile publicului pentru o anumită perioadă nu are nicio incidență asupra intereselor legitime ale societăților care furnizează informații comerciale și nici asupra necesității prelucrării.

68. În cazul în care stocarea datelor cu caracter personal provenite din registre publice nu ar fi necesară pentru a permite SCHUFA să ofere serviciul său comercial clienților acesteia, prelucrarea respectivă nu ar putea fi legală în temeiul articolului 6 alineatul (1) primul paragraf litera (f) din RGPD. În schimb, în cazul în care ar fi îndeplinită a doua condiție din această dispoziție, instanța de trimitere ar trebui să examineze în continuare a treia și ultima condiție cumulativă prevăzută de dispoziția menționată.

3) Evaluarea comparativă a diferitelor interese aflate în joc

69. În sfârșit, în ceea ce privește evaluarea comparativă, pe de o parte, a intereselor operatorului de date și, pe de altă parte, a intereselor sau a drepturilor și libertăților fundamentale ale persoanei vizate, potrivit jurisprudenței Curții, revine instanței de trimitere sarcina de a realiza o evaluare comparativă a intereselor aflate în joc [28]. În această privință, orientările fostului Grup de lucru

[27] A se vedea Hotărârea din 4 mai 2017, Rīgas satiksme (C-13/16, EU:C:2017:336, punctul 30), și Hotărârea din 17 iunie 2021, M. I. C. M. (C-597/19, EU:C:2021:492, punctul 110).

[28] Hotărârea din 4 mai 2017, Rīgas satiksme (C-13/16, EU:C:2017:336, punctul 31), și Hotărârea din 17 iunie 2021, M.I.C.M. (C-597/19, EU:C:2021:492, punctul 111).

„Articolul 29”, devenit „Comitetul European pentru Protecția Datelor”, ale cărui sarcini sunt prevăzute la articolul 70 din RGPD, enumeră următoarele criterii care trebuie luate în considerare la efectuarea acestei evaluări comparative: (i) evaluarea interesului legitim al operatorului de date; (ii) impactul asupra persoanelor vizate; (iii) bilanțul provizoriu și (iv) garanțiile suplimentare instituite de operatorul de date pentru a preveni orice impact nejustificat asupra persoanelor vizate [29]. În interesul unei analize detaliate și logice, propunem aplicarea acestor criterii în cauzele principale. O astfel de abordare va contribui, în plus, la o aplicare mai coerentă a RGPD, în conformitate cu obiectivele urmărite de legiuitorul Uniunii.

i) Evaluarea „interesului legitim” al operatorului de date

70. În ceea ce privește primul criteriu, trebuie constatat că interesul atât al SCHUFA, cât și al clienților săi este *de natură pur economică*. Unele societăți private stochează date cu caracter personal luate din registre publice pentru a oferi clienților lor serviciul constând în furnizarea de informații privind bonitatea persoanei vizate folosind în special aceste date. După cum am explicat anterior [30], un astfel de interes pare legitim în scopul prezentei analize.

ii) Impactul prelucrării asupra persoanelor vizate

71. În ceea ce privește al doilea criteriu, și anume impactul prelucrării asupra persoanei vizate, *termenul de ștergere* pare a fi factorul relevant. Cu cât durata de stocare a datelor în bazele de date ale unor societăți private care furnizează informații comerciale este mai lungă, cu atât efectele asupra persoanei vizate sunt mai importante. În speță, datele cu caracter personal ale reclamanților din cauzele principale au fost prelucrate în registrul public în vederea „unei mai bune informări a creditorilor și a instanțelor relevante și pentru a preveni deschiderea de proceduri paralele de insolvență”, astfel cum se prevede în considerentul (76) al Regulamentului 2015/848. Cu ocazia evaluării comparative a diferitelor interese, legiuitorul german a considerat că perioada necesară pentru publicarea datelor referitoare la o procedură de insolvență în astfel de registre publice în vederea atingerii acestui obiectiv era de șase luni. Prin urmare, stocarea datelor cu caracter personal după această perioadă de șase luni pare *a priori* a avea un impact negativ considerabil asupra persoanei vizate.

72. Rezultă din jurisprudența Curții că există alți factori care trebuie luați în considerare în cadrul analizei, și anume *modalitățile de acces la bazele de date*, precum și *facilitățile oferite pentru diseminarea datelor* cu caracter personal [31]. În termeni simpli, cu cât informațiile sunt mai ușor accesibile publicului, cu atât ingerința în drepturile fundamentale ale persoanei vizate este mai gravă. Acest lucru este valabil în special atunci când *numărul de utilizatori* care au acces la datele persoanei vizate este unul semnificativ [32]. În consecință, este evident, în opinia noastră că, chiar dacă datele sunt deja disponibile în registre publice pentru perioada menționată de șase luni, faptul că acestea sunt stocate și disponibile în paralel în bazele de date ale societăților private care furnizează informații comerciale are un impact suplimentar asupra vieții private a persoanei, care se adaugă la consecințele negative ale disponibilității acestor date în registre publice.

[29] Avizul 06/2014 privind noțiunea de interes legitim urmărit de operatorul de date în sensul articolului 7 din Directiva 95/46/CE, WP 217 din 9 aprilie 2014, titlul III.3.4 („Factori-cheie care trebuie luați în considerare la aplicarea criteriului evaluării comparative”).

[30] A se vedea punctele 61-63 din prezentele concluzii.

[31] Hotărârea din 13 mai 2014, Google Spain și Google (C-131/12, EU:C:2014:317, punctele 86 și 87), și Hotărârea din 11 decembrie 2019, Asociația de Proprietari bloc M5A-ScaraA (C-708/18, EU:C:2019:1064, punctul 57).

[32] Hotărârea din 1 august 2022, Vyriausioji tarnybinės etikos komisija (C-184/20, EU:C:2022:601, punctul 92).

73. Un factor suplimentar care trebuie luat în considerare în cadrul analizei este *natura eventual sensibilă a datelor* în cauză [33]. În general, se poate afirma că impactul asupra persoanei vizate crește în funcție de sensibilitatea datelor cu caracter personal. În această privință, trebuie remarcat că din jurisprudența Curții rezultă că datele cu caracter personal referitoare la recuperarea creanțelor sunt într-adevăr date sensibile pentru viața privată a persoanei vizate [34]. Punerea la dispoziția unui *număr în principiu nelimitat de utilizatori* a acestui tip de date trebuie considerată, așadar, o ingerință substanțială în drepturile fundamentale ale persoanei respective [35].

74. În sfârșit, este indispensabil, în opinia noastră, să se țină seama și de *factorul timp*. Într-adevăr, chiar și o prelucrare legală a datelor poate să nu mai fie conformă cu RGPD de-a lungul timpului, atunci când aceste date nu sunt sau nu mai sunt relevante ori sunt excesive în raport cu scopul pentru care au fost stocate inițial. Din această perspectivă, ne întrebăm în mod serios cum s-ar putea justifica stocarea datelor cu caracter personal pentru o perioadă de trei ani, în condițiile în care legiuitorul național consideră că o perioadă de stocare de șase luni, adică o durată mult mai scurtă, este mai mult decât suficientă pentru a ține seama de interesele comerciale ale operatorilor economici. Trebuie să remarcăm că SCHUFA nu a fost în măsură să ofere un răspuns clar și convingător la această întrebare [36], chiar dacă, potrivit articolului 5 alineatul (2) din RGPD, îi revine sarcina de a demonstra că au fost respectate principiile referitoare la prelucrarea datelor cu caracter personal [37].

iii) Bilanț provizoriu

75. O evaluare a tuturor elementelor menționate la punctele anterioare ne conduce la concluzia că consecințele negative considerabile pe care stocarea datelor le va avea asupra persoanei vizate după perioada de șase luni în cauză par să prevaleze asupra interesului comercial al societății private și al clienților săi de stocare a datelor după această perioadă. În acest context, este important de subliniat că liberarea de restul de datorie acordată este menită *să permită beneficiarului să participe din nou la viața economică* [38]. Reclamanții din cauzele principale și Comisia au atras atenția asupra acestui aspect și în ședință. Or, acest obiectiv ar fi contracarat dacă s-ar permite societăților private care furnizează informații comerciale să stocheze date cu caracter personal în bazele lor de date după ce aceste date au fost șterse din registrul public.

iv) Garanții suplimentare

76. În sfârșit, în ceea ce privește eventualele garanții suplimentare oferite de operatorul de date pentru a preveni orice impact nejustificat asupra persoanelor vizate, în decizia de trimitere sau în observațiile formulate de SCHUFA nu există indicii care să permită identificarea unor astfel de garanții.

33 Hotărârea din 11 decembrie 2019, Asociația de Proprietari bloc M5A-ScaraA (C-708/18, EU:C:2019:1064, punctul 57).

34 Hotărârea din 13 mai 2014, Google Spain și Google (C-131/12, EU:C:2014:317, punctul 98).

35 A se vedea Hotărârea din 22 noiembrie 2022, Luxembourg Business Registers (C-37/20 și C-601/20, EU:C:2022:912, punctele 39-42), în care Curtea a considerat că punerea la dispoziția publicului larg a informațiilor privind beneficiarii reali ai societăților și ai altor entități juridice constituie o încălcare a drepturilor garantate de articolele 7 și 8 din cartă. În raționamentul său, Curtea a luat în considerare natura sensibilă a datelor cu caracter personal în cauză, precum și faptul că aceste informații erau accesibile unui număr potențial nelimitat de persoane.

36 SCHUFA a făcut referire în ședință la faptul că unele persoane ar deveni din nou insolvabile, ceea ce, potrivit acestei societăți, ar justifica o perioadă de stocare de trei ani.

37 Gutowski, M., „OLG Schleswig: Eintragung erfolgter Restschuldbefreiung in Datenbanken von Auskunfteien über die Löschungsfrist für das Insolvenzbekanntmachungsportal hinaus”, *Neue Zeitschrift für Insolvenz- und Sanierungsrecht*, 18/2021, p. 799, exprimă îndoieli cu privire la utilitatea de a prevedea stocarea datelor unei persoane timp de trei ani în scopul stabilirii situației sale economice.

38 A se vedea în acest sens Heyer, H.-U., „Schein-Datenschutz”, *Zeitschrift für Verbraucher-, Privat- und Nachlassinsolvenz*, 2019, p. 46.

4) Concluzie intermediară

77. Având în vedere considerațiile precedente, considerăm că stocarea datelor de către o societate privată care furnizează informații comerciale nu poate fi legală în temeiul articolului 6 alineatul (1) primul paragraf litera (f) din RGPD din momentul în care datele cu caracter personal referitoare la o insolvență vor fi fost șterse din registrele publice.

78. În ceea ce privește perioada de șase luni în cursul căreia datele cu caracter personal sunt disponibile și în registre publice, revine instanței de trimitere sarcina de a efectua o evaluare comparativă a intereselor și a efectelor menționate anterior asupra persoanei vizate pentru a stabili dacă stocarea paralelă a acestor date de societăți private care furnizează informații comerciale este legală în temeiul articolului 6 alineatul (1) primul paragraf litera (f) din RGPD.

b) Cu privire la conformitatea cu principiile limitărilor legate de scop și reducerii la minimum a datelor [articolul 5 alineatul (1) literele (b) și (c) din RGPD]

79. În conformitate cu principiul limitărilor legate de scop prevăzut la articolul 5 alineatul (1) litera (b) din RGPD, trebuie să se asigure faptul că datele cu caracter personal colectate în scopuri determinate nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri. În speță, datele referitoare la insolvență și la o liberare de restul de datorie au fost prelucrate de autorități publice în contextul îndeplinirii unor obligații legale.

80. Cu toate acestea, în ceea ce privește utilizarea ulterioară a datelor de către o societate privată, este necesar să se examineze, în raport cu RGPD și aplicând criteriile prevăzute la articolul 6 alineatul (4) din acest regulament, dacă scopul urmărit este compatibil cu scopul inițial. Literele (a), (b) și (d) ale acestei dispoziții sunt deosebit de relevante în speță. Acestea stabilesc următoarele criterii: (i) legătura dintre scopul inițial și scopul ulterior, (ii) contextul în care datele au fost colectate și în special relația dintre persoanele vizate și operatorul de date, precum și (iii) posibilele consecințe pentru persoana vizată ale prelucrării ulterioare preconizate.

81. În primul rând, se pare că *legătura dintre scopuri este slabă*, fie și numai pentru că scopul inițial este prevăzut de lege, mai concret de dreptul Uniunii care impune statelor membre obligația să instituie și să mențină registre [39], iar operatorul de date este o autoritate publică care acționează în cadrul sarcinilor care i-au fost încredințate prin lege, în timp ce scopul ulterior este urmărit de o entitate privată, în cadrul unei activități comerciale care constă în furnizarea de informații economice despre particulari.

82. În al doilea rând, în ceea ce privește contextul în care au fost colectate datele, trebuie constatat că *nu există nicio legătură între operatorul de date și persoana vizată*, deoarece colectarea datelor se realizează indirect, prin intermediul unor registre, iar persoana vizată nu cunoaște, prin urmare, faptul că datele sale pot fi utilizate ulterior, nici de către cine și nici în ce scop. Acest lucru ni se pare deosebit de grav din punctul de vedere al protecției datelor cu caracter personal, întrucât, în general, nimeni nu se poate în mod rezonabil aștepta ca datele sale cu caracter personal să fie prelucrate ulterior [40]. Faptul că legea prescrie o anumită perioadă pentru stocarea datelor în registrele publice este de natură să dea naștere unei așteptări rezonabile ca datele în cauză să fie șterse după expirarea acestei perioade.

[39] A se vedea punctul 31 din prezentele concluzii.

[40] A se vedea Hotărârea din 11 decembrie 2019, Asociația de Proprietari bloc M5A-ScaraA (C-708/18, EU:C:2019:1064, punctul 58).

83. În al treilea rând, în ceea ce privește posibilele consecințe pe care prelucrarea ulterioară a datelor le poate avea pentru persoanele vizate, trebuie subliniat că informațiile referitoare la procedurile de insolvență vor fi întotdeauna utilizate ca *factor negativ cu ocazia unei evaluări viitoare a bonității și a capacității de plată* a persoanei fizice vizate, ceea ce are un impact important asupra drepturilor acestei persoane. O imagine falsă a situației sale economice poate produce efecte negative asupra persoanei în cauză, complicând în mod semnificativ exercitarea libertăților sale și chiar stigmatizând-o în societate. În măsura în care persoana vizată se poate confrunta cu un refuz de a beneficia de bunuri și servicii, aceasta poate fi victima unei discriminări nejustificate.

84. Având în vedere aceste trei criterii care trebuie îndeplinite pentru ca utilizarea datelor cu caracter personal să fie conformă cu scopul inițial, astfel cum prevede articolul 6 alineatul (4) din RGPD, avem dubii că utilizarea ulterioară a acestor date poate fi conformă cu acest scop.

85. În plus, trebuie arătat că, prin stabilirea unui termen maxim de șase luni în care situația de insolvență și hotărârea judecătorească privind liberarea de restul de datorie fac obiectul unei publicări în cazul în care sunt îndeplinite condițiile legale, *legiuitorul național a luat deja în considerare realizarea interesului public* și a făcut o evaluare comparativă a interesului creditorilor, pe de o parte, și a intereselor, precum și a drepturilor persoanelor insolvabile, pe de altă parte [41]. Prelucrarea datelor cu caracter personal de către societăți private în cursul unei perioade de șase ori mai lungă decât cea prevăzută de Legea privind registrele publice *pare excesivă și penalizează* de facto *persoana vizată, deși legea nu prevede în mod clar nicio astfel de măsură*. Într-adevăr, după cum am subliniat deja, liberarea de restul de datorie acordată este menită să permită beneficiarului să participe din nou la viața economică. Or, acest obiectiv ar fi zădărnicit dacă s-ar permite unor societăți private care furnizează informații comerciale să păstreze datele cu caracter personal în bazele lor de date după ce acestea au fost șterse din registrul public [42]. În lipsa probei contrare, există temerea că condițiile de acces la baza de date ar fi putut fi concepute cu intenția de *a eluda legislația națională*, adoptată de statul membru în scopul îndeplinirii obligațiilor care îi revin în temeiul dreptului Uniunii [43].

86. De altfel, ar fi disproporționat să se „reutilizeze”, în cadrul unor evaluări viitoare, o situație trecută și deja clarificată pe plan juridic, cum este liberarea de restul de datorie, decât să se utilizeze factori actualizați la momentul analizei riscurilor pentru a asigura o evaluare mai exactă și mai obiectivă a situației economice a persoanei vizate. Într-adevăr, se poate pune sub semnul întrebării *valoarea unor informații privind situația economică a unei persoane care datează de mai mulți ani*. Unele date cu caracter personal legate de o împrejurare legată de o anumită perioadă din trecut nu vor oferi niciun fel de informații fiabile cu privire la situația economică actuală a persoanei vizate. Legiuitorul german pare să fi recunoscut această problemă și să fi desprins concluziile corecte atunci când a optat pentru o perioadă de stocare a datelor considerabil mai scurtă.

[41] Argumentul invocat de SCHUFA în ședință că legiuitorul german nu ar fi făcut nimic pentru a scurta termenul de trei ani aplicat de această societate privată, nu pare să infirme această constatare. De fapt, pot exista diverse motive pentru care un stat membru nu a abordat încă problematica legată de bazele de date paralele. Obiectul cererilor de decizie preliminară prezentate de instanța de trimitere este tocmai acela de a găsi răspunsuri la această problematică pentru a crea o situație conformă cu cerințele RGPD.

[42] A se vedea punctul 75 din prezentele concluzii.

[43] Ehmann, E., „Bundesdatenschutzgesetz”, Simitis, S., Hornung, G., Spiecker, I. (editori), Datenschutzrecht – *DSGVO mit BDSG*, ediția a opta, Baden-Baden, 2014, paragraful 29, punctul 192, consideră că nu mai există un interes legitim în diseminarea datelor cu caracter personal de o bază de date gestionată de o societate privată atunci când a expirat un termen prevăzut de legislația națională pentru publicarea acestora de către un registru public, deoarece, în caz contrar, obiectivul legislativ ar fi subminat.

87. În sfârșit, considerăm că modul în care procedează societățile care furnizează informații comerciale contravine principiului reducerii la minimum a datelor consacrat la articolul 5 alineatul (1) litera (c) din RGPD, în temeiul căruia datele cu caracter personal trebuie să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate. În această privință, se pune efectiv problema de a ști *ce sens are punerea la dispoziție a datelor cu caracter personal care sunt deja disponibile public* în registrele înființate de statele membre. O astfel de activitate este, în opinia noastră, mai degrabă susceptibilă să conducă la diseminarea de informații sensibile care nu este neapărat necesară pentru a răspunde intereselor comerciale ale operatorilor economici [44].

88. Pentru motivele menționate anterior, considerăm că stocarea acestor date de către o societate privată care furnizează informații comerciale nu constituie o practică conformă cu principiile limitărilor legate de scop și reducerii la minimum a datelor, consacrate la literele (b) și, respectiv, (c) ale articolului 5 alineatul (1) din RGPD.

c) Concluzie intermediară

89. Analiza de mai sus ne determină să concluzionăm că practica societăților care furnizează informații comerciale constând în stocarea de date cu caracter personal provenite din registre publice pentru o perioadă de trei ani nu este conformă cu principiile care guvernează prelucrarea datelor cu caracter personal consacrate în RGPD. Trebuie precizat însă că această concluzie se bazează pe o apreciere a situației de fapt care, în cele din urmă, este de competența instanței de trimitere sesizată cu soluționarea litigiului.

2. Cu privire la exercitarea dreptului la ștergerea datelor [articolul 17 alineatul (1) din RGPD]

90. Instanța de trimitere solicită de asemenea să se stabilească dacă „dreptul de a fi uitat”, consacrat la articolul 17 din RGPD, implică ștergerea datelor cu caracter personal din bazele de date ale unei societăți private care furnizează informații comerciale care există în paralel cu registrele publice și care conține aceleași date. Instanța de trimitere face o distincție între perioada în care datele cu caracter personal sunt disponibile și în registrul public și perioada în care aceste date nu mai sunt disponibile în registrul respectiv.

91. Articolul 17 alineatul (1) litera (d) din RGPD prevede *dreptul absolut* al persoanei vizate de a obține ștergerea datelor sale cu caracter personal în cazul în care acestea au fost prelucrate ilegal [45]. În consecință, în cazul în care, având în vedere concluzia la care am ajuns în cadrul analizei noastre [46], instanța de trimitere ar trebui să constate că SCHUFA nu a putut prelucra în mod legal datele cu caracter personal ale reclamanților, în temeiul articolului 6 alineatul (1) primul paragraf litera (f) din RGPD, o astfel de prelucrare ar fi ilegală în cazul în care nu ar fi aplicabil niciun alt motiv menționat la articolul 6 alineatul (1) din RGPD. Într-un astfel de caz, SCHUFA ar fi obligată să șteargă datele cu caracter personal ale reclamanților, iar aceștia din urmă ar dispune de un drept în acest sens, indiferent dacă au solicitat ștergerea datelor în perioada anterioară sau ulterioară ștergerii acestora din registrul public. Un astfel de rezultat pare de asemenea conform cu cerințele articolului 5 alineatul (1) litera (e) din RGPD, care prevede că datele cu caracter

[44] A se vedea Hotărârea din 1 august 2022, Vyriausioji tarnybinės etikos komisija (C-184/20, EU:C:2022:601, punctul 93), din care rezultă că condiția privind „necesitatea prelucrării” trebuie examinată împreună cu principiul „reducerii la minimum a datelor”.

[45] Dix, A., *Datenschutzrecht DSGVO mit BDSG*, Simitis, S., Hornung, G., Spiecker, I. (editori), Baden-Baden 2018, articolul 17, punctul 14.

[46] A se vedea punctul 77 din prezentele concluzii.

personal sunt „păstrate într-o formă care permite identificarea persoanelor vizate *pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele*” (sublinierea noastră).

92. În această privință, dorim să atragem atenția asupra articolului 79 alineatul (5) din Regulamentul 2015/848, care evidențiază importanța acordată de legiuitorul Uniunii dreptului la ștergerea datelor, în special atunci când autoritățile prelucrează date cu caracter personal de o sensibilitate deosebită, cum ar fi cele legate de solvabilitatea persoanelor vizate. Potrivit acestei dispoziții, „[c]a parte a informațiilor care ar trebui furnizate persoanelor vizate *astfel încât să li se permită să își exercite drepturile, în special dreptul la ștergerea datelor*, statele membre informează persoanele vizate în legătură cu perioada de accesibilitate stabilită pentru datele cu caracter personal stocate în registrele de insolvență” (sublinierea noastră). Legiuitorul Uniunii a recunoscut, în mod evident, necesitatea de a șterge acest tip de date atunci când stocarea lor nu se mai justifică.

93. Chiar dacă cererile de decizie preliminară privesc numai interpretarea articolului 17 alineatul (1) litera (d) din RGPD, considerăm că litera (c) a alineatului (1) se poate dovedi de asemenea relevantă pentru hotărârea ce urmează a fi pronunțată în prezentele cauze, și anume în cazul în care instanța de trimitere ar considera, contrar concluziei la care am ajuns pe baza informațiilor disponibile, că SCHUFA a putut prelucra în mod legal datele cu caracter personal ale reclamanților în conformitate cu articolul 6 alineatul (1) primul paragraf litera (f) din RGPD. Această dispoziție prevede dreptul la ștergerea datelor cu caracter personal în cazul în care persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (1) din RGPD și nu există motive legitime și imperioase care justifică prelucrarea. Această formulare implică faptul că orice „motive legitime și imperioase care justifică prelucrarea” constituie o excepție de la dreptul persoanei vizate de a se opune prelucrării și de a obține ștergerea datelor sale cu caracter personal. În consecință, se prezumă că persoana vizată dispune de dreptul de a se opune prelucrării și de dreptul la ștergerea datelor, cu excepția cazului în care există motive legitime și imperioase [47].

94. Considerăm că, pentru o protecție efectivă a datelor cu caracter personal, nu ar trebui să existe obstacole semnificative în calea exercitării dreptului la ștergerea datelor, în special atunci când pe piață există mai multe societăți care furnizează informații comerciale care stochează date în paralel cu registrul public. În cazul în care exercitarea acestui drept ar fi îngreunată în mod excesiv ca urmare a unei interpretări stricte a articolului 17 alineatul (1) din RGPD, există riscul ca protecția pe care RGPD urmărește să o ofere să fie eludată de concurenți. Or, trebuie reamintit că obiectivul legiuitorului Uniunii a fost acela ca „[*a*]*plicarea consecventă și omogenă* a normelor în materie de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal […] să fie asigurată în întreaga Uniune” (sublinierea noastră), după cum rezultă din considerentul (10) al RGPD. În consecință, persoana vizată trebuie să își poată exercita drepturile împotriva tuturor societăților care încalcă aceste norme. Având în vedere că SCHUFA este numai una dintre numeroasele societăți mari care furnizează informații comerciale în Germania, va fi necesar să se stabilească dacă stocarea datelor cu caracter personal în paralel cu registrul public constituie o practică răspândită în rândul acestor societăți.

[47] Kranenborg, H., „Article 17. Right to erasure («right to be forgotten»)”, *The EU General Data Protection Regulation (GDPR)*, Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L. (editori), Oxford, 2020 p. 481, explică faptul că articolul 21 alineatul (1) din RGPD are ca efect răsturnarea sarcinii probei, astfel încât mai curând operatorul de date, iar nu persoana vizată trebuie să demonstreze existența unor motive legitime și imperioase pentru a justifica prelucrarea. În cazul în care acest operator nu reușește să facă acest lucru, datele în cauză trebuie șterse.

95. Prin urmare, trebuie reținut în această etapă a analizei că reclamanții pot, în principiu, să se prevaleze de un drept la ștergerea datelor în temeiul articolului 17 alineatul (1) din RGPD. Rezultatul ar fi diferit numai în cazul în care o societate privată care furnizează informații comerciale a reușit să „demonstre[ze] că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate”, în sensul articolului 21 alineatul (1) din RGPD. Întrucât informațiile disponibile nu permit discernerea motivelor imperioase care ar putea apărea în litigiul principal, revine instanței de trimitere sarcina de a stabili situația de fapt și de a efectua, dacă este cazul, o evaluare comparativă a intereselor aflate în joc.

96. Având în vedere considerațiile menționate anterior, articolul 17 alineatul (1) litera (d) din RGPD trebuie interpretat în sensul că *persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate*, în cazul în care aceste date au făcut obiectul unei prelucrări ilegale potrivit articolului 6 alineatul (1) din acest regulament. Articolul 17 alineatul (1) litera (c) din regulament trebuie interpretat în sensul că persoana vizată are, în principiu, dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, în cazul în care se opune prelucrării în conformitate cu articolul 21 alineatul (1) din regulamentul menționat. Revine instanței de trimitere sarcina de a examina dacă există, în mod excepțional, motive legitime și imperioase pentru prelucrare.

3. Cu privire la utilizarea unui cod de conduită în sensul articolului 40 din RGPD pentru a prevedea termene de examinare și de ștergere care depășesc perioadele de stocare prevăzute pentru registrele publice

97. Instanța de trimitere solicită de asemenea să se stabilească dacă este conform cu dreptul Uniunii ca, într-un cod de conduită în sensul articolului 40 din RGPD, să se prevadă termene de examinare și de ștergere care depășesc perioadele de stocare prevăzute pentru registrele publice, fără a fi necesară efectuarea evaluării comparative prevăzute la articolul 6 alineatul (1) primul paragraf litera (f) din acest regulament.

98. În această privință, trebuie observat de la bun început că, potrivit instanței de trimitere, în prezent nu există nicio reglementare națională care să stabilească termene de ștergere pentru bazele de date deținute de societățile care furnizează informații comerciale. Cu toate acestea, s-ar părea că părțile interesate consideră codul de conduită adoptat în comun de autoritățile de supraveghere și de asociația ce regrupează societățile care furnizează informații comerciale ca fiind un fel de „temei juridic” de natură să legitimeze practica descrisă mai sus. Considerăm că o astfel de concepție este criticabilă în drept pentru motivele prezentate în continuare.

99. Din punct de vedere juridic, un astfel de cod de conduită nu reprezintă decât un *angajament voluntar* al celor care l-au elaborat și adoptat, și anume al asociației menționate mai sus și al membrilor săi. În mod similar, faptul că acest cod de conduită a fost aprobat de o autoritate de supraveghere înseamnă doar că aceasta din urmă, în calitate de autoritate administrativă, *se consideră obligată să respecte codul de conduită respectiv*. Cu toate acestea, este evident, în opinia noastră, că acesta nu are forță obligatorie în raport cu terții conform principiului juridic *„pacta tertiis nec nocent nec prosunt”*. În caz contrar, ar fi afectate nu doar persoanele fizice ale căror date sunt prelucrate, ci și birourile care nu au participat la elaborarea unui astfel de cod de conduită.

100. Prin definiție, un cod de conduită nu are valoare normativă în cadrul unei ordini juridice, ci urmărește mai degrabă *să specifice dispozițiile unui act normativ pentru a facilita aplicarea lui*. Această interpretare este susținută de articolul 40 alineatele (1) și (2) din RGPD, din care rezultă că codurile de conduită care urmează să fie elaborate de asociații și alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori sunt menite, pe de o parte, „să *contribuie* la buna aplicare” și, pe de altă parte, să „*specific*[*e*] modul de aplicare” a acestui regulament (sublinierea noastră). În consecință, în măsura în care funcția codului de conduită în cauză este limitată la asigurarea bunei aplicări a RGPD într-un anumit sector, acesta nu poate constitui în sine temeiul juridic care să justifice o prelucrare a datelor cu caracter personal [48].

101. Temeiul juridic care justifică o astfel de prelucrare poate fi găsit numai la articolul 6 din RGPD sau, dacă există o clauză de deschidere aplicabilă, în dreptul național. Am precizat deja în prezentele concluzii că articolul 6 din RGPD prevede o listă exhaustivă și limitativă de cazuri în care o prelucrare a datelor cu caracter personal poate fi considerată legală [49]. În consecință, normele din codul de conduită *nu ar putea avea ca efect extinderea acestei liste* fără a încălca, în același timp, dreptul Uniunii.

102. Or, considerăm că tocmai aceasta este situația atunci când, precum în speță, aceste norme impun societăților care furnizează informații comerciale obligația de a stoca datele persoanelor vizate pentru o perioadă de trei ani, adică pentru o perioadă extinsă care nu poate fi justificată în raport cu principiile care guvernează prelucrarea datelor cu caracter personal consacrate în RGPD. Mai exact, după cum am arătat în cadrul analizei noastre, stocarea acestor date nu poate fi considerată legală în temeiul articolului 6 alineatul (1) primul paragraf litera (f) din RGPD pentru perioada ulterioară ștergerii din registrele publice a datelor cu caracter personal referitoare la o insolvență [50].

103. Prin urmare, trebui reținut în acest stadiu al analizei că codurile de conduită care ar conduce la un *rezultat diferit* de cel care ar fi fost obținut în conformitate cu articolul 6 alineatul (1) primul paragraf litera (f) din RGPD nu ar putea fi luate în considerare în cadrul evaluării comparative efectuate în temeiul acestei dispoziții. În calitate de „operator[i]” în sensul articolului 4 alineatul (7) din RGPD, societățile care furnizează informații comerciale nu se pot ascunde în spatele normelor din codul de conduită elaborat chiar de ele pentru a se sustrage în mod valabil de la obligațiile care decurg în privința lor din acest regulament.

104. În lumina considerațiilor care precedă, considerăm că articolul 40 alineatele (2) și (5) din RGPD trebuie interpretat în sensul că codurile de conduită elaborate în conformitate cu aceste dispoziții și aprobate eventual de autoritatea de supraveghere nu pot stabili în mod obligatoriu din punct de vedere juridic condițiile unei prelucrări legale a datelor cu caracter personal care diferă de cele definite la articolul 6 alineatul (1) din RGPD.

[48] Trebuie atrasă atenția asupra faptului că în codul de conduită în cauză [Verhaltensregeln für die Prüf- und Löschfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien (Codul de conduită privind termenele de verificare și de ștergere a datelor cu caracter personal de către societățile private germane care furnizează informații comerciale), din 25 mai 2018] se precizează că normele sale „nu conțin *nicio reglementare privind justificarea materială a stocării* datelor cu caracter personal”. Rezultă de asemenea din acest cod de conduită că „reglementarea perioadelor de stocare și de ștergere *nu indică legalitatea stocării acestor [date]*. Următoarele perioade de ștergere și de stocare se aplică indiferent dacă datele subiacente au fost colectate și stocate *în baza unui temei legal* sau pe baza consimțământului” (sublinierea noastră). Acest lucru demonstrează, în opinia noastră, că autorii codului menționat trebuie să fi fost conștienți de faptul că codul de conduită nu constituie un temei juridic apt să legitimeze prelucrarea datelor.

[49] A se vedea punctul 59 din prezentele concluzii.

[50] A se vedea punctul 77 din prezentele concluzii.

VI. Concluzie

105. Având în vedere considerațiile menționate anterior, propunem Curții să răspundă la întrebările preliminare adresate de Verwaltungsgericht Wiesbaden (Tribunalul Administrativ din Wiesbaden, Germania) după cum urmează:

1) Articolul 78 alineatul (1) 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

   rezultă din această dispoziție că o decizie obligatorie din punct de vedere juridic a unei autorități de supraveghere este supusă unui control jurisdicțional complet pe fond.

2) Articolul 6 alineatul (1) primul paragraf litera (f) din Regulamentul 2016/679

   trebuie interpretat în sensul că

   se opune stocării de către o societate privată care furnizează informații comerciale a datelor cu caracter personal provenite dintr-un registru public precum „bazele de date naționale”, în sensul articolului 79 alineatele (4) și (5) din Regulamentul (UE) 2015/848 al Parlamentului European și al Consiliului din 20 mai 2015 privind procedurile de insolvență, pentru o perioadă mai mare decât cea în care datele sunt stocate în registrul public. Revine instanței de trimitere sarcina de a verifica dacă stocarea datelor pentru perioada autorizată pentru registrul public îndeplinește condițiile prevăzute la articolul 6 alineatul (1) primul paragraf litera (f) din Regulamentul 2016/679.

3) Articolul 17 alineatul (1) litera (d) din Regulamentul 2016/679

   trebuie interpretat în sensul că

   persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, în cazul în care aceste date au făcut obiectul unei prelucrări ilegale potrivit articolului 6 alineatul (1) din acest regulament.

   Articolul 17 alineatul (1) litera (c) din Regulamentul 2016/679

   trebuie interpretat în sensul că

   persoana vizată are, în principiu, dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, în cazul în care se opune prelucrării în conformitate cu articolul 21 alineatul (1) din regulamentul menționat. Revine instanței de trimitere sarcina de a examina dacă există, în mod excepțional, motive legitime și imperioase pentru prelucrare.

4) Articolul 40 alineatele (2) și (5) din Regulamentul 2016/679

   trebuie interpretat în sensul că

codurile de conduită elaborate în conformitate cu aceste dispoziții și aprobate eventual de autoritatea de supraveghere nu pot stabili în mod obligatoriu din punct de vedere juridic condițiile unei prelucrări legale a datelor cu caracter personal care diferă de cele definite la articolul 6 alineatul (1) din acest regulament.