

**Cauza C-61/22****Rezumatul cererii de decizie preliminară întocmit în temeiul articolului 98 alineatul (1) din Regulamentul de procedură al Curții de Justiție****Data depunerii:**

1 februarie 2022

**Instanța de trimitere:**

Verwaltungsgericht Wiesbaden (Germania)

**Data deciziei de trimitere:**

13 ianuarie 2022

**Reclamant:**

RL

**Pârâtă:**

Landeshauptstadt Wiesbaden

**Obiectul procedurii principale**

Includerea și stocarea amprentelor digitale în cărțile de identitate – Articolul 3 alineatul (5) din Regulamentul (UE) 2019/1157 – Aplicabilitate – Procedura de adoptare a regulamentului – Articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene – Articolul 35 alineatul (10) din Regulamentul general privind protecția datelor

**Obiectul și temeiul juridic al trimiterii preliminare**

Aplicabilitatea articolului 3 alineatul (5) din Regulamentul 2019/1157; articolul 267 TFUE

**Întrebarea preliminară**

Obligația privind includerea și stocarea amprentelor digitale în cărțile de identitate, în conformitate cu articolul 3 alineatul (5) din Regulamentul (UE) 2019/1157 al Parlamentului European și al Consiliului din 20 iunie 2019 privind

consolidarea securității cărților de identitate ale cetățenilor Uniunii și a documentelor de ședere eliberate cetățenilor Uniunii și membrilor de familie ai acestora care își exercită dreptul la liberă circulație (JO 2019, L 188, p. 67), încalcă dreptul Uniunii de rang superior și, în special:

- a) articolul 77 alineatul (3) TFUE;
- b) articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene;
- c) articolul 35 alineatul (10) din Regulamentul general privind protecția datelor,

și, din această cauză, este nevalidă pentru unul dintre motive?

### **Dispozițiile de drept al Uniunii invocate**

Carta drepturilor fundamentale a Uniunii Europene: articolele 7, 8 și 52;

Tratatul privind funcționarea Uniunii Europene: articolele 21, 77 și 289;

Regulamentul (UE) 2019/1157 al Parlamentului European și al Consiliului din 20 iunie 2019 privind consolidarea securității cărților de identitate ale cetățenilor Uniunii și a documentelor de ședere eliberate cetățenilor Uniunii și membrilor de familie ai acestora care își exercită dreptul la liberă circulație: considerentele (2), (17), (18), (19), (21), (22), (40), (41) și articolele 3 și 11;

Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor, denumit în continuare „RGPD”): articolele 9 și 35

### **Dispoziții naționale invocate**

Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Legea privind cărțile de identitate și dovada electronică a identității – Personalausweisgesetz, denumită în continuare „PAuswG”): articolele 5 și 9.

### **Prezentare succintă a situației de fapt și a procedurii**

- 1 Reclamantul solicită emiterea unei cărți de identitate fără includerea amprentelor digitale. Acest lucru este refuzat de pârâtă, întrucât articolul 5 alineatul (9) din PAuswG, care are la bază Regulamentul (UE) 2019/1157, prevede în mod obligatoriu includerea a două amprente digitale.

- 2 Regulamentul (UE) 2019/1157 se aplică începând de la 2 august 2021. Articolul 3 alineatul (5) din Regulamentul (UE) 2019/1157 prevede că în cărțile de identitate emise de statele membre este inclus un suport de stocare de înaltă securitate care conține o imagine facială a titularului cărții și două amprente digitale în format digital interoperabil. În dreptul german, au fost adoptate de asemenea dispoziții privind includerea amprentelor digitale în cărțile de identitate [articolul 5 alineatul (9) din PAuswG], legiuitorul german considerând – conform expunerii de motive – că amprente digitale trebuie incluse în conformitate cu articolul 3 alineatul (5) din Regulamentul (UE) 2019/1157.
- 3 La 30 noiembrie 2021, reclamantul a solicitat o nouă carte de identitate fără amprente digitale, deoarece cipul vechii sale cărți de identitate era defect. Reemiterea a fost refuzată, întrucât includerea amprentelor digitale era obligatorie de la data de 2 august 2021. În plus, reclamantul nu avea dreptul la eliberarea unui nou document de identitate, întrucât se afla deja în posesia unui document de identitate valabil. O carte de identitate era în continuare valabilă chiar cu un cip defect.
- 4 Autoritatea competentă, în temeiul dreptului german, pentru emiterea cărților de identitate acționează în calitate de autoritate de prevenire a pericolelor. Cu toate acestea, emiterea cărților de identitate și prelucrarea datelor aferentă acestora nu fac obiectul Directivei (UE) 2016/680, ci, după cum reiese din considerentul (40) al Regulamentului (UE) 2019/1157, al Regulamentului general privind protecția datelor (denumit în continuare „RGPD”). Prin urmare, în speță, primarul general al orașului (der Oberbürgermeister) nu acționează în domeniul dreptului european în materie de prevenire a pericolelor, care trebuie interpretat în mod autonom. Potrivit articolului 1 alineatul (1) și articolului 2 alineatul (1) din Directiva (UE) 2016/680, această directivă se aplică numai în cazul în care autoritățile acționează în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora. Sistemul de pașapoarte și de cărți de identitate nu face parte din această categorie.

### **Prezentare succintă a motivării trimiterii preliminare**

- 5 Decizia privind întrebarea preliminară este necesară pentru pronunțarea hotărârii. În cazul în care articolul 3 alineatul (5) din Regulamentul (UE) 2019/1157 încalcă dreptul Uniunii Europene de rang superior, reclamantul are dreptul la emiterea unei cărți de identitate fără includerea amprentelor digitale, astfel cum prevede articolul 9 alineatul (1) prima teză din PAuswG. Dispoziția națională prevăzută la articolul 5 alineatul (9) din PAuswG și-ar pierde temeiul, întrucât ar încălca dreptul Uniunii.
- 6 Chiar dacă vechea carte de identitate a reclamantului continuă să fie valabilă în pofida unui cip defect, în conformitate cu articolul 28 alineatul (3) din PAuswG, reclamantului trebuie să i se emită o nouă carte de identitate cel târziu după

expirarea perioadei de valabilitate, stabilită la 10 ani. În plus, în conformitate cu articolul 6 alineatul (2) din PAuswG, reclamantul poate solicita o nouă carte de identitate înainte de expirarea valabilității unei cărți de identitate, în cazul în care demonstrează un interes legitim în ceea ce privește reemiterea. În cazul unui cip defect, utilizarea funcției de identificare online nu mai este posibilă. De asemenea, controlul automatizat la frontieră nu mai poate fi făcut. Această posibilitate limitată de utilizare permite identificarea unui interes legitim în ceea ce privește reemiterea.

- 7 Instanța de trimitere are îndoieli cu privire la conformitatea articolului 3 alineatul (5) din Regulamentul (UE) 2019/1175 cu dreptul Uniunii. Aceste îndoieli se bazează pe adoptarea Regulamentului (UE) 2019/1157 în cadrul procedurii legislative ordinare, pe compatibilitatea articolului 3 alineatul (5) din Regulamentul (UE) 2019/1157 cu articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”) și pe lipsa unei decizii de evaluare a impactului, în sensul articolului 35 alineatul (10) din RGPD.
- 8 Convingerea instanței de trimitere este că, pentru adoptarea Regulamentului (UE) 2019/1157, ar fi trebuit să se recurgă la procedura legislativă specială prevăzută la articolul 77 TFUE.
- 9 La articolul 289 TFUE, se face distincție între procedura legislativă ordinară și procedurile legislative speciale. Regulamentul (UE) 2019/1157 s-a întemeiat pe articolul 21 alineatul (2) TFUE și a fost adoptat în conformitate cu procedura legislativă ordinară. Potrivit articolului 21 alineatul (2) TFUE, Parlamentul European și Consiliul, hotărând în conformitate cu procedura legislativă ordinară, pot adopta dispoziții pentru a facilita exercitarea dreptului la liberă circulație, în cazul în care o acțiune a Uniunii se dovedește necesară pentru atingerea acestui obiectiv, iar tratatele nu au prevăzut atribuții în acest sens.
- 10 Articolul 77 alineatul (3) prima teză TFUE conține o altă normă de competență care se referă, printre altele, la dispoziții referitoare la cărțile de identitate. În conformitate cu această normă, Consiliul, hotărând în conformitate cu o procedură legislativă specială, poate adopta dispoziții referitoare la pașapoarte, cărți de identitate, permise de ședere sau documente asimilate acestora, în cazul în care tratatele nu prevăd alte atribuții în acest sens, în cazul în care o acțiune a Uniunii este necesară pentru a facilita libera circulație a persoanelor. Consiliul hotărăște în unanimitate, după consultarea Parlamentului European. Prin această cerință a unanimității este lăsată statelor membre cea mai largă suveranitate în acest domeniu.
- 11 Articolul 77 TFUE corespunde fostului articol 62 TCE (Tratatul CE). Regulamentul (CE) nr. 2252/2004, al cărui articol 1 alineatul (2) prevede că amprentele digitale sunt stocate în pașapoarte, a fost întemeiat de legiuitor la momentul respectiv pe articolul 62 TCE. În Hotărârea sa din 17 octombrie 2013, Schwarz (C-291/12, EU:C:2013:670), Curtea de Justiție a statuat că articolul 62 alineatul (2) litera (a) TCE a constituit un temei juridic adecvat pentru adoptarea

Regulamentului (CE) nr. 2252/2004 și în special a articolului 1 alineatul (2) din acesta.

- 12 Competența prevăzută la articolul 77 alineatul (3) TFUE prevalează în raport cu articolul 21 alineatul (2) TFUE, întrucât articolul 77 alineatul (3) TFUE, fiind o dispoziție specială din punctul de vedere al conținutului, impune cerințe mai ridicate în ceea ce privește procedura legislativă, iar articolul 21 alineatul (2) TFUE este relevant numai în cazul în care tratatele nu prevăd alte atribuții pentru atingerea obiectivului de promovare a liberei circulații a persoanelor. Deși Regulamentul (UE) 2019/1157 nu se referă la dezvoltarea în continuare a acquis-ului Schengen, acesta urmărește, la fel ca Regulamentul (CE) nr. 2252/2004, apropierea elementelor de securitate și includerea identificatorilor biometrici ca un pas important către utilizarea de noi elemente în vederea evoluțiilor viitoare la nivel european. La fel ca în cazul Regulamentului (CE) nr. 2252/2004, aceasta are ca scop consolidarea securității documentelor (în speță, cărțile de identitate în locul pașapoartelor).
- 13 Având în vedere toate considerațiile anterioare, instanța de trimitere apreciază că adoptarea efectivă a Regulamentului (UE) 2019/1157 – și, prin urmare, inclusiv a articolului 3 alineatul (5) din acest regulament – ar fi necesitat procedura legislativă specială prevăzută la articolul 77 alineatul (3) TFUE.
- 14 În plus, există îndoieli în ceea ce privește compatibilitatea colectării și stocării amprentelor digitale pe cărțile de identitate cu articolele 7 și 8 din cartă.
- 15 Potrivit articolului 7 din cartă, orice persoană are dreptul la respectarea vieții private și de familie, a domiciliului și a secretului comunicațiilor. Din articolul 8 din cartă, decurge dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc.
- 16 Încă în Hotărârea din 17 octombrie 2013, Schwarz (C-291/12, EU:C:2013:670, punctele 27 și 30), Curtea de Justiție a Uniunii Europene a considerat, făcând trimitere la Hotărârea CEDO din 4 decembrie 2008, S. și Marper/Regatul Unit (*Reports of judgments and decisions 2008-V*, p. 213, articolele 68 și 84), că colectarea și stocarea amprentelor digitale în pașapoarte de către autoritățile naționale, reglementată de articolul 1 alineatul (2) din Regulamentul 2252/2004, constituie o atingere adusă drepturilor la respectarea vieții private și la protecția datelor cu caracter personal. Ampretele digitale sunt date cu caracter personal, întrucât conțin în mod obiectiv informații unice privind persoane fizice și permit identificarea precisă a acestora. Aceleași drepturi fundamentale sunt afectate și în cazul colectării și stocării amprentelor digitale pe cărțile de identitate.
- 17 Instanța are îndoieli că colectarea amprentelor digitale și, prin urmare, o atingere adusă articolelor 7 și 8 din cartă, ar fi de asemenea justificată în cazul cărților de identitate, în special având în vedere articolul 52 și articolul 8 alineatul (2) din cartă. Din cuprinsul articolului 8 alineatul (2) din cartă rezultă că datele cu

caracter personal pot fi tratate numai pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege.

- 18 În speță, instanța este convinsă – la fel precum a hotărât Curtea de Justiție în cazul pașapoartelor – că nu există un consimțământ al persoanelor care solicită o carte de identitate pentru colectarea amprentelor lor digitale. Cu toate acestea, articolul 3 alineatul (5) din Regulamentul (UE) 2019/1157 stabilește acest lucru ca reglementare legală în privința tuturor cărților de identitate.
- 19 În conformitate cu articolul 1 alineatul (1) prima teză din PAuswG, toți germanii sunt obligați să dețină o carte de identitate valabilă de îndată ce împlinesc vârsta de 16 ani și sunt supuși obligației generale de înregistrare sau, fără a fi supuși acestei obligații, au reședința în principal în Germania. Astfel, prelevarea amprentelor digitale este obligatorie pentru emiterea acestui document. Întrucât există obligația privind cartea de identitate, nu se poate considera că cei care solicită o carte de identitate și-au dat consimțământul pentru o astfel de prelucrare a datelor (a se vedea și Hotărârea Curții de Justiție din 17 octombrie 2013, Schwarz, C-291/12, EU:C:2013:670, punctul 31).
- 20 Prin urmare, în conformitate cu articolul 52 alineatul (1) din Cartă, este necesar un temei juridic *legitim*.
- 21 Este adevărat că includerea amprentelor digitale în cărțile de identitate este prevăzută de lege la articolul 3 alineatul (5) din Regulamentul (UE) 2019/1157. De asemenea, acest lucru corespunde, cel puțin în parte, obiectivelor de interes general recunoscute de Uniune, astfel cum sunt exprimate în considerentele (1), (2), (4), (18) și (46).
- 22 În cadrul Uniunii Europene, cartea de identitate poate fi utilizată în contextul trecerii frontierei. În plus, statele care nu fac parte din UE permit de asemenea intrarea cu o carte de identitate, precum în special Elveția, Islanda, Norvegia, Albania și Muntenegru. În acest context, cartea de identitate este folosită cel puțin și ca document de călătorie, astfel încât regulamentul are de asemenea rolul de a preveni intrarea ilegală pe teritoriu dinspre aceste țări. Acest lucru ar constitui un obiectiv de interes public recunoscut de Uniune (Hotărârea Curții din 17 octombrie 2013, Schwarz, C-291/12, EU:C:2013:670, punctul 38). Cu toate acestea, scopul principal al cărții de identitate nu este tocmai acela de a fi un document de călătorie în spațiul Schengen precum pașaportul. În această privință, considerentele Regulamentului (UE) 2019/1157, spre deosebire de cele ale Regulamentului (CE) nr. 2252/2004, nu se referă la spațiul Schengen ca spațiu de libertate.
- 23 Nici Regulamentul (UE) 2019/1157 nu reglementează utilizarea datelor biometrice stocate în acest sens, la articolul 11 alineatul (6) din acest regulament, fiind prevăzut că datele biometrice stocate pot fi utilizate numai cu scopul de a verifica autenticitatea sau identitatea titularului. În consecință, Regulamentul (UE) 2019/1157 nu precizează modul în care ar trebui să fie facilitată libera circulație.

În această privință, obiectivul de prevenire a intrării ilegale nu poate fi asimilat cu facilitarea libertății de circulație.

- 24 Cu toate acestea, chiar dacă dispoziția ar urmări un obiectiv de interes general, există îndoieli cu privire la proporționalitatea articolului 3 alineatul (5) din Regulamentul (UE) 2019/1157. Această dispoziție ar fi proporțională numai în cazul în care restrângerile aduse drepturilor care decurg din cartă sunt proporționale în raport cu obiectivele urmărite de Regulamentul (UE) 2019/1157 și, prin urmare, în raport cu scopul de a preveni intrarea ilegală a persoanelor pe teritoriul Uniunii și de a-l identifica în mod corect pe titularul documentului de identitate. În acest scop, mijloacele puse în aplicare de acest regulament trebuie să fie apte să realizeze aceste obiective și să nu depășească ceea ce este necesar pentru atingerea lor (Hotărârea din 17 octombrie 2013, Schwarz, C-291/12, EU:C:2013:670, punctele 38 și 40).
- 25 În acest caz, potrivit opiniei instanței, trebuie să se țină seama de împrejurarea că o carte de identitate nu poate fi *de iure* și *de facto* asimilată pașaportului, existând diferențe clare în ceea ce privește utilizarea acestor documente. Cu toate acestea, articolul 3 alineatul (5) din Regulamentul (UE) 2019/1157 tratează cele două documente în același mod în ceea ce privește amprente digitale.
- 26 Într-adevăr, cartea de identitate poate fi folosită și ca document de călătorie – astfel cum s-a arătat mai sus. Cu toate acestea, cărțile de identitate și pașapoartele diferă atât din punct de vedere juridic, cât și din punct de vedere practic. Chiar dacă cărțile de identitate sunt folosite și ca documente de călătorie în contextul liberei circulații, nu există un control de rutină, cel puțin atunci când se călătorește între statele membre ale Uniunii Europene. În plus, pentru majoritatea cetățenilor Uniunii, funcția principală a cărții naționale de identitate nu ar fi legată de libertatea de circulație. Mai precis, cărțile de identitate prezintă modalități de utilizare care merg dincolo de acest aspect. Astfel, cărțile de identitate sunt utilizate în viața de zi cu zi pentru interacțiunea cu autoritățile administrative naționale sau cu terți privați, cum ar fi băncile sau societățile aeriene. Cetățenii Uniunii care ar dori să își exercite libertatea de circulație pot face acest lucru deja cu ajutorul pașaportului lor (a se vedea în acest sens și Avizul Autorității Europene pentru Protecția Datelor privind introducerea planificată a stocării amprentelor digitale în cărțile de identitate din 10 august 2018).
- 27 În plus, în Germania există obligația de a deține o carte de identitate, în conformitate cu articolul 1 alineatul (1) prima teză din PAuswG. Spre deosebire de pașaport, cetățeanul nu poate decide singur dacă să solicite sau nu o carte de identitate. Și Autoritatea Europeană pentru Protecția Datelor consideră că includerea și stocarea amprentelor digitale au efecte importante pentru un număr de până la 370 milioane de cetățeni ai Uniunii Europene, din moment ce impune prelevarea obligatorie a amprentelor digitale pentru 85 % din populația UE. Acest domeniu de aplicare larg, precum și datele extrem de sensibile care sunt prelucrate (imagini faciale combinate cu amprente digitale) necesită o examinare aprofundată bazată pe o verificare strictă a necesității. Instanța de trimitere

urmează raționamentul Autorității Europene pentru Protecția Datelor potrivit căreia, având în vedere diferențele dintre cărțile de identitate și pașapoarte, introducerea elementelor de securitate care sunt, eventual, considerate adecvate în privința pașapoartelor nu se poate aplica automat în privința cărților de identitate, acest lucru necesitând un raționament și o analiză aprofundată. Acestea lipsesc în speță.

- 28 Prezenta instanță este de părere că, raportat la posibilitățile largi de utilizare descrise mai sus și la numărul mare de cetățeni ai Uniunii vizați, atingerea adusă are o intensitate mult mai mare decât în cazul pașapoartelor, ceea ce necesită în schimb și o justificare mai solidă.
- 29 În cadrul interpretării articolelor 7 și 8 din cartă, ar trebui să se țină seama și de scara de valori a RGPD, astfel cum reiese din considerentele (1) și (2) ale acestuia.
- 30 Datele dactiloscopice sunt tipuri speciale de date cu caracter personal în conformitate cu articolul 9 alineatul (1) din RGPD, și anume date biometrice. Acestea din urmă sunt definite la articolul 4 punctul 14 din RGPD drept date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice. În conformitate cu articolul 9 alineatul (1) din RGPD, prelucrarea acestor date biometrice este în principiu interzisă, fiind permisă numai în cazuri excepționale strict definite.
- 31 În măsura în care amprentele digitale trebuie incluse în cărțile de identitate pentru a promova securitatea împotriva falsificării, avizul Autorității Europene pentru Protecția Datelor privind introducerea planificată a stocării amprentelor digitale în cărțile de identitate subliniază că, în perioada cuprinsă între anul 2013 și anul 2017, ar fi fost detectate doar 38 870 de cărți de identitate falsificate, iar utilizarea unor cărți de identitate falsificate este în scădere de mai mulți ani.
- 32 Nu este însă suficient de clar dacă includerea amprentelor digitale este într-adevăr de natură să promoveze securitatea împotriva contrafacerii. O potrivire între datele biometrice stocate pe cipul cărții de identitate și amprentele digitale ale titularului cărții de identitate confirmă doar faptul că documentul aparține celui care îl deține. Potrivirea în sine nu constituie o dovadă a identității atât timp cât nu s-a stabilit că însăși cartea de identitate este autentică. Desigur, este recunoscut faptul că utilizarea datelor biometrice reduce probabilitatea falsificării cu succes a unui document, astfel încât includerea amprentelor digitale poate contribui, cel puțin parțial, la atingerea acestui scop.
- 33 Dacă însă această posibilitate este în măsură să justifice atingerea de mare amploare adusă pare să fie extrem de îndoielnic, cu atât mai mult cu cât, în temeiul dreptului german, și o carte de identitate cu un cip defect este în continuare valabilă, contrar Regulamentului (UE) 2019/1157. Referitor la acest aspect, Bundesamt für Sicherheit in der Informationstechnik (Oficiul Federal



pentru Securitate în domeniul Tehnologiei Informației, Germania) precizează că „o carte de identitate cu un cip nefuncțional [rămâne] valabilă chiar dacă cipul integrat este în mod evident defect. Securitatea sa ca document de identitate este dată de caracteristicile fizice de securitate”. Cu toate acestea, în cazul în care securitatea este asigurată exclusiv de elementele de securitate fizică (în special microcaractere, suprainprimare cu raze ultraviolete etc.), se pune cu atât mai clar problema necesității includerii amprentelor digitale.

- 34 De asemenea, Autoritatea Europeană pentru Protecția Datelor a subliniat că măsurile de securitate legate de tipărirea documentului, cum este de exemplu utilizarea hologramelor sau a filigranelor, ar presupune o atingere de mult mai mică intensitate. Aceste metode nu ar conține o prelucrare de date cu caracter personal, dar și ele ar permite totuși prevenirea falsificării documentelor de identitate și verificarea autenticității unui document.
- 35 În acest context, este necesar să se respecte de asemenea unul dintre cele mai importante principii ale dreptului european în materie de protecție a datelor: principiul reducerii la minimum a datelor sau de economisire a datelor. Potrivit acestui principiu, colectarea și utilizarea de date cu caracter personal trebuie să fie proporțională și necesară, precum și limitată la ceea ce este necesar pentru scopurile prelucrării.
- 36 În cazul în care este necesară prelevarea amprentelor digitale, se pune de asemenea întrebarea de ce este necesară fotocopierea întregii amprente. Desigur, acest lucru face posibilă interoperabilitatea diferitor tipuri de sisteme capabile să recunoască amprentele digitale. Aceste sisteme pot fi împărțite în trei categorii. Pe de o parte, există sisteme care stochează și compară fotocopiile complete ale amprentelor digitale. Alte sisteme utilizează așa-numitele minuții. Aceste minuții descriu un subset de caracteristici obținute din fotocopiile amprentelor digitale. A treia categorie este reprezentată de sistemele care lucrează cu modele individuale extrase din fotocopiile amprentelor digitale. Dacă ar fi stocată doar o minuție, un stat membru care lucrează cu un sistem care utilizează o fotocopie a întregii amprente digitale nu ar putea să o folosească. Stocarea întregii amprente digitale face posibilă interoperabilitatea, dar crește cantitatea de date personale stocate și, prin urmare, riscul furtului de identitate în cazul unei scurgeri de date.
- 37 Cipurile RFID utilizate în cărțile de identitate pot fi citite, în anumite împrejurări, și de scanere neautorizate. Acest lucru se datorează faptului că acestea sunt activate printr-un câmp radio și, ulterior, transmit datele în formă criptată. Astfel, securitatea procedurii depinde în cele din urmă de calitatea transmisiei și de tehnologia de criptare. Tocmai utilizarea întregii amprente digitale are ca efect creșterea riscului în acest context.
- 38 În acest proces, trebuie să se țină seama de asemenea de faptul că amprentele digitale sunt date biometrice. Prin introducerea, printre altele, a articolului 9 în RGPD, legiuitorul Uniunii a arătat că acestea fac obiectul unei protecții speciale.

- 39 Chiar Regulamentul (UE) 2019/1157 renunță la „caracteristica de securitate” a amprentei digitale pentru copiii cu vârsta sub 12 ani și exonerează complet copiii cu vârsta sub 6 ani de obligația de a o furniza, în conformitate cu articolul 3 alineatul (7) din Regulamentul (UE) 2019/1157. Mult mai important este însă faptul că, în ceea ce privește persoanele pentru care prelevarea amprentelor digitale nu este fizic posibilă, acestea sunt scutite de obligația de a le furniza. Chestiunea privind care trebui să mai fie, în acest caz, scopul acestei caracteristici de securitate rămâne nereglementată și, pur și simplu, neprecizată în Regulamentul (UE) 2019/1157.
- 40 De asemenea, Autoritatea Europeană pentru Protecția Datelor subliniază în avizul său că articolul 35 alineatul (10) din RGPD se aplică în ceea ce privește colectarea și prelucrarea amprentelor digitale. Potrivit articolului 35 alineatul (1) din RGPD, înaintea unei prelucrări susceptibile să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, trebuie să se efectueze o evaluare a impactului asupra protecției datelor. Această evaluare a impactului asupra protecției datelor ar trebui să abordeze în special o evaluare a riscurilor la adresa drepturilor și libertăților persoanelor vizate și a măsurilor de abordare a acestor riscuri, cum ar fi garanțiile și măsurile de securitate.
- 41 Întrucât temeiul juridic se bazează pe dreptul Uniunii, căruia îi este supus operatorul, și întrucât această legislație reglementează operațiunea de prelucrare specifică, evaluarea generală a impactului trebuie să fie efectuată în contextul adoptării respectivului temei juridic [articolul 35 alineatul (10) din RGPD]. Prin urmare, o astfel de evaluare a impactului ar fi trebuit să fie efectuată atunci când a fost adoptat Regulamentul (UE) 2019/1157. Conform considerentelor, acest lucru nu a fost făcut.
- 42 La fel ca Autoritatea Europeană pentru Protecția Datelor în avizul său, instanța de trimitere consideră că evaluarea impactului nu ar susține includerea obligatorie atât a imaginilor faciale, cât și a (două) amprente digitale în cărțile de identitate. Deja în cursul procedurii legislative, Autoritatea Europeană pentru Protecția Datelor a recomandat să fie reexamine în acest context necesitatea și proporționalitatea prelucrării datelor biometrice (imaginea facială în combinație cu amprentele digitale).
- 43 Legiuitorul Uniunii abordează această chestiune, în cuprinsul considerentului (40), doar în termeni foarte generali în ceea ce privește RGPD. Se rămâne la declarații vagi, cum ar fi că cetățenii UE ar trebui să fie informați cu privire la mediul de stocare și că ar trebui să se precizeze în continuare ce garanții se aplică datelor cu caracter personal prelucrate și, în special, datelor sensibile precum, de exemplu, identificatorii biometrici. Mediul de stocare ar trebui să fie de înaltă securitate și să protejeze în mod eficace datele cu caracter personal stocate în acesta împotriva accesului neautorizat. Rămâne vag ce ar trebui să se înțeleagă prin „foarte sigur” și cum ar trebui să fie concepute garanțiile și măsurile de protecție. În special, nu poate fi identificată o evaluare a impactului riscurilor existente în cazul unei scurgeri de date din cip și a încălcării articolelor 7 și 8 din cartă.

- 44 Prin urmare, se pune întrebarea dacă omisiunea unei evaluări obligatorii a impactului în ceea ce privește riscurile poate lăsa neafectată eficacitatea unei norme sau dacă, dimpotrivă, în cazul unei impuneri obligatorii de către legiuitor a efectuării unei evaluări a impactului în ceea ce privește riscurile, omisiunea sa trebuie să conducă la o invaliditate a normei. În caz contrar, legiuitorul ar fi recompensat pentru comportamentul său necorespunzător.

DOCUMENT DE LUCRU