Jurisprudența Breyer – o reafirmare nuanțata

La data de 26 aprilie 2023, Curtea de Justiție a Uniunii Europene (“CJUE” sau “Curtea”) a pronunțat o noua decizie interesanta care readuce în discuție problematica protecției juridice cu privire la datele pseudonimizate. Prin Tribunalul Camerei a opta extinse, Curtea a emis hotarârea în cauza T-557/20 care a implicat Comitetul Unic de Rezoluție, ca autoritate de rezoluție a uniunii bancare europene (“Single Resolution Board” sau “SRB”) și Autoritatea Europeana pentru Protecția Datelor (“AEPD”), disponibila *aici*.

Hotarârea stabilește criteriile privind calificarea datelor pseudonimizate ca fiind anonime, clarifica faptul ca opiniile unei persoane nu sunt considerate automat date personale, ci necesita o evaluare contextuala și indica nevoia evaluarii riscului de reidentificare din perspectiva destinatarului datelor. Curtea amintește și reafirma jurisprudența Breyer, care a influențat considerabil abordarea Curții în acest caz.

1. Context

În iunie 2017, SRB a luat decizia de a implementa o schema de rezoluție pentru Banco Popular Español, SA. Ca parte a acestui proces, SRB a primit evaluari și opinii ale diferitelor parți interesate, inclusiv cu privire la evaluarea diferenței de tratament a acționarilor și creditorilor bancii efectuata de firma de consultanța Deloitte.

Raspunsurile primite cu privire la evaluarea de tratament anterior menționata au fost transmise și catre Deloitte, care, în calitatea sa de evaluator independent, trebuia sa examineze daca evaluarea sa ramâne valabila în lumina acestor comentarii. Pentru a proteja confidențialitatea persoanelor implicate, SRB a distribuit aceste informații utilizând date pseudonimizate, înlocuind numele fiecarei persoane cu un cod alfanumeric.

Dupa mai multe plângeri primite de AEDP întemeiata pe faptul ca respondenților nu li s-a comunicat ca datele colectate prin intermediul chestionarului vor fi transferate unei terțe parți, a aparut întrebarea daca a existat o încalcare a articolului 15 (dreptul persoanei vizate de a fi informata) alineatul (1)(d) din Regulamentul (UE) 2018/1725[1]. AEPD a susținut acest lucru, considerând ca datele continua sa reprezinte date cu caracter personal daca au fost transferate doar sub forma pseudonimizata.

Astfel, potrivit AEPD, diferența dintre datele „pseudonimizate” și datele anonime consta în faptul ca, în cazul datelor anonime, nu exista „informații suplimentare” care sa poata fi utilizate pentru a atribui datele unei anumite persoane vizate, în timp ce, în cazul datelor „pseudonimizate”, exista asemenea informații suplimentare. Dupa cum se cunoaște deja, în cazul datelor anonime, nu este posibil sa se traga concluzii cu privire la identitatea persoanei în cauza, motiv pentru care acestea nu sunt supuse legislației privind protecția datelor.

2. Decizia Curții

Curtea a realizat o analiza din mai multe perspective, întarind jurisprudența sa anterioara.

Astfel, Curtea a avut în vedere faptul ca AEPD a calificat drept date cu caracter personal toate comentariile formulate de acționarii și de creditorii afectați în cadrul fazei de consultare, fara a analiza însa conținutul informațiilor transmise de SRB catre Deloitte. Astfel, Curtea a decis ca deși opiniile sau punctele de vedere personale pot constitui date personale, ele nu se prezuma în mod automat ca fiind date cu caracter personal. O asemenea concluzie trebuie sa se bazeze "*pe examinarea prin care se urmarește sa se stabileasca daca,* ***prin conținutul, prin finalitatea sau prin efectul sau, un punct de vedere este legat de o anumita persoana***", sens în care Curtea a reamintit Hotarârea din 20 decembrie 2017, Nowak (C-434/16, EU:C:2017:994).

De asemenea, CJUE a subliniat ca, pentru a determina daca datele pseudonimizate transmise constituie date personale, este esențial sa se ia în considerare **perspectiva destinatarului de date**. Astfel, Curtea a continuat prin a face referire la Hotarârea din 19 octombrie 2016, Breyer (C-582/14, EU:C:2016:779), care a statuat: "*o adresa de protocol internet dinamica înregistrata de un furnizor de servicii de comunicații electronice cu ocazia consultarii de catre o persoana a unui site internet pe care acest furnizor îl pune la dispoziția publicului constituie, pentru furnizorul respectiv, o data cu caracter personal, în cazul în care acesta dispune de mijloace legale care îi permit sa identifice persoana vizata cu ajutorul informațiilor suplimentare de care dispune furnizorul de acces la internet al acestei persoane".*

Așadar, pentru a determina daca informațiile pseudonimizate transmise unui destinatar de date constituie date personale, **este necesar sa se ia în considerare perspectiva destinatarului de date: daca acesta nu are nicio informație suplimentara care sa-i permita sa reidentifice subiecții datelor și nu are mijloace legale disponibile pentru a accesa astfel de informații, atunci datele transmise pot fi considerate anonimizate și, prin urmare, nu reprezinta date personale.**

CJUE a subliniat totodata ca era responsabilitatea AEPD sa examineze daca datele transmise catre Deloitte constituiau, în raport cu Deloitte însași, date cu caracter personal. Cu toate acestea, AEPD s-a limitat sa examineze posibilitatea de a reidentifica autorii comentariilor din punctul de vedere al SRB, iar nu al Deloitte. Faptul ca transmițatorul de date are mijloacele de a reidentifica subiecții datelor este irelevant și nu înseamna ca datele transmise sunt automat și date personale pentru destinatar.

Prin urmare, întrucât AEPD nu a cercetat daca Deloitte dispunea de mijloace legale și realizabile în practica care sa îi permita accesul la informațiile suplimentare necesare pentru reidentificarea autorilor comentariilor, AEPD nu putea concluziona ca informațiile transmise Deloitte constituiau informații privind o „*persoana fizica identificabila* " în sensul articolului 3 punctul 1 din Regulamentul 2018/1725.

Analiza detaliata a hotarârii CJUE și a jurisprudenței Breyer releva importanța evaluarii perspectivei destinatarului și a mijloacelor tehnice disponibile în procesul de determinare a calificarii datelor ca fiind personale sau anonime. Faptul ca transmițatorul datelor deține informațiile și posibilitațile necesare pentru reidentificare este irelevant pentru a stabili daca datele transferate sunt date cu caracter personal pentru destinatar. Astfel, Curtea a adaugat o dimensiune esențiala analizei calificarii datelor, luând în considerare nu numai natura în sine a datelor, ci și contextul și mijloacele tehnice de care dispune destinatarul.

3. Concluzii și dezvoltari

În practica, exista diverse situații în care se utilizeaza date pseudonimizate sub forma unor coduri alfanumerice. De exemplu, în industria medicala, o societate poate deține un set de date sensibile privind starea de sanatate a persoanelor vizate (*e.g.* numele acestora, afecțiunile medicale și istoricul tratamentelor). Pentru a proteja

confidențialitatea acestor informații în timp ce sunt transmise catre terțe organizații de cercetare științifica sau medicala, societatea poate înlocui aceste date sensibile cu coduri alfanumerice unice. Similar, bancile și instituțiile financiare pot utiliza pseudonimizarea alfanumerica atunci când transmit datele privind tranzacțiile clienților catre firme de audit externe, în scopul detectarii fraudelor.

Așadar, prin raționamentul expus în aceasta noua jurisprudența, CJUE aduce o contribuție semnificativa la evoluția practicilor de prelucrare a datelor cu caracter personal în Uniunea Europeana. Prin referirea la jurisprudența anterioara în cazul Breyer, se aduce o clarificare esențiala: autoritațile de supraveghere sunt obligate sa efectueze o evaluare particulara pentru a stabili daca datele în cauza pot fi considerate sau nu date cu caracter personal. Acest lucru deschide o adevarata cutie a Pandorei, prin faptul ca aceleași date pot fi considerate atât date cu caracter personal, cât și date fara caracter personal, în funcție de circumstanțele specifice și de capacitatea reala a fiecarei parți de a identifica persoana vizata. Prin urmare, aceasta abordare aduce cu sine o provocare susceptibila de a genera rezultate imprevizibile.

---

1. Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de catre instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE – conform articolul 15 alineatul (1) (d) "*[î]n cazul în care date cu caracter personal referitoare la o persoana vizata se colecteaza de la aceasta, operatorul, în momentul obținerii acestor date cu caracter personal, furnizeaza persoanei vizate […] informațiile [privind] destinatarii sau categoriile de destinatari ai datelor cu caracter personal, dupa caz*".