TUCA ZBARCEA
ASOCIATII

30 octombrie 2015

Buletin Legislativ

Protecția datelor

Hotărârea Curții de Justiție a Uniunii Europene în Cauza C-362/14, Schrems

În data de 6 octombrie 2015 Curtea de Justiție a Uniunii Europene a emis hotărârea în Cauza C-362/14 Schrems vs. Data Protection Commissioner[1], prin care a invalidat Decizia 2000/520/CE[2] de recunoaștere a sistemului Safe Harbor ca oferind un nivel de protecție adecvat în vederea transferului de date cu caracter personal din Uniune către Statele Unite ale Americii.

Cu titlu preliminar trebuie menționat că, potrivit articolului 25 din Directiva 95/46/CE (Directiva generală privind protecția datelor cu caracter personal), transferul datelor cu caracter personal către un stat terț nu poate avea loc decât dacă statul terț în cauză asigură un nivel de protecție adecvat, chestiune care poate fi constatată de către Comisie prin decizie. Asemenea decizii de asigurare a unui nivel de protecție adecvat au fost emise[3] până acum de Comisie pentru Andorra, Argentina, Canada, Elveția, Insulele Feroe, Guernsey, Israel, Insula Man, Jersey, Noua Zeelandă și, nu în ultimul rând, Statele Unite potrivit principiilor Safe Harbor – Decizia 2000/520/CE. Cea din urmă a fost pusă în discuție și invalidată de Curte prin decizia în Cauza C-362/14, Schrems, chestiune care afectează toate organizațiile din Uniunea Europeană care transferă date cu caracter personal către cele aproximativ 4500 de companii Statele Unite auto-certificate că respectă principiile Safe Harbor.

---

1 Textul hotărârii este disponibil la *http://goo.gl/tfzktH*.

2 Decizia Comisiei 2000/520/CE privind caracterul adecvat al protecției oferite de principiile „sferei de siguranță" privind protecția vieții private și întrebările de bază aferente, publicate de Departamentul Comerțului al S.U.A., publicată în Jurnalul Oficial nr. L215/7 din 25 august 2000, disponibilă la *http://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32000D0520&from=RO*.

3 Lista țărilor și legături către deciziile relevante ale Comisiei pot fi accesate la *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm*.

SITUAȚIA PREMISĂ

Max Schrems, un tânăr austriac, utilizator Facebook începând din 2008, a făcut în iunie 2013 o plângere la autoritatea de supraveghere din Irlanda (Data Protection Commissioner) prin care solicita un control cu privire la modul în care datele sale cu caracter personal sunt transferate de la filiala irlandeză (Facebook Ireland Ltd.) către sediul central al Facebook, în Statele Unite. El acuza faptul că în Statele Unite legea nu asigură nicio protecție reală a datelor păstrate, iar datele sunt cu ușurință accesate de către serviciile de informații, în special National Security Agency – NSA, după cum a reieșit din informațiile făcute publice de Edward Snowden în 2013.

Autoritatea de supraveghere din Irlanda a respins plângerea ca nefondată, considerând că nu era obligată să deschidă o investigație cu privire la faptele denunțate de Schrems în plângerea sa, întrucât pe de o parte nu existau dovezi că NSA ar fi avut acces la datele cu caracter personal ale persoanei interesate, iar pe de altă parte orice problemă referitoare la caracterul adecvat al protecției datelor cu caracter personal în Statele Unite trebuia să fie soluționată în conformitate cu Decizia 2000/520/CE, prin care Comisia constatase că Statele Unite ale Americii asigură un nivel de protecție adecvat.

Schrems a atacat respectiva decizie la High Court[4] care, constatând că în baza documentelor și declarațiilor de la dosar prin care „nu se contestă exactitatea unui număr semnificativ din dezvăluirile făcute de Edward Snowden" se demonstrează săvârșirea de către NSA și alte organe federale a unor „excese considerabile" față de care cetățenii Uniunii nu dispun de niciun remediu, a suspendat judecata, transmițând CJUE o serie de întrebări preliminare menite să clarifice validitatea stabilirii de către Comisie a caracterului adecvat de protecție conferit de acordul Safe Harbor. Mai exact:

„1) În cursul analizei unei plângeri adresate unui funcționar independent învestit prin lege cu funcții de administrare și de aplicare a legislației privind protecția datelor, referitoare la faptul că date cu caracter personal sunt transferate într-o țară terță (în speță, Statele Unite) ale cărei legi și practici se pretinde că nu conțin măsuri de protecție adecvate pentru persoana în cauză, acest funcționar, având în vedere articolele 7, 8 și 47 din [cartă] și fără a aduce atingere dispozițiilor articolului 25 alineatul (6) din Directiva 95/46[…], este ținut în mod absolut să respecte constatarea contrară a Uniunii cuprinsă în Decizia [2000/520]?

2) Sau, dimpotrivă, funcționarul poate și/sau trebuie să desfășoare o investigație proprie asupra problemei în lumina evoluțiilor factuale ulterioare datei la care decizia Comisiei a fost publicată pentru prima dată?"

HOTĂRÂREA

Curtea de Justiție a disociat analiza în funcție de cele două componente relevate de întrebările preliminare – pe de o parte competențele autorităților naționale de

[4] În ciuda denumirii, în Irlanda "High Court" este o instanță de prim grad.

supraveghere în cazul unei decizii de adecvare a Comisiei, iar pe de alta - validitatea Deciziei 2000/520/CE.

În ceea ce privește primul aspect, Curtea a concluzionat că o decizie prin care Comisia constată că o țară terță asigură un nivel de protecție adecvat, cum este Decizia 2000/520/CE, nu se opune ca o autoritate de supraveghere dintr-un stat membru să examineze cererea unei persoane de protecție a drepturilor și libertăților sale în ceea ce privește prelucrarea datelor cu caracter personal care o privesc, care au fost transferate dintr-un stat membru către această țară terță, atunci când această persoană invocă faptul că dreptul și practicile în vigoare în țara terță menționată nu asigură un nivel de protecție adecvat (par. 66). Totuși, a subliniat că doar Curtea este singura competentă să constate nevaliditatea unui act al Uniunii (cum este Decizia 2000/520/CE), caracterul exclusiv al acestei competențe având ca obiectiv garantarea securității juridice prin asigurarea aplicării uniforme a dreptului Uniunii (par. 61).

Sub cea de-a doua component, Curtea a analizat Decizia 2000/52/CE, cu precădere faptul că cerințele „privind securitatea națională, interesul public și respectarea legilor Statelor Unite ale Americii" prevalează asupra principiilor Safe Harbor, ceea ce înseamnă în opinia Curții că „organizațiile americane autocertificate care primesc date cu caracter personal din Uniune sunt obligate să înlăture, fără limitare, aceste principii atunci când acestea din urmă intră în conflict cu aceste cerințe și se dovedesc, așadar, incompatibile cu ele" (par 86). Mai mult, Decizia 2000/52/CE (i) „nu cuprinde nicio constatare în privința existenței în Statele Unite a unor norme cu caracter statal destinate să limiteze eventualele ingerințe în drepturile fundamentale ale persoanelor ale căror date sunt transferate din Uniune către Statele Unite" (par. 88) și nici (ii) „nu menționează existența unei protecții juridice eficiente împotriva unor ingerințe de această natură" (par. 89). Tocmai pe aceste două paliere Curtea a găsit motive de invalidare a articolului 1 al Deciziei 2000/520/CE, găsind că (i) posibilitatea autorităților publice să acceadă în mod generalizat la conținutul comunicărilor electronice „aduce atingere substanței dreptului fundamental la respectarea vieții private" reglementat de art. 7 din Carta Drepturilor Fundamentale a Uniunii Europene (par. 94), și că lipsa unei posibilități pentru justițiabil „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" încalcă dreptul fundamental la o protecție jurisdicțională efectivă, consacrat de art. 47 din aceeași Cartă (par. 95).

Curtea a invalidat de asemenea și articolul 3 din Decizia 2000/520/CE, întrucât prevede reguli derogatorii referitoare competențele autorităților naționale de supraveghere în raport cu o constatare efectuată de Comisie referitoare la nivelul de protecție adecvat (par. 100), în condițiile în care competența Comisiei potrivit Directivei 95/46/CE nu include posibilitatea de a restrânge competențele autorităților naționale de supraveghere (par. 103), ceea ce înseamnă că prin adoptarea articolului 3 din Decizie Comisia și-a depășit competența atribuită la articolul 25 alineatul (6) din Directiva 95/46/CE, interpretat în lumina Cartei (par. 104).

Ca urmare a constatării nevalidității articolelor 1 și 3 din Decizia 2000/520/CE, și constatând că restul Deciziei - articolele 2 și 4 și anexele - nu poate fi disociat de acestea, Curtea a concluzionat că întreaga Decizie 2000/520/CE este nevalidă (par. 105).

Nu a fost prevăzut niciun termen tranzitoriu pentru efectele acestei decizii, ceea ce înseamnă că nevaliditatea Deciziei 2000/520/CE și implicit ineficacitatea principiilor Safe Harbor au intervenit imediat, de la 6 octombrie 2015.

CE ÎNSEAMNĂ HOTĂRÂREA SCHREMS PENTRU OPERATORII ROMÂNI DE DATE CARE AU NOTIFICAT TRANSFERUL ÎN TEMEIUL SAFE HARBOR?

Hotărârea în discuție are implicații foarte largi atât la nivel statal cât mai ales la nivelul societăților în cadrul cărora transferul transatlantic de date joacă un rol important. Una din concluziile principale de tras este aceea că în cadrul Uniunii Europene cerințele de protecție a datelor cu caracter personal au ajuns la un nivel extrem de ridicat, iar dreptul la protecția acestor date este unul fundamental, pe care Curtea de Justiție nu va ezita să îl proclame ca atare. De altfel, această hotărâre conturează o practică constantă după celelalte hotărâri semnificative în domeniul supravegherii în masă (C-293/12 și C-594/12, Digital Rights Ireland – invalidarea Directivei 2006/24/CE privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice), activității persoanelor juridice (C-131/12, Google Spain – dreptul de a fi uitat) și a persoanelor fizice (C-212/13, Ryneš – sisteme CCTV ale persoanelor fizice).

O dificultate practică este ușor de anticipat datorită faptului că, în special ca urmare a recentei hotărâri Weltimmo, aceleași fapte ar putea fi supuse analizei (și, posibil, sancțiunilor) în mai multe state membre. Acest lucru este o problemă reală pentru societățile multinaționale, în special având în vedere opiniile divergente ale autorităților naționale de supraveghere. În plus, o asemenea abordare fragmentată diminuează extrem de mult încrederea în implementarea unui sistem „one-stop-shop" preconizat a fi reglementat în viitorul regulament general de protecție a datelor.

Realitatea de la care pleacă analiza măsurilor de implementat este aceea că, în prezent, transferul de date cu caracter personal către Statele Unite în baza Safe Harbor nu mai este legal, iar în conformitate cu punctul de vedere al Grupului de Lucru Art. 29 (organism care reunește reprezentanții autorităților de supraveghere din statele membre ale Uniunii) din 16 octombrie 2015[5], companiile au la dispoziție un timp scurt – până pe 31 ianuarie 2016, să găsească și să implementeze un temei alternativ.

[5] Disponibil la *http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf*.

Având în vedere orientarea exprimată de Autoritatea Națională pentru Supravegherea Prelucrării Datelor cu Caracter Personal[6], temeiurile alternative ce pot fi avute în vedere de societățile române ar putea fi clauzele contractuale standard, regulile corporatiste obligatorii, sau consimțământul expres pentru efectuarea transferului. Niciuna din aceste opțiuni nu este simplu sau rapid de implementat, astfel că apare oportună analizarea în primul rând a necesității transferului de date personale în Statele Unite, cu scopul de a reduce sau elimina transferurile care nu sunt necesare. O asemenea reducere ar avea loc în situația în care, de exemplu, ar fi folosite centre de date din Uniunea Europeană, deși chiar și în acest caz trebuie avut în vedere faptul că societățile americane pot fi obligate, în anumite condiții, să predea informații pe care afiliații lor le dețin în străinătate referitor la cetățeni străini.

În al doilea rând, trebuie efectuată o analiză a contractelor încheiate cu furnizori americani cu scopul ca, în măsura în care contractele nu conțin deja clauzele standard aprobate de Comisia Europeană (prin Deciziile 2010/87/UE sau 2001/497/CE), contractele existente să fie înlocuite cu asemenea clauze standard. În acest caz trebuie avut în vedere faptul că există două tipuri de clauze standard: operator-operator și operator-împuternicit, fiecare potrivit în alt tip de situații. Mai mult, pe lângă clauzele care nu pot fi modificate, clauzele standard aprobate de Comisie includ și anexe al căror conținut nu este prestabilit și pe care părțile contractului trebuie să le introducă după o analiză detaliată – între altele, categoriile de date transferate, modalitatea prelucrării, măsurile tehnice și organizatorice prin care importatorul de date american asigură un nivel de protecție adecvat potrivit standardelor Uniunii Europene.

Este însă posibil ca, deși transferul de date a fost notificat în temeiul Safe Harbor, contractul care îi stă la bază să conțină deja clauzele standard. Aceasta pentru că, până în 6 octombrie 2015, notificarea de către un operator român a transferului de date în Statele Unite în temeiul Safe Harbor elimina complet necesitatea autorizării transferului de către ANSPDCP, chestiune care nu subzista în cazul transferului întemeiat pe clauze standard; drept urmare, atunci când operatorul a avut încheiat un contract cu clauze standard dar partenerul american (importator de date) era și certificat Safe Harbor, atunci notificarea a fost făcută pe acest din urmă temei pentru a elimina timpul suplimentar și formalitățile mai stricte aferente autorizării. Acum, după hotărârea Schrems, operatorii respectivi trebuie să modifice notificările depuse și să schimbe temeiul transferului în clauze contractuale standard (atașând copie), după care să aștepte autorizarea din partea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal. În prezent, această formalitate poate dura chiar și 4 luni, ceea ce înseamnă că modificarea trebuie făcută cât mai curând.

[6] A se vedea comunicatul de la *http://dataprotection.ro/?page=Transper_date_conf_CJUE&lang=ro*.

Pentru transferurile intra-grup de date personale (în special date ale angajaților în cadrul companiilor multinaționale) operatorii pot implementa reguli corporatiste obligatorii (BCR), deși acest proces este în general dificil și costisitor.

Nu în ultimul rând, operatorii de date pot solicita consimțământul persoanelor vizate pentru efectuarea transferului. Deși acest temei are avantajul de a exclude necesitatea autorizării transferului, obținerea consimțământului se poate dovedi foarte oneroasă sau chiar imposibilă – de exemplu, în ce privește datele deja colectate de la un număr semnificativ de persoane vizate, și care continuă să fie deținute, chiar și pasiv, de către operatorii în cauză prin intermediul unor împuterniciți stabiliți în Statele Unite.

În fine, o chestiune care nu poate fi ignorată este faptul că motivarea hotărârii Schrems (anume existența unor mijloace de supraveghere necontrolată din partea autorităților SUA) poate fi aplicată și în ceea ce privește toate celelalte temeiuri de transfer al datelor cu caracter personal către Statele Unite. O asemenea interpretare drastică ar conduce, practic, la imposibilitatea transferului de date către Statele Unite, în ciuda celor mai bune eforturi depuse atât de companiile din Uniune cât și de cele de peste ocean. Din fericire, cel puțin deocamdată orientarea autorității române de supraveghere este una moderată, care permite recurgerea la toate celelalte temeiuri înafara Safe Harbor. Acest lucru însă nu elimină necesitatea ca operatorii români de date să își facă propria analiză și să își decidă propriile măsuri de implementat ca urmare a invalidării acordului Safe Harbor.

andreea.lisievici@tuca.ro

Editori

Avocații Țuca Zbârcea & Asociații dețin o experiență notabilă în domeniul **Protecției Datelor cu Caracter Personal**, consolidată ca urmare a creșterii cerințelor de protecție a datelor cu caracter personal, atât la nivel intern, cât și la nivelul Uniunii Europene. Serviciile noastre acoperă toate aspectele legate de protecția datelor cu caracter personal, de la notificarea autorității locale de reglementare (Autoritatea Națională pentru Supravegherea Datelor cu Caracter Personal – „ANSPDCP") cu privire la intenția operatorilor de date de a prelucra date cu caracter personal, până la realizarea unor analize complexe pe probleme sensibile din domeniul protecției datelor cu caracter personal, cum ar fi în cazul transferului de diverse categorii de date în străinătate; accesul la datele personale de către personalul din cadrul societăților membre ale unui grup internațional; monitorizarea salariaților, geolocație, istoricul apelurilor; crearea de baze de date cu datele persoanelor vizate și utilizarea de către alte entități decât entitatea care a colectat datele; regimul juridic al accesului la fișiere de tip *cookie*; prelucrarea datelor de trafic; aspecte de protecție a datelor cu caracter personal în legătură cu implementarea soluțiilor de *cloud computing* atât pentru clienții care achiziționează soluții *cloud*, cât și pentru furnizorii de soluții *cloud* etc. Cei interesați de noutățile din acest domeniu pot accesa blogul Țuca Zbârcea & Asociații – *dataprivacyblog.tuca.ro*

Cornel Popa
Partner
+4 021 204 88 94
cornel.popa@tuca.ro

Andreea Lisievici
Managing Associate
+4 021 204 88 90
andreea.lisievici@tuca.ro

Ciprian Dragomir
Partner
+4 021 204 88 98
ciprian.dragomir@tuca.ro

Cătălin Băiculescu
Partner
+4 021 204 76 34
catalin.baiculescu@tuca.ro

TUCA ZBARCEA
ASOCIATII

Șos. Nicolae Titulescu nr. 4-8
America House, Aripa de Vest, et. 8
Sector 1, 011141, București, România
T + 4 021 204 88 90
F + 4 021 204 88 99
E office@tuca.ro
www.tuca.ro

Acest material informativ are numai un caracter orientativ. Scopul său nu este de a oferi consultanță juridică cu caracter definitiv, care se va solicita conform fiecărei probleme legale în parte. Pentru detalii și clarificări privind oricare dintre subiectele tratate în Buletinul Legislativ, vă rugăm să contactați avocații sus-menționați.