



19.2.2010

## COMUNICARE CĂTRE MEMBRI

Ref.: **Petiția nr. 1097/2009, adresată de Alexander Junger, de cetățenie austriacă, privind propunerea schimbului de informații bancare între UE și Statele Unite, sub pretextul combaterii terorismului**

### 1. Rezumatul petiției

Petiționarul consideră că propunerea de a împărtăși date bancare autorităților din SUA – sub pretextul combaterii terorismului – este o încălcare a secretului bancar și a integrității personale a cetățenilor europeni.

### 2. Admisibilitate

Declarată admisibilă la 19 noiembrie 2009. Comisia a fost invitată să furnizeze informații [articolul 202 alineatul (6) din Regulamentul de procedură].

### 3. Răspunsul Comisiei, primit la 19 februarie 2010

Petiționarul susține că împărtășirea datelor bancare autorităților SUA constituie o încălcare a secretului bancar. Acesta se îndoiește de valoarea Programului de urmărire a finanțărilor în scopuri teroriste (TFTP) al SUA și critică suspiciunea preventivă a tuturor.

TFTP există de opt ani. A fost înființat de Departamentul de Trezorerie al Statelor Unite la scurt timp după atacurile teroriste de la 11 septembrie 2001. TFTP se bazează pe autoritățile statutare ale SUA, pe rezoluțiile Consiliului de Securitate al Organizației Națiunilor Unite și pe ordinele executive aferente. O serie de articole de presă din 2006 au dezvăluit existența TFTP, ceea ce a provocat critici potrivit cărora TFTP nu a ținut seama de legislația UE privind protecția datelor. Pentru a răspunde acestor îngrijorări, Președinția germană a Consiliului Uniunii Europene (primul semestru 2007), sprijinită de Comisie, a negociat o serie

de angajamente cu Departamentul de Trezorerie al Statelor Unite cu privire la modul în care datele cu caracter personal care provin din UE vor fi procesate în cadrul TFTP. Aceste angajamente au fost publicate în Jurnalul Oficial al Uniunii Europene în iulie 2007 [C 166/18 din 20.7.2007] și includ, de exemplu, o limitare strictă a scopului în ceea ce privește lupta împotriva terorismului, interdicția privind extragerea datelor și obligații de ștergere a datelor în intervalele de timp specificate. În plus, filiala din SUA a SWIFT s-a alăturat programului privind sfera de securitate (Safe Harbour programme) care asigură un nivel adecvat al protecției datelor și permite transferul datelor cu caracter personal din spațiul comunitar către Statele Unite în scopuri comerciale.

În raportul său către Comisia Europeană din decembrie 2008, judecătorul francez specializat în combaterea terorismului, Jean-Louis Bruguière, a evaluat valoarea TFTP pentru securitatea UE și pentru punerea în aplicare a angajamentelor SUA. Raportul a concluzionat că TFTP a avut o valoare considerabilă pentru statele membre UE în lupta acestora împotriva terorismului. Peste 1450 de piste generate de TFTP au fost transmise până în prezent guvernelor europene, 800 au fost transmise unor guverne din afara Europei, în timp ce peste 100 de noi piste generate de TFTP au fost furnizate țărilor UE în perioada ianuarie-septembrie 2009. Printre exemplele concrete de beneficii aduse de informațiile extrase în cadrul TFTP se numără:

- (i) Informațiile din cadrul TFTP au oferit o asistență substanțială guvernelor europene în timpul investigațiilor pe marginea complotului dirijat de Al-Qaeda care viza atacarea zborurilor transatlantice între UE și Statele Unite. Informațiile din cadrul TFTP au oferit noi piste, au coroborat identități și au dezvăluit relații între persoanele responsabile de acest complot terorist. La mijlocul lunii septembrie 2009, trei persoane au fost condamnate în Regatul Unit și fiecare dintre acestea a primit o sentință de minimum 30 de ani de închisoare;
- (ii) La începutul anului 2009, informațiile extrase în cadrul TFTP au fost utilizate pentru a identifica activitatea financiară a unei persoane aparținând Al-Qaeda aflate în Europa, care a jucat un rol în planificarea unui presupus atac asupra unui avion. Informațiile au fost transmise guvernelor din țări din Europa și Orientul Mijlociu;
- (iii) În vara anului 2007, TFTP a fost utilizat pentru a identifica activitățile financiare ale unor membri ai Uniunii Jihadului Islamic (UJI) în Germania. Aceste informații au contribuit la investigarea și în final la arestarea membrilor UJI care complotau pentru atacarea unor obiective în Germania. TFTP a continuat să ofere noi informații utile autorităților germane în urma arestărilor. Ulterior, persoanele respective au mărturisit.

Valoarea TFTP a fost acceptată de toate statele membre atunci când acestea au adoptat în unanimitate Mandatul Consiliului pentru negocierea acordului UE-SUA. La începutul anului 2010, judecătorul Bruguière va prezenta un al doilea raport care va trata mai pe larg valoarea informațiilor extrase în cadrul TFTP pentru securitatea UE.

La finalul anului 2009, SWIFT a introdus noua „arhitectură a sistemului”. În acest scop, SWIFT a menținut serverele existente din UE și SUA și a dat în funcțiune un nou centru operațional în Elveția. Efectul concret al acestui nou aranjament constă în faptul că un volum

semnificativ de date care au fost primite în trecut de Departamentul de Trezorerie al SUA în cadrul TFTP nu mai sunt stocate în Statele Unite și nu se mai află sub jurisdicția guvernului Statelor Unite. Prin urmare, mesageria financiară în materie de plăți și datele aferente sunt stocate pe teritoriul Uniunii Europene și pot fi furnizate numai la cererea Departamentului de Trezorerie al SUA.

Pentru a garanta că TFTP continuă să aducă pentru UE și la nivel global beneficiile în materie de securitate menționate, anterior, a fost necesar să se instituie un acord internațional care să permită punerea în continuare la dispoziția Departamentului de Trezorerie al SUA a datelor relevante de mesagerie financiară. De aceea, în luna iulie a acestui an, cele 27 de state membre au adoptat unanim în Consiliu un mandat și linii directoare privind negocierea unui acord UE-SUA pentru transferul datelor de mesagerie financiară în cadrul TFTP. Echipa de negociere a UE a fost condusă de Președinția suedeză, asistată de Comisia Europeană.

În septembrie 2009, Parlamentul European a emis Rezoluția privind un acord UE-SUA avut în vedere pentru transferul datelor de mesagerie financiară în cadrul TFTP. Rezoluția precizează că acordul trebuie să fie valabil pe o perioadă scurtă, procesarea datelor de mesagerie financiară trebuie efectuată numai în scopul combaterii terorismului, iar cererile de date trebuie să se bazeze pe anumite cazuri vizate și să fie supuse autorizării judiciare.

În urma mai multor runde de negocieri, Consiliul a adoptat la 30 noiembrie o Decizie privind semnarea, în numele Uniunii Europene, a Acordului dintre Uniunea Europeană și Statele Unite ale Americii privind prelucrarea și transferul datelor de mesagerie financiară din Uniunea Europeană către Statele Unite în cadrul Programului de urmărire a finanțării în scopuri teroriste („Acord interimar”). Înainte ca acordul interimar să poată fi încheiat, Parlamentul European ar fi trebuit să își dea acordul - lucru pe care l-a refuzat în sesiunea plenară din februarie 2010. Acordul prevedea aplicarea provizorie începând cu 1 februarie 2010 (dată la care intră în vigoare Acordul multilateral dintre UE și SUA) și o durată maximă de 9 luni. Prim urmare, acesta ar fi expirat și ar fi încetat să producă efecte la 31 octombrie 2010 sau mai devreme. Comisia a intenționat să propună un nou mandat la începutul anului 2010 pentru un acord ulterior bazat pe Tratatul de la Lisabona, care să conțină măsuri de siguranță și mai solide în ceea ce privește protecția datelor și o implicare și mai mare a Parlamentului European. Între timp, ar fi fost nevoie de un acord interimar pentru a asigura că acoperirea TFTP nu înregistrează lacune care ar împiedica UE să obțină informații importante referitoare la atacuri teroriste sau la investigații privind terorismul.

Acordul interimar conținea garanții importante pentru protecția datelor cu caracter personal transferate în temeiul acordului. Acestea includeau, de exemplu, o interdicție strictă de utilizare a datelor pentru orice alt scop decât prevenirea, investigarea, depistarea sau urmărirea penală a actelor de terorism sau a finanțării acestora, o interdicție strictă privind orice formă de extragere de date și obligația de a oferi soluții eficiente. Acordul interimar prevedea că Departamentul de Trezorerie are obligația de a identifica date care nu mai sunt necesare în combaterea terorismului și de a le elimina. În alte cazuri, datele din baza de date TFTP trebuiau, în general, să fie șterse în termen de cinci ani de la primire. Acordul interimar impunea obligații stricte în materie de securitate a datelor și cu privire la persoanele care aveau drept de acces la datele TFTP.

Una dintre cele mai importante garanții era aceea că, înainte ca datele TFTP să fie puse la

dispoziția SUA, Departamentul de Trezorerie al SUA trebuia să emită o solicitare bazată pe o investigație în curs cu privire la un anumit comportament privind crimele teroriste care au fost comise sau acolo unde, pe baza unor informații sau dovezi preexistente, exista motivul să se creadă că acestea puteau fi comise. În absența unei astfel de solicitări bine întemeiate, datele nu ar fi putut să fie puse la dispoziția SUA. Această obligație ar fi fost supusă unei verificări efectuate de autoritatea judiciară a statului membru solicitat și unui audit extern și subliniază faptul că TFTP nu poate fi utilizat decât în cazul în care există o suspiciune demonstrabilă și rezonabilă că o persoană identificată este implicată în acțiuni de terorism sau în finanțarea acestora.

Reducerea rigurozității privind secretul bancar este acceptată ca o măsură necesară și proporționată pentru lupta împotriva crimelor grave, inclusiv a finanțării terorismului. Acest lucru este demonstrat, de exemplu, de Directiva 2005/60/CE din 26 octombrie 2005 privind prevenirea utilizării sistemului financiar în scopul spălării banilor și finanțării terorismului și de Regulamentul (CE) nr. 1781/2006 din 15 noiembrie 2006 cu privire la informațiile privind plătitorul care însoțesc transferurile de fonduri. Acordul UE-SUA privind prelucrarea și transferul datelor de mesagerie financiară din Uniunea Europeană către Statele Unite în cadrul TFTP include garanții importante privind accesul la datele de mesagerie financiară, ceea ce evidențiază abordarea proporționată adoptată de Acordul interimar.

## Concluzie

Prin Acordul interimar s-a dorit să se atingă un echilibru corespunzător între măsurile necesare pentru asigurarea securității UE, pe de o parte, și protecția datelor cu caracter personal, pe de altă parte. Acordul ar fi fost valabil pe o perioadă scurtă, ar fi interzis orice utilizare a datelor de mesagerie financiară în alte scopuri decât lupta împotriva terorismului și prevedea în mod clar că solicitările de date trebuie să se bazeze pe anumite cazuri vizate și că acestea sunt supuse autorizării judiciare. În special, datele TFTP nu ar fi făcut obiectul unor căutări nelimitate și ar fi putut fi utilizate numai dacă s-ar fi demonstrat existența unei legături directe cu crime teroriste sau s-ar fi dovedit finanțarea acestora. Proporționalitatea Acordului interimar, inclusiv respectarea angajamentelor privind protecția datelor și o evaluare a valorii curente a TFTP pentru securitatea UE, ar fi făcut obiectul unei revizuirii comunitare detaliate, care ar fi fost efectuată în 2010, *inter alia*, de reprezentanții autorităților din domeniul protecției datelor din statele membre.

TFTP este necesar pentru securitatea europeană. În ceea ce privește securitatea, breșa creată prin respingerea acordului interimar trebuie să fie acoperită. Ar putea exista, de asemenea, acorduri bilaterale privind transferul de date, întrucât datele sunt situate fizic într-un singur stat membru. Cu toate acestea, datele provin din toate statele membre ale UE, motiv pentru care este viabilă doar o soluție comunitară. Prin urmare, Comisia va propune un nou mandat pentru o cooperare UE-SUA în ceea ce privește durabilitatea TFTP.