GRUPUL DE LUCRU „ARTICOLUL 29” PENTRU PROTECȚIA DATELOR

16/RO
GL 238

Avizul 01/2016 cu privire la proiectul de decizie privind caracterul adecvat al Scutului de confidențialitate UE-SUA

Adoptat la 13 aprilie 2016

REZUMAT

La 29 februarie 2016, Comisia Europeană a publicat o comunicare, un proiect de decizie privind caracterul adecvat și textele anexate la acesta, care constituie un nou cadru pentru schimburile transatlantice de date cu caracter personal în scopuri comerciale: Scutul de confidențialitate UE-SUA (denumit în continuare „Scutul de confidențialitate"), care urmărește să înlocuiască sistemul anterior al sferei de siguranță anulat de Curtea de Justiție a Uniunii Europene (denumită în continuare „CJUE") la 6 octombrie 2015, prin hotărârea în cauza Schrems.

În conformitate cu articolul 30 alineatul (1) litera (c) din Directiva 95/46/CE, grupul de lucru „articolul 29" pentru protecția datelor (denumit în continuare „GL29") a evaluat documentele respective pentru a emite un aviz cu privire la proiectul de decizie privind caracterul adecvat. GL29 a evaluat atât aspectele comerciale, cât și eventualele derogări de la principiile Scutului de confidențialitate din motive legate de securitatea națională, aplicarea legii și interese publice.

GL29 a luat în considerare cadrul juridic aplicabil al UE privind protecția datelor, astfel cum este prevăzut în Directiva 95/46/CE, precum și drepturile fundamentale la viață privată și protecția datelor, codificate la articolul 8 din Convenția europeană a drepturilor omului și la articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene. De asemenea, acesta a examinat dreptul la o cale de atac eficientă și la un proces echitabil, prevăzut la articolul 47 din Carta drepturilor fundamentale, precum și în jurisprudența referitoare la diferitele drepturi fundamentale.

În plus, analiza reflectă raționamentul Curții de Justiție a Uniunii Europene în cauza Schrems cu privire la marja de apreciere a Comisiei în ceea ce privește evaluarea caracterului adecvat al nivelului de protecție. Verificarea și controlul cerințelor privind caracterul adecvat al nivelului de protecție trebuie să fie efectuate strict, ținând cont de drepturile fundamentale la viață privată și la protecția datelor și de numărul persoanelor care ar putea fi afectate de transferuri.

Scutul de confidențialitate trebuie să fie analizat în contextul internațional actual, caracterizat de apariția volumelor mari de date și de creșterea nevoilor în materie de securitate. Domeniul de aplicare și sfera colectării și utilizării datelor cu caracter personal au crescut dramatic de la adoptarea inițială a deciziei privind sfera de siguranță în 2000. Autoritățile europene pentru protecția datelor afirmă cu tărie importanța principiilor pe care le apără.

În primul rând, GL29 salută îmbunătățirile semnificative introduse de Scutul de confidențialitate în raport cu decizia privind sfera de siguranță. Grupul de lucru ia act de faptul că negociatorii au abordat un număr mare de deficiențe ale programului privind sfera de siguranță pe care acesta le-a subliniat în scrisoarea din 10 aprilie 2014 adresată vicepreședintelui Reding.

Faptul că principiile și garanțiile oferite de Scutul de confidențialitate sunt prevăzute atât în decizia privind caracterul adecvat, cât și în anexele la aceasta face ca informațiile să fie dificil de găsit și, uneori, inconsecvente. Acest lucru contribuie la o lipsă de claritate în ceea ce privește noul cadru și crește dificultatea accesibilității pentru persoanele vizate, organizații și autoritățile de protecție a datelor. De asemenea, limbajul utilizat este lipsit de claritate. Prin urmare, GL29 recomandă Comisiei să clarifice formulările pentru a fi ușor de înțeles pe ambele părți ale Atlanticului.

În ceea ce privește legea aplicabilă, GL29 subliniază că, în cazul în care decizia privind caracterul adecvat al Scutului de confidențialitate este adoptată în temeiul Directivei 95/46/CE, aceasta trebuie să fie în concordanță cu cadrul juridic al UE privind protecția datelor în ceea ce privește atât domeniul, cât și terminologia. GL29 consideră că, la scurt timp după intrarea în vigoare a Regulamentului general privind protecția datelor, trebuie realizată o revizuire pentru a se asigura că nivelul mai ridicat de protecție a datelor oferit de regulament este respectat în decizia privind caracterul adecvat și anexele sale.

În ceea ce privește aspectele comerciale ale Scutului de confidențialitate

Obiectivul principal al GL29 este de a garanta faptul că se menține un nivel, în esență, echivalent de protecție acordat persoanelor atunci când datele cu caracter personal sunt prelucrate în conformitate cu dispozițiile Scutului de confidențialitate. Deși GL29 nu se așteaptă ca Scutul de confidențialitate să reprezinte o simplă copie exhaustivă a cadrului juridic al UE, acesta consideră că Scutul de confidențialitate ar trebui să conțină fondul principiilor fundamentale și, prin urmare, să asigure un nivel „în mod esențial echivalent” de protecție.

În afară de îmbunătățirile aduse de Scutul de confidențialitate, GL29 consideră că unele principii fundamentale de protecție a datelor, astfel cum sunt prevăzute în legislația europeană, nu sunt reflectate în proiectul de decizie privind caracterul adecvat și în anexe sau au fost înlocuite în mod inadecvat de noțiuni alternative.

De exemplu, principiul păstrării datelor nu este menționat în mod expres și nu poate fi clar desprins din actuala formulare a principiului integrității datelor și limitării scopului. În plus, nu există nicio formulare privind protecția care ar trebui acordată împotriva deciziilor individuale automate bazate exclusiv pe prelucrarea automată. Punerea în aplicare a principiului limitării scopului prelucrării datelor este, de asemenea, neclară. Pentru a asigura o mai mare claritate în ceea ce privește utilizarea mai multor noțiuni importante, GL29 sugerează că UE și SUA ar trebui să convină asupra unor definiții clare, care să facă parte dintr-un glosar de termeni pentru a fi inclus în secțiunea de întrebări frecvente privind Scutul de confidențialitate

Întrucât Scutul de confidențialitate va fi utilizat, de asemenea, pentru transferul de date în afara SUA, GL29 insistă asupra faptului că transferurile ulterioare de la o entitate parte la Scutul de confidențialitate către beneficiarii dintr-o țară terță ar trebui să asigure același nivel de protecție cu privire la toate aspectele Scutului de confidențialitate (inclusiv securitatea

națională) și nu ar trebui să conducă la scăderea sau încălcarea principiilor UE privind protecția datelor. În cazul în care este prevăzut un transfer ulterior către o țară terță în temeiul Scutului de confidențialitate, fiecare organizație parte la Scutul de confidențialitate ar trebui să aibă obligația de a evalua toate cerințele obligatorii din legislația națională a țării terțe aplicabile importatorului de date, înainte de transfer. În general, GL29 consideră că transferurile ulterioare de date cu caracter personal din UE nu sunt suficient de reglementate, în special în ceea ce privește domeniul lor de aplicare, limitarea scopului și garanțiile aplicabile transferurilor către agenți.

În cele din urmă, deși GL29 notează măsurile suplimentare puse la dispoziția persoanelor fizice pentru a-și exercita drepturile, acesta este preocupat de faptul că noul mecanism de recurs, în practică, se poate dovedi a fi prea complex, dificil de utilizat pentru cetățenii UE și, prin urmare, ineficace. În consecință, sunt necesare clarificări suplimentare cu privire la diferitele proceduri de recurs; în special, dacă doresc, autoritățile UE pentru protecția datelor ar putea fi considerate drept un punct de contact natural pentru cetățenii UE în diferite proceduri, având opțiunea de a acționa în numele acestora.

Derogările în scopuri de securitate națională

În ceea ce privește accesul la date al autorităților publice, atât în UE, cât și în țările terțe, GL29 reamintește analiza sa cu privire la drepturile fundamentale relevante cuprinsă în documentul de lucru privind justificarea ingerințelor în drepturile fundamentale la viață privată și protecția datelor prin măsuri de supraveghere atunci când transferă date cu caracter personal (garanții esențiale europene) (WP237).

Un mare pas înainte față de decizia privind sfera de siguranță constă în faptul că proiectul de decizie privind caracterul adecvat abordează în prezent pe scară largă accesul la datele prelucrate în temeiul Scutului de confidențialitate în scopuri de securitate națională și de aplicare a legii. GL29 recunoaște acest pas important, precum și gradul sporit de transparență oferit de administrația SUA cu privire la legislația aplicabilă pentru colectarea de informații (anexa VI).

Cu toate acestea, GL29 observă că declarațiile Biroului Directorului Serviciului Național de Informații (ODNI) al SUA nu exclud colectarea masivă și nediferențiată de date cu caracter personal provenite din UE. GL29 își reiterează poziția adoptată în urmă cu mult timp conform căreia supravegherea masivă și arbitrară a persoanelor nu poate fi considerată proporțională și necesară într-o societate democratică, astfel cum se solicită în temeiul protecției oferite de drepturile fundamentale aplicabile. În plus, supravegherea atentă a tuturor programelor de supraveghere este esențială. GL29 remarcă faptul că există o tendință de a colecta date din ce în ce mai mult pe o scară masivă și nediferențiată în contextul luptei împotriva terorismului. Având în vedere preocupările pe care acest fapt le generează cu privire la protecția drepturilor fundamentale la viață privată și protecția datelor, GL29 așteaptă hotărârile viitoare ale CJUE în cauzele privind colectarea masivă și nediferențiată de date.

În ceea ce privește căile de atac, GL29 salută înființarea funcției de Ombudsman ca un nou mecanism de recurs. Acest mecanism ar putea constitui o îmbunătățire semnificativă a drepturilor cetățenilor UE în ceea ce privește activitățile de spionaj ale SUA. Cu toate acestea, GL29 este preocupat de faptul că noua instituție nu este suficient de independentă și nu este investită cu competențe adecvate pentru a-și exercita în mod efectiv sarcina și nu garantează o cale de atac satisfăcătoare în caz de dezacord.

Revizuirea comună

Mecanismul de revizuire comună anuală menționat în proiectul de decizie privind caracterul adecvat este un factor-cheie pentru credibilitatea globală a Scutului de confidențialitate, iar GL29 salută călduros ocazia prezentată de acest mecanism pentru revizuirea deciziei privind caracterul adecvat. În această privință, GL29 consideră că reprezentanții naționali ai GL29 vor putea să participe pe deplin la procesul de revizuire, dar solicită clarificări cu privire la modalitățile exacte. Modalitățile (inclusiv raportul rezultat, publicitatea acestuia și posibilele consecințe, precum și finanțarea) trebuie să fie convenite înaintea primei revizuiri.

Concluzie

GL29 remarcă îmbunătățirile majore pe care le oferă Scutul de confidențialitate în comparație cu decizia anulată privind sfera de siguranță. Având în vedere preocupările exprimate și clarificările solicitate, GL29 recomandă Comisiei să soluționeze aceste aspecte, să identifice soluții corespunzătoare și să furnizeze clarificările solicitate pentru a îmbunătăți proiectul de decizie privind caracterul adecvat și a asigura că protecția oferită de Scutul de confidențialitate este într-adevăr, în esență, echivalentă cu cea din UE.

CUPRINS

1. INTRODUCERE

În urma hotărârii emise de Curtea de Justiție a Uniunii Europene (denumită în continuare „CJUE") la 6 octombrie 2015 în cauza Schrems[1], Grupul de lucru „articolul 29" pentru protecția datelor (denumit în continuare „GL29" sau „grupul de lucru") a invitat statele membre ale Uniunii Europene (denumită în continuare „UE") și celelalte instituții europene să inițieze discuții cu autoritățile din Statele Unite (denumite în continuare „SUA") cu scopul de a identifica soluții politice, juridice și tehnice care să permită transferuri de date către teritoriul Statelor Unite cu respectarea drepturilor fundamentale.

La 2 februarie 2016, după mai mult de doi ani de negocieri, Comisia Europeană și Departamentul Comerțului al Statelor Unite (DoC) au ajuns la un acord politic cu privire la un *Nou cadru pentru schimburile transatlantice de date cu caracter personal în scopuri comerciale: Scutul de confidențialitate UE-SUA* (denumit în continuare „Scutul de confidențialitate"), care vizează să înlocuiască fostul program privind sfera de siguranță.

La 29 februarie 2016, Comisia a publicat o comunicare[2], un proiect de decizie privind caracterul adecvat și textele anexate la aceasta care vor constitui Scutul de confidențialitate. În conformitate cu articolul 30 alineatul (1) litera (c) din Directiva 95/46/CE (denumită în continuare „directiva"), GL29 a evaluat documentele respective pentru a emite prezentul aviz cu privire la proiectul de decizie privind caracterul adecvat pregătit de Comisie, inclusiv documentele Scutului de confidențialitate care stau la baza acestuia. În evaluarea sa, GL29 și-a împărțit activitatea între o evaluare a părții comerciale a Scutului de confidențialitate și o analiză a măsurilor de protecție puse în aplicare în ceea ce privește derogările de la principiile Scutului de confidențialitate din motive legate de protejarea securității naționale, aplicarea legii și interesele publice.

În urma hotărârii Schrems, GL29 a organizat mai multe reuniuni cu delegații din partea administrației SUA, reprezentanți ai organizațiilor societății civile din UE și SUA, precum și specialiști, pentru a pregăti evaluarea consecințelor hotărârii Schrems. Cu ocazia evaluării Scutului de confidențialitate, au avut loc reuniuni suplimentare cu reprezentanți ai Comisiei Europene și ai administrației SUA. În cadrul acestor reuniuni, au fost furnizate o serie de clarificări care au fost luate în considerare, de asemenea, în prezentul aviz. GL29 subliniază că, în stadiul actual, clarificările respective au fost doar informale și nu pot fi considerate ca făcând parte integrantă din proiectul de decizie privind caracterul adecvat, întrucât nu au fost consemnate în scris până în prezent.

Cu toate acestea, GL29 salută, în special, angajamentul asumat de Departamentul Comerțului în cursul reuniunilor de a coopera cu autoritățile de protecție a datelor din statele membre ale UE în ceea ce privește aplicarea Scutului de confidențialitate și de a stabili instrucțiuni privind aplicarea și interpretarea juridică a Scutului de confidențialitate care să fie publicate pe site-urile internet ale acestora.

[1] Cauza C-362/14, Maximillian Schrems/Data Protection Commissioner din 6 octombrie 2015 (denumită în continuare „Schrems").
[2] COM(2016)117 final, 29 februarie 2016.

1.1 Observații generale

1.1.1 Domeniul de aplicare a evaluării GL29

GL29 a luat în considerare, în primul rând, cadrul de protecție a datelor aplicabil în statele membre ale Uniunii Europene, inclusiv articolul 8 din Convenția europeană a drepturilor omului (denumită în continuare „CEDO") care protejează dreptul la viața privată și de familie, precum și articolele 7, 8 și 47 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „Carta") care consacră dreptul la viața privată și de familie, dreptul la protecția datelor cu caracter personal și dreptul la o cale de atac eficientă și la un proces echitabil. De asemenea, GL29 a luat în considerare jurisprudența relevantă, precum și cerințele directivei.

Cerința ca o țară terță să asigure un nivel adecvat de protecție a datelor a fost clarificată de CJUE în hotărârea Schrems. Curtea nu doar a explicat că dispozițiile directivei trebuie interpretate „în lumina drepturilor fundamentale garantate de cartă"[3], în special articolele 7 și 8. Aceasta a indicat, de asemenea, că sintagma „nivel de protecție adecvat" trebuie interpretată în sensul că „impune ca această țară terță să asigure efectiv, în temeiul legislației interne sau al angajamentelor sale internaționale, un nivel de protecție a drepturilor și libertăților fundamentale în esență echivalent cu cel garantat în cadrul Uniunii Europene în temeiul Directivei, interpretată în lumina cartei"[4]. Pentru decizia anulată privind sfera de siguranță, o astfel de evaluare nu a fost realizată niciodată suficient de detaliat. Prin urmare, GL29 a evaluat proiectul de decizie privind caracterul adecvat având în vedere cerința de a furniza o analiză a nivelului de protecție a drepturilor fundamentale și a libertăților fundamentale ca fiind *în esență echivalent* cu cel garantat la nivelul UE. GL29 subliniază că prezentul aviz conține principalele sale preocupări, dar că, dat fiind timpul scurt care a trecut de la publicarea proiectului de decizie privind caracterul adecvat, ulterior se pot descoperi și alte aspecte.

GL29 recunoaște că, prin definirea termenului „adecvat" de la articolul 25 alineatul (6) din directivă ca fiind „în esență echivalent", CJUE a clarificat ceea ce înseamnă caracterul adecvat prin hotărârea în cauza Schrems. Curtea a subliniat faptul că termenul „nivel de protecție adecvat", deși nu impune țării terțe să asigure un nivel de protecție identic cu cel garantat în cadrul ordinii juridice a Uniunii, trebuie să fie înțeles în sensul de a impune țării terțe să asigure, în temeiul legislației interne sau al angajamentelor sale internaționale, un nivel de protecție a drepturilor și libertăților fundamentale *în esență echivalent* cu cel garantat în cadrul Uniunii Europene în temeiul directivei, interpretată în lumina Cartei.

1.1.2 Evaluarea părții comerciale din proiectul de decizie privind caracterul adecvat

GL29 a explicat deja modul în care a aplicat principiile esențiale ale UE în materie de protecție a datelor pentru transferurile de date cu caracter personal către țări terțe în documentul de lucru 12 „Transferuri de date cu caracter personal către țări terțe: aplicarea

[3] Schrems punctul 38.
[4] Schrems punctul 73.

articolelor 25 și 26 din directiva referitoare la protecția datelor”[5]. GL29 a urmărit să identifice garanțiile echivalente care asigură un nivel de protecție echivalent cu principiile garantate de directivă, în special în ceea ce privește limitarea scopului, calitatea datelor și proporționalitatea, transparența, securitatea, drepturile de acces, rectificarea și opoziția, păstrarea datelor și restricțiile privind transferurile ulterioare. O metodă similară a fost utilizată în avizele emise de GL29 la momentul evaluării deciziei inițiale privind caracterul adecvat al programului privind sfera de siguranță[6], precum și în recomandările formulate de grupul de lucru în scrisoarea acestuia către fostul vicepreședinte al Comisiei Europene și comisar pentru justiție Viviane Reding, publicată la 10 aprilie 2014[7].

1.1.3 Evaluarea derogărilor privind accesul autorităților publice și garanțiile acestora

Evaluarea derogărilor privind accesul autorităților publice la datele cu caracter personal care fac obiectul Scutului de confidențialitate este de natură complexă, în special ținând seama de creșterea gradului de conștientizare în rândul autorităților pentru protecția datelor și al publicului larg cu privire la programele de supraveghere ale SUA în urma dezvăluirilor lui Edward Snowden. Grupul de lucru recunoaște și salută eforturile depuse de administrația SUA pentru a spori transparența cu privire la programele de supraveghere, precum și disponibilitatea acestora de a include garanții suplimentare în Scutul de confidențialitate. În același timp, GL29 subliniază că orice ingerință în drepturile fundamentale la viață privată și protecția datelor trebuie să fie justificată într-o societate democratică. CJUE a criticat faptul că decizia privind sfera de siguranță nu conținea nicio constatare cu privire la existența, în Statele Unite, a unor norme adoptate de stat menite să limiteze orice ingerință. Decizia nu făcea referire nici la existența vreunei protecții juridice efective împotriva ingerințelor de această natură[8].

Prin urmare, GL29 a analizat actualul cadru juridic al SUA și practicile agențiilor americane de informații, astfel cum sunt descrise în anexele la proiectul de decizie, precum și condițiile în care acestea permit orice ingerință în drepturile fundamentale cu privire la respectarea vieții private și la protecția datelor cu caracter personal, astfel cum sunt consfințite în temeiul cadrului juridic european.

Pentru a stabili dacă orice ingerință ar fi justificată într-o societate democratică, evaluarea a fost efectuată din perspectiva jurisprudenței europene privind drepturile fundamentale, care stabilește patru garanții esențiale[9] pentru activitățile de spionaj:

A. Prelucrarea ar trebui să fie efectuată în conformitate cu dispozițiile legii și să se bazeze pe norme clare, precise și accesibile: aceasta înseamnă că orice persoană care este

[5] Adoptată de GL29 la 24 iulie 1998, a se vedea în special pagina 6.
[6] A se vedea GL62, GL32, GL27, GL23, GL21, GL19, GL15, GL7.
[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_GL29_to_ec_on_sh_recommendations.pdf
[8] Schrems, punctele 87, 88.
[9] Garanțiile esențiale europene se bazează pe jurisprudența Curții de Justiție a Uniunii Europene și a Curții Europene a Drepturilor Omului și sunt stabilite în detaliu în documentul de lucru WP237 al grupului de lucru „articolul 29”, publicat la 13 aprilie 2016.

suficient de informată ar trebui să fie capabilă să prevadă ce s-ar putea întâmpla cu datele sale proprii în cazul în care sunt transferate;

B. Trebuie să se demonstreze necesitatea și proporționalitatea în ceea ce privește obiectivele legitime urmărite: trebuie găsit un echilibru între scopul pentru care datele sunt colectate și accesate și drepturile persoanei;
C. Ar trebui să existe un mecanism de supraveghere independent, care să fie atât eficient, cât și imparțial: acesta poate fi un judecător sau un alt organism independent, atât timp cât are capacitatea suficientă pentru a efectua controalele necesare;
D. Persoana trebuie să dispună de căi de atac eficiente: orice persoană ar trebui să aibă dreptul de a-și apăra drepturile în fața unui organism independent.

1.2 Proiectul de decizie privind caracterul adecvat

În primul rând, GL29 salută faptul că se poate lansa o nouă procedură de stabilire a caracterului adecvat la mai puțin de șase luni după ce Curtea de Justiție a Uniunii Europene a declarat nulă decizia privind sfera de siguranță. Având în vedere numărul de transferuri de date care au loc între UE și SUA zilnic, despre care GL29 recunoaște că reprezintă o parte esențială a economiei de pe ambele maluri ale Atlanticului, claritatea juridică este necesară mai degrabă mai devreme decât mai târziu.

Cu toate acestea, GL29 regretă faptul că proiectul de decizie privind caracterul adecvat publicat de Comisie nu include o evaluare detaliată a legislației naționale și a angajamentelor internaționale ale SUA sub forma unui raport privind caracterul adecvat, astfel cum a fost practica anterioară în cadrul unor proceduri similare și în conformitate cu articolul 25 din directivă. Acest fapt a împiedicat GL29 să efectueze o analiză completă cu privire la cadrul juridic în care va funcționa Scutul de confidențialitate. De exemplu, grupul de lucru constată că actualul proiect de decizie privind caracterul adecvat nu cuprinde constatări referitoare la legislația privind protecția datelor și a vieții private care există în SUA, atât la nivel federal, cât și la nivel de stat, inclusiv legislația sectorială, nici constatări referitoare la legislația care permite forme de acces public care nu sunt legate de supraveghere. De asemenea, nu este definită relația dintre transferurile de date în temeiul Scutului de confidențialitate și în temeiul altor constatări existente privind caracterul adecvat precum acordul UE-SUA privind registrul cu numele pasagerilor (PNR) și acordul privind programul de urmărire a finanțării activităților teroriste (TFTP).

1.2.1 Domeniul de aplicare a cadrului UE privind protecția datelor, în special a principiilor Directivei 95/46/CE

GL29 reamintește că, în temeiul cadrului juridic al UE privind protecția datelor, în special în conformitate cu articolul 4 alineatul (1) din directiva menționată, legislația statelor membre se aplică nu doar în cazul operațiunilor de prelucrare efectuate de operatorii de date stabiliți pe teritoriul lor, ci și în cazul în care operatorii de date (deși nu sunt stabiliți în UE) utilizează echipamente situate pe teritoriul UE, în special pentru colectarea de date cu caracter personal. În consecință, legislația unui stat membru se aplică în cazul oricărei prelucrări care are loc înainte de transferul către SUA, fie în cadrul activităților unei organizații cu sediul în UE sau

prin intermediul echipamentelor situate în UE, utilizate de o organizație care nu are sediul în UE. GL29 solicită ca acest lucru să fie menționat în mod explicit în proiectul de decizie privind caracterul adecvat.

Ar trebui să fie clar că principiile Scutului de confidențialitate se vor aplica din momentul în care are loc transferul de date. În plus, GL29 reamintește că operatorii de date stabiliți în UE care transferă date către o persoană împuternicită de un operator de date din SUA continuă să facă obiectul legislației UE privind protecția datelor.

1.2.2 Lipsa de claritate în ceea ce privește documentele Scutului de confidențialitate

Faptul că principiile și garanțiile oferite de Scutul de confidențialitate sunt prevăzute atât în decizia privind caracterul adecvat, cât și în anexele la aceasta face ca informațiile să fie dificil de găsit și, uneori, inconsecvente. Acest lucru contribuie la o lipsă de claritate în ceea ce privește noul cadru și crește dificultatea accesibilității pentru persoanele vizate, organizații și autoritățile de protecție a datelor. De asemenea, limbajul utilizat este lipsit de claritate. Prin urmare, GL29 recomandă Comisiei să utilizeze un limbaj clar și ușor de înțeles de ambele părți ale Atlanticului.

GL29 sugerează includerea unei anexe separate conținând termenii de bază, cu definiții, care se aplică în documentele Scutului de confidențialitate. O înțelegere comună și lipsită de ambiguitate a obligațiilor impuse de decizia privind caracterul adecvat al Scutului de confidențialitate este esențială pentru a asigura funcționarea sa eficientă pe ambele maluri ale Atlanticului și, ca atare, GL29 este preocupat de faptul că, din cauza numeroaselor trimiteri încrucișate și formulări nealiniate, precum și a complexității documentelor-cadru, vor apărea dificultăți în ceea ce privește coerența, lizibilitatea și claritatea punerii în aplicare a Scutului de confidențialitate.

Mai important, documentele Scutului de confidențialitate utilizează o terminologie care nu este în concordanță cu vocabularul utilizat în general în UE în ceea ce privește protecția datelor. Aceasta nu este o problemă atât timp cât este clar care ar fi terminologia corespunzătoare în temeiul legislației UE (și în temeiul legislației SUA). Cu toate acestea, GL29 regretă să constate că acest lucru nu este valabil, inclusiv în proiectul de decizie privind caracterul adecvat. De exemplu, cuvântul „acces” este utilizat în capitolul 3 din proiectul de decizie privind caracterul adecvat într-un sens care presupune colectarea de date cu caracter personal, și nu acordarea permisiunii unei persoane să vadă date care sunt deja colectate. Accesul întreprinderilor la date și dreptul de acces al persoanelor fizice sunt două noțiuni care nu trebuie confundate.

GL29 subliniază că terminologia ar trebui, de asemenea, să fie utilizată în mod consecvent pe tot cuprinsul documentelor, inclusiv în proiectul de decizie privind caracterul adecvat. Acest lucru nu se întâmplă în prezent, de exemplu în ceea ce privește noțiunile de „prelucrare” și „date cu caracter personal”. Ambele sunt, în principiu, bine definite în anexa II, dar nu sunt

aplicate consecvent în cuprinsul documentelor, ceea ce conduce la lacune în ceea ce privește protecția[10,11].

GL29 salută faptul că definițiile anumitor termeni utilizați au fost incluse în documentele care constituie Scutul de confidențialitate. Acest lucru nu este însă valabil pentru o serie de alți termeni esențiali, inclusiv „agent" sau „persoană împuternicită de către operator", „date codate cu cheie", „date anonimizate" și „persoană din UE", care, în opinia GL29, necesită o definiție clară, convenită de SUA și UE, pentru a evita confuzia într-o etapă ulterioară, atât pentru operatori, cât și persoanele împuternicite de către aceștia care utilizează Scutul de confidențialitate, autoritățile de supraveghere și publicul larg. O metodă simplă ar fi să se adauge un glosar de termeni la secțiunea de întrebări frecvente privind Scutul de confidențialitate.

De asemenea, GL29 atrage atenția asupra motivelor legitime pentru prelucrarea datelor sensibile în principiul suplimentar 1 (anexa II punctul III.1) în cazul în care o organizație nu are obligația de a obține consimțământul explicit („opt-in"). Acest principiu suplimentar 1 poate fi înțeles ca prezentând motivele legitime pentru colectarea datelor în UE, întrucât lista este similară cu articolul 8 din directivă. GL29 dorește să reamintească faptul că orice prelucrare (inclusiv colectarea și transferul) de date sensibile care fac obiectul legislației UE trebuie să fie făcută din motive legitime în conformitate cu articolul 8 din directivă. Scutul de confidențialitate nu poate fi interpretat ca oferind motive alternative pentru o astfel de prelucrare. De exemplu, GL29 consideră că nu este posibil ca o organizație din Statele Unite ale Americii să colecteze date care fac obiectul legislației UE pe baza dreptului muncii din SUA (a se vedea anexa II punctul III.1.a.v). Prin urmare, GL29 subliniază că orice interpretare a principiului suplimentar 1 poate conduce doar la aplicarea sa în cazul datelor sensibile deja transferate după ce au fost colectate în UE din motive legitime menționate la articolul 8 din directivă.

În final, GL29 arată că există o lipsă de claritate în ceea ce privește întrebarea cine poate fi considerat persoană din UE și, prin urmare, cine beneficiază de protecție în conformitate cu Scutul de confidențialitate: toți cetățenii UE sau toate persoanele rezidente în UE? Acest lucru

[10] Unele dintre clauze doar enumeră anumite tipuri de operațiuni de prelucrare a datelor, în loc să utilizeze termenul de „prelucrare". Acest lucru conduce la lacune în ceea ce privește protecția. De exemplu, în conformitate cu formularea din anexa II punctul III.6.f, principiile Scutului de confidențialitate s-ar aplica numai „în cazul în care organizația „păstrează, utilizează sau divulgă" datele primite (și anume, nu pentru alte operațiuni din sfera noțiunii de „prelucrare", cum ar fi colectarea, înregistrarea, modificarea, extragerea, consultarea, ștergerea). Securitatea datelor ar putea fi impusă numai pentru „crearea, menținerea, utilizarea sau difuzarea" de date cu caracter personal (anexa II punctul II.4). Definiția datelor cu caracter personal este limitată, de asemenea, la date „primite" și „înregistrate". Ca un alt exemplu, principiul notificării (anexa II punctul II.1.a.iv) prevede că organizația autorizată trebuie să informeze persoanele cu privire la scopurile pentru care „colectează și utilizează" date cu privire la acestea. Anexa II punctul III.9.a.11 menționează numai date care sunt „transferate" sau „accesate". Chiar dacă se pare că, în cele mai multe dintre cazurile respective, intenția nu este de a limita domeniul de aplicare a principiilor sau de a crea lacune în materie de protecție, terminologia inconsecventă implică riscul de a crea astfel de lacune. Dat fiind că termenul „prelucrare" este definit în cadrul principiilor, este esențial ca acesta să fie utilizat într-un mod coerent pentru a evita lacunele existente în prezent. În caz contrar, ar exista probabil prea mult loc pentru interpretări nedorite, care ar putea conduce la o interpretare greșită a textului deciziei.

[11] Definiția „datelor cu caracter personal" inclusă în anexa II punctul I.8.a se referă la „informațiile referitoare la o persoană fizică identificată sau identificabilă". Cu toate acestea, principiul suplimentar arată că, în ceea ce privește datele privind resursele umane, principiile se aplică numai atunci când „dosarele identificate sunt transferate sau accesate". GL29 consideră că aceasta deschide posibilitatea de a prelucra datele cu caracter personal într-un mod care nu este în conformitate cu principiile de protecție a datelor prevăzute de legislația UE, nici cu definiția generală a datelor cu caracter personal în temeiul Scutului de confidențialitate.

este deosebit de important în ceea ce privește dreptul la căi de atac, inclusiv accesul la mecanismul Ombudsmanului. În plus, decizia privind caracterul adecvat ar trebui să abordeze chestiunea măsurii în care Scutul de confidențialitate se va aplica, de asemenea, cetățenilor/rezidenților țărilor din SEE și Elveția, care în trecut au beneficiat de acoperirea oferită de programul privind sfera de siguranță.

1.2.3 Revizuire comună și suspendare

GL29 salută faptul că administrația SUA și Comisia Europeană au convenit să revizuiască în mod regulat aplicarea practică a Scutului de confidențialitate. O astfel de revizuire comună este o practică cunoscută de un număr de ani în comunitatea UE de protecție a datelor, în special în ceea ce privește acordurile privind schimbul de date PNR cu țări terțe și acordul TFTP. În plus, GL29 salută faptul că un număr nedeterminat de reprezentanți ai autorităților de protecție a datelor pot lua parte la revizuirile comune.

Având în vedere experiența sa în ceea ce privește revizuirile comune din ultimii ani, GL29 dorește să clarifice că se așteaptă ca revizuirea comună a Scutului de confidențialitate să fie mai amplă decât revizuirile comune cu privire la PNR și TFTP. În special, este de dorit ca revizuirea comună să includă nu numai reuniuni cu reprezentanți ai agențiilor, organizațiilor și întreprinderilor din SUA, ci și verificări la fața locului privind anumite elemente ale Scutului de confidențialitate. Reprezentanții autorităților pentru protecția datelor la revizuirea comună ar trebui să poată prezenta sugestii pentru astfel de verificări la fața locului.

GL29 consideră că o revizuire comună necesită o evaluare comună a constatărilor. Până în prezent, rezultatele revizuirilor comune au fost prezentate într-un document de lucru al serviciilor Comisiei, pentru care nu este necesară aprobarea din partea membrilor echipei de revizuire comună din afara Comisiei. Pentru revizuirea comună a Scutului de confidențialitate, GL29 ar aprecia dacă constatările raportului ar putea, într-adevăr, să fie un produs comun. În mod alternativ, s-ar putea lua în considerare publicarea unui raport separat de revizuire comună al autorităților pentru protecția datelor.

În sfârșit, în ceea ce privește revizuirea comună, GL29 reamintește promisiunea Comisiei că respectivele costuri suportate de reprezentanții GL29 în cursul revizuirilor comune sunt rambursate de către Comisie. Grupul de lucru presupune că aceasta se va aplica, de asemenea, revizuirii comune a Scutului de confidențialitate, în orice caz pentru un număr rezonabil de reprezentanți ai autorităților pentru protecția datelor.

GL29 recomandă ca, cel târziu cu trei luni înainte să aibă loc prima revizuire comună a Scutului de confidențialitate, modalitățile de revizuire comună să fie convenite între Comisie, administrația SUA și GL29 și să fie consemnate în scris.

1.2.4 Cadrul juridic al UE în curs de revizuire

Decizia privind caracterul adecvat al Scutului de confidențialitate este prima decizie privind caracterul adecvat care a fost elaborată după acordul de principiu cu privire la textul Regulamentului general privind protecția datelor. Cu toate acestea, GL29 a constatat că Scutul

de confidențialitate nu reflectă deocamdată situația viitoare. De exemplu, noi noțiuni importante precum dreptul la portabilitatea datelor și obligațiile suplimentare pentru operatorii de date, inclusiv necesitatea de a efectua studii de impact privind protecția datelor, precum și respectarea principiilor privind luarea în considerare a vieții private începând cu momentul conceperii și confidențialitatea implicită nu au fost incluse în Scutul de confidențialitate. Prin urmare, GL29 ar dori să sugereze ca Scutul de confidențialitate, precum și oricare dintre deciziile privind caracterul adecvat, să fie revizuit la scurt timp după intrarea în vigoare a Regulamentului general privind protecția datelor. Ar fi binevenită o trimitere explicită la acest proces de revizuire în textul final al deciziei privind caracterul adecvat.

2. EVALUAREA PĂRȚII COMERCIALE DIN PROIECTUL DE DECIZIE PRIVIND CARACTERUL ADECVAT

2.1 Observații generale

2.1.1 Îmbunătățiri

GL29 salută îmbunătățirile aduse de Scutul de confidențialitate și dorința negociatorilor săi de a încerca să abordeze deficiențele programului privind sfera de siguranță pe care acesta le-a subliniat. În special, spre deosebire de programul privind sfera de siguranță, se pot observa îmbunătățiri cu privire la următoarele elemente: introducerea unor definiții-cheie pentru, de exemplu, „date cu caracter personal”, „prelucrare” și „operator”, mecanismele instituite pentru a asigura supravegherea Scutului de confidențialitate și revizuirile interne sau externe ale conformității care sunt în prezent obligatorii. De asemenea, s-au adus îmbunătățiri principiului accesului și GL29 observă că, în prezent, sunt asigurate drepturile de corectare și de ștergere atunci când datele sunt utilizate într-un mod incompatibil cu principiile Scutului de confidențialitate. În plus, în prezent este clarificat faptul că persoana în cauză trebuie să primească atât confirmarea faptului că sunt prelucrate date care o privesc, cât și comunicarea datelor prelucrate.

De asemenea, GL29 salută consolidarea garanțiilor juridice în cazul în care au loc transferuri ulterioare, precum și angajamentele Departamentului Comerțului și ale Comisiei Federale pentru Comerț (FTC) în vederea punerii în aplicare a obligațiilor stabilite de Scutul de confidențialitate.

2.1.2 Aplicarea Scutului de confidențialitate în cazul organizațiilor care acționează în calitate de persoană împuternicită de către operator (agent)

Măsura în care principiile Scutului de confidențialitate se aplică organizațiilor certificate care primesc date cu caracter personal din Uniunea Europeană doar pentru prelucrare (denumite în continuare „agenți” sau „persoane împuternicite de către operator”) rămâne din păcate neclară. Deși dispozițiile din cadrul anexei II punctul III.10.a. menționează transferurile de date către organizațiile autorizate în acest scop – și anume, menționând cerința de a încheia un contract – acestea nu oferă niciun indiciu privind modul în care principiile Scutului de confidențialitate se aplică persoanelor împuternicite de către operator (agenților). Acest fapt cauzează incertitudine atât pentru organizațiile din Statele Unite ale Americii care primesc

date certificate pentru prelucrare și pentru întreprinderile din UE care efectuează transferurile de date către organizațiile autorizate în calitate de persoană împuternicită de către operator, cât și pentru persoanele ale căror date sunt prelucrate. În consecință, este dificil să se determine obligațiile care se aplică efectiv organizațiilor parte la Scutul de confidențialitate care prelucrează datele cu caracter personal primite din UE în rolul lor de persoane împuternicite de către operatori. Prin urmare, clarificarea este, cu siguranță, necesară.

Trebuie să se țină seama de faptul că mai multe dintre obligațiile cuprinse în principii nu sunt adecvate pentru persoanele împuternicite de către operatorul de date, întrucât operatorul de date este cel care stabilește întotdeauna scopurile și mijloacele de prelucrare a datelor (a se vedea definiția termenului „operator” din anexa II punctul I.8.c). Acesta este motivul pentru care unele dintre obligațiile cuprinse în principii, dacă se aplică unei organizații care acționează în calitate de agent, pot fi în contradicție cu contractul de prelucrare a datelor solicitat în temeiul dreptului UE (contractul menționat în anexa II punctul III.10.a.). De exemplu, un contract de prelucrare a datelor, în general, nu va autoriza persoana împuternicită de către operator (agent) pentru transferuri ulterioare de date către un operator terț, inclusiv în circumstanțele menționate în anexa II punctul II.3.a. Transferurile ulterioare către agenți terți nu ar trebui să fie autorizate decât după aprobarea prealabilă a operatorului de date. În plus, în conformitate cu cerințele dreptului Uniunii, o persoană împuternicită de către operator (agent) nu va fi în măsură să ofere persoanelor notificarea deplină astfel cum urmărește principiul notificării (anexa II punctul II.1), de exemplu, pentru că organizația respectivă nu determină scopurile prelucrării.

Prin urmare, este esențial să se clarifice în cadrul principiilor că, în cazul unei astfel de contradicții, dispozițiile contractului de prelucrare a datelor și, în special, instrucțiunile organizației care transferă date din UE vor avea prioritate. Fără această clarificare, principiile ar putea fi interpretate și aplicate într-un mod care oferă prea multe capacități de control agentului Scutului de confidențialitate, iar acest lucru ar putea genera riscul ca exportatorul de date din UE să încalce obligațiile care îi revin în calitate de operator de date în conformitate cu legislația UE privind protecția datelor și care se aplică atunci când transferă date către o organizație parte la Scutul de confidențialitate care acționează ca agent. În plus, această lipsă de claritate creează impresia că persoana împuternicită de către operator ar putea reutiliza datele după cum dorește.

În plus, ar trebui să se prevadă norme specifice în cazul în care o organizație acționează în calitate de persoană împuternicită de către operator (agent), pentru a se asigura că organizația respectivă respectă instrucțiunile operatorului de date. Ar trebui să se clarifice faptul că organizațiile din Statele Unite ale Americii care primesc date pentru prelucrare nu pot decide să prelucreze datele în nume propriu. În absența unor norme specifice aplicabile organizațiilor care acționează în calitate de persoană împuternicită de către operator, este dificil să se determine normele în raport cu care persoana împuternicită de operator (agenți) ar putea să se autocertifice.

2.1.3 Limitările dreptului de a adera la principii

Anexa II punctul I.5 prevede, printre altele, derogări de la principii în cazul în care datele care intră sub incidența Scutului de confidențialitate sunt utilizate din motive care țin de securitatea națională[12], interesul public, aplicarea legii sau în baza textelor legislative, a regulamentelor administrative sau a jurisprudenței care creează obligații contradictorii sau prevăd autorizații exprese. Fără o cunoaștere deplină a legislației SUA, atât la nivel federal, cât și la nivel de stat, este dificil ca GL29 să evalueze domeniul de aplicare a acestei scutiri și să analizeze dacă astfel de limitări sunt justificate într-o societate democratică. De asemenea, este esențial ca, în proiectul său de decizie privind caracterul adecvat, Comisia Europeană să includă o analiză a nivelului de protecție în cazul în care se vor aplica derogările respective. GL29 solicită Comisiei să se asigure că UE este informată cu privire la orice texte legislative sau regulamente administrative care ar afecta aderarea la principii, fie aplicabile în prezent sau în momentul în care noi texte legislative sau regulamente intră în vigoare în SUA.

2.1.4 Lipsa unui principiu al limitării privind păstrarea datelor

Principiul limitării privind păstrarea datelor [articolul 6 alineatul (1) din directivă] este un principiu fundamental în dreptul UE privind protecția datelor care impune ca datele cu caracter personal să fie păstrate numai atât timp cât este necesar pentru atingerea scopului pentru care au fost colectate datele sau pentru care acestea sunt prelucrate ulterior.

Cu toate acestea, GL29 nu poate găsi în documentele care constituie Scutul de confidențialitate nicio trimitere la necesitatea ca operatorii de date să se asigure că datele sunt șterse de îndată ce scopul pentru care au fost colectate sau pentru care sunt prelucrate ulterior nu mai este valabil. Prin urmare, după cum se pare, principiile nu impun organizațiilor autorizate o limită pentru perioada de păstrare a datelor comparabilă cu cea impusă de principiul limitării privind păstrarea datelor în temeiul legislației UE.

Textul principiului privind integritatea datelor și limitarea scopului (anexa II punctul II.5) nu poate fi considerat în niciun caz ca impunând unei organizații care acționează în calitate de operator obligația de a șterge datele după ce nu mai sunt necesare pentru scopurile pentru care acestea au fost colectate sau prelucrate ulterior, sau ca impunând unei organizații care acționează în calitate de persoană împuternicită de către operator obligația de a șterge datele după încetarea contractului de servicii.

Grupul de lucru subliniază că lipsa unor dispoziții care impun o limită pentru păstrarea datelor în cadrul Scutului de confidențialitate oferă organizațiilor posibilitatea de a păstra datele atât timp cât doresc, inclusiv după ce au părăsit Scutul de confidențialitate, ceea ce nu este în conformitate cu principiul esențial al limitării privind păstrarea datelor.

[12] A se vedea capitolul 3 pentru mai multe observații cu privire la utilizarea datelor cu caracter personal acoperite de Scutul de confidențialitate în scopuri legate de securitate națională și capitolul 4 în scopul aplicării legii.

2.1.5 Lipsa unor garanții pentru deciziile automate care produc efecte juridice sau care afectează în mod semnificativ persoana

Scutul de confidențialitate nu oferă nicio garanție juridică în cazul în care persoanele fac obiectul unei decizii care produce efecte juridice în ceea ce le privește sau care le afectează în mod semnificativ și care se bazează exclusiv pe prelucrarea automată a datelor menită să evalueze anumite aspecte personale referitoare la acestea, cum ar fi randamentul lor profesional, solvabilitatea, încrederea, conduita etc.

Necesitatea de a institui garanții juridice pentru deciziile automate (care produc efecte juridice sau care afectează în mod semnificativ persoana) cu scopul de a asigura un nivel adecvat de protecție a fost deja subliniată de către GL29 în documentul său de lucru 12.

Această necesitate devine și mai stringentă deoarece noile tehnologii în continuă dezvoltare permit unui număr mai mare de întreprinderi să ia în considerare punerea în aplicare a sistemelor de luare de decizii automate, ceea ce poate conduce la slăbirea poziției persoanelor rămase nicio cale de atac împotriva unor decizii luate de calculator. În cazul în care deciziile adoptate exclusiv de sisteme automate produc efecte asupra situației juridice a persoanelor sau o afectează în mod semnificativ (de exemplu, prin înscrierea pe o listă neagră și, în consecință, lipsirea persoanelor de drepturile lor), este esențial să se ofere suficiente garanții care să includă dreptul de a cunoaște logica implicată și de a solicita reexaminarea în mod neautomatizat.

2.1.6 Perioada intermediară pentru relațiile comerciale existente

Scutul de confidențialitate prevede că principiile se aplică imediat după certificare. Cu toate acestea, organizațiile care se certifică în primele două luni după data efectivă de intrare în vigoare a cadrului Scutului de confidențialitate trebuie să aducă orice relații comerciale cu terți în conformitate cu principiul responsabilității pentru transferul ulterior, cât mai curând posibil. În orice caz, acestea trebuie să facă acest lucru în termen de cel mult nouă luni de la data la care se certifică în cadrul Scutului de confidențialitate.

Acest lucru înseamnă că, în măsura necesară, contractele existente trebuie să fie aduse în conformitate cu principiile într-o perioadă între două și nouă luni de la certificare. În această perioadă intermediară, notificarea și opțiunea sunt suficiente. GL29 insistă asupra faptului că transferurile pot avea loc în temeiul Scutului de confidențialitate numai din momentul în care organizația poate respecta pe deplin toate cerințele Scutului de confidențialitate. Nu se poate considera că posibilitatea de a transmite date în timpul unei perioade intermediare, fără ca beneficiarul să fie în măsură să respecte pe deplin principiile Scutului de confidențialitate, îndeplinește condițiile unui transfer legal, prin urmare, aceasta nu este acceptabilă.

2.2 Observații specifice

2.2.1 Transparență

a) Observații generale privind notificarea

GL29 salută cerințele mai cuprinzătoare și mai detaliate stabilite în cadrul principiului notificării, în special faptul că notificarea va trebui să includă un link sau o adresă internet a Scutului de confidențialitate și să se refere la dreptul de acces al persoanelor, precum și la mecanismele alternative de soluționare a litigiilor[13]. Cu toate acestea, GL29 recomandă ca acestea să fie mai explicite cu privire la alte drepturi vizate (de a corecta și de a șterge datele atunci când acestea sunt inexacte sau sunt prelucrate cu încălcarea principiilor).

Documentele care constituie Scutul de confidențialitate nu ridică semne de întrebare cu privire la momentul în care o organizație parte la Scutul de confidențialitate trebuie să asigure notificarea unei persoane. Anexa II punctul II.1.b prevede că „notificarea trebuie să fie formulată (...) atunci când persoanele sunt invitate pentru prima dată să furnizeze informații cu caracter personal sau cât mai curând posibil după această invitație, dar, în orice caz, înainte ca datele să fie folosite într-un scop diferit de cel pentru care au fost inițial colectate sau prelucrate de organizația care a efectuat transferul sau înainte să fie comunicate pentru prima dată unui terț". GL29 consideră că, în multe situații, o organizație din SUA parte la Scutul de confidențialitate nu va colecta în mod direct date de la persoana vizată și, prin urmare, momentul notificării ar trebui să fie punctul la care datele sunt înregistrate de organizația parte la Scutul de confidențialitate.

GL29 remarcă faptul că punerea efectivă în aplicare a cerințelor cu privire la principiul notificării și a politicii de confidențialitate ar trebui evaluată în prima revizuire anuală a Scutului de confidențialitate.

b) Disponibilitatea publică a politicii de confidențialitate

GL29 salută prevederea explicită în prezent a faptului că Departamentul Comerțului va verifica dacă societățile care au site-uri internet publice și-au publicat politicile de confidențialitate pe site sau, dacă nu au site-uri internet publice, locul în care politica de confidențialitate este pusă la dispoziția publicului[14].

c) Publicarea condițiilor de confidențialitate din contractele cu persoanele împuternicite de operator

Scutul de confidențialitate prevede, printre condițiile în care organizațiile parte la Scutul de confidențialitate pot transfera date unei persoane împuternicite de operator (agent), obligația organizațiilor autocertificate de a „furniza Departamentului, la cerere, un rezumat sau o copie reprezentativă a dispozițiilor de confidențialitate relevante ale contractului cu agentul respectiv" (a se vedea anexa II punctul II. 3.b.v). Grupul de lucru salută această cerință de transparență față de Departamentul Comerțului.

[13] Anexa II punctul II.1; GL29 face trimitere, de asemenea, la cea de a doua recomandare a Comisiei formulată în Comunicarea COM(2103)847, precum și la scrisoarea GL29 către vicepreședintele Reding din 10 aprilie 2014, în special punctul 4 din secțiunea „Transparență".

[14] A se vedea prima recomandare formulată de Comisia Europeană în comunicarea sa COM(2013)847 și scrisoarea GL29 adresată doamnei vicepreședinte Reding, la 10 aprilie 2014, în special punctul 3 din secțiunea „Transparență".

2.2.2 Opțiune

Scutul de confidențialitate prevede un drept de a refuza divulgarea informațiilor cu caracter personal unui terț sau utilizarea informațiilor cu caracter personal într-un scop care diferă în mod semnificativ[15] (anexa II punctul III.2). În plus, persoanele au dreptul de a refuza (opt-out) utilizarea informațiilor cu caracter personal în scopuri de marketing direct în orice moment (anexa II punctul III.12.a)[16].

Cu excepția cazului privind scopurile de marketing direct, nu se oferă niciun detaliu cu privire la modul și momentul în care se poate exercita acest refuz. GL29 consideră că simpla trimitere la existența acestui drept în politica de confidențialitate nu poate fi suficientă, ci ar trebui să se ofere o posibilitate *individualizată* de a exercita acest drept *înainte* de divulgarea sau reutilizarea informațiilor cu caracter personal.

În plus, GL29 subliniază că, în cadrul Scutului de confidențialitate, ar trebui să se prevadă un drept general de opoziție (din motive întemeiate legate de situația persoanei vizate), acesta fiind înțeles ca un drept de a solicita încetarea prelucrării datelor în cazul în care o persoană are motive întemeiate și legitime legate de situația sa particulară[17]. GL29 recomandă cu fermitate ca proiectul de decizie privind caracterul adecvat să clarifice faptul că dreptul de opoziție ar trebui să existe în orice moment, precum și că această obiecție nu este limitată la utilizarea datelor în scopuri de marketing direct[18].

GL29 consideră că lipsa unei definiții a ceea ce se consideră a fi un scop „care diferă în mod semnificativ" va conduce la confuzie și incertitudine juridică. Ar trebui să se clarifice faptul că, în orice caz, principiul opțiunii nu poate fi utilizat pentru a eluda principiul limitării scopului[19]. Opțiunea ar trebui să se aplice numai în cazul în care obiectivul diferă în mod semnificativ, dar este în continuare compatibil, întrucât prelucrarea în scopuri incompatibile este interzisă (anexa II punctul II.5.a). Trebuie clarificat faptul că dreptul de a refuza nu poate permite organizației să utilizeze date în scopuri incompatibile. Prin urmare, se recomandă armonizarea formulării aferente, prin utilizarea unei formulări unice și definite (de exemplu „scop care diferă în mod semnificativ, dar, cu toate acestea, compatibil").

Ar fi utile clarificări în ceea ce privește cazurile în care o decizie luată de a prelucra date în alt scop sau de a divulga informații intră sub incidența dreptului Uniunii. În această situație, condițiile juridice obișnuite ale UE cu privire la acest tip de prelucrare (de exemplu, interzicerea prelucrării datelor în scopuri incompatibile, prevederea unui motiv legitim pentru prelucrare și necesitatea de a informa persoana) se vor aplica direct, inclusiv organizației din SUA care intră în domeniul de aplicare a legislației UE. În practică, aceasta înseamnă că

[15] Principiul suplimentar 14.c.I prevede dreptul de a se retrage dintr-un studiu clinic, care ar putea fi considerat ca fiind dreptul de a se opune sau de a-și retrage consimțământul.
[16] Acesta este identic cu ceea ce se prevedea în programul privind sfera de siguranță (întrebarea frecventă nr. 12) și nu s-a făcut nicio modificare în această privință.

[18] A se vedea scrisoarea GL29 către vicepreședintele Reding, secțiunea „Opțiune".
[19] Un exemplu concret de prelucrare incompatibilă ulterioară autorizată în conformitate cu principiul opțiunii este oferit în cadrul principiului suplimentar 9.b.i (a se vedea observația GL29 cu privire la aceasta, la punctul referitor la „datele privind resursele umane").

rămâne la latitudinea exportatorului din UE să ia o astfel de decizie pentru a asigura transparența și legalitatea prelucrării datelor în conformitate cu legislația UE. Prin urmare, principiul opțiunii se va aplica doar în cazul în care decizia este luată exclusiv de către organizația din SUA parte la Scutul de confidențialitate care nu este supusă dreptului UE.

2.2.3 Transferurile ulterioare

a) Domeniul de aplicare

GL29 este preocupat de situația în care transferurile ulterioare de date cu caracter personal sunt efectuate de la o organizație certificată parte la Scutul de confidențialitate din SUA către un beneficiar dintr-o țară terță.

Scutul de confidențialitate nu ar trebui considerat doar ca un instrument pentru transferul de date din UE către SUA, ci va servi, de asemenea, ca instrument care să fie utilizat pentru transferul de date din SUA către țări terțe. Dispozițiile privind transferurile ulterioare reprezintă, prin urmare, un element important al Scutului de confidențialitate, care ar trebui să ofere garanții suficiente și un nivel corespunzător de protecție atunci când datele sunt transferate ulterior în afara SUA. O problemă anume este legată de securitatea națională și aplicarea legii.

Principiul responsabilității pentru transferurile ulterioare în temeiul Scutului de confidențialitate nu se limitează la operatorii de date beneficiari, persoanele împuternicite de operator sau agenții stabiliți în SUA. Prin urmare, transferurile de date către o țară terță pot avea loc în temeiul Scutului de confidențialitate chiar dacă țara terță are legi care prevăd accesul public la datele cu caracter personal, de exemplu în scopuri de supraveghere. Aceasta pune datele UE în pericol de interferențe nejustificate în ceea ce privește protecția drepturilor fundamentale.

În cazul unui transfer ulterior către o țară terță, fiecare organizație parte la Scutul de confidențialitate ar trebui să fie obligată să evalueze cerințele obligatorii din legislația națională a țării terțe aplicabile importatorului de date înainte de efectuarea transferului. În cazul în care este identificat un risc de efect advers considerabil asupra garanțiilor, obligațiilor și nivelului de protecție oferit de Scutul de confidențialitate, organizația din SUA parte la Scutul de confidențialitate care acționează în calitate de persoană împuternicită de operator (agent) notifică de îndată operatorul de date din UE înainte de efectuarea oricărui transfer ulterior. În acest caz, exportatorul de date are dreptul să suspende transferul de date și/sau să rezilieze contractul. În cazul în care există un astfel de risc de efecte negative semnificative, o organizație parte la Scutul de confidențialitate care acționează ca operator nu ar trebui să fie autorizată să efectueze transferuri ulterioare de date, întrucât acest lucru ar compromite obligația sa de a oferi același nivel de protecție conform principiilor în cazul transferurilor ulterioare (a se vedea anexa II punctul II.3.a).

În mod similar, în cazul unei modificări în legislația țării terțe care ar putea avea un efect negativ considerabil asupra garanțiilor, obligațiilor și nivelului de protecție oferit de Scutul de

confidențialitate, organizația din SUA parte la Scutul de confidențialitate care acționează ca persoană împuternicită de operator (agent) ar trebui să aibă obligația – în temeiul Scutului de confidențialitate – să notifice fără întârziere modificarea către exportatorul de date, de îndată ce are cunoștință de aceasta, caz în care exportatorul de date are dreptul să suspende transferul de date și/sau să rezilieze contractul. Prin urmare, într-un asemenea caz, o organizație parte la Scutul de confidențialitate care acționează ca operator nu ar trebui să aibă permisiunea de a efectua transferuri ulterioare, întrucât aceasta are datoria de a oferi același nivel de protecție conform principiilor (a se vedea anexa II punctul II.3.a).

GL29 reamintește poziția sa conform căreia, dacă operatorul de date din UE are cunoștință de un transfer ulterior către un terț în afara SUA, chiar înainte ca transferul să aibă loc în SUA sau dacă operatorul de date din UE este responsabil în solidar pentru decizia de a permite transferurile ulterioare, transferul ar trebui considerat un transfer direct din UE către țara terță din afara SUA. Aceasta înseamnă că articolele 25 și 26 din directivă sunt aplicabile transferului, în loc de principiul transferului ulterior în temeiul Scutului de confidențialitate.

b) Transferuri de la o organizație parte la Scutul de confidențialitate către un operator terț

GL29 salută obligația de a încheia contracte (anexa II punctul II.3.a) pentru a se asigura că un operator terț va oferi cel puțin același nivel de protecție a confidențialității cu cel impus de principiile Scutului de confidențialitate. Obiectivul este de a se asigura că datele cu caracter personal sunt protejate în mod adecvat, inclusiv după ce au fost transmise mai departe. Cu toate acestea, GL29 are o serie de observații privind condițiile propuse.

Lipsa trimiterilor la principiul limitării scopului

GL29 recomandă, de asemenea, introducerea unei trimiteri explicite la principiul limitării scopului (anexa II punctul II.5) în condițiile pentru transferurile ulterioare către un operator terț (anexa II punctul II.3.a). Acest lucru ar clarifica faptul că transferurile ulterioare nu pot avea loc în cazul în care operatorul terț va prelucra date în scopuri incompatibile.

Scutire de la necesitatea contractului pentru transferuri intragrup între operatori

O scutire de la necesitatea contractului este prevăzută pentru transferurile intragrup între operatori. Într-o astfel de situație, principiile prevăd că regulile corporatiste obligatorii (Binding Corporate Rules — BCR) sau „alte instrumente intragrup (de exemplu, programe de conformitate și de control)" ar putea asigura continuitatea protecției (anexa II III. 10.c). GL29 consideră că referirea la „alte instrumente intragrup" nu garantează angajamente obligatorii din punct de vedere juridic făcute de ceilalți membri ai grupului. Întrucât GL29 și legislația UE[20] favorizează, în general, angajamentele cu caracter obligatoriu pentru încadrarea transferurilor intragrup, este important să se evite ca Scutul de confidențialitate să fie utilizat într-un mod care să eludeze această cerință. GL29 subliniază că, în orice caz, transferurile ulterioare de date din SUA către țări terțe planificate chiar și înainte să aibă loc transferul

[20] Necesitatea unor angajamente cu caracter obligatoriu și executoriu este subliniată, de asemenea, în Regulamentul general privind protecția datelor, indiferent de instrumentul utilizat (reguli corporatiste obligatorii, clauze contractuale, coduri de conduită și certificare).

către SUA sau care fac obiectul unui control exercitat în comun cu operatorul de date din UE[21] trebuie să fie considerate ca un transfer direct din UE către țări terțe în afara SUA. Prin urmare, articolele 25 și 26 din directivă sunt aplicabile transferului.

c) Transferurile de la o organizație parte la Scutul de confidențialitate către o persoană terță împuternicită de operator (agent)

GL29 salută faptul că, în prezent, este obligatoriu un contract pentru transferurile ulterioare pentru entitățile beneficiare care acționează în calitate de persoane împuternicite de operator (agenți), indiferent de participarea lor la Scutul de confidențialitate sau dacă beneficiază de o altă soluție de constatare a caracterului adecvat. De asemenea, GL29 salută garanțiile suplimentare care reglementează astfel de transferuri ulterioare (anexa II punctele II.3.a.i; II.3.a.iii; II.3.a.iv; II.3.a.v; II.7.d). Ultimul punct (anexa II punctul II.7.d) se referă la obligația de a rămâne răspunzător atunci când datele sunt comunicate unui agent. Cu toate acestea, se pare că această garanție nu se aplică în cazul în care o organizație a ales să coopereze cu o autoritate pentru protecția datelor (a se vedea anexa II partea III.5.a in fine). GL29 nu înțelege motivul pentru o astfel de exceptare și consideră că responsabilitatea ar trebui să se aplice inclusiv în acest caz.

Lipsa trimiterilor la principiul limitării scopului

GL29 remarcă faptul că principiul responsabilității pentru transferurile ulterioare (anexa II punctul II.3) explică faptul că datele cu caracter personal pot fi transferate către un terț care acționează ca agent exclusiv în scopuri specificate și limitate, dar nu menționează în mod explicit că aceste scopuri specificate și limitate trebuie să fie compatibile cu scopurile inițiale pentru care au fost colectate datele, precum și cu instrucțiunile operatorului. Este nevoie de mai multă claritate în această privință. Prin urmare, GL29 recomandă să se asigure că decizia privind caracterul adecvat oferă mai multe detalii, de exemplu prin introducerea unei trimiteri clare la principiul limitării scopului (anexa II punctul II.5), conform căruia datele nu pot fi prelucrate (inclusiv divulgate) în scopuri incompatibile în cadrul principiului transferurilor ulterioare (în plus față de principiul „opt-out").

Necesitatea unui număr mai mare de obligații suplimentare pentru organizațiile parte la Scutul de confidențialitate care acționează în calitate de persoană împuternicită de către operator (agent) care transferă ulterior datele către o altă persoană împuternicită de către operator (agent)

Absența unor norme clare pentru cazul în care organizația parte la Scutul de confidențialitate acționează ca agent (și anume, în numele unui operator de date din UE) implică o lacună și ar putea împiedica operatorul din UE să păstreze controlul. O organizație parte la Scutul de confidențialitate care primește datele ca agent al unui operator de date din UE trebuie să respecte instrucțiunile operatorului din UE. Acest lucru ar trebui să fie menționat în mod expres în text pentru a se asigura că nerespectarea acestor instrucțiuni va conduce nu numai la

[21] De exemplu, în cazul datelor privind resursele umane.

o încălcare a contractului (anexa II punctul III.10.a.ii), ci și la o încălcare a principiilor Scutului de confidențialitate.

Posibilitatea ca o organizație parte la Scutul de confidențialitate care acționează ca agent să transfere ulterior date către un agent terț trebuie să fie comunicată în mod transparent operatorului și să facă obiectul aprobării prealabile a acestuia. Ar trebui specificat în mod clar că faptul dacă este permis un transfer ulterior este determinat de contractul semnat de agent cu operatorul UE (menționat la întrebarea frecventă nr. 10 drept „contractul de la articolul 17")[22].

Condițiile actuale aplicabile transferului ulterior către un agent se bazează pe presupunerea că organizația parte la Scutul de confidențialitate acționează în calitate de operator de date și, prin urmare, poate decide singură cu privire la o eventuală intervenție a unui agent terț. Cu toate acestea, acest lucru nu ar trebui să fie posibil în cazul în care organizația parte la Scutul de confidențialitate acționează ca agent. În caz contrar, operatorul din UE va fi lipsit de capacitățile sale de control.

Dispozițiile relevante privind confidențialitatea ale contractului încheiat cu agentul terț trebuie să fie puse la dispoziția operatorului și trebuie, de asemenea, să ofere cel puțin același nivel de protecție precum cel asigurat de contractul încheiat cu operatorul.

2.2.4 Integritatea datelor și limitarea scopului

a) Proporționalitate

Cu privire la un punct de importanță minoră, GL29 face referire la scrisoarea adresată doamnei vicepreședinte Reding, în care a menționat că „o prelucrare a datelor cu caracter personal ar putea, chiar și cu respectarea strictă a principiilor notificării și opțiunii, să nu fie proporțională în ceea ce privește interesele, drepturile și libertățile persoanei vizate sau ale societății. Principiul proporționalității sau al caracterului rezonabil al cererii trebuie să fie respectat în toate etapele prelucrării și ar trebui să se aplice în plus față de principiile notificării și opțiunii"[23].

Scutul de confidențialitate (anexa II punctul II.5.a) prevede că informațiile trebuie să se limiteze la ceea ce este relevant pentru prelucrare. GL29 ar prefera ca această formulare să se modifice în decizia finală privind caracterul adecvat, din moment ce simplul fapt că datele sunt relevante pentru prelucrare nu este suficient pentru asigurarea unei prelucrări proporționale. Pentru a respecta principiul proporționalității, prelucrarea ar trebui limitată la datele care sunt necesare pentru prelucrarea în cauză.

b) Precizie

Principiul integrității datelor și limitării scopului (anexa II punctul II.5) prevede, de asemenea: „În limita acestor obiective, orice organizație trebuie să ia măsurile necesare pentru a asigura

[22] A se vedea scrisoarea GL29 adresată doamnei vicepreședinte Reding, 10 aprilie 2014, punctul 4 din secțiunea „Transfer ulterior".
[23] A se vedea scrisoarea GL29 adresată doamnei vicepreședinte Reding, 10 aprilie 2014, p. 8.

fiabilitatea datelor în raport cu utilizarea prevăzută, precum și acuratețea, exhaustivitatea și actualitatea acestora". GL29 observă că este utilizată exact aceeași formulare precum cea din acordul privind sfera de siguranță. GL29 are îndoieli că formularea „în limita acestor obiective" ar trebui să fie inclusă, întrucât, în opinia sa, acuratețea datelor nu ar trebui să depindă de scopul prelucrării. GL29 ar prefera ca această conexiune să nu fie inclusă în decizia finală privind caracterul adecvat.

c) Limitarea scopului

În cazul în care datele cu caracter personal sunt transferate către o organizație din SUA de un operator de date stabilit în UE, exportatorul de date informează în mod explicit organizația din SUA cu privire la scopurile pentru care au fost colectate inițial datele. Acest lucru este esențial pentru a determina dacă, după transfer, intervine o modificare a scopului, determinând astfel principiile notificării și opțiunii și ar contribui, de asemenea, la alocarea riscului și a responsabilității.

Principiul integrității datelor și limitării scopului (anexa II punctul II.5) prevede că o organizație nu poate prelucra date cu caracter personal într-un mod incompatibil cu scopul pentru care acestea au fost colectate sau cu scopurile aprobate ulterior de persoana în cauză. Cu toate acestea, principiul opțiunii (anexa II punctul II.2) prevede un sistem de consimțământ pentru „utilizarea" informațiilor sensibile (și anume, informațiile cu caracter personal privind situația medicală sau starea de sănătate, originea rasială sau etnică, opiniile politice, convingerile religioase sau filozofice, apartenența la sindicate sau date care descriu viața sexuală a persoanei respective, precum și datele privind cazierele judiciare) în scopuri care sunt semnificativ diferite de scopurile pentru care datele au fost colectate inițial sau de scopurile aprobate ulterior de persoana în cauză. Acest consimțământ nu este necesar în situațiile menționate în principiul suplimentar 1.a (anexa II punctul III.1.a). În ceea ce privește informațiile cu caracter personal nesensibile, sistemul prevede un regim de excludere voluntară.

GL29 remarcă faptul că domeniul de aplicare a principiului limitării scopului este diferit în cadrul principiilor notificării, opțiunii și integrității datelor și limitării scopului. Astfel, termenii „scop incompatibil" și „scop care diferă în mod semnificativ" sunt utilizați în același text fără o definiție clară a celor două noțiuni[24].

GL29 are motive serioase de preocupare cu privire la faptul că astfel de neconcordanțe ar putea da naștere unor mari dificultăți în reconcilierea principiului integrității datelor și limitării scopului (anexa II punctul II.5) cu principiul opțiunii (anexa II punctul II.2), întrucât unul prevede că datele nu pot fi prelucrate într-o manieră incompatibilă cu scopurile pentru care au fost colectate, în timp ce celălalt prevede un mecanism de tip opt-out în cazul în care datele sunt prelucrate într-un scop care diferă în mod semnificativ de scopul inițial.

[24] GL29 remarcă faptul că sunt utilizate și alte expresii: „o utilizare care nu este în concordanță cu" (anexa II punctul III.14.b.ii), o „utilizare în alte scopuri" (anexa II punctul III. 9.B.i), o „utilizare în alte scopuri decât cele pentru care au fost colectate inițial" (anexa II punctul II.1.b). Această neclaritate poate conduce la absența unor garanții suficiente în ceea ce privește principiul limitării scopului.

Prin urmare, principiul opțiunii poate fi interpretat în sensul că acesta autorizează o prelucrare incompatibilă ulterioară[25]. În opinia GL29, trebuie să se menționeze în mod explicit că o organizație nu este autorizată să prelucreze datele într-un scop care diferă în mod semnificativ, în cazul în care acest scop este incompatibil cu principiul limitării scopului. Cu alte cuvinte, trebuie să fie clar că principiul opțiunii nu constituie o derogare de la principiul limitării scopului.

În orice caz, dacă prelucrarea ulterioară poate fi considerată compatibilă, atunci ar trebui să se aplice, de asemenea, principiile notificării și opțiunii.

2.2.5 Excepțiile jurnalistice

Excepțiile jurnalistice privind prelucrarea datelor cu caracter personal sunt reglementate de principiul suplimentar 2 (anexa II punctul III.2). Este de la sine înțeles că aceste dispoziții reflectă protecția constituțională în SUA a libertății de exprimare. Astfel, documentele Scutului de confidențialitate prevăd că „informațiile care au fost publicate anterior și apoi arhivate nu sunt supuse principiilor Scutului de confidențialitate" (anexa II punctul III.2.b). Această excepție pare să includă orice prelucrare ulterioară de către orice operator sau persoană împuternicită de acesta, și anume nu se limitează la prelucrarea în continuare în scopuri jurnalistice. Astfel cum s-a afirmat deja în scrisoarea adresată vicepreședintelui Reding din 10 aprilie 2014, GL29 ar fi preferat o abordare mai limitată a excepțiilor jurnalistice, în conformitate cu principiul, astfel cum este aplicat în UE, precum și cu dreptul la scoaterea de pe listă în urma cauzei Google Spania[26].

2.2.5 Dreptul de acces, de rectificare și de ștergere a datelor pentru persoanele vizate

În conformitate cu Scutul de confidențialitate, persoanele fizice au dreptul de a obține *confirmarea* faptului dacă datele lor sunt prelucrate de către organizație, precum și dreptul *să le fie comunicate* aceste date (anexa II punctul III.8.a.i). Cu toate acestea, este destul de slabă obligația organizațiilor de a răspunde cererilor din partea persoanelor fizice în ceea ce privește scopurile prelucrării, categoriile de date cu caracter personal vizate și beneficiarii sau categoriile de beneficiari cărora le sunt divulgate datele cu caracter personal. GL29 consideră că detaliile care trebuie furnizate persoanelor vizate ar trebui să fie menționate în corpul textului, nu doar într-o notă de subsol și trebuie să fie formulate ca o obligație clară (în legătură cu anexa II punctul iii.8.a.i.1).

În conformitate cu principiul suplimentar 8, „accesul trebuie furnizat numai în măsura în care organizația stochează informațiile cu caracter personal" (anexa II III.8.d.ii). Această normă nu trebuie interpretată în mod restrictiv, în sensul că accesul trebuie să fie furnizat, în principiu, la datele prelucrate în orice alt mod de către o organizație, nu doar la datele stocate. Prin urmare, în scopul eficacității dreptului de acces, este important să se clarifice faptul că

[25] A se vedea, de asemenea, observația privind principiul opțiunii. GL29 consideră că faptul că normele referitoare la transferul ulterior (anexa II punctul II.3) se referă doar la principiul opțiunii și nu la principiul limitării scopului crește riscul unei astfel de înțelegeri.
[26] Cauza C-131/12 – Google Spania/Agencia Española de Protección de Datos și Mario Costeja González, 13 mai 2014.

„stochează” înseamnă „prelucrează” în sensul definiției prevăzute în anexa II punctul I.8.b. Aplicarea acestei norme ar trebui să fie examinată cu atenție în cursul revizuirii comune a Scutului de confidențialitate.

Persistă preocupări cu privire la lista excepțiilor prevăzute în anexa II punctul iii.8.e. (i), care este similară celei prevăzute la întrebarea frecventă nr. 8 din programul privind sfera de siguranță și care are tendința de a înclina balanța în favoarea intereselor organizațiilor. În acest sens, accesul la propriile date cu caracter personal nu va fi acordat persoanelor fizice, din următoarele motive: „încălcarea unui privilegiu sau a unei obligații profesionale” (anexa II punctul III.8.e.3), „o barieră în calea anchetelor privind la securitatea angajaților și a procedurilor de arbitraj sau în legătură cu organizarea înlocuirilor și a restructurărilor” (anexa II punctul III.8.e.4) și „compromiterea confidențialității necesare în legătură cu funcțiile de control, de inspecție sau de reglementare în raport cu o bună gestiune sau în cadrul negocierilor viitoare sau în curs, în care este implicată organizația” (anexa II punctul III.8.e.5). Aceste motive ar trebui să fie coroborate cu scutirea generală pentru informațiile comerciale confidențiale iii.8.c. inclusă în anexa II III.8.c. Prin urmare, o persoană nu va avea niciodată acces la datele sale în situațiile enumerate mai sus și nu se stabilește un echilibru între drepturile și interesele persoanei și cele ale organizației pentru a ajunge la o soluție la cererea de acces.

GL29 subliniază că dreptul de a accesa propriile date este acordat persoanelor prin articolul 8 alineatul (2) din Cartă. Deși nu este un drept absolut, acesta este fundamental pentru dreptul la protecția datelor cu caracter personal deoarece facilitează exercitarea drepturilor persoanei vizate precum rectificarea și ștergerea datelor.

În ceea ce privește drepturile de rectificare și ștergere, GL29 salută o îmbunătățire semnificativă adusă de principiile Scutului de confidențialitate, în raport cu principiile programului privind sfera de siguranță, care prevede că drepturile respective sunt acordate nu doar în situațiile în care datele sunt inexacte, ci și atunci când datele au fost prelucrate cu încălcarea principiilor (anexa II punctul II.6).

2.2.6 Posibilitatea de recurs, aplicarea legii și responsabilitatea (mecanisme de recurs)

a) Exercitarea efectivă a dreptului de recurs al cetățenilor UE

GL29 recunoaște angajamentele autorităților americane în ceea ce privește diferitele niveluri ale mecanismului de recurs. Cu toate acestea, având în vedere complexitatea și lipsa de claritate a arhitecturii globale a mecanismului, GL29 se teme că, în practică, exercitarea efectivă a dreptului persoanei vizate ar putea fi compromisă. GL29 subliniază că ar trebui să prevaleze calitatea mecanismului de redresare asupra cantității mecanismelor disponibile pentru cetățenii UE. De asemenea, există preocupări că majoritatea, dacă nu toate mecanismele de soluționare, prevăd o procedură desfășurată în SUA, ceea ce ar complica monitorizarea procedurii de către autoritățile pentru protecția datelor din UE.

În fapt, mecanismul de recurs prevăzut în cadrul Scutului de confidențialitate se concentrează în primul rând asupra posibilității ca persoana vizată să „își apere drepturile și să urmărească cazurile de nerespectare a principiilor de confidențialitate, prin stabilirea de contacte directe cu compania autocertificată din SUA”[27]. În plus, organizațiile trebuie să desemneze un organism independent de soluționare a litigiilor pentru a investiga și a soluționa plângerile individuale. GL29 salută faptul că acesta va fi organizat fără ca persoana în cauză să plătească vreo taxă.

De asemenea, plângerile pot fi depuse direct la Comisia Federală pentru Comerț, chiar dacă nu există nicio obligație pentru FTC de a le soluționa. O autoritate pentru protecția datelor poate adresa o plângere, iar Departamentul Comerțului s-a angajat să examineze și să depună toate eforturile pentru a facilita soluționarea reclamațiilor (anexa I) cărora li se va acorda „prioritate” de către Comisia Federală pentru Comerț (anexa II punctul III.7.e). Cu toate acestea, prioritizarea reclamațiilor de către FTC nu oferă nicio certitudine persoanei vizate că reclamațiile sale vor fi abordate.

În ultimă instanță, persoanele vor avea posibilitatea de a invoca un arbitraj obligatoriu. Comisia de arbitraj își va avea sediul în SUA și va face obiectul controlului de către instanțele din SUA.

De asemenea, Scutul de confidențialitate oferă organizației posibilitatea de a alege cooperarea cu autoritățile pentru protecția datelor din UE (anexa II punctul III.5.a). Acest lucru este chiar obligatoriu pentru datele privind resursele umane colectate în contextul unui raport de muncă (anexa II punctul III.9.d.ii). Într-o astfel de situație, soluționarea alternativă a litigiilor (SAL) nu va fi aplicabilă (anexa II punctul III.5.a). Scutul de confidențialitate nu stabilește în mod clar modul în care va fi organizată în practică cooperarea cu autoritățile pentru protecția datelor din UE. În special, este neclar dacă o comisie va trata toate cazurile sau dacă fiecare caz în parte va fi tratat de o comisie diferită.

GL29 consideră că sunt necesare mai multe detalii în decizia privind caracterul adecvat cu privire la competența autorităților pentru protecția datelor de a soluționa plângerile. Aparent, acest lucru depinde de calificarea organizației, dar nu este clar în ce măsură.

În cazul în care o organizație acționează în calitate de agent în numele unui operator de date din UE, persoanele vor avea oricum posibilitatea de a depune o plângere la autoritatea competentă din UE. Situația va fi similară pentru prelucrarea datelor privind resursele umane și a altor date.

În cazul în care organizația parte la Scutul de confidențialitate acționează în calitate de operator de date, competența autorității pentru protecția datelor de a trata reclamația va fi limitată la prelucrarea supusă legislației UE (prelucrarea sub responsabilitatea operatorului din UE – inclusiv controlul comun cu organizația din SUA – sau atunci când organizația parte la Scutul de confidențialitate ar fi supusă direct legislației UE, de exemplu prin utilizarea de echipamente în UE). Cu toate acestea, pentru prelucrarea datelor efectuată doar în temeiul

[27] Comisia Europeană, proiectul de decizie privind caracterul adecvat, punctul 30.

legislației Statelor Unite, se vor aplica în mod exclusiv mecanismele Scutului de confidențialitate. Pentru a depăși barierele lingvistice și lipsa de cunoaștere a sistemului juridic din SUA, ar putea fi util dacă autoritățile pentru protecția datelor din UE ar avea dreptul să acționeze ca intermediar pentru plângerile persoanei sau să le asiste în procedurile de soluționare alternativă a litigiilor cu organizații din SUA sau cu ocazia contactelor acestora cu autoritățile din SUA, în cazul în care autoritatea pentru protecția datelor consideră acest lucru oportun.

GL29 subliniază că mecanismul explicat în Scutul de confidențialitate nu dă curs recomandării anterioare conform căreia persoanele din UE ar trebui „să poată introduce cereri de despăgubiri în Uniunea Europeană" și să li se „acorde dreptul de a introduce o acțiune în fața unei instanțe naționale competente din UE"[28]. Ar fi binevenit dacă organizațiile parte la Scutul de confidențialitate ar include o astfel de posibilitate în politicile lor de confidențialitate.

Pentru a se asigura eficacitatea, GL29 recomandă că sistemul ar trebui, de preferință, să permită autorităților pentru protecția datelor din UE să reprezinte persoana vizată și să acționeze în numele său sau să acționeze în calitate de intermediar. În mod alternativ, acesta ar trebui să cuprindă clauze specifice de competență care permit persoanelor vizate să își exercite drepturile în Europa.

b) Arbitrajul

Procedurile definitive de arbitraj nu sunt încă finalizate, ceea ce îngreunează evaluarea de către GL29. Întrucât se pare că arbitrajul va avea loc în temeiul legislației SUA și că singura limbă de procedură va fi limba engleză, autoritățile pentru protecția datelor din UE pot dori să aibă dreptul de a asista persoanele în acest proces.

În plus, procedura de arbitraj a fost pusă în practică din cauza faptului că nu exista o asigurare că o plângere va fi tratată, întrucât FTC nu are obligația de a trata fiecare plângere. În cazul în care persoana din UE simte nevoia de a fi asistată de un avocat, GL29 observă că aceasta va trebui să suporte onorariul avocatului său, ceea ce ar putea împiedica persoanele să își depună plângerea în cadrul procedurii de arbitraj.

c) Supravegherea, aplicarea și eficacitatea mecanismelor de recurs

<u>Condiții pentru a intra în Scutul de confidențialitate</u>

Conform CJUE, „fiabilitatea unui sistem de autocertificare [...] se bazează în esență pe instituirea unor mecanisme de supraveghere care să permită detectarea eficientă și eventualele încălcări ale normelor care asigură protecția drepturilor fundamentale […]"[29].

GL29 remarcă faptul că rolul Departamentului Comerțului în procesul de certificare în cadrul Scutului de confidențialitate pare a fi redus la simpla verificare a integralității documentelor.

[28] A se vedea scrisoarea GL29 adresată doamnei vicepreședinte Reding, 10 aprilie 2014.
[29] CJUE, Schrems, punctul 81.

Deși GL29 recunoaște că autocertificarea nu implică o verificare sistematică a priori a punerii în aplicare a politicilor de confidențialitate, Departamentul Comerțului ar trebui cel puțin să se angajeze să verifice în mod sistematic dacă politicile de confidențialitate includ toate principiile Scutului de confidențialitate. Un astfel de angajament este menționat în proiectul de decizie privind caracterul adecvat, dar nu poate fi identificat în mod clar în declarațiile conducerii Departamentul Comerțului[30].

O încălcare a principiilor Scutului de confidențialitate ar putea trece neobservată pentru o perioadă lungă de timp și ar putea fi detectată doar după ce a fost cauzat un prejudiciu grav drepturilor fundamentale ale persoanei vizate, eventual dincolo de punctul la care acesta poate fi reparat. Prin urmare, o astfel de abordare ar putea contraveni principiului european al precauției.

Transparența prin intermediul listei Scutului de confidențialitate și al registrului organizațiilor eliminate din listă

S-au realizat îmbunătățiri considerabile în ceea ce privește transparența față de persoana vizată. Pe lângă toate organizațiile din SUA care s-au autocertificat la Departamentul Comerțului, noua listă a Scutului de confidențialitate va conține, de asemenea, o listă a tuturor organizațiilor eliminate din lista Scutul de confidențialitate, inclusiv motivul pentru care o organizație a fost eliminată[31]. Site-ul internet al Scutului de confidențialitate al Departamentului Comerțului va continua să se concentreze mai mult pe publicul țintă într-un mod care să faciliteze verificarea tipului de informații vizate de autocertificarea unei organizații, precum și a politicii de confidențialitate care se aplică informațiilor vizate și a metodei utilizate de organizație pentru a verifica respectarea principiilor[32]. GL29 salută prevederea explicită în prezent a faptului că Departamentul Comerțului va verifica dacă societățile care au site-uri internet publice își publică politica de confidențialitate pe site sau, în cazul în care acestea nu dispun de un site internet public, locul în care politica de confidențialitate este pusă la dispoziția publicului[33]. De asemenea, documentele conțin mai multe informații cu privire la conținutul politicii de confidențialitate[34].

GL29 consideră că ar putea apărea o problemă dacă o organizație care este deja inclusă în lista Scutului de confidențialitate își extinde ulterior certificarea la alte categorii de date. În astfel de cazuri, lista nu va reflecta diferitele perioade de aplicabilitate a principiilor pentru diferitele categorii de date. Acest lucru creează riscul ca persoanele și întreprinderile din UE să nu poată evalua pe deplin dacă un anumit set de date este într-adevăr supus principiilor Scutului de confidențialitate și, în caz afirmativ, de când. Pentru a evita această deficiență,

[30] Comisia Europeană, proiectul de decizie privind caracterul adecvat, punctul 34.
[31] Anexa I, p. 5 și anexa II punctul II.1; GL29 face referire, de asemenea, la cea de a patra recomandare a Comisiei din comunicarea COM(2103)847, precum și la scrisoarea GL29 adresată doamnei vicepreședinte Reding, din 10 aprilie 2014, în special punctul 5 din secțiunea „Transparență”.
[32] Anexa I, p. 8; GL29 face referire, de asemenea, la scrisoarea GL29 adresată doamnei vicepreședinte Reding, din 10 aprilie 2014, în special punctul 2 din secțiunea „Transparență”.
[33] Anexa I, p. 3 și 4; GL29 face referire, de asemenea, la prima recomandare a Comisiei din comunicarea COM(2103)847, precum și la scrisoarea GL29 adresată doamnei vicepreședinte Reding, din 10 aprilie 2014, în special punctul 3 din secțiunea „Transparență”.
[34] Anexa I, p. 5 și 6 și anexa II punctul III.6.

grupul de lucru recomandă ca un registru al organizațiilor din lista Scutul de confidențialitate să specifice separat, pentru fiecare categorie de date cu caracter personal, data intrării în vigoare a autocertificării.

GL29 salută faptul că Departamentul Comerțului va menține un registru al organizațiilor care au fost scoase de pe lista Scutului de confidențialitate și că acest registru va include o explicație care să clarifice faptul că organizațiile respective nu mai beneficiază de avantajele Scutului de confidențialitate, însă principiile trebuie să aplice în continuare pentru datele cu caracter personal primite pe perioada în care acestea au avut calitatea de organizație certificată în cadrul Scutului de confidențialitate, atât timp cât organizațiile păstrează datele respective (anexa I, p. 3). Cu toate acestea, întrucât unele organizații care au fost eliminate de pe lista Scutului de confidențialitate pot alege să returneze sau să șteargă datele primite în temeiul Scutului de confidențialitate, în timp ce alte organizații vor păstra datele pe care le-au primit în temeiul Scutului de confidențialitate, este important să se asigure o mai mare transparență în materie pentru persoanele fizice. Prin urmare, registrul companiilor administrat de Departamentul Comerțului trebuie să precizeze dacă organizația păstrează în continuare datele cu caracter personal primite în temeiul Scutului de confidențialitate sau dacă aceasta a returnat sau a șters datele respective. În cazul în care organizația păstrează în continuare astfel de date, registrul ar trebui să menționeze în mod explicit că organizația trebuie să aplice în continuare principiile pentru datele respective.

De asemenea, registrul menținut de Departamentul Comerțului ar trebui să menționeze că aceste organizații nu mai beneficiază de avantajele Scutului de confidențialitate pentru transferurile noi, ceea ce înseamnă că organizația nu mai este autorizată să primească date cu caracter personal din UE în baza principiilor.

Proceduri de verificare

Pentru a verifica eficacitatea în practică a autocertificării, organizațiile pot efectua o autoevaluare sau un control extern al conformității. GL29 regretă faptul că formarea lucrătorilor este necesară numai în cazul în care o organizație optează pentru verificarea prin autoevaluări (anexa II punctul III.7.c). De asemenea, se pare că trebuie să se verifice dacă politicile sunt exacte, complete, prezentate în mod vizibil, puse în aplicare și accesibile numai în cazul în care organizația optează pentru controlul intern (autoevaluări) și că un astfel de control efectuat de un mecanism extern este limitat numai la conformitatea cu politica de confidențialitate a organizației.

A posteriori

GL29 salută faptul că FTC și Departamentul Comerțului sunt învestite cu competențe de investigare în cazul plângerilor. În plus, GL29 observă că Departamentul Comerțului va avea posibilitatea de a efectua verificări din oficiu, în special prin trimiterea de chestionare. Cu toate acestea, GL29 ar dori să se asigure că o astfel de abordare este suficientă pentru a îndeplini cerința CJUE privind mecanismele de detectare eficace și de supraveghere ale

încălcării. În fapt, GL29 are în continuare întrebări rămase cu privire la competența autorităților de aplicare a legii din SUA de a efectua inspecții la fața locului la sediile organizațiilor autocertificate pentru a investiga încălcările Scutului de confidențialitate, la modul în care un *exequatur* la decizia unei autorități a UE se poate obține pe teritoriul Statelor Unite și la faptul dacă sancțiunile în conformitate cu Scutul de confidențialitate sunt disuasive în practică.

2.2.7 Prelucrarea datelor privind resursele umane

Domeniul de aplicare

Principiul suplimentar 9 (anexa II punctul III.9) se referă la informații cu caracter personal despre un angajat (trecute sau prezente) colectate în contextul unui raport de muncă. Conform textului principiului suplimentar 9.a.ii, principiile Scutului de confidențialitate se aplică numai atunci când „registrele identificate sunt transferate sau accesate". Termenul „registru identificat" nu este în concordanță cu definiția „datelor cu caracter personal" în conformitate cu anexa II punctul I.8.a, care cuprinde „informații referitoare la o persoană fizică identificată sau identificabilă" și, prin urmare, nu este în concordanță cu definiția utilizată în directivă[35].

Principiul suplimentar 9.a.ii prevede că „raportarea statistică bazată pe date globale cu privire la ocuparea forței de muncă și/sau utilizarea datelor anonime sau pseudoanonime nu prezintă riscuri pentru viața privată". Această afirmație este în contradicție cu o serie de avize emise de către GL29. GL29 dorește să sublinieze că datele agregate pot fi reidentificate și, prin urmare, ar trebui să fie considerate drept date cu caracter personal[36].

Principiile notificării, opțiunii și limitării scopului

Principiul suplimentar 9.b.i oferă un exemplu de aplicare a principiilor notificării și opțiunii în cazul în care datele privind resursele umane sunt utilizate în alte scopuri. Exemplul se referă la o organizație din SUA care „intenționează să utilizeze informațiile cu caracter personal colectate prin intermediul raportului de muncă pentru scopuri care nu sunt legate de muncă, cum ar fi informații de marketing". În acest scenariu, modificarea scopului este autorizată cu condiția ca aceasta să respecte principiul notificării și principiul opțiunii. În opinia GL29, prelucrarea ulterioară a datelor privind resursele umane în scopuri de marketing direct, în majoritatea cazurilor, va trebui să fie considerată un scop incompatibil și, prin urmare, contrară principiului limitării scopului (anexa II punctul II.5.a). În plus, GL29 consideră că opțiunea nu poate să constituie o bază adecvată pentru ca un angajat să „consimtă" (opt-out) la o modificare a scopului, în contextul unei relații de muncă, în cazul în care un astfel de consimțământ ar putea să nu fie pe deplin liber.

[35] Astfel cum s-a subliniat deja, limitarea la registre care sunt „transferate sau accesate" nu este în concordanță nici cu termenul „prelucrare" (anexa II punctul I.8.b).
[36] A se vedea Avizul 4/2007 privind conceptul de date cu caracter personal, precum și Avizul nr. 5/2014 privind tehnicile de păstrare a anonimității.

GL29 are mari îndoieli că principalul obiectiv al Scutului de confidențialitate în ceea ce privește principiul opțiunii ca o condiție pentru a utiliza ulterior datele în alt scop respectă Orientările OCDE privind protecția vieții private, întrucât nu există suficiente garanții pentru a preveni ca acest mecanism de excludere să poată fi utilizat, de asemenea, pentru o prelucrare ulterioară incompatibilă. Principiul suplimentar 9.b.iv prevede o scutire amplă și explicită de la principiile notificării și opțiunii „în măsura și pe durata necesară pentru a evita lezarea capacității organizației în cadrul promovărilor, angajamentelor sau altor decizii similare privind ocuparea forței de muncă". În primul rând, utilizarea datelor privind resursele umane în acest scop ar trebui să fie declarată deja în mod explicit la colectarea datelor. În plus, formularea „altor decizii similare privind ocuparea forței de muncă" este prea vagă și prea amplă. Aceasta va avea drept consecință faptul că datele privind resursele umane vor fi pe deplin exceptate de la principiile notificării și opțiunii în cazul în care sunt prelucrate în cadrul unui raport de muncă. Termenul este atât de amplu, încât nu permite să se determine dacă utilizarea ulterioară este compatibilă cu scopul inițial. GL29 recomandă eliminarea acestei excepții.

Dreptul de acces

Principiul suplimentar 9.e.i prevede, de asemenea, o exceptare de la aplicarea principiului accesului sau de la încheierea unui contract cu un operator terț pentru datele privind resursele umane atunci când se referă la operațiuni ocazionale legate de relațiile de muncă, cum ar fi rezervarea unui zbor, a unei camere de hotel sau acoperirea unei asigurări, transferurile de date cu caracter personal ale unui număr mic de angajați și cu condiția respectării principiilor notificării și opțiunii. GL29 nu vede nicio justificare rezonabilă pentru o astfel de exceptare și recomandă eliminarea acestui alineat.

2.2.8 Produse farmaceutice și medicale

Domeniul de aplicare

În cadrul Scutului de confidențialitate, se consideră că transferurile de date codificate din Uniunea Europeană către Statele Unite în contextul produselor farmaceutice și medicale nu constituie transferuri care ar face obiectul Scutului de confidențialitate (anexa II punctul III.14.g.i). Cu toate acestea, transferul de date codificate beneficiază de protecție în temeiul legislației europene privind protecția datelor. Aceasta înseamnă că, în practică, Scutul de confidențialitate nu poate reglementa astfel de transferuri. GL29 solicită Comisiei Europene să prevadă în mod explicit faptul că proiectul de decizie privind caracterul adecvat nu va viza transferul de date codificate din motive medicale sau farmaceutice și, prin urmare, orice astfel de transfer trebuie să fie reglementat de alte garanții, cum ar fi clauzele contractuale standard (denumite în continuare „CCS") sau regulile corporatiste obligatorii. GL29 sugerează că acest lucru ar putea fi clarificat în textul final al deciziei privind caracterul adecvat.

Transferurile în scopuri de reglementare și supraveghere (anexa II punctul III.14.d)

GL29 este preocupat de faptul că, în temeiul dispozițiilor în cauză, datele cu caracter personal care sunt, datorită contextului medical, în mare parte date sensibile, pot fi transferate către autoritățile din SUA. Întrucât Scutul de confidențialitate este conceput pentru transferurile de date între entități private, se pare că un organism public precum autoritatea de reglementare din SUA nu este eligibil să se autocertifice în temeiul Scutului de confidențialitate, ceea ce ridică problema protecției adecvate a datelor pentru astfel de transferuri. În cazul în care astfel de transferuri trebuie administrate în scopuri de reglementare, trebuie luate măsuri adecvate pentru a garanta protecția continuă a drepturilor fundamentale ale persoanei vizate. GL29 subliniază că proiectul de decizie privind caracterul adecvat nu cuprinde nicio constatare cu privire la acest aspect. Prin urmare, GL29 nu are nicio garanție că datele sensibile ale persoanelor din UE vizate vor beneficia de o protecție adecvată în acest context.

În plus, GL29 subliniază că nu înțelege de ce scopul „comercializării" este menționat ca un exemplu de prelucrare pentru cercetare științifică viitoare. De asemenea, motivul pentru transferurile ulterioare către întreprinderi și alți cercetători (anexa II punctul III.14.d) sub titlul „transferuri în scopul reglementării și controlului" este neclar. Aceste chestiuni necesită clarificare în textul final al deciziei privind caracterul adecvat.

Siguranța produselor, eficacitatea monitorizării (inclusiv raportarea către agențiile guvernamentale) și urmărirea pacienților care folosesc anumite medicamente sau dispozitive medicale

Scutul de confidențialitate prevede o exceptare de la principiile notificării, opțiunii, transferului ulterior și accesului în măsura în care respectarea principiului respectiv interferează cu respectarea cerințelor de reglementare. Proiectul de decizie privind caracterul adecvat nu prevede nicio constatare privind situația în care principiile de protecție a confidențialității contravin cerințelor de reglementare. În timp ce GL29 ar putea înțelege că anchetele guvernelor pot justifica limitarea notificării și a dreptului de acces pentru a proteja activitățile de anchetă, acesta nu vede niciun motiv care poate justifica astfel de derogări ample în cazul în care prelucrarea este efectuată de către o organizație sau de un terț din sectorul privat. De exemplu, pe măsură ce tratamentele pacienților sunt din ce în ce mai personalizate, o astfel de exceptare amplă de la principiile protecției vieții private în cazul urmăririi pacienților care folosesc anumite medicamente sau dispozitive medicale este inacceptabilă, întrucât acest tip de asistență medicală va deveni comun. Aceasta se aplică, de asemenea, atunci când datele sunt utilizate de companiile farmaceutice pentru a monitoriza siguranța și eficacitatea produselor (testarea sau vânzarea de medicamente noi).

2.2.9 Informațiile puse la dispoziția publicului

Excepția de la dreptul de acces în cazul informațiilor disponibile în mod public și al informațiilor extrase din registrele publice (anexa II punctul III.15.d și e) ridică semne de întrebare, în măsura în care o persoană, în exercitarea dreptului său de acces, este interesată să afle dacă un anumit operator prelucrează date despre aceasta și, de asemenea, să știe ce date

sunt prelucrate, pentru a putea să controleze prelucrarea datelor sale. GL29 a declarat în mod repetat că, în conformitate cu legislația UE, persoanele vizate au dreptul să acceseze propriile date și, după caz, să solicite rectificarea sau ștergerea datelor, în cazul în care datele nu au fost prelucrate în mod legal sau dacă acestea sunt incomplete sau inexacte, indiferent dacă datele cu caracter personal au fost publicate[37]. În cazul în care cererea de acces este respinsă pe motiv că datele au fost obținute din surse aflate la dispoziția publicului sau din registre publice, persoana în cauză își va pierde capacitatea de a controla acuratețea datelor și de a verifica dacă datele au fost făcute publice în mod legal în primul rând.

Cu toate acestea, Scutul de confidențialitate scutește registrele publice și informațiile accesibile publicului de la principiile notificării, opțiunii, accesului și responsabilității pentru transferurile ulterioare (anexa II punctul II.15.b). Aceste exceptări par a fi prea ample în comparație cu directiva și generează preocupare deoarece afectează, printre altele, posibilitățile cetățenilor de a controla acuratețea datelor lor și de a restricționa difuzarea acestora.

2.3 Concluzii

GL29 recunoaște că autoritățile din SUA și Comisia Europeană au adus îmbunătățiri semnificative în ceea ce privește aspectele comerciale privind transferul de date între cele două continente. Cu toate acestea, ținând seama de analiza de mai sus, GL29 consideră că partea comercială a Scutului de confidențialitate necesită clarificări suplimentare cu privire la mai multe puncte. De exemplu, lipsa unui principiu explicit privind păstrarea datelor reprezintă un motiv de preocupare. Prin urmare, GL29 are îndoieli serioase că Scutul de confidențialitate poate asigura un nivel de protecție care este, în esență, echivalent cu cel din UE.

Decizia privind caracterul adecvat trebuie să clarifice în continuare principiul limitării scopului și principiul opțiunii. Persistă riscul unor lacune în ceea ce privește mai multe principii, în special cu referire la transferurile ulterioare, sistemul de soluționare a reclamațiilor și prelucrarea datelor privind resursele umane sau a datelor farmaceutice. În plus, modul în care principiile Scutului de confidențialitate trebuie aplicate persoanelor împuternicite de către operator (agenți) necesită clarificare și este nevoie de o atenție deosebită pentru a se asigura o aplicare clară și lipsită de ambiguități terminologice.

3. EVALUAREA GARANȚIILOR DE SECURITATE NAȚIONALĂ DIN PROIECTUL DE DECIZIE PRIVIND CARACTERUL ADECVAT

3.1 Garanții și limitări aplicabile autorităților naționale americane în materie de securitate

Ingerințele în drepturile fundamentale la viață privată și la protecția datelor cu caracter personal pot fi permise, cu condiția ca o astfel de ingerință să fie justificată într-o societate democratică. Acest lucru înseamnă că principiile privind protecția vieții private nu sunt

[37] A se vedea GL20, p. 4.

absolute și că sunt posibile derogări, dar numai în cazul în care sunt asigurate garanțiile (esențiale) aplicabile. În conformitate cu obiectivul de a consolida protecția vieții private, organizațiile ar trebui, de asemenea, să depună eforturi pentru a pune în aplicare principiile în mod integral și transparent, inclusiv indicând în politicile lor de confidențialitate domeniile în care excepțiile de la principii, permise de cadrul juridic al SUA, se vor aplica cu regularitate. Din același motiv, atunci când principiile și/sau legile Statelor Unite ale Americii permit organizațiilor să aleagă, acestea sunt invitate să opteze, în limita posibilului, pentru nivelul cel mai înalt de protecție.

În anexa II punctul I.5 se afirmă că „aderarea la principiile privind protecția vieții private poate fi limitată de: (a) cerințele privind securitatea națională, interesul public și respectarea legilor Statelor Unite ale Americii; (b) textele legislative, regulamentele administrative sau jurisprudența care creează obligații contradictorii sau prevăd autorizații exprese, cu condiția ca organizația care a recurs la o asemenea autorizație să poată demonstra că nerespectarea principiilor se limitează la măsurile necesare pentru garantarea intereselor legitime superioare pe care această autorizație urmărește să le servească; (c) excepțiile sau derogările prevăzute de directivă sau de legislația statului membru, cu condiția ca aceste excepții sau derogări să fie aplicate în contexte comparabile.”

Întrebarea este dacă derogările menționate în anexa II sunt justificate într-o societate democratică. Conform proiectului de decizie privind caracterul adecvat al Scutului de confidențialitate, Comisia a constatat că „există norme în vigoare în Statele Unite menite să limiteze orice ingerință în scopul securității naționale cu drepturile fundamentale ale persoanelor ale căror date cu caracter personal sunt transferate din Uniunea Europeană către Statele Unite ale Americii în cadrul Scutului de confidențialitate la ceea ce este strict necesar pentru atingerea obiectivului legitim în cauză”[38].

Utilizând cadrul astfel cum se prevede în secțiunea 1.2 din prezentul aviz și luând în considerare declarațiile autorităților americane și constatările Comisiei, GL29 a evaluat actualul cadru juridic al SUA și practicile agențiilor de informații americane și condițiile în care acestea permit orice ingerință în drepturile fundamentale la respectarea vieții private și la protecția datelor cu caracter personal, astfel cum sunt consfințite în cadrul juridic european. Această evaluare se bazează pe analiza Directivei nr. 28 privind politica prezidențială (PPD-28), a Decretului 12333 și a diferitelor temeiuri juridice stabilite de Legea privind serviciile de informații externe (Foreign Intelligence Act – FISA, secțiunea 104, secțiunea 402, secțiunea 215, secțiunea 501 și secțiunea 702). GL29 s-a bazat pe anexa VI la Scutul de confidențialitate care constă într-o scrisoare redactată de Biroul Directorului Serviciului Național de Informații (ODNI) cu privire la garanțiile și limitările aplicabile autorităților naționale americane în materie de securitate, sintetizând informațiile care au fost furnizate Comisiei Europene în ceea ce privește activitățile SUA de colectare de informații pe baza semnalelor electromagnetice.

[38] Proiect de decizie a Comisiei în conformitate cu Directiva 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al Scutului de confidențialitate UE-SUA, punctul 75.

3.2 Garanția A – prelucrarea ar trebui să fie în conformitate cu dispozițiile legii și să se bazeze pe norme clare, precise și accesibile

În conformitate cu legislația europeană, o ingerință trebuie să fie în conformitate cu legile, politicile și procedurile instituite și suficient de clare și accesibile (în limitele marjei de apreciere acordate statelor membre), pentru a oferi cetățenilor o indicație adecvată privind circumstanțele și condițiile în care autoritățile publice sunt abilitate să recurgă la măsuri de supraveghere[39].

GL29 remarcă faptul că activitățile de colectare de informații pe baza semnalelor electromagnetice se efectuează pe baza unui cadru juridic accesibil. Toate actele cu putere de lege menționate în anexa VI (PPD-28, FISA, SUA Freedom Act, FOIA) sunt disponibile online pentru publicul larg (în interiorul și în afara SUA). Anexa VI oferă un rezumat al cadrului juridic care reglementează limitările de colectare, limitările de păstrare și difuzare, conformitatea și supravegherea, transparența și recursul. Sistemul juridic al SUA pentru activitățile de spionaj constă într-o serie de documente diferite, inclusiv rapoartele, politicile și procedurile agențiilor individuale, care trebuie să fie analizate pentru a obține o mai bună înțelegere a modului în care se desfășoară activitățile, atât în teorie, cât și în practică. În această privință, GL29 s-a concentrat pe un număr limitat de puncte pe care le consideră esențiale.

3.2.1 Decretul 12333 și Directiva nr. 28 privind politica prezidențială

Domeniul de aplicare a Decretului 12333 este amplu; în principiu, toate activitățile de colectare ale serviciilor de informații străine pot avea loc la discreția președintelui SUA în baza decretului. Cu toate acestea, s-a susținut că, de la introducerea FISA, Decretul 12333 poate fi utilizat numai pentru colectarea de date în afara teritoriului SUA. GL29 remarcă faptul că Decretul 12333 nu oferă multe detalii referitoare la domeniul său de aplicare teritorială, măsura în care datele pot fi colectate, păstrate sau diseminate pe scară mai largă, nici natura infracțiunilor care pot da naștere la supraveghere sau tipul de informații care pot fi colectate sau utilizate.

În înțelegerea GL29, scopul principal al Directivei nr. 28 privind politica prezidențială (PPD-28) este de a stabili limitele pentru colectarea și prelucrarea datelor cu caracter personal, indiferent de programul de supraveghere care este utilizat și de locul unde au fost obținute datele.

[39] CEDO, ZAHAROV, punctul 247 „Curtea a apreciat deja că cerința de «previzibilitate» din lege nu merge atât de departe încât să impună statelor să adopte dispoziții legale indicând în detaliu orice comportament care poate determina o decizie de a supune o persoană la supravegherea secretă cu privire la motivele de «securitate națională»". Prin natura lucrurilor, amenințările la adresa securității naționale pot varia în mod substanțial și poate fi neașteptate sau dificil să se definească în prealabil (a se vedea Kennedy, citată anterior, punctul 159). În același timp, Curtea a subliniat, de asemenea, că în chestiunile care afectează drepturile fundamentale, ar fi contrar principiilor statului de drept, unul dintre principiile de bază ale unei societăți democratice consacrate în convenție, ca o putere discreționară acordată executivului în domeniul securității naționale să fie exprimată în termeni de putere nelimitată. În consecință, legea trebuie să indice sfera puterilor discreționare oferite autorităților competente și modul de exercitare a acestora cu suficientă claritate, având în vedere scopul legitim al măsurii în chestiune, pentru a proteja corespunzător individul împotriva abuzurilor".

PPD-28 este o directivă a președintelui Statelor Unite de stabilire a principiilor de coerență cu care este autorizată și efectuată activitatea de colectare de informații pe baza semnalelor electromagnetice, dar nu reprezintă un temei juridic pentru colectare. PPD-28 produce efecte prin impunerea acestor principii pentru organismele comunității de informații în punerea în aplicare a politicilor și procedurilor acestora. Directiva se aplică activităților de colectare de informații pe baza semnalelor electromagnetice, indiferent de locația geografică a operatorului de date atunci când se efectuează colectarea, în interiorul sau în afara SUA. Prin urmare, aceasta se aplică, de asemenea, datelor colectate în scopuri de colectare de informații atunci când acestea sunt transferate din UE către SUA.

În special, PPD-28 prevede că activitățile de colectare de informații pe baza semnalelor electromagnetice trebuie să fie cât mai precise posibil[40]. În ceea ce privește utilizarea datelor, aceasta stabilește procedurile de minimizare a datelor (inclusiv condițiile pentru păstrarea și difuzarea datelor), securitatea datelor și accesul personalului relevant [și anume normele conțin garanții care limitează riscurile de abuz și utilizare necorespunzătoare], calitatea datelor și supravegherea. Aceste garanții se aplică independent de cetățenia persoanelor vizate, și anume cetățenilor americani și persoanelor care nu sunt cetățeni americani.

În timpul transmisiei de date către SUA, sunt aplicabile, de asemenea, garanțiile stabilite de PPD-28. Anexa VI conține un angajament al ODNI conform căruia, în cazul în care serviciile de informații americane ar colecta date de la cablurile transatlantice, acestea ar face acest lucru „sub rezerva limitărilor și măsurilor de protecție stabilite, inclusiv cerințele PPD-28”[41]. GL29 remarcă faptul că există în continuare o lipsă de jurisprudență stabilită pentru determinarea legalității interceptării cablurilor, dacă ar fi realizată de orice țară. În orice caz, SUA nici nu confirmă, nici nu infirmă că utilizează interceptarea cablurilor ca mijloc de colectare de date operative.

Conceptul de „informații pe bază de semnale electromagnetice” nu este definit în PPD-28, nici într-un alt text.

3.2.2 Legea privind supravegherea activităților străine de spionaj

În ansamblu, textul FISA pare să fie mai clar și mai precis. Cu toate acestea, interpretarea mai multor dispoziții în lumina PPD-28 și, prin urmare, aplicarea practică a acestora depinde în mare măsură de aplicarea realizată de diferitele agenții. În timp ce un raport complet privind punerea în aplicare a noii măsuri nu este încă disponibil, delegații americani au informat reprezentanții GL29 că punerea în aplicare a garanțiilor PPD-28 a fost finalizată și este efectuată în mod similar în întreaga comunitate a serviciilor de informații americane.

[40] „Activitățile de colectare de informații electromagnetice trebuie să fie cât mai adaptate posibil. Pentru a decide dacă să colecteze sau nu informații pe baza semnalelor electromagnetice, Statele Unite trebuie să țină seama de disponibilitatea altor informații, inclusiv surse publice sau diplomatice. Ar trebui să se acorde prioritate unor astfel de alternative adecvate și fezabile la informațiile pe bază de semnale electromagnetic” [secțiunea 1 litera (d)].

[41] Anexa VI la Scutul de confidențialitate, scrisoarea Biroului Directorului Serviciului Național de Informații (ODNI) cu privire la garanții și limitările aplicabile autorităților naționale americane în materie de securitate, p. 2.

Mai precis, secțiunea 501 este relativ clară cu privire la tipul de informații care pot fi mandatate: „producția de orice elemente concrete (inclusiv cărți, înregistrări, acte, documente și alte elemente)”. Cu toate acestea, trebuie remarcat că faptul că definiția „elementelor concrete” ca incluzând „alte elemente” face ca domeniul de aplicare a acestei autorități să fie destul de cuprinzător.

Secțiunea 702, care permite ca datele să fie colectate de la persoane care nu sunt cetățeni americani despre care se presupune, în mod întemeiat, că sunt în afara Statelor Unite pentru a obține informații operative străine[42] nu oferă același nivel de detaliere ca secțiunea 501. În ceea ce privește domeniul său de aplicare, secțiunea 702 se referă la furnizorii de servicii de comunicații electronice cu sediul în SUA pentru colectarea de informații operative străine ale persoanelor aflate în afara SUA. Definiția pentru „informații operative străine” este amplă. Aceasta include, printre altele, „informații cu privire la o putere străină sau un teritoriu străin care se referă la desfășurarea afacerilor externe ale Statelor Unite ale Americii”[43], ceea ce prezintă un anumit grad de incertitudine cu privire la tipul de informații care pot fi colectate în practică.

În pofida declasificării documentelor, a rapoartelor către Congres și a rapoartelor de supraveghere ale Comitetului de supraveghere a vieții private și a libertăților civile (denumit în continuare PCLOB), aplicarea FISA, inclusiv domeniul de aplicare și utilizarea termenilor de selecție specificați, rămâne neclară și creează confuzie. Utilizarea anumitor termeni de selecție specificați („selectoarele cu sarcini specifice”) este menționată într-un raport PCLOB[44], însă GL29 consideră că acest lucru nu corespunde normelor de direcționare conform secțiunii 702[45]. Acestea nu sunt menționate în normele general accesibile, în măsura în care a putut să confirme GL29.

3.2.3 Concluzie

În ansamblu, GL29 observă că textele aplicabile referitoare la activitățile de spionaj sunt disponibile online și că autoritățile americane au luat o serie de măsuri importante în vederea asigurării transparenței.

GL29 recunoaște că, începând din 2013, s-a publicat un număr mare de documente, cum ar fi politici, proceduri, decizii FISC și alte documente declasificate. În plus, PCLOB a publicat rapoarte importante privind activitățile desfășurate în temeiul secțiunii 702 și al Legii SUA privind libertatea (USA FREEDOM Act). Un raport similar este prevăzut pentru activitățile în temeiul Decretului 12333.

Mai multe anexe legislative care ar putea aduce clarificări cu privire la implicațiile decretului asupra persoanelor fizice din afara Statelor Unite și garanțiile aplicabile sunt clasificate și, prin urmare, nu ar trebui să fie accesibile publicului sau persoanelor vizate de aplicarea

[42] Codul SUA titlul 50 secțiunea 1881a (D)(1).
[43] Codul SUA titlul 50 secțiunea 1801(e)(2).
[44] Raportul PCLOB privind programul de supraveghere gestionat în temeiul secțiunii 702 din FISA, p. 32.
[45] Codul SUA titlul 50 secțiunea 1881a(D).

acestora. În cazul în care textele au fost declasificate, acestea prezintă doar o valoare și o perspectivă limitată privind activitățile de spionaj.

În pofida eforturilor depuse pentru a explica funcționarea Decretului 12333 în urma dezvăluirilor Snowden, în special prin adoptarea PPD-28, aplicarea practică actuală a Decretului 12333 rămâne neclară. GL29 remarcă faptul că anexa VI la Scutul de confidențialitate nu oferă informații detaliate privind funcționarea Decretului 12333.

În timp ce GL29 salută limitările suprapuse de PPD-28, este dificil să se examineze dacă actualul cadru juridic al SUA privind supravegherea este suficient de previzibil, și anume dacă acesta conține „indiciu (indicii) suficient(e) cu privire la cazurile și condițiile în care autoritățile publice sunt abilitate să recurgă la astfel de măsuri", întrucât sunt așteptate clarificări suplimentare, inclusiv publicarea raportului PCLOB privind Decretul 12333.

3.3 Garanția B – trebuie să se demonstreze necesitatea și proporționalitatea în ceea ce privește obiectivele legitime urmărite

3.3.1 Directiva nr. 28 privind politica prezidențială

PPD-28 a introdus limitări cu privire la scopurile pentru care datele cu caracter personal pot fi utilizate și la condițiile în care acestea pot fi difuzate, cu efect asupra colectării de informații pe bază de semnale electromagnetice indiferent de baza juridică utilizată.

În special, secțiunea 1 din PPD-28 prevede că activitățile SUA de colectare de informații pe baza semnalelor electromagnetice trebuie să fie întotdeauna „cât mai adaptate posibil". Recunoscând această limitare, este dificil să se stabilească dacă formularea „cât mai adaptată posibil" înseamnă că toate datele colectate sunt necesare și proporționale.

PPD-28 recunoaște că este permisă în continuare colectarea masivă de date „în scopul de a identifica amenințările noi sau emergente și alte informații de securitate naționale vitale care sunt adesea ascunse în sistemul vast și complex de comunicații globale moderne"[46]. GL29 remarcă faptul că PPD-28 prevede că „informațiile pe baza semnalelor electromagnetice colectate în «masă» înseamnă colectarea autorizată de cantități mari de informații pe baza semnalelor electromagnetice care, din cauza unor considerații de ordin tehnic sau operațional, se obțin fără a se utiliza elemente discriminante (de exemplu, identificatori specifici, termeni de selecție etc.)".

PPD-28 impune limite privind utilizarea de informații pe baza semnalelor electromagnetice colectate în masă în ceea ce privește scopul utilizării. Cele șase scopuri pentru care datele pot fi colectate în „masă" includ combaterea terorismului și a altor forme de infracțiuni grave (transnaționale). Analiza GL29 sugerează că limitarea scopului este destul de extinsă (chiar prea extinsă) pentru a fi considerată direcționată.

[46] Secțiunea 2 din PPD-28 și anexa VI la Scutul de confidențialitate, scrisoarea Biroului Directorului Serviciului Național de Informații (ODNI) cu privire la garanțiile și limitările aplicabile autorităților naționale americane în materie de securitate, p. 3.

PPD-28 nu a eliminat posibilitatea colectării nediferențiate de date cu caracter personal în masă, iar amploarea posibilităților acestei colectări este în continuare neclară și potențial semnificativă. În această privință, GL29 observă că, în anexa VI, ODNI afirmă că „orice activități de colectare în masă în ceea ce privește comunicarea prin internet pe care serviciile de informații ale Statelor Unite le efectuează prin colectarea de informații pe baza semnalelor electromagnetice se desfășoară pe o mică parte din internet”[47] și, prin urmare, ar aprecia furnizarea de dovezi suplimentare prin măsuri de transparență.

3.3.2 Legea privind supravegherea activităților străine de spionaj

Procedurile de minimizare prevăzute la secțiunea 215 și secțiunea 702 din FISA au fost introduse în vederea protejării cetățenilor americani împotriva accesului prea amplu al guvernului la datele lor. Aceste restricții nu se aplică în mod oficial în cazul străinilor, deși guvernul SUA a afirmat în mod repetat, în reuniuni atât publice, cât și private cu reprezentanții GL29, că domeniul de aplicare a procedurilor de minimizare a fost extins pentru a acoperi, în practică, toate persoanele, indiferent de naționalitate sau de locul de reședință obișnuit.

Secțiunea 702 prevede că o achiziție autorizată „se desfășoară în conformitate cu cel de al patrulea amendament la Constituția Statelor Unite care limitează colectarea datelor la ceea ce este considerat ca fiind conform cu principiul căutării rezonabile. În acest sens, nu se face nicio distincție între întreprinderile din SUA și din afara SUA”. Cu alte cuvinte, cu condiția ca cel de al patrulea amendament să se aplice tuturor datelor colectate în SUA, colectarea „în masă” care are loc în SUA ar fi „nerezonabilă” și, prin urmare, incompatibilă cu normele constituționale.

GL29 salută constatările din raportul PCLOB conform cărora „în practică, «persoanele care nu sunt cetățeni americani» beneficiază, de asemenea, de restricțiile de acces și păstrare impuse de diferitele proceduri ale agențiilor de reducere la minimum și/sau de direcționare din cauza costului și dificultății de a identifica și elimina informațiile despre cetățenii americani pentru un volum mare de date înseamnă că, de regulă, întregul set de date se prelucrează în conformitate cu standardele americane mai ridicate privind datele”.

GL29 remarcă, de asemenea, că, potrivit constatărilor PCLOB, „programul nu funcționează prin colectarea comunicărilor în masă”. Raportul statistic de transparență pentru 2014 publicat de ODNI confirmă această constatare. În plus, conform raportului PCLOB, sunt utilizate „selectoare cu sarcini specifice”, cum ar fi o adresă de e-mail sau un număr de telefon, pentru a direcționa supravegherea[48].

[47] Anexa VI la Scutul de confidențialitate, scrisoarea Biroului Directorului Serviciului Național de Informații (ODNI) cu privire la garanțiile și limitările aplicabile autorităților naționale americane în materie de securitate, p. 4; GL29 reamintește în acest sens Raportul privind concluziile copreședinților UE ai Grupului de lucru ad-hoc UE-SUA privind protecția datelor, care prevede că „Datele de comunicații reprezintă o parte foarte redusă din traficul internet global”, dat fiind că „marea majoritate a traficului pe internet la nivel mondial constă în vizualizarea prin flux continuu (streaming) și descărcări într-un volum mare, cum ar fi seriale TV, filme și evenimente sportive” (punctul 3.1.2 din raport), 44.
[48] Raportul PCLOB privind programul de supraveghere gestionat în temeiul secțiunii 702 din FISA, p. 32.

Normele publice disponibile corespunzătoare referitoare la direcționare nu prevăd, cu toate acestea, astfel de dispoziții specifice și au drept scop doar să evite vizarea cetățenilor americani sau a persoanelor cu reședință în SUA. În plus, avantajele care, potrivit PCLOB, se aplică în practică persoanelor care nu sunt cetățeni americani nu sunt obligatorii din punct de vedere juridic, nici stabilite prin lege, întrucât legislația referitoare la direcționare nu prevede astfel de norme și este menită doar să evite vizarea cetățenilor americani sau a persoanelor cu reședință în SUA.

În plus, GL29, reamintește că, în scopurile secțiunii 702, persoane nu înseamnă doar persoane fizice, ci și grupuri, entități, asociații, societăți sau puteri externe. În plus, faptul că activitatea de colectare este justificată de aceea că „un scop semnificativ al achiziției este obținerea de informații operative străine" lasă un anumit grad de incertitudine în ceea ce privește scopul și necesitatea acesteia. Cu toate acestea, GL29 salută informațiile furnizate în anexa VI conform cărora numărul total al persoanelor vizate în temeiul secțiunii 702 din 2014 a fost de aproximativ 90 000[49]. Prima revizuire a Scutului de confidențialitate va oferi posibilitatea furnizării unor dovezi suplimentare privind normele de direcționare.

Până în prezent, nu există o jurisprudență concludentă cu privire la legalitatea colectării masive și nediferențiate de date și utilizarea ulterioară a datelor cu caracter personal în scopul combaterii criminalității, inclusiv întrebarea în ce condiții poate avea loc o astfel de colectare și utilizare a datelor cu caracter personal. Curtea de Justiție a Uniunii Europene ar trebui să abordeze această chestiune, cel puțin într-o anumită măsură, în cursul anului 2016, atât în cauzele conexate Tele2 Sverige AB v. Post- och telestyrelsen și Secretary of State for the Home Department/Davis și alții[50], cât și în consultanța acordată cu privire la validitatea acordului PNR cu Canada[51]. În același timp, GL29 reamintește că a afirmat în mod constant că, în orice caz, activitatea de colectare masivă și nediferențiată de date nu poate fi considerată ca fiind proporțională[52].

3.3.3 Concluzie

În pofida limitărilor stabilite în urma introducerii PPD-28, preocupările GL29 persistă, în special în ceea ce privește proporționalitatea colectării de date. În primul rând, există indicii că SUA continuă activitățile de colectare masivă și nediferențiată de date sau cel puțin nu exclud faptul că pot continua să facă acest lucru în viitor. GL29 a susținut în mod constant că o astfel de colectare de date nu este conformă cu dreptul Uniunii și, prin urmare, nu este acceptabilă.

În al doilea rând, GL29 observă că prelucrarea de date direcționată sau prelucrarea care este „cât mai adaptată posibil" poate fi considerată, de asemenea, ca fiind masivă. Faptul dacă o astfel de colectare masivă de date ar trebui sau nu să fie permisă face în prezent obiectul unei acțiuni în fața Curții de Justiție a Uniunii Europene. Din acest motiv, GL29 nu realizează o

[49] Anexa VI, p. 11.
[50] CJUE, cauzele conexate C-203/15 și C-698/15.
[51] CJUE, cauza A-1/15.
[52] WP215 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_ro.pdf.

evaluare finală în ceea ce privește legalitatea prelucrării direcționate, dar masive de date. Cu toate acestea, GL29 subliniază că, în cazul în care ar fi admisă prelucrarea direcționată, dar masivă de date, principiile de direcționare ar trebui să se aplice atât colectării, cât și utilizării ulterioare a datelor și nu se pot limita doar la utilizare. În orice caz, o clarificare a proiectului de decizie privind caracterul adecvat este necesară în raport cu cele șase scopuri menționate în PPD-28 pentru care datele pot fi colectate în „masă". GL29 nu este convins, în stadiul actual, că scopurile sunt suficient de restricționate pentru a se asigura că activitatea de colectare de date este limitată la ceea ce este necesar și proporțional.

3.4 Garanția C - ar trebui să existe un mecanism de supraveghere independent

SUA nu dispune de un organism de supraveghere unic la nivel federal însărcinat să supravegheze impactul programelor de informații și supraveghere asupra protecției datelor și vieții private. În schimb, activitățile serviciilor de informații din SUA fac obiectul unui proces de supraveghere la mai multe niveluri: se poate face o distincție între supravegherea internă și cea externă. GL29 recunoaște că practica de raportare a organismelor de supraveghere din SUA este foarte detaliată și, în cea mai mare parte, publică.

3.4.1 Supravegherea internă

Toate agențiile de informații și securitate dispun de membri ai personalului care sunt responsabili pentru asigurarea respectării cadrului lor legislativ, inclusiv inspectori generali a căror sarcină principală este de a evalua conformitatea globală a activităților agențiilor cu legislația, inclusiv, dar fără a se limita la, legislația privind protecția datelor și a vieții private. Inspectorii generali sunt instituiți prin lege și sunt (sau vor fi în curând) numiți de președinte și confirmați ulterior de Senat, în scopul de a se asigura ca aceștia vor fi independenți din punct de vedere organizațional, și raportează Congresului. Prin urmare, GL29 consideră că inspectorii generali pot îndeplini criteriul de independență organizațională, astfel cum este definit de Curtea de Justiție a Uniunii Europene și de Curtea Europeană a Drepturilor Omului (CEDO), cel puțin din momentul în care noul proces de numire se va aplica tuturor. Pentru moment, persistă unele preocupări în ceea ce privește inspectorii generali care sunt numiți în continuare de directorul executiv al agenției pe care o supraveghează.

Inspectorii generali pot prezenta recomandări care pot fi transmise ulterior Departamentului de Justiție și PCLOB sau chiar comitetului Congresului care poate pune în aplicare recomandările. În cazul în care inspectorul general constată o încălcare, aceasta poate fi abordată prin măsuri interne și de politică și raportată către Congres. Inspectorul general are competența, de exemplu, de a efectua atât audituri, cât și inspecții.

GL29 remarcă faptul că rapoartele inspectorului general pot să nu fie divulgate publicului și că un inspector general poate fi, de asemenea, împiedicat să raporteze în cazul în care informațiile verificate sunt clasificate. Cu toate acestea, în orice moment, rapoartele fac obiectul supravegherii Congresului, ceea ce constituie o măsură de protecție esențială, chiar dacă nu oferă o cale de atac individuală.

Toate agențiile au responsabili pentru protecția vieții private și a libertăților civile care contribuie la sistemul de auto-raportare obligatorie sub supravegherea Congresului.

În general, mecanismele de supraveghere internă în vigoare pot fi considerate ca fiind destul de solide; cu toate acestea, pentru a justifica o ingerință în drepturile fundamentale la viață privată și protecția datelor, supravegherea trebuie să fie complet independentă. În timp ce GL29 respectă și apreciază activitatea diferiților responsabili pentru protecția vieții private și a libertăților civile, grupul de lucru nu poate concluziona că aceștia respectă nivelul de independență necesar pentru a acționa în calitate de supraveghetor.

3.4.2 Supravegherea externă

Supravegherea externă constă într-o serie de mecanisme diferite: supravegherea judiciară în temeiul secțiunilor 501 și 702 asigurată de Curtea FISA (denumită în continuare „FISC"), supravegherea din către comisiile restrânse de informații ale Congresului și sarcinile îndeplinite de PCLOB.

GL29 reamintește că, în mod ideal, astfel cum a fost stabilit de Curtea de Justiție a Uniunii Europene și de Curtea Europeană a Drepturilor Omului, supravegherea ar trebui să fie asigurată de un judecător, în vederea garantării independenței și imparțialității procedurii. Până de curând, procedura FISC a fost o procedură ex parte, fără posibilitatea persoanelor în cauză de a fi audiate sau chiar de a cunoaște cauza. În prezent, procedura FISC rămâne în continuare ex parte, dar, în urma adoptării USA FREEDOM Act, la FISC au fost introduși amici curiae. Amici curiae acționează în mod independent, dar nu sunt stabiliți pentru a proteja anumite persoane care pot fi implicate în cauză.

USA FREEDOM Act a creat un grup de amici curiae pentru a informa FISC cu privire la cauzele importante. Curtea a selectat cinci avocați care au obținut autorizațiile de securitate corespunzătoare și care oferă consultanță tehnică, participă la audierile FISC și prezintă informări și își exprimă punctul de vedere pe fondul cauzei dintr-o perspectivă a vieții private și a drepturilor civile. Cu toate acestea, acest lucru se va întâmpla numai în cauzele importante sau atunci când apar chestiuni juridice noi[53].

Secțiunea 215 face aproape în întregime obiectul unei supravegheri judiciare ex ante (dar nu ex post), întrucât toate programele care utilizează secțiunea 215 ca bază pentru colectare fac obiectul aprobării de către FISC. Raportul PCLOB precizează că „secțiunea 702 diferă de acest cadru de supraveghere electronică tradițional al FISA atât din punct de vedere al standardelor aplicate, cât și prin lipsa unor decizii individuale luate de către FISC. În conformitate cu statutul, procurorul general și directorul serviciilor naționale de informații fac certificări anuale autorizând vizarea persoanelor care nu sunt cetățeni americani despre care, din motive întemeiate, se consideră că se află în afara Statelor Unite pentru a dobândi informații operative străine, fără a specifica la FISC persoanele specifice care nu sunt cetățeni americani care vor fi vizate. […] de asemenea, nu impune guvernului să demonstreze o cauză

[53] Freedom Act TITLUL IV – REFORMELE CURȚII DE SUPRAVEGHERE A ACTIVITĂȚILOR STRĂINE DE SPIONAJ secțiunea 401. Numirea de amici curiae.

probabilă pentru a crede că o țintă în temeiul secțiunii 702 este o putere străină sau un agent al unei puteri străine, astfel cum se impunea potrivit cerințelor tradiționale FISA”[54].

În Congres, comisiile restrânse de informații au, de asemenea, o sarcină de supraveghere, aprobând activitățile serviciilor de informații, în special prin intermediul votării bugetului. Comisiile Senatului și Camerei primesc informații clasificate cu privire la activitățile serviciilor de informații. Procurorul general trebuie să raporteze acestor comisii o dată la șase luni cu privire la supravegherea electronică FISA. GL29 nu înțelege în continuare în ce măsură acestea pot să discute despre prelucrarea datelor cu caracter personal ale persoanelor fizice, mai ales ale persoanelor care nu sunt cetățeni americani.

PCLOB este o parte independentă a ramurii executive a guvernului SUA, care este învestită cu două autorități: (1) să revizuiască și să analizeze acțiunile executivului pentru a proteja [SUA] împotriva terorismului, garantând astfel că necesitatea unei astfel de acțiuni este coordonată cu necesitatea protejării vieții private și a libertăților civile și (2) să se asigure că preocupările legate de libertăți sunt luate în considerare în mod corespunzător în elaborarea și punerea în aplicare a legilor, reglementărilor și politicilor legate de eforturile de a proteja țara împotriva terorismului. GL29 remarcă faptul că PCLOB are competența de a emite citații și de a accesa informații clasificate. În îndeplinirea misiunii sale, acesta verifică, de asemenea, eficacitatea programelor. Supravegherea din partea PCLOB nu este efectuată a priori, ci a posteriori. PCLOB și-a demonstrat competențele autonome prin exprimarea dezacordului cu președintele Statelor Unite ale Americii cu privire la aspecte juridice. În special, acesta a considerat că programul de metadate telefonice în temeiul secțiunii 215 nu era autorizat din punct de vedere legal și a concluzionat că acesta nu a fost eficient, întrucât nu există dovezi privind atacuri dejucate. PCLOB a realizat, de asemenea, un studiu cu durata de un an privind programul în temeiul secțiunii 702 și a constatat că acesta este legal și autorizat în mod clar prin lege și că secțiunea 702 s-a dovedit a fi foarte eficace, inclusiv pe probleme de terorism. În cele din urmă, PCLOB a acționat în ceea ce privește cerința de transparență și a constatat că anumite informații clasificate nu era necesar să fie clasificate. Se înțelege că PCLOB va raporta cu privire la punerea în aplicare a PPD-28 în viitorul apropiat. În această privință, PCLOB consideră că, pentru a păstra informații privind un străin, nu este suficient simplul fapt că persoana în cauză este cetățean străin.

În final, GL29 observă că Decretul 12333 nu prevede eventuale reexaminări judiciare, mecanisme de supraveghere sau de recurs pentru programele de supraveghere desfășurate pe baza acestuia.

3.4.3 Concluzie

Proiectul de decizie privind caracterul adecvat demonstrează că în SUA se aplică o abordare pe mai multe planuri a mecanismelor de supraveghere atât interne, cât și externe. Chiar dacă funcționarea mecanismelor de supraveghere poate crea confuzie, GL29 consideră că, în general, există suficiente mecanisme de supraveghere interne. Cu toate acestea, GL29 este

[54] Raportul PCLOB privind programul de supraveghere în conformitate cu secțiunea 702 din FISA, p. 24, 25.

preocupat de faptul că există o supraveghere insuficientă a programelor de supraveghere derulate în baza Decretului 12333.

GL29 remarcă faptul că observațiile sale critice anterioare cu privire la faptul că procedurile în fața FISC nu sunt contencioase au fost atenuate într-o oarecare măsură prin introducerea de amici curiae care au sarcina de a „promova protecția vieții private și a libertăților civile". Cu toate acestea, FISC nu asigură o supraveghere judiciară eficace asupra vizării persoanelor care nu sunt cetățeni americani. De asemenea, rămân unele îndoieli cu privire la capacitatea FISC de a evalua în mod eficient procedurile de vizare și de reducere la minimum, astfel cum a indicat, de asemenea, PCLOB[55].

3.5 Garanția D - persoana trebuie să dispună de căi de atac eficiente

3.5.1 Căi de atac de natură juridică

3.5.1.1 Cerință permanentă

Sistemul SUA referitor la căile de atac judiciare conține o limită importantă: Constituția SUA solicită persoanei să demonstreze că are calitate procesuală activă, prin „cerința că reclamanții au suferit sau vor suferi un prejudiciu direct și că acest prejudiciu este redresabil. La nivel federal, acțiunile în justiție nu pot fi introduse doar pentru motivul că o persoană sau un grup este nemulțumit de o acțiune guvernamentală sau o lege"[56]. Această cerință pare să fie neutralizată de lipsa de notificare a persoanelor care fac obiectul supravegherii, inclusiv după ce aceste măsuri au expirat. Curtea de Justiție a Uniunii Europene și Curtea Europeană a Drepturilor Omului au afirmat în repetate rânduri că persoanele trebuie să poată avea acces la căi de atac administrative sau judiciare. Curtea Europeană a Drepturilor Omului a confirmat în decizia în cauza ZAHAROV că, pe baza jurisprudenței, oricine poate sesiza instanța în cazul în care are un motiv întemeiat să suspecteze o încălcare a drepturilor sale fundamentale[57].

În plus, străinii care se află în afara SUA nu beneficiază de o protecție constituțională deplină în SUA, ca urmare a jurisprudenței Curții Supreme a Statelor Unite[58]. Acest lucru este valabil, în special, în ceea ce privește cel de al patrulea amendament, care protejează cetățenii americani – dar nu și persoanele care nu sunt cetățeni americani – împotriva perchezițiilor și sechestrelor nerezonabile, și din care este derivată cea mai mare parte a dreptului la viață privată în SUA. Cetățenii europeni și alte persoane din Europa care locuiesc în afara SUA sunt pur și simplu excluși de la protecția în baza celui de al patrulea amendament[59].

Aplicarea limitată a Legii privind căile de atac judiciare (atât din punct de vedere al conținutului, întrucât aceasta exclude securitatea națională, cât și în ceea ce privește persoanele care pot invoca dreptul), numărul mare de derogări și incertitudinea juridică în

[55] Raportul PCLOB privind programul de supraveghere gestionat în temeiul secțiunii 702 din FISA, p. 11.
[56] https://www.law.cornell.edu/wex/standing; https://www.law.cornell.edu/wex/standinghttps://www.law.cornell.edu/wex/standing; Clapper/Amnesty International USA
[57] CEDO, ZAHAROV, punctul 171.
[58] U.S./Verdugo - Urquidez , p. 264-266.
[59] Raport al copreședinților UE, secțiunea 2.

ceea ce privește agențiile cărora li se aplică Legea privind căile de atac judiciare nu îndeplinesc cerința de a oferi un mecanism eficient de recurs tuturor persoanelor implicate în cazuri de supraveghere din partea serviciilor de informații pentru securitatea națională.

3.5.1.2 Directiva nr. 28 privind politica prezidențială

GL29 remarcă faptul că PPD-28 este doar o directivă și, prin urmare, nu creează drepturi pentru persoanele fizice. Acest lucru poate fi realizat numai prin intermediul legislației. Prin urmare, persoanele fizice nu pot să acționeze în instanță pe baza unei presupuse încălcări a garanțiilor oferite de PPD-28.

3.5.1.3 Legea privind supravegherea activităților străine de spionaj

În temeiul FISA, persoanele fizice dispun de unele căi de atac în cazul supravegherii ilegale. Conform FISA, „persoana prejudiciată, alta decât o putere străină sau un agent al unei puteri străine [...], respectiv, care a fost supusă unei supravegheri electronice sau cu privire la care informațiile obținute prin supravegherea electronică a persoanei au fost divulgate sau utilizate cu încălcarea secțiunii 1809 din prezentul titlu are motiv de a introduce o acțiune împotriva oricărei persoane care a săvârșit respectiva încălcare”. Totuși, aceasta exclude în mod explicit puterile străine sau un agent al unei puteri străine care a făcut obiectul măsurii. Cu toate acestea, astfel cum s-a arătat deja, reclamantul va trebui să facă dovada că are calitate procesuală activă, ceea ce nu va mai fi posibil în practică.

USA FREEDOM Act a creat un grup consultativ amicus curiae la Curtea FISA pentru a oferi consiliere (opțională) în cazul unei noi interpretări juridice semnificative. Cu toate acestea, sarcina acestora este de a oferi consiliere obiectivă și nu de a apăra interesele unei anumite persoane, la solicitarea acesteia.

3.5.2 Căi de atac administrative

3.5.2.1 Inspectori generali

O altă cale de atac constă în a apela la inspectorul general ca intermediar la care se poate depune o plângere. Cu toate acestea, inspectorii generali nu au obligația de a examina fiecare plângere: nu există un drept de a fi audiat, ci mai degrabă o putere discreționară. Inspectorul general poate, de asemenea, să emită rapoarte de constatare a încălcărilor în cazul în care informațiile sunt declasificate. În cazul în care o persoană ar putea presupune că raportul o afectează, aceasta ar fi în măsură să introducă o acțiune în instanță pe baza constatării încălcării legii.

3.5.2.2 Legea privind libertatea de informare

O cale de atac la dispoziția tuturor persoanelor este depunerea unei cereri privind libertatea de informare, care se bazează pe Legea privind accesul liber la informații (FOIA). După cum afirmă guvernul SUA, o cerere FOIA poate fi depusă, în general, de orice persoană – fie că este sau nu cetățean american – solicitând pur și simplu orice înregistrări ale agenției. Aceasta

include înregistrări privind persoana, însă în acest caz este necesar să se prezinte o dovadă a identității. Cu toate acestea, în cazul în care informațiile sunt clasificate pentru a se proteja securitatea națională, este puțin probabil ca o cerere FOIA să primească un răspuns pozitiv, având în vedere că se aplică o excepție: agențiile nu sunt obligate să ofere acces la informații clasificate, inclusiv în cazul în care aceste informații se referă la persoana care a formulat cererea. Informațiile din investigații în curs ale organelor de aplicare a legii sunt complet excluse din cererile FOIA. În cele din urmă, în înțelegerea GL29, cererea FOIA nu prevede dreptul de a solicita verificarea legalității prelucrării de către o autoritate independentă.

3.5.3 Ombudsmanul pentru Scutul de confidențialitate

3.5.3.1 Instituirea unui Ombudsman

Scutul de confidențialitate stabilește un nou mecanism „pentru persoanele din UE" pentru prezentarea de cereri privind „activitățile SUA de colectare de informații pe baza semnalelor electromagnetice" către funcția nou-creată de Ombudsman al Scutului de confidențialitate. Funcția de Ombudsman, astfel cum se explică în memorandumul anexat la scrisoarea Secretarului de stat John Kerry, din 22 februarie 2016, va fi ocupată de subsecretarul C. Novelli. Subsecretarul va îndeplini funcția în plus față de rolul său de „coordonator principal pentru diplomația internațională privind tehnologia informației", un post creat prin secțiunea 4(d) din PPD-28. În scrisoare și în memorandum se evidențiază faptul că „sub secretarul se află în subordinea directă a secretarului de stat și este independent de comunitatea serviciilor de informații".

În pofida denumirii sale, se explică în memorandum că Ombudsmanul pentru Scutul de confidențialitate va prelucra nu numai cererile referitoare la accesul la informațiile privind securitatea națională trimise din UE către SUA în temeiul Scutului de confidențialitate, ci și cererile în cazul în care datele respective au fost transmise în conformitate cu clauze contractuale standard, reguli corporatiste obligatorii, derogări (în sensul articolului 26 din Directiva 95/46/CE) sau „posibile viitoare derogări", astfel cum sunt definite în nota de subsol 2 din memorandum.

Modul în care ar trebui să funcționeze mecanismul Ombudsmanului poate fi rezumat după cum urmează: o persoană depune o cerere la un organism dintr-un stat membru competent pentru supravegherea serviciilor de securitate națională sau la un „organism [centralizat] de tratare a plângerilor persoanelor din UE", în cazul în care acesta din urmă va fi creat sau desemnat. Autoritatea care transmite cererea Ombudsmanului va trebui să verifice în primul rând dacă cererea este completă, astfel cum este descris la punctul 3 litera (b) din scrisoare[60].

[60] b. Organismul UE de tratare a plângerilor individuale se va asigura că cererea este completă, pe baza următoarelor acțiuni:
(i) Verifică identitatea persoanei în cauză și dacă persoana acționează în nume propriu și nu ca reprezentant al unei organizații guvernamentale sau interguvernamentale.
(ii) Se asigură că cererea se face în scris și conține următoarele informații de bază:
• orice informație care face obiectul cererii,
• natura informațiilor sau a măsurilor solicitate,
• entitățile Guvernului Statelor Unite despre care se crede că sunt implicate, dacă este cazul, și
• alte măsuri luate pentru a obține informațiile sau măsurile solicitate și răspunsul primit prin intermediul măsurilor respective.

Odată cererea transferată către Ombudsmanul pentru Scutul de confidențialitate și dacă se constată că aceasta este în conformitate cu punctul 3 litera (b), Ombudsmanul pentru Scutul de confidențialitate va furniza un răspuns, ceea ce înseamnă că acesta va confirma că „(i) plângerea a fost examinată în mod corespunzător și (ii) s-a respectat dreptul SUA, textele legislative, ordinele executive, directivele prezidențiale și politicile agenției, care prevăd limitele și garanțiile descrise în scrisoarea Biroului Directorului Serviciului Național de Informații (ODNI) sau, în caz de neconformitate, o astfel de neconformitate a fost remediată”[61]. Răspunsul „nici nu va confirma, nici nu va infirma că persoana a fost vizată de supraveghere, nici nu va confirma măsura reparatorie care a fost aplicată”[62]. În ceea ce privește modalitatea în care este efectuată ancheta Ombudsmanului, se explică faptul că Ombudsmanul pentru Scutul de confidențialitate „va lucra îndeaproape cu alți agenți guvernamentali din Statele Unite, inclusiv organisme de supraveghere independente adecvate”[63], mai precis „va putea să colaboreze îndeaproape cu Biroul Directorului Serviciului Național de Informații, Departamentul de Justiție și cu alte departamente și agenții implicate în securitatea națională din Statele Unite, după caz, și cu inspectorii generali, responsabilii pentru Legea privind liberul acces la informații (Freedom of Information Act) și responsabilii pentru protecția libertăților civile și a vieții private”[64]. Această coordonare trebuie să asigure că Ombudsmanul pentru Scutul de confidențialitate poate trimite un răspuns cuprinzând confirmările descrise mai sus.

3.5.3.2 Evaluarea noului mecanism de Ombudsman

Grupul de lucru recunoaște eforturile depuse de Comisia Europeană și de guvernul SUA pentru a introduce un nou mecanism în vederea îmbunătățirii posibilelor căi de atac cu privire la activitățile de supraveghere ale SUA. Acesta înțelege că evaluarea acestui mecanism, care constituie o noutate în relațiile internaționale în ceea ce privește colectarea de informații pe baza semnalelor electromagnetice sau securitatea națională, are o importanță deosebită.

În această secțiune, GL29 va evalua modul în care stabilirea Ombudsmanului pentru Scutul de confidențialitate se raportează la cerințele necesare pentru recursul persoanelor fizice la proceduri judiciare, astfel cum au fost stabilite în Carta drepturilor fundamentale a Uniunii Europene, Convenția europeană a drepturilor omului și jurisprudența instanțelor europene.

3.5.3.3 Este posibil ca stabilirea în sine a mecanismului Ombudsmanului să fie suficientă?

În primul rând, trebuie stabilit dacă instituirea unui „ombudsman” poate fi considerată ca fiind în conformitate cu articolul 47 din Cartă – care prevede o cale de atac eficientă în fața unei

(iii) Verifică dacă cererea se referă la date despre care se poate considera în mod rezonabil că au fost transferate din UE către Statele Unite în temeiul Scutului de confidențialitate, al CCS, al RCO, al derogărilor sau posibilelor derogări viitoare.
(iv) Face o determinare inițială că cererea nu este neserioasă, nejustificată sau făcută cu rea-credință..
[61] Scutul de confidențialitate anexa III secțiunea 4.e.
[62] Scutul de confidențialitate anexa III secțiunea 4.e.
[63] Scutul de confidențialitate anexa III secțiunea 2.a.
[64] Scutul de confidențialitate anexa III secțiunea 2.a.

instanțe judecătorești imparțiale[65] – cel puțin în cazul în care nu este disponibilă nicio altă cale pentru a recurge la proceduri judiciare eficace. Acest lucru este semnificativ deoarece CJUE, în cauza Schrems, în importantul considerent 95, face trimitere la articolul 47 din Cartă, fără a oferi nicio indicație că articolul 47 ar trebui să fie înțeles cu modificări în contextul măsurilor de supraveghere. Dimpotrivă, CJUE a aplicat deja articolul 47 din Cartă în hotărârea Kadi II[66] la măsuri de supraveghere la nivel național și, respectiv, de securitate internațională[67].

Cu toate acestea, jurisprudența CEDO face foarte clar faptul că o cale de atac la instanțele de drept comun nu este o condiție pentru a considera că programele de supraveghere sunt în conformitate cu articolul 8 (și articolul 13 din Convenția europeană a drepturilor omului)[68]. Dimpotrivă, Curtea a precizat, în temeiul articolului 8, ca o măsură de protecție necesară față de activitățile de supraveghere, că se poate recurge la căi de atac în fața altor autorități. Cu toate acestea, CEDO are așteptări foarte ridicate ca aceste alte autorități competente să ofere o cale de atac eficientă, afirmând că o astfel de autoritate trebuie să fie „independentă de autoritățile care efectuează supravegherea, învestită cu puteri suficiente și competența de a exercita un control eficace și continuu”[69].

În cauza Kennedy și în cauza Klass, CEDO a oferit o mai bună înțelegere a ceea ce ar putea însemna astfel de așteptări în contextul supravegherii secrete, atunci când persoana vizată nu este notificată cu privire la prelucrarea datelor sale. În cele două hotărâri, autoritățile au fost considerate de către Curtea Europeană a Drepturilor Omului ca fiind independente, în special independente de organismele care efectuează supravegherea, precum și independente de instrucțiunile furnizate[70] de orice altă autoritate. În special în cauza Kennedy, Curtea și-a exprimat aprobarea cu privire la o autoritate independentă și imparțială care și-a adoptat propriul regulament de procedură și a fost alcătuită din membri care dețineau sau au deținut înalte funcții judiciare sau erau avocați cu experiență[71].

În cadrul examinării plângerilor depuse de persoane fizice, autoritățile vizate de ambele hotărâri au avut, de asemenea, acces la toate informațiile pertinente, inclusiv materiale închise. În cele din urmă, ambele au avut competența de a remedia cazurile de nerespectare[72].

[65] În explicațiile referitoare la Carta drepturilor fundamentale a Uniunii Europene, se arată, de asemenea, că articolul 47 ar trebui interpretat ca oferind o garanție pentru dreptul la o cale de atac eficientă în fața unei instanțe judecătorești [explicații cu privire la Carta drepturilor fundamentale, Explicații referitoare la articolul 47 (2007/C 303/02)].
[66] Cauzele conexate C-584/10 P, C-593/10 P și C-595/10 P, Comisia Europeană și Regatul Unit/Kadi, 18 iulie 2013.
[67] Hotărârea Kadi II, punctele 97 și 100: toate actele Uniunii, inclusiv cele care vizează punerea în aplicare a unor rezoluții adoptate de consilierul de securitate în temeiul capitolului VII din Carta Organizației Națiunilor Unite, se află sub controlul de legalitate efectuat de instanțele Uniunii Europene (capitolul VII se referă la acțiunea în caz de amenințări împotriva păcii, de încălcări ale păcii și de acte de agresiune).
[68] Articolul 13 din Convenție prevede obligația statelor membre de a se asigura că „orice persoană ale cărei drepturi și libertăți (...) sunt încălcate are dreptul să se adreseze efectiv unei instanțe naționale”. Aceasta nu trebuie neapărat să fie o autoritate judiciară, astfel cum a precizat Curtea Europeană a Drepturilor Omului, în cauza Klass, punctele 56 și 67.
69 Klass, punctele 56 și 67.
[70] Curtea Europeană a Drepturilor Omului, cauza Klass, punctele 21 și 53.
[71] Comisia G 10 (la data hotărârii) este formată din trei membri, dintre care președintele trebuie să fie calificat pentru a exercita o funcție judiciară (Klass, punctele 21 și 53).
[72] Curtea Europeană a Drepturilor Omului, cauza Kennedy, punctul 167 și cauza Klass, punctele 21 și 53.

În plus față de întrebarea dacă Ombudsmanul poate fi considerat o „instanță”, aplicarea articolului 47 alineatul (2) din Cartă implică o provocare suplimentară, întrucât acesta prevede că instanța trebuie să fie „constituită prin lege”. Cu toate acestea, nu este clar dacă un memorandum care prezintă modul de funcționare a unui nou mecanism poate fi considerat „legislație”.

În consecință – având în vedere principiul echivalenței esențiale – mai degrabă decât să evalueze dacă un Ombudsman poate fie considerat o instanță constituită prin lege, grupul de lucru a decis să dezvolte în continuare nuanțele jurisprudenței în ceea ce privește cerințele specifice necesare pentru a considera „calea de atac” și „recursul” ca fiind în conformitate cu drepturile fundamentale prevăzute la articolele 7, 8 și 47 din Cartă și la articolul 8 (și 13) din CEDO. În analiza sa în continuare, în discutarea domeniului de aplicare a noului mecanism, grupul de lucru se va concentra pe următoarele criterii: cerința de a depune o cerere la Ombudsman și de a primi un răspuns („calitate procesuală activă”), independența Ombudsmanului, puterea sa de investigare pentru a avea acces la materialele necesare, inclusiv documentele clasificate și pentru a solicita asistență de la alte agenții, și, în cele din urmă, competența sa de a remedia cazurile de nerespectare.

3.5.3.4 Domeniul de aplicare a mecanismului Ombudsmanului

În ceea ce privește accesul la mecanismul Ombudsmanului, GL29 consideră că toate persoanele supuse legislației UE ar trebui să facă obiectul garanțiilor în conformitate cu Scutul de confidențialitate. Nu ar fi acceptabil să se facă o distincție pe motiv de cetățenie sau naționalitate, în special având în vedere faptul că drepturile fundamentale în UE se aplică tuturor, nu doar celor care dețin un pașaport UE. Anexa III se referă la „persoana din UE” fără să o definească. Grupul de lucru regretă această incertitudine și sugerează să se prevadă clarificări în sensul că toate persoanele supuse legislației UE au dreptul la prelucrarea cererilor lor către Ombudsman conform condițiilor din memorandum. În plus, Comisia și SUA ar trebui să abordeze întrebarea în ce măsură Scutul de confidențialitate se va aplica, de asemenea, cetățenilor/rezidenților țărilor din SEE și Elveția, care în trecut au beneficiat de acoperirea oferită de programul privind sfera de siguranță.

În plus, GL29 observă o anumită incertitudine cu privire la domeniul de aplicare a mecanismului Ombudsmanului. În timp ce memorandumul prevede că Ombudsmanul este însărcinat cu tratarea cererilor privind securitatea națională legate de informațiile trimise din UE către SUA în temeiul tuturor instrumentelor de transfer disponibile în cadrul legislației UE, este la fel de clar în memorandum că se stabilește un mecanism „în ceea ce privește colectarea de informații pe baza semnalelor electromagnetice”. Aceasta sugerează că sunt reglementate numai transferurile în cazul în care datele au fost colectate prin intermediul unor activități de colectare de informații pe baza semnalelor electromagnetice, ceea ce conduce la întrebarea dacă, de exemplu, datele colectate în temeiul FISA sunt considerate „informații pe baza semnalelor electromagnetice”. Acest lucru pare să fie valabil în ceea ce privește secțiunea 702, astfel cum se explică în declarația ODNI, p. 10[73]. Cu toate acestea, GL29

[73] Scutul de confidențialitate anexa VI, p. 10.

regretă faptul că utilizarea termenului „informații pe baza semnalelor electromagnetice” creează o incertitudine inutilă în acest context.

Prin urmare, grupul de lucru consideră că mecanismul Ombudsmanului nu se referă la cererile privind accesul agențiilor de aplicare a legii[74]. În cazul unui răspuns afirmativ, ar rămâne neclar dacă cererile formulate de anumite agenții, în special CIA, ar fi reglementate de acest mecanism.

3.5.3.5 „Calitatea procesuală activă” și procedura de solicitare

Inițierea de acțiuni în justiție în fața instanțelor de drept comun din Statele Unite împotriva măsurilor de supraveghere întreprinse de guvernul SUA este foarte dificilă. Grupul de lucru este conștient de faptul că Curtea Supremă a refuzat calitatea procesuală activă în cazurile în care solicitantul nu a fost în măsură să demonstreze „prejudiciu concret, individual și efectiv sau iminent” individual[75]. În această privință, constituirea Ombudsmanului reprezintă un pas important, întrucât mecanismul contribuie la o anumită formă de cale de atac, care altfel nu ar exista. Prin urmare, grupul de lucru salută clarificările din secțiunea 3 litera (c). Pe baza acestei secțiuni, nu este necesară o dovadă a faptului că datele solicitantului au fost, de fapt, accesate prin intermediul activităților de colectare de informații pe baza semnalelor electromagnetice pentru a depune o cerere în cadrul noului mecanism.

Grupul de lucru sprijină în mare parte procedura de identificare a solicitantului în cadrul mecanismului Ombudsmanului. Este perfect logic ca identificarea să aibă loc pe teritoriul UE, acest lucru fiind valabil, de asemenea, pentru mecanismul de acces în temeiul acordului UE-SUA TFTP2. Cu toate acestea, grupul de lucru nu reușește să înțeleagă de ce verificarea în UE ar trebui să fie efectuată de către „organismele statelor membre competente pentru supravegherea serviciilor de securitate națională”. În primul rând, pare puțin probabil ca, în conformitate cu articolul 4 alineatul (2) din Tratatul privind Uniunea Europeană, Comisia Europeană să fie în măsură să atribuie sarcini acestor organisme, care intră în mod clar în sfera de competență a statelor membre.

În plus, având în vedere varietatea mecanismelor de supraveghere a serviciilor de securitate națională din statele membre, implicarea autorităților omoloage pot afecta grav eficiența sistemului pentru resortisanții statelor membre. De exemplu, acest lucru poate fi valabil în cazul în care există mai multe autorități responsabile cu supravegherea serviciilor de securitate națională și ar putea fi dificil ca persoana să o identifice pe cea relevantă, în cazul în care normele juridice naționale aplicabile nu prevăd posibilitatea că persoanele pot intra în contact cu organismul de supraveghere relevant sau în cazul în care aceste autorități nu sunt astfel stabilite încât să îndeplinească sarcinile care le sunt impuse în proiectul de decizie privind caracterul adecvat[76]. Având în vedere implicarea autorităților pentru protecția datelor în aplicarea și supravegherea Scutului de confidențialitate, precum și rolul lor similar în

[74] Comunicare privind instituirea unui Ombudsman, p. 1.
[75] Clapper/Amnesty International, USA, 568 SUA ___ (2013) II p. 10.
[76] De exemplu, în unele state membre ale UE, persoanele fizice pot avea acces la informațiile deținute de serviciile de securitate națională numai în baza unei cereri la Înalta Curte de Justiție.

temeiul acordului TFTP2, este mai justificat să se atribuie această sarcină autorităților naționale de protecție a datelor din statele membre. Grupul de lucru subliniază că acesta consideră puțin probabilă prelucrarea de informații clasificate în cadrul unei proceduri în fața Ombudsmanului pentru Scutul de confidențialitate, întrucât orice răspuns va fi de tipul „conformă sau neconformă, însă remediată”.

3.5.3.6 Independență

Declarațiile Secretarului de Stat precizează că funcția Ombudsmanului va fi îndeplinită de un subsecretar al Departamentului de Stat. Acesta este numit de președintele SUA și necesită confirmarea de către Senat. Rolul Ombudsmanului nu necesită o confirmare suplimentară; alocarea acestui rol este suficientă. Subsecretarul este numit de președintele SUA, desemnat de Secretarul de Stat ca Ombudsman și confirmat de Senatul SUA în rolul său de subsecretar. Astfel cum evidențiază declarațiile din scrisoare și memorandum, Ombudsmanul este „independent de serviciile de informații ale Statelor Unite”. Cu toate acestea, GL29 se întreabă dacă Ombudsmanul este creat în cadrul celui mai adecvat departament. Pentru îndeplinirea în mod eficient a rolului Ombudsmanului, pare a fi necesar un anumit nivel de cunoștințe și înțelegere a modului de funcționare a comunității serviciilor de informații, dar în același timp, este necesară, într-adevăr, o distanță suficientă față de comunitatea serviciilor de informații pentru a fi în măsură să acționeze independent.

Scutul de confidențialitate nu creează criterii specifice pentru destituirea Ombudsmanului. Astfel, grupul de lucru înțelege că Ombudsmanul poate fi destituit din funcția de Ombudsman în același mod în care poate fi destituit din funcția sa de subsecretar în Departamentul de Stat, ceea ce ar putea submina independența Ombudsmanului.

La prima vedere, desemnarea unui subsecretar din cadrul Departamentului de Stat în calitate de Ombudsman este diferită, în mod evident, în ceea ce privește independența față de stabilirea competenței unei instanțe ordinare la care o persoană poate recurge. Prin urmare, întrebarea este dacă Ombudsmanul poate fi considerat, din punct de vedere al independenței, egal cu alte organe de supraveghere independente care au fost considerate conforme. În contextul supravegherii, acestea ar fi, în special, Investigatory Powers Tribunal (IPT) în Regatul Unit și Comisia G10 în Germania.

Acest aspect trebuie evaluat, de asemenea, prin analizarea competențelor acordate organismului „independent”.

3.5.3.7 Competențele de investigare

În hotărârea Kadi II, CJUE s-a pronunțat în ceea ce privește articolul 47 din Cartă, afirmând că „persoana interesată trebuie să poată lua cunoștință de motivele deciziei luate în privința sa fie chiar din cuprinsul deciziei, fie dintr-o comunicare a acestor motive făcută la cererea sa, fără a se aduce atingere posibilității instanței competente de a dispune ca autoritatea în cauză să comunice motivele menționate, pentru a-i permite să își apere drepturile în cele mai bune

condiții posibile”[77]. Instanțele Uniunii Europene trebuie să se asigure că această decizie se întemeiază pe o bază factuală suficient de solidă[78]. Acesta prevede în mod clar că „secretul sau confidențialitatea [...] informațiilor sau a probelor nu este o obiecție validă”, cel puțin nu în fața instanțelor Uniunii Europene[79]. Prin urmare, grupul de lucru concluzionează că Ombudsmanului trebuie să i se ofere informații și dovezi care să susțină motivele reținute pentru efectuarea unei măsuri, în scopul de a îndeplini cerințele Curții de Justiție a Uniunii Europene[80].

Este încă neclar care ar fi amploarea competențelor de investigare ale Ombudsmanului. Nici proiectul de decizie a Comisiei, nici anexa III de la Departamentul de Stat nu sunt foarte clare cu privire la acest aspect. Grupul de lucru consideră că Ombudsmanul ar trebui să primească informații suficiente pentru a fi în măsură să se pronunțe dacă o operațiune de prelucrare a datelor de către serviciile de securitate se desfășoară în conformitate cu legea și, în caz contrar, să se asigure că situația neconformă este remediată. Cu toate acestea, nici scrisoarea de la Departamentul de Stat, nici proiectul de decizie al Comisiei nu precizează dacă Ombudsmanul ar avea acces direct la datele deținute cu privire la persoana în cauză și poate, prin urmare, să efectueze propria anchetă sau dacă acesta se poate baza doar pe rapoartele provenite de la ceilalți funcționari ai guvernului SUA.

3.5.3.8 Competențe de remediere

Rămâne neclar în memorandum modul în care Ombudsmanul poate dispune remedierea neconformității. În combinație cu lipsa de claritate în ceea ce privește competențele de investigare, rămâne neclar în continuare în ce măsură Ombudsmanul ca atare va fi capabil efectiv să dispună remedierea neconformității și care ar fi rezultatul unui astfel de exercițiu. Ar putea însemna acest lucru că datele obținute în mod neconform (adică ilegal) nu mai pot fi utilizate în experimente și ar trebui să fie eliminate?

De asemenea, grupul de lucru consideră că Scutul de confidențialitate nu prevede nicio cale de atac sau măsură de control cu privire la „decizia” Ombudsmanului.

În sfârșit, în ceea ce privește comunicarea Ombudsmanului către reclamant după examinarea unei plângeri, Ombudsmanul nu trebuie să indice dacă a existat vreun comportament ilegal din partea comunității serviciilor de informații. Răspunsul oferit va fi întotdeauna același, iar acesta va fi nespecific. În cauza Kadi II, CJUE a hotărât că autoritatea competentă (în calitate de organism de supraveghere) este obligată să indice motivele care implică toate circumstanțele, deși articolul 296 din TFUE nu impune un răspuns detaliat[81].

[77] Hotărârea Kadi II, punctul 100.
78 Hotărârea Kadi II, punctul 119.
79 Hotărârea Kadi II, punctul 125.
[80] Hotărârea Kadi II punctul 122; deși autoritatea în cauză nu trebuie să prezinte toate informațiile și toate elementele de probă inerente motivelor pentru o măsură.
[81] Hotărârea Kadi II, punctul 116.

3.5.4 În concluzie

Existența unor căi de atac eficiente pentru persoanele fizice reprezintă în continuare un motiv de preocupare pentru GL29. În primul rând, proiectul de decizie privind caracterul adecvat nu oferă un răspuns clar la întrebarea în ce situații și în ce condiții prealabile persoanele fizice pot să introducă o acțiune pentru a stabili drepturile lor.

GL29 recunoaște și salută introducerea unui mecanism de soluționare alternativă a litigiilor sub forma Ombudsmanului, care este o realizare unică în relațiile dintre UE și o țară terță. Pe lângă necesitatea de a clarifica termenul de „persoane din UE", astfel cum s-a arătat mai sus, mecanismul creează o cale de atac suplimentară pentru acestea împotriva administrației SUA, în scopul de a garanta că toate datele cu caracter personal ale reclamantului sunt prelucrate în conformitate cu legislația SUA.

În același timp, atunci când evaluează mecanismul Ombudsmanului pe baza criteriilor pentru o instanță independentă în sensul articolului 47 din Carta drepturilor fundamentale, precum și în conformitate cu cerințele pe care Curtea de Justiție a Uniunii Europene și Curtea Europeană a Drepturilor Omului le-au stabilit în jurisprudența lor în cauzele privind supravegherea, GL29 constată deficiențe semnificative. În primul rând, există preocupări cu privire la faptul că Ombudsmanul poate fi considerat independent (formal și pe deplin), în special datorită relativei ușurințe cu care persoanele numite pe criterii politice pot fi destituite. În al doilea rând, persistă preocupări în ceea ce privește competențele Ombudsmanului de a exercita un control efectiv și continuu. Pe baza informațiilor disponibile în anexa III, GL29 nu poate ajunge la concluzia că Ombudsmanul va avea în orice moment acces direct la toate informațiile, documentele și sistemele informatice necesare pentru a realiza propria sa evaluare și nici că acesta poate obliga agențiile de informații să înceteze orice prelucrare neconformă a datelor, mai ales în caz de dezacord cu privire la chestiunea dacă prelucrarea datelor este sau nu în conformitate cu legea. Eventual, clarificarea suplimentară a poziției și competențelor Ombudsmanului poate înlătura preocupările grupului de lucru.

3.6 Concluzii privind garanțiile și limitările aplicabile autorităților naționale americane de securitate

În primul rând, GL29 salută toate eforturile depuse de Comisie și de autoritățile americane pentru a spori transparența în ceea ce privește efectul pe care programele de supraveghere ale SUA îl pot avea asupra datelor transferate în cadrul Scutului de confidențialitate – sau orice alt instrument de transfer. Au fost luate măsuri semnificative de la primele dezvăluiri ale lui Edward Snowden din iunie 2013. Cu toate acestea, GL29 observă că există încă motive de preocupare. Se impun cel puțin explicații și clarificări suplimentare cu privire la drepturile și obligațiile în temeiul Scutului de confidențialitate.

Cele două preocupări principale ale GL29 sunt că autoritățile SUA nu exclud în totalitate posibilitatea colectării masive și nediferențiate de date și că nu au fost stabilite mai în detaliu competențele și poziția Ombudsmanului. De asemenea, autoritățile naționale pentru protecția datelor, și nu organismele de supraveghere pentru agențiile de informații, ar trebui să aibă

competența de a iniția, în numele unei persoane, o procedură în fața Ombudsmanului. În plus, deși GL29 recunoaște, cu siguranță, încercările de a răspunde preocupărilor exprimate de autoritățile pentru protecția datelor, ar fi binevenite mai multe garanții pentru a se asigura că orice ingerințe care pot fi generate de programele de supraveghere ale SUA sunt justificate într-o societate democratică.

4. EVALUAREA GARANȚIILOR DE APLICARE A LEGII ALE SCUTULUI DE CONFIDENȚIALE

4.1 Introducere

În ceea ce privește accesul public la datele cu caracter personal în scopul aplicării legii, GL29 observă că principiile privind protecția vieții private din anexa II la Scutul de confidențialitate conțin o derogare care este identică cu derogarea prevăzută la principiile privind confidențialitatea ale programului privind sfera de siguranță. Prin urmare, s-a menținut natura generală a derogării, ceea ce înseamnă că noile principii ale Scutului de confidențialitate permit ingerințe în drepturile fundamentale ale persoanelor ale căror date cu caracter personal sunt transferate din UE către SUA, „bazate pe cerințe de securitate națională și de interes public sau pe legislația națională din Statele Unite”[82].

Cu toate acestea, una dintre principalele critici aduse de Curte deciziei privind sfera de siguranță în cauza Schrems a fost că aceasta „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”.

Prin urmare, GL29 salută eforturile depuse de administrația SUA pentru a furniza mai multe informații privind cadrul juridic referitor la ingerința în ceea ce privește datele cu caracter personal transferate în cadrul Scutului de confidențialitate în scopul aplicării legii, inclusiv limitările și garanțiile aplicabile. În același timp, GL29 subliniază că acesta analizează aspectul accesului public luând în considerare faptul că orice ingerință în drepturile fundamentale la viață privată și protecția datelor trebuie să fie justificată într-o societate democratică. Prin urmare, GL29 a analizat garanțiile de aplicare a legii ale Scutului de confidențialitate, utilizând cadrul astfel cum este prevăzut în secțiunea 1.2 din prezentul aviz.

4.2 Aplicarea garanțiilor esențiale europene la accesul autorităților de aplicare a legii la datele deținute de societăți

4.2.1 Accesul autorităților de aplicare a legii la date cu caracter personal ar trebui să respecte legea și să fie bazat pe norme clare, precise și accesibile

Anexa VII la Scutul de confidențialitate conține o scrisoare din partea Departamentului de Justiție al SUA care „cuprinde o scurtă descriere a principalelor instrumente de anchetă utilizate pentru obținerea de date comerciale și alte informații din registrul societăților în

[82] Schrems, punctul 87.

Statele Unite pentru aplicarea legii penale sau în interes public (civil și de reglementare), inclusiv limitări privind accesul prevăzute în aceste mecanisme".

Toate procedurile menționate în anexa VII decurg direct din Constituția SUA (al patrulea amendament), din dispoziții legale și procedurale sau din orientări și politici ale Departamentului de Justiție. Cu toate acestea, anexa VII nu se referă în mod specific la toate textele legislative care prevăd aceste proceduri, ci se axează pe descrierea pe scurt a procedurilor. Anexa VII menționează, de asemenea, că „există alte temeiuri juridice pentru care companiile pot să conteste solicitările de date provenind de la agenții administrative, pe baza propriilor produse și a tipurilor de date pe care le dețin", oferind mai multe exemple neexhaustive, cum ar fi Legea secretului bancar, Fair Credit Reporting Act, Legea privind dreptul la confidențialitate financiară.

GL29 remarcă faptul că acest cadru de texte legislative, proceduri și politici este fragmentat și că temeiul juridic aplicabil pentru o anumită cerere de acces va depinde de natura datelor solicitate, natura companiei, natura procedurilor judiciare (penale, administrative, legate de un alt interes public) și natura entității care solicită accesul.

Întrucât toate normele aplicabile pentru limitarea accesului autorităților de aplicare a legii la date transferate în temeiul Scutului de confidențialitate se bazează pe Constituție, pe dreptul comun și pe politici transparente ale Departamentului de Justiție, GL29 ia în considerare prezumția de accesibilitate a acestor norme. Cu toate acestea, claritatea și precizia normelor pot fi evaluate numai pentru fiecare tip de procedură și cerere de acces. Prin urmare, GL29 regretă să constate că, având în vedere datele disponibile în anexa VII la Scutul de confidențialitate și constatările din proiectul de decizie, la acest moment nu poate fi efectuată o astfel de evaluare.

4.2.2 Trebuie să se demonstreze necesitatea și proporționalitatea în ceea ce privește obiectivele legitime urmărite

GL29 constată în mod corespunzător că solicitarea accesului la date în scopul aplicării legii poate fi considerată ca urmărind un obiectiv legitim. De exemplu, articolul 8 alineatul (2) din CEDO admite ingerințe în dreptul la protecția vieții private de către o autoritate publică „în interesul (...) siguranței publice, (...) în vederea prevenirii dezordinii sau criminalității". Cu toate acestea, astfel de intervenții sunt acceptabile doar în cazul în care sunt necesare și proporționale[83].

Conform unei jurisprudențe constante a CJUE, principiul proporționalității impune ca măsurile legislative care propun ingerințe în dreptul la viață privată și la protecția datelor cu caracter personal „să fie de natură să atingă obiectivele legitime urmărite de *reglementarea în cauză* și să nu depășească limitele a ceea ce este adecvat și necesar pentru realizarea acestor

[83] A se vedea documentul de lucru privind garanțiile esențiale europene, p. 7-9. Pentru o evaluare generală a conceptelor de necesitate și proporționalitate, a se vedea WP29 „Avizul 01/2014 privind aplicarea conceptelor de necesitate și proporționalitate și protecția datelor pentru asigurarea respectării legii", 27 februarie 2014.

obiective”[84] (sublinierea noastră). Prin urmare, evaluarea necesității și proporționalității se face întotdeauna în funcție de o anumită măsură prevăzută de legislație.

Autoritățile SUA specifică în anexa VII că procurorii federali și agenții federali de investigație sunt în măsură să obțină acces la documente și alte informații din registrul organizațiilor prin „mai multe tipuri de procese juridice obligatorii, inclusiv citații emise de marele juriu, citații administrative și mandate de percheziție” și pot obține alte comunicări „în baza mecanismelor de interceptare a convorbirilor (Pen Register)”[85]. În plus, agențiile cu responsabilități civile și de reglementare pot emite citații organizațiilor pentru „documente comerciale, informații stocate electronic sau alte elemente tangibile”[86]. Anexa VII precizează în continuare că aceste proceduri judiciare sunt utilizate, în general, pentru a obține informații de la „companii” din SUA, indiferent dacă acestea sunt certificate sau nu în cadrul Scutului de confidențialitate și „fără a ține cont de cetățenia persoanei vizate”. Cu alte cuvinte, se pare că entitățile vizate de aceste măsuri de protecție sunt organizațiile, nu persoanele fizice însele.

În plus față de anexa VII, proiectul de decizie – care se bazează pe principiile Scutului de confidențialitate – cuprinde constatările Comisiei cu privire la existența în SUA a normelor care vizează limitarea ingerințelor în drepturile fundamentale ale persoanelor ale căror date cu caracter personal sunt transferate din UE către SUA în cadrul Scutului de confidențialitate.

În special, concluziile din proiectul de decizie se referă la limitările și garanțiile aplicabile în temeiul celui de al patrulea amendament la Constituția SUA, conform căruia perchezițiile și sechestrele efectuate de către autoritățile de aplicare a legii necesită în principal un mandat judecătoresc pe baza unui motiv întemeiat[87]. Concluziile se referă, de asemenea, la faptul că, în cazuri excepționale în care cerința mandatului nu se aplică, aplicarea legii trebuie să facă obiectul unei verificări a caracterului rezonabil[88].

Cu toate acestea, constatările nu clarifică modul în care aceste garanții se aplică persoanelor care nu sunt cetățeni americani. În realitate, proiectul de decizie recunoaște într-un considerent că „protecția în temeiul celui de al patrulea amendament nu se extinde la persoanele care nu sunt cetățeni americani care nu sunt rezidente în Statele Unite”[89]. De asemenea, se arată în aceleași alineate din proiectul de decizie că persoanele care nu sunt cetățeni americani „beneficiază indirect, prin protecția acordată companiilor americane care dețin date cu caracter personal și care primesc astfel de cereri de la autorități de aplicare a legii”. Cu toate acestea, GL29 regretă să constate că această constatare nu face nicio trimitere la un temei legal, fie în dreptul comun sau în jurisprudență.

În ansamblu, GL29 observă că sistemul de instrumente de investigare utilizate pentru obținerea de date comerciale și alte informații din registrul societăților din Statele Unite în scopuri de interes public sau de drept penal – inclusiv limitele și garanțiile accesului –

[84] Digital Rights Ireland, punctul 46 și jurisprudența citată.
[85] Anexa VII, p. 2.
[86] Anexa VII, p. 4.
[87] Proiectul de decizie privind caracterul adecvat, punctul 107.
[88] Scutul de confidențialitate, punctul 107.
[89] Proiect de decizie privind caracterul adecvat, punctul 108.

constituie un mediu complex de măsuri. Pe baza informațiilor disponibile, acest sistem nu poate fi evaluat în general la acest moment. Este necesară o evaluare specifică în cazuri individuale pentru a stabili necesitatea și proporționalitatea măsurilor de investigare ale autorităților de aplicare a legii în ceea ce privește drepturile fundamentale la viață privată și protecția datelor.

4.2.3 Ar trebui să existe un mecanism de supraveghere independent

GL29 constată că majoritatea procedurilor descrise în anexa VII presupun implicarea unei decizii a instanței înainte ca autoritățile să obțină acces la date [de exemplu, hotărâri judecătorești de interceptare (Pen Register) și capturare și trasabilitate (Trap and Traces), hotărâri judecătorești de supraveghere conform Legii federale privind interceptarea convorbirilor, mandate de percheziție – norma 41]. Cu toate acestea, se pare că nu toate aceste proceduri necesită implicarea a priori a unei instanțe. De exemplu, autoritățile civile și de reglementare „pot emite citații”[90]. În aceste cazuri, există posibilitatea unui control judiciar ex post privind caracterul rezonabil al citației, întrucât „destinatarul unei somații administrative poate contesta executarea respectivei somații în instanță”[91].

Pe baza informațiilor disponibile, GL29 observă că, în ceea ce privește accesul autorităților de aplicare a legii la datele deținute de companii în SUA, pare să existe un mecanism independent de supraveghere destul de robust.

4.2.4 Persoana trebuie să dispună de căi de atac eficiente

Astfel cum s-a menționat anterior, „protecția în temeiul celui de al patrulea amendament nu se extinde la persoanelor care nu sunt cetățeni americani care nu sunt rezidente în Statele Unite”[92]. Acest lucru înseamnă că o persoană care nu este cetățean american nu ar fi în măsură să conteste în instanță mandate sau citații invocând cel de al patrulea amendament. Proiectul de decizie privind caracterul adecvat precizează că persoanele care nu sunt cetățeni americani beneficiază indirect prin protecția acordată companiilor americane care dețin date cu caracter personal și care primesc astfel de cereri de la autorități de aplicare a legii. Cu toate acestea, GL29 observă că, inclusiv în cazul în care această protecție ar fi eficace, aceasta nu înseamnă că sunt disponibile căi de atac eficace pentru persoanele fizice, întrucât entitatea care face obiectul dreptului la o cale de atac eficace în acest scenariu pare să fie compania care primește cererea de acces și nu persoana fizică a căror date sunt vizate.

Anexa VII nu conține informații suplimentare cu privire la posibilele soluții decurgând din dreptul comun care sunt puse la dispoziția persoanelor care nu sunt cetățeni americani atunci când autoritățile sau companiile oferă sau obțin acces în mod ilegal la conținutul datelor acestora.

[90] Anexa VII, p. 4.
[91] Anexa VII, p. 4.
[92] Proiect de decizie privind caracterul adecvat, punctul 108.

GL29 salută faptul că Legea privind căile de atac[93] recent adoptată prevede dreptul la o cale de atac judiciară pentru persoanele care nu sunt cetățeni americani. Aceste drepturi sunt însă limitate la cauze de acțiune clar definite: dreptul de a obține corectarea și accesul la date și onorariile avocaților atunci când o „componentă sau o agenție federală desemnată" refuză modificarea datelor sau refuză accesul la aceste date, precum și dreptul de a obține despăgubiri civile în cazurile de publicare a datelor „în mod intenționat sau deliberat".

În plus, jurisprudența SUA la care se face trimitere în notele de subsol la considerentele relevante din proiectul de decizie, în special Orașul Ontario/Quon[94], Maryland/King[95] și Samson/California[96], nu este relevantă pentru a evalua dacă persoanele care nu sunt cetățeni americani pot intenta o acțiune în fața instanței pentru a contesta legalitatea unei ingerințe în viața lor privată[97]. Toate cauzele se referă la dreptul la viață privată al persoanelor din SUA și toate conțin decizii ale Curții Supreme a SUA care, în realitate, limitează aplicarea celui de al patrulea amendament.

Cu toate acestea, GL29 recunoaște și salută adoptarea Legii privind căile de atac judiciare, dar are în continuare îndoieli dacă sunt disponibile căi de atac eficiente pentru persoanele vizate individuale.

4.3 Observații finale

GL29 salută și recunoaște eforturile depuse de administrația SUA pentru a furniza mai multe informații privind cadrul juridic referitor la ingerința în ceea ce privește datele cu caracter personal transferate în baza Scutului de confidențialitate UE-SUA în scopul aplicării legii, inclusiv limitările și garanțiile aplicabile.

GL29 remarcă faptul că sistemul instrumentelor de investigare ale autorităților de aplicare a legii, inclusiv limitările și garanțiile aplicabile, este amplu și complex și că informațiile incluse în Scutul de confidențialitate sunt concise. Prin urmare, GL29 regretă că, pe baza informațiilor limitate (și anume, anexa VII la Scutul de confidențialitate și constatările din proiectul de decizie) nu este în măsură să furnizeze o evaluare globală în ceea ce privește accesibilitatea, previzibilitatea și necesitatea, precum și proporționalitatea normelor aplicabile la momentul actual. Fără a aduce atingere altor constatări ale GL29 cu privire la Scutul de confidențialitate din prezentul aviz, o astfel de evaluare ar putea face parte dintr-o revizuire anuală a Scutului de confidențialitate.

---

[93] Legea din 2015 privind căile de atac judiciare, resurse umane 1428.
[94] *Orașul Ontario, Cal./Quon*, 130 S. Ct. 2619, 2630 (2010).
[95] *Maryland/King*, 133 S. CT. 1958, 1970 (2013).
[96] *Samson/California*, 547 U.S. 843, 848 (2006).
[97] În *Ontario/Quon*, Curtea a statuat că orașul Ontario nu încalcă drepturile în temeiul celui de al patrulea amendament ale angajaților, întrucât accesul la conținutul mesajelor personale ale angajatului în cauză ar fi fost acceptabil deoarece aceasta a fost motivat de un scop legitim legat de muncă și nu este excesiv în domeniul său de aplicare. În *Samson/California*, Curtea a constatat că „cel de al patrulea amendament nu interzice unui agent de poliție să efectueze o percheziție nebazată pe suspiciuni întemeiate a unui deținut eliberat condiționat". În *Maryland/King*, Curtea a hotărât că, în cazul în care ofițerii arestează o persoană pe baza unei cauze întemeiate de a reține o persoană suspectată de o infracțiune gravă și a o aduce la postul de poliție să fie reținut în custodie, prelevarea și analizarea unei probe de ADN a persoanei arestate cu ajutorul unui tampon de obraz este, la fel ca amprentarea și fotografierea, o procedură polițienească legitimă de înregistrare în sistem care este rezonabilă în temeiul celui de al patrulea amendament.

În ceea ce privește accesul autorităților de aplicare a legii, GL29 observă că există un mecanism de supraveghere independent destul de robust. În plus, GL29 salută adoptarea Legii privind căile de atac judiciare, care garantează dreptul la o cale de atac judiciară pentru persoanele care nu sunt cetățeni americani. Cu toate acestea, GL29 observă că drepturile respective au un caracter limitat. În plus față de constatarea că o persoană care nu este cetățean american nu ar fi în măsură să conteste în instanță mandate sau citații invocând cel de al patrulea amendament, există în continuare motive de preocupare cu privire la faptul dacă sunt disponibile căi de atac eficiente pentru persoanele vizate individuale în domeniul aplicării legii.

5. CONCLUZII ȘI RECOMANDĂRI

În primul rând, GL29 salută faptul că, în termen de cinci luni de la anularea programului privind sfera de siguranță, a fost prezentat un nou proiect de decizie privind caracterul adecvat, care conține multiple îmbunătățiri în comparație cu mecanismul precedent. Grupul de lucru este deosebit de mulțumit de transparența sporită oferită prin introducerea a două liste ale Scutului de confidențialitate pe site-ul Departamentului Comerțului: o listă cu registrele organizațiilor care aderă la Scutul de confidențialitate și o listă cu registrele organizațiile care au aderat la Scutul de confidențialitate în trecut, dar acest lucru nu mai este valabil. De asemenea, este binevenită sporirea transparenței în ceea ce privește accesul public la datele transferate în temeiul Scutului de confidențialitate, fie din motive de securitate națională, fie pentru aplicarea legii. În final, WP29 este deosebit de încântat să afle că toate transferurile de date către SUA vor beneficiat din acest moment de aceeași protecție: nu există dispoziții legale specifice care să favorizeze un instrument sau altul.

5.1 Trei motive de preocupare

Cu toate acestea, rămân trei motive majore de preocupare, care, în opinia GL29, vor trebui abordate.

Primul motiv de preocupare este faptul că formularea utilizată în proiectul de decizie privind caracterul adecvat nu obligă organizațiile să șteargă datele dacă acestea nu mai sunt necesare. Acesta este un element esențial al legislației UE în materie de protecție a datelor pentru a se asigura că datele nu sunt păstrate mai mult timp decât este necesar pentru îndeplinirea scopului în care au fost colectate. În al doilea rând, GL29 înțelege din anexa VI că administrația SUA nu exclude pe deplin continuarea colectării masive și nediferențiate de date. GL29 a susținut în mod constant că o astfel de colectare de date constituie o ingerință nejustificată în drepturile fundamentale ale persoanelor. Al treilea motiv de preocupare se referă la instituirea mecanismului Ombudsmanului. Deși GL29 salută pasul fără precedent reprezentat de crearea unui mecanism de recurs și de supraveghere suplimentar pentru persoanele fizice, există încă motive de preocupare cu privire la faptul dacă Ombudsmanul dispune de competențe suficiente să funcționeze eficient. Ca o condiție minimă, atât competențele, cât și poziția Ombudsmanului trebuie să fie clarificate pentru a demonstra că rolul său este cu adevărat independent și poate oferi o cale de atac eficientă în cazul prelucrării neconforme a datelor.

5.2 Clarificări recomandate

În plus față de punctele menționate mai sus, GL29 a indicat în cuprinsul prezentului aviz mai multe puncte în care sunt necesare clarificări suplimentare ale deciziei privind caracterul adecvat. Cel mai important, este vizată necesitatea de a se asigura că principalele noțiuni privind protecția datelor utilizate în cadrul Scutului de confidențialitate sunt definite și aplicate în mod consecvent. Acest lucru nu este valabil în prezent. Ar fi binevenită introducerea unui glosar de termeni în secțiunea de întrebări frecvente privind Scutul de confidențialitate, în mod ideal cu definiții convenite între UE și SUA. GL29 concluzionează, de asemenea, că transferurile ulterioare de date cu caracter personal din UE nu sunt suficient de reglementate, în special în ceea ce privește domeniul lor de aplicare, limitarea scopului și garanțiile aplicabile transferurilor către agenți. În ceea ce privește accesul organelor de aplicare a legii la datele Scutului de confidențialitate, în special caracterul previzibil al legislației constituie un motiv de preocupare, având în vedere natura vastă și complexă a sistemului de aplicare a legii din SUA, atât la nivel federal, cât și la nivel de stat, precum și informațiile limitate incluse în decizia privind caracterul adecvat.

Scutul de confidențialitate este prima decizie privind caracterul adecvat care a fost elaborată după ce au fost convenite, în principiu, textele Regulamentului general privind protecția datelor. Cu toate acestea, multe dintre îmbunătățirile la nivelul protecției datelor oferite de acesta persoanelor fizice nu sunt reflectate în Scutul de confidențialitate. Prin urmare, GL29 recomandă efectuarea unei revizuiri a actualei decizii privind nivelul adecvat, precum și a deciziilor privind caracterul adecvat emise pentru alte țări terțe, la scurt timp după intrarea în vigoare a Regulamentului general privind protecția datelor.

O ultimă recomandare a GL29 subliniată aici se referă la revizuirea comună. GL29 salută faptul că decizia privind caracterul adecvat al Scutului de confidențialitate va fi într-adevăr revizuită anual, cu o largă implicare a autorităților pentru protecția datelor și a altor părți relevante. GL29 ar saluta ajungerea la un acord, cu mult timp înainte de prima revizuire, cu privire la elementele revizuirilor comune, inclusiv în ceea ce privește elaborarea și prezentarea raportului de revizuire de către toate părțile.