GRUPUL DE LUCRU „ARTICOLUL 29” PENTRU PROTECȚIA DATELOR

819/14/RO
WP 215

Avizul 04/2014 privind supravegherea comunicațiilor electronice în scopul colectării de date operative și al asigurării securității naționale

Adoptat la 10 aprilie 2014

Acest grup de lucru a fost instituit în temeiul articolului 29 din Directiva 95/46/CE. Acesta este un organ consultativ independent european privind protecția datelor și a vieții private. Atribuțiile sale sunt prezentate la articolul 30 din Directiva 95/46/CE și la articolul 15 din Directiva 2002/58/CE.

Secretariatul este asigurat de Direcția C (Drepturi fundamentale și cetățenia Uniunii) din cadrul Comisiei Europene, Direcția Generală Justiție, B-1049 Bruxelles, Belgia, Biroul MO- 59 02/013.

Adresa web: http://ec.europa.eu/justice/data-protection/index_ro.htm

Rezumat

Începând cu vara anului 2013, mai multe mijloace de comunicare în masă din întreaga lume au prezentat pe larg informații cu privire la activitățile de supraveghere desfășurate de serviciile de informații, atât în Statele Unite, cât și în Uniunea Europeană, pe baza documentelor furnizate, în principal, de Edward Snowden. Dezvăluirile au declanșat o dezbatere internațională cu privire la consecințele unei astfel de supravegheri pe scară largă asupra vieții private a cetățenilor. Modul în care serviciile de informații utilizează atât datele referitoare la comunicațiile noastre de zi cu zi, cât și conținutul respectivelor comunicații subliniază necesitatea de a se stabili limite în ceea ce privește amploarea supravegherii.

Dreptul la viață privată și la protecția datelor cu caracter personal este un drept fundamental consacrat în Pactul internațional cu privire la drepturile civile și politice, în Convenția europeană a drepturilor omului și în Carta drepturilor fundamentale a Uniunii Europene. Rezultă că respectarea statului de drept implică în mod necesar ca acestui drept să i se acorde cel mai înalt nivel de protecție posibil.

În urma analizei sale, Grupul de lucru concluzionează că programele de supraveghere secretă, masivă și nediscriminatorie sunt incompatibile cu legile noastre fundamentale și nu pot fi justificate de lupta împotriva terorismului sau de alte amenințări importante la adresa securității naționale. Restricțiile în ceea ce privește drepturile fundamentale ale tuturor cetățenilor ar putea fi acceptate numai în cazul în care măsura este strict necesară și proporțională în cadrul unei societăți democratice.

Din acest motiv, Grupul de lucru recomandă o serie de măsuri menite să asigure garantarea și respectarea statului de drept.

În primul rând, Grupul de lucru solicită o mai mare transparență cu privire la modul în care funcționează programele de supraveghere. Transparența contribuie la îmbunătățirea și la restabilirea unui climat de încredere între cetățeni, guverne și entități private. O astfel de transparență include o mai bună informare a persoanelor în cazul în care serviciile de informații au fost autorizate să aibă acces la date care le vizează. În vederea unei mai bune informări a persoanelor cu privire la consecințele pe care le-ar putea avea utilizarea serviciilor de comunicații electronice online și offline, precum și cu privire la modul în care aceștia se pot proteja mai eficient, Grupul de lucru intenționează să organizeze, în a doua jumătate a anului 2014, o conferință privind supravegherea care să reunească toate părțile interesate relevante.

De asemenea, Grupul de lucru pledează cu fermitate pentru o monitorizare mai atentă a activităților de supraveghere. Supravegherea eficace și independentă a serviciilor de informații, inclusiv a prelucrării datelor cu caracter personal, este esențială pentru asigurarea faptului că nu se va abuza de aceste programe. Prin urmare, Grupul de lucru consideră că o supraveghere eficace și independentă a serviciilor de informații presupune o implicare efectivă a autorităților pentru protecția datelor.

Grupul de lucru recomandă, de asemenea, aplicarea obligațiilor existente ale statelor membre ale UE și ale părților la CEDO în vederea protejării drepturilor la respectarea vieții private și la protecția datelor cu caracter personal. În plus, Grupul de lucru reamintește faptul că operatorii de date care fac obiectul jurisdicției UE trebuie să respecte legislația aplicabilă în vigoare a UE în materie de protecție a datelor. Grupul de lucru reamintește, de asemenea, faptul că autoritățile pentru protecția datelor pot suspenda fluxurile de date și ar trebui să decidă, în conformitate cu atribuțiile care le revin în temeiul legislației naționale, dacă într-o anumită situație se impun sancțiuni.

Nici principiul „sferei de siguranță", nici clauzele contractuale standard, nici regulile corporatiste obligatorii nu ar putea servi drept temei juridic pentru a justifica transferul de date cu caracter personal către o autoritate a unei țări terțe în scopul unei supravegheri în masă și generalizate. În fapt, excepțiile prevăzute în aceste instrumente au un domeniu de aplicare limitat și ar trebui interpretate în mod restrictiv. Acestea nu ar trebui să fie niciodată puse în aplicare în detrimentul nivelului de protecție garantat de normele și de instrumentele UE care reglementează transferurile.

Grupul de lucru solicită instituțiilor UE să finalizeze negocierile referitoare la pachetul de reforme privind protecția datelor. Acesta salută, în special, propunerea Parlamentului European privind un nou articol 43a, care prevede informarea obligatorie a persoanelor în cazul în care, în ultimele douăsprezece luni, s-a permis unei autorități publice să aibă acces la date care le vizează. Transparența cu privire la aceste practici va spori în mod semnificativ încrederea.

De asemenea, Grupul de lucru consideră că domeniul de aplicare a exceptării privind securitatea națională ar trebui clarificat pentru a oferi securitate juridică în ceea ce privește domeniul de aplicare a dreptului UE. Până în prezent, legiuitorul european nu a adoptat nicio definiție clară a conceptului de securitate națională și nici jurisprudența instanțelor europene nu este concludentă în acest sens.

În fine, Grupul de lucru recomandă începerea rapidă a negocierilor privind un acord internațional pentru a acorda persoanelor garanții adecvate în materie de protecție a datelor în cazul în care se desfășoară activități operative. Grupul de lucru sprijină, de asemenea, elaborarea unui instrument aplicabil la nivel mondial care să prevadă principii executorii pentru a se asigura un nivel ridicat de protecție a vieții private și a datelor.

GRUPUL DE LUCRU PENTRU PROTECȚIA PERSOANELOR

ÎN CEEA CE PRIVEȘTE PRELUCRAREA DATELOR CU CARACTER PERSONAL

instituit prin Directiva 95/46/CE a Parlamentului European și a Consiliului din

24 octombrie 1995,

având în vedere articolul 29 și articolul 30 alineatul (1) litera (c) și alineatul (3) din directivă,

având în vedere regulamentul său de procedură, în special articolele 12 și 14,

ADOPTĂ PREZENTUL AVIZ:

1. Introducere

Începând cu vara anului 2013, mai multe mijloace de comunicare în masă din întreaga lume au prezentat pe larg informații cu privire la activitățile de supraveghere electronică desfășurate de serviciile de informații, atât în Statele Unite ale Americii (SUA) și în Uniunea Europeană (UE), cât și în întreaga lume, în special pe baza documentelor furnizate de Edward Snowden. Dezvăluirile au declanșat o dezbatere internațională cu privire la consecințele unei astfel de supravegheri electronice pe scară largă asupra vieții private a cetățenilor. De asemenea, au fost formulate întrebări referitoare la amploarea sferei de acțiune care ar trebui să fie permisă din punct de vedere juridic serviciilor de informații atât în ceea ce privește colectarea, cât și utilizarea de informații referitoare la viața noastră de zi cu zi. Prezentul aviz conține rezultatele analizelor juridice efectuate de autoritățile pentru protecția datelor din UE, reunite în cadrul Grupului de lucru „articolul 29” („Grupul de lucru”), cu privire la implicațiile programelor de supraveghere electronică pentru protejarea dreptului fundamental la protecția datelor și la viață privată.

Principala sarcină a autorităților pentru protecția datelor este de a proteja dreptul fundamental la protecția datelor pentru toate persoanele și de a asigura faptul că operatorii de date respectă dispozițiile legislative aplicabile. Cu toate acestea, în ceea ce privește serviciile de informații, numeroase autorități pentru protecția datelor au doar competențe de supraveghere limitate sau nu au nicio competență de supraveghere. Pentru supravegherea serviciilor de informații, inclusiv în ceea ce privește prelucrarea datelor cu caracter personal, statele membre au instituit alte mecanisme. Prin urmare, Grupul de lucru a făcut un inventar al diferitelor mecanisme din UE cu rol de supraveghere a serviciilor de informații, care este inclus în prezentul aviz.

Prezentul aviz nu analizează scenariile referitoare la interceptarea datelor cu caracter personal transmise prin cablu. În această etapă, Grupul de lucru nu are suficiente informații disponibile cu privire la această presupusă situație pentru a evalua regimul juridic aplicabil, chiar și într-un mod ipotetic.

2. Metadate

Pentru a evalua amploarea posibilelor încălcări ale normelor privind protecția datelor, este necesar, în primul rând, să fie clar subiectul abordat. Funcționarii guvernamentali se referă deseori la colectarea de metadate, sugerând că acest lucru este mai puțin grav decât colectarea de conținut. Aceasta nu este o ipoteză corectă. Metadatele sunt toate datele cu privire la o comunicare efectuată, cu excepția conținutului convorbirii. Acestea pot include numărul de telefon sau adresa IP a persoanei care a efectuat un apel telefonic sau care a trimis un e-mail, informații privind ora și locul, obiectul, destinatarul etc. Analiza acestora poate dezvălui date sensibile despre persoane, de exemplu, pentru că sunt formate anumite numere de informații către centre medicale sau religioase. Astfel cum s-a pronunțat deja Curtea Europeană a Drepturilor Omului în cauza Malone [1], prelucrarea metadatelor, în speță „contorizarea", „constituie un element integrant al comunicărilor efectuate prin telefon. În consecință, punerea informațiilor respective la dispoziția poliției fără consimțământul abonatului constituie, de asemenea, [...] o ingerință într-un drept garantat de articolul 8". Curtea și-a menținut această poziție de-a lungul anilor.

De asemenea, este deosebit de important să se aibă în vedere faptul că, adesea, metadatele generează mai ușor informații decât conținutul efectiv al comunicațiilor[2]. Acestea sunt ușor de agregat și de analizat datorită caracterului lor structurat. Instrumentele informatice sofisticate permit analizarea unor seturi considerabile de date în vederea identificării unor tipare și relații integrate, inclusiv date personale, obiceiuri și comportamente. Acest lucru nu este valabil în cazul conversațiilor, care pot avea loc în orice formă sau limbă. Instrumentele informatice sofisticate permit analizarea unor seturi considerabile de date în vederea identificării unor tipare și relații integrate, inclusiv date personale, obiceiuri și comportamente.

Conform articolului 2 litera (a) din Directiva 95/46/CE, date cu caracter personal înseamnă „orice informație referitoare la o persoană fizică identificată sau identificabilă (persoana vizată); o persoană identificabilă este o persoană care poate fi identificată, direct sau indirect". O definiție similară este prevăzută la articolul 2 litera (a) din Convenția 108 a Consiliului Europei pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal. Prin urmare, spre deosebire de alte țări, în Europa, metadatele sunt date cu caracter personal și ar trebui să fie protejate[3].

În hotărârea recentă în cauzele privind păstrarea datelor, Curtea de Justiție a Uniunii Europene a confirmat faptul că în condițiile în care sunt „considerate în ansamblu, datele respective [din telecomunicații] pot permite deducerea unor concluzii foarte precise privind viața privată a persoanelor ale căror date au fost păstrate"[4]. În fine, în hotărârea respectivă, Curtea a decis că „obligația de a păstra pentru o anumită perioadă date referitoare la viața privată a unei

[1] CEDO, Malone/Regatul Unit, 2 august 1984.

[2] ACLU/Clapper, cauza nr. 13-3994 (WHP) – Declarație scrisă a profesorului Edward W. Felten în fața *United States District Court for the Southern District of New York*.

[3] Aceasta este o interpretare tradițională a legislației privind protecția datelor. În avizul său nr. 4/2007 privind conceptul de date cu caracter personal, Grupul de lucru a declarat deja că, inclusiv „în cazurile în care, la prima vedere, numărul identificatorilor disponibili nu permite separarea unei anumite persoane, persoana respectivă ar putea fi în continuare «identificabilă», întrucât informațiile respective în combinație cu alte informații (indiferent dacă acestea din urmă sunt reținute de operator sau nu) permit identificarea persoanei de alți subiecți".

[4] A se vedea CEJ, cauzele conexate C-293/12 și C-594/12, 8 aprilie 2014, punctul 27.

persoane și la comunicațiile sale constituie *per se* o ingerință în drepturile garantate de articolul 7 din cartă. În plus, accesul autorităților naționale competente la date constituie o ingerință suplimentară în acest drept fundamental. [...] În plus, împrejurarea că păstrarea datelor și utilizarea lor ulterioară sunt efectuate fără ca abonatul sau utilizatorul înregistrat să fie informați cu privire la aceasta este susceptibilă să genereze în mintea persoanelor vizate sentimentul că viața lor privată face obiectul unei supravegheri constante”[5].

3. Puncte principale

Dezvăluirile făcute de Snowden au fost un puternic semnal de alarmă pentru mulți. Niciodată înainte nu a mai fost divulgată existența unui număr atât de mare de programe de supraveghere derulate de către serviciile de informații și capabile să colecteze date cu privire la practic orice persoană. În trecut au mai existat unele cazuri, însă acum au fost aduse pentru prima dată în dezbatere dovezi ample cu privire la omniprezența acestora. Modul în care serviciile de informații utilizează atât datele privind comunicațiile noastre de zi cu zi, cât și conținutul comunicațiilor respective subliniază necesitatea de a se stabili limite în ceea ce privește amploarea supravegherii.

Chiar și cei care sunt atenți la modul în care își gestionează viața online nu pot, în prezent, să se protejeze împotriva programelor de supraveghere în masă. Având în vedere, de asemenea, numeroasele provocări juridice, tehnice și practice, nici măcar autoritățile pentru protecția datelor din întreaga lume nu pot furniza o protecție satisfăcătoare. Prin urmare, se impune o schimbare.

În secțiunile următoare, Grupul de lucru „articolul 29” analizează activitatea de colectare în masă a datelor care este efectuată de serviciile de informații în cadrul programelor lor de supraveghere. Din punct de vedere juridic, trebuie să se facă distincția între programele de supraveghere derulate de serviciile de informații din statele membre și cele derulate de serviciile de informații din țările terțe care utilizează date referitoare la cetățenii din UE.

Programele de supraveghere derulate de statele membre ale UE nu fac, în general, obiectul dreptului UE, respectându-se exceptarea privind securitatea națională prevăzută în tratatele europene, și, în urma deciziei statelor membre contractante, nu fac nici obiectul mai multor regulamente și directive ale UE, inclusiv Directiva 95/46/CE privind protecția datelor. Acest lucru nu înseamnă însă că astfel de programe fac doar obiectul legislației naționale. Analiza efectuată de Grupul de lucru „articolul 29” arată că, deși dreptul UE, în general, și Directiva privind protecția datelor, în particular, nu se aplică, principiile de protecție a datelor[6], în conformitate cu dispozițiile Convenției Europene a Drepturilor Omului și ale Convenției 108 a Consiliului Europei privind protecția datelor cu caracter personal, trebuie, în cea mai mare parte, să fie respectate de către serviciile de informații pentru a-și îndeplini atribuțiile în mod legal. Deseori, aceste principii sunt, de asemenea, incluse în constituțiile naționale ale statelor membre. Programele de supraveghere bazate pe colectarea generalizată și nediferențiată de date cu caracter personal nu pot îndeplini, sub nicio formă, cerințele de necesitate și

[5] A se vedea CEJ, cauzele conexate C-293/12 și C-594/12, 8 aprilie 2014, punctele 34, 35 și 37.

[6] Cele mai importante principii de protecție a datelor sunt următoarele: prelucrarea corectă și legală a datelor, limitarea scopului, necesitatea și proporționalitatea, exactitatea, transparența, respectarea drepturilor persoanelor și securitatea adecvată a datelor.

proporționalitate prevăzute în aceste principii de protecție a datelor. Limitările drepturilor fundamentale trebuie să fie interpretate în mod restrictiv, în conformitate cu jurisprudența Curții Europene a Drepturilor Omului (CEDO)[7] și a Curții de Justiție a Uniunii Europene (CJUE)[8]. Aceasta implică faptul că toate intervențiile trebuie să fie necesare și proporționale în raport cu scopul urmărit. De asemenea, ar trebui să se țină seama de faptul că nu există nicio prezumție automată conform căreia argumentul referitor la securitatea națională utilizat de o autoritate națională există și este valabil. Acest lucru trebuie să fie demonstrat.

Grupul de lucru subliniază faptul că guvernele statelor membre au responsabilitatea de a-și respecta toate obligațiile naționale și internaționale, inclusiv cele care rezultă în temeiul Pactului internațional cu privire la drepturile civile și politice. Nerespectarea acestor obligații constituie nu numai o încălcare a drepturilor fundamentale ale cetățenilor lor, ci și o acțiune care are ca efect diminuarea încrederii societății în statul de drept.

În ceea ce privește programele de supraveghere derulate de țările terțe, situația este mai complexă. Atunci când sunt colectate date, fie direct de la o sursă din UE, fie în urma unui transfer către țara terță respectivă (sau către o altă țară terță), dreptul UE poate fi aplicabil în continuare în cazul divulgărilor efectuate în cadrul programelor de supraveghere. În fapt, exceptarea privind securitatea națională menționată mai sus se aplică numai în cazul securității naționale a unui stat membru al UE, și nu în cazul securității naționale a unei țări terțe. Desigur, pot apărea situații în care interesul de securitate națională al unei țări terțe coincide cu cel al unui stat membru, caz în care operațiunile comune de supraveghere pot fi justificate. Și în acest caz, autoritățile publice implicate în supraveghere trebuie să poată fi în măsură să dovedească motivul și modul în care interesele de securitate națională coincid, excluzând astfel aplicarea dreptului UE.

Toate condițiile privind transferurile internaționale de date cu caracter personal, stabilite în Directiva 95/46/CE, trebuie să fie respectate: acest lucru înseamnă, mai întâi de toate, că destinatarul trebuie să asigure un nivel adecvat de protecție și că transferurile trebuie să se efectueze în conformitate cu scopul inițial pentru care au fost colectate datele. De asemenea, transferurile trebuie să se bazeze pe un temei juridic adecvat pentru o prelucrare corectă și legală.

Niciunul dintre instrumentele disponibile care pot fi utilizate ca o alternativă pentru a transfera date cu caracter personal în țări care nu au fost considerate adecvate (principiul „sferei de siguranță”, clauzele contractuale standard și regulile corporatiste obligatorii) nu permite autorităților publice din țările terțe să obțină acces la datele cu caracter personal transferate pe baza acestor instrumente, în scopul unei supravegheri în masă și generalizate. De fapt, excepțiile incluse în aceste instrumente au un domeniu de aplicare limitat și ar trebui să fie interpretate în mod restrictiv (și anume, să fie utilizate în anumite cazuri și pentru anchete specifice). Întrucât instrumentele de adecvare sunt destinate, în principal, să ofere protecție datelor cu caracter personal care provin din UE, acestea nu ar trebui să fie niciodată

[7] A se vedea hotărârile CEDO în cauza Delcourt, 17 ianuarie 1970, și în cauza Klass, 6 septembrie 1978.

[8] A se vedea CEJ, cauzele conexate C-293/12 și C-594/12, 8 aprilie 2014, în care Curtea a hotărât că păstrarea datelor de trafic „fără a face vreo diferențiere, limitare sau excepție” constituie „o ingerință în aceste drepturi fundamentale, care este de o mare amploare și de o gravitate deosebită în ordinea juridică a Uniunii, fără ca o astfel de ingerință să fie încadrată în mod precis de dispoziții care să permită garantarea faptului că ea este limitată efectiv la strictul necesar” (punctele 57 și 65).

puse în aplicare în detrimentul nivelului de protecție garantat de normele și instrumentele UE care reglementează transferurile. De asemenea, Grupul de lucru subliniază faptul că, în temeiul Directivei privind protecția datelor, actuala evaluare a nivelului de protecție a datelor în țările terțe, în general, nu acoperă prelucrarea datelor în scopul asigurării respectării legii sau în scopuri de supraveghere.

De asemenea, întreprinderile trebuie să fie conștiente de faptul că pot să încalce dreptul Uniunii dacă serviciile de informații din țările terțe obțin accesul la datele cetățenilor europeni stocate pe serverele lor sau se conformează unui ordin de transmitere de date cu caracter personal pe scară largă. În această privință, întreprinderile se pot afla într-o poziție dificilă atunci când trebuie să decidă dacă să respecte sau nu ordinul de a furniza date cu caracter personal pe scară largă: în oricare din cele două cazuri, acestea riscă să încalce legislația Uniunii sau legislația unei țări terțe. Măsurile executorii împotriva acestor întreprinderi nu ar trebui să fie excluse, în special în situațiile în care operatorii de date au cooperat de bunăvoie și în cunoștință de cauză cu serviciile de informații pentru a le oferi acces la datele pe care le dețin. Întreprinderile trebuie să fie cât se poate de transparente și să se asigure că persoanele vizate sunt informate că, din momentul în care datele lor cu caracter personal sunt transferate către țări terțe care nu asigură un nivel adecvat de protecție, pe baza instrumentelor disponibile pentru astfel de transferuri, datele respective ar putea face obiectul supravegherii de către autoritățile publice din țările terțe sau ar putea să fie accesate de autoritățile publice din țările terțe, în măsura în care astfel de derogări sunt prevăzute de instrumentele menționate anterior. Principalul obiectiv este însă acela de a identifica o soluție eficientă la nivel politic. Un acord internațional care să ofere garanții ar putea să asigure respectarea drepturilor fundamentale de către serviciile de informații.

Pentru a se asigura faptul că serviciile de informații respectă, într-adevăr, limitele impuse în ceea ce privește programele de supraveghere, este necesar să fie puse în aplicare mecanisme de supraveghere adecvată în legislația tuturor statelor membre. Aceasta ar trebui să cuprindă controale complet independente ale operațiunilor de prelucrare a datelor, efectuate de un organism independent, precum și competențe efective în materie de asigurare a respectării legii. În paralel cu un control parlamentar eficace și solid, această sarcină de supraveghere ar putea să fie îndeplinită de o autoritate pentru protecția datelor sau de un alt organism independent adecvat, în funcție de acordurile de supraveghere adoptate de statul membru. În cazul în care supravegherea ar urma să fie asigurată de un alt organism, Grupul de lucru încurajează contactele regulate între organismul respectiv și autoritatea națională pentru protecția datelor în vederea garantării unei aplicări coerente și consecvente a principiilor de protecție a datelor.

Ar trebui subliniat faptul că mecanismele de supraveghere nu trebuie să existe doar pe hârtie, ci și să fie aplicate, de asemenea, în mod consecvent. Dezvăluirile făcute de Snowden au arătat că, deși pe hârtie există numeroase mecanisme de control și echilibru, inclusiv controlul jurisdicțional al sistemelor utilizate pentru colectarea de date, eficacitatea modului în care garanțiile au fost puse în aplicare rămâne îndoielnică. În cazul în care garanțiile împotriva accesului nejustificat nu sunt aplicabile tuturor programelor de supraveghere și nici tuturor persoanelor, acestea nu contribuie la ceea ce Grupul de lucru consideră a fi o supraveghere adecvată.

4. Supravegherea serviciilor de informații

În timp ce alte entități au efectuat anul trecut analize de specialitate privind mecanismele de supraveghere a serviciilor de securitate și de informații din țările terțe, mai puține analize de specialitate au avut ca obiect serviciile naționale de informații din fiecare stat membru al UE. Pentru a obține o imagine mai clară asupra diferitelor mecanisme din Europa care au rolul de a supraveghea serviciilor naționale de informații, Grupul de lucru a publicat un chestionar adresat tuturor autorităților pentru protecția datelor (inclusiv celor doi observatori din afara UE), în scopul de a afla mai multe informații cu privire la practicile lor naționale de supraveghere în materie[9].

Există două aspecte care merită să fie analizate, în special:

1. existența unei supravegheri cuprinzătoare în cadrul juridic pentru serviciile naționale de securitate și de informații;

2. rolul (sau absența rolului) autorității naționale de supraveghere pentru protecția datelor în cadrul respectiv.

În continuare, Grupul de lucru răspunde, de asemenea, solicitării formulate de dna Reding, vicepreședintele Comisiei Europene, de a analiza rolul pe care l-ar putea îndeplini autoritățile pentru protecția datelor[10].

4.1. Prezentare generală a mecanismelor naționale de supraveghere aplicabile

Activitățile de supraveghere analizate în prezentul aviz și în documentul de lucru anexat sunt derulate, în principal, de serviciile de informații în cadrul misiunii lor de a proteja securitatea națională. Există o mare diversitate de modele de supraveghere, în funcție de tradițiile juridice naționale și de structurile responsabile de asigurarea securității naționale. În 26 din 27 de state membre care au răspuns la chestionar[11], serviciile de informații sunt instituite și își desfășoară activitatea în temeiul unor legi care prevăd competențele, structura și responsabilitățile

[9] La chestionar au răspuns 27 de autorități naționale pentru protecția datelor din UE, autoritatea pentru protecția datelor din Saxonia (Germania), precum și autoritățile pentru protecția datelor din Elveția și din Serbia, care nu fac parte din UE.
[10] Scrisoarea doamnei vicepreședinte Reding către președintele Grupului de lucru „articolul 29”, 30 august 2013.
[11] Austria, Belgia, Bulgaria, Cipru, Republica Cehă, Danemarca, Estonia, Finlanda, Franța, Germania, Grecia, Ungaria, Italia, Letonia, Lituania, Luxemburg, Malta, Țările de Jos, Polonia, Portugalia, România, Slovacia, Slovenia, Spania, Suedia, Regatul Unit.

acestora. Într-un singur stat membru nu există un serviciu de informații, iar funcția de asigurare a securității statului este îndeplinită de serviciul național de poliție[12].

Majoritatea respondenților au menționat existența unui număr cuprins între una și trei autorități responsabile de asigurarea securității și de activitatea de informații la nivel național. În general, există o separare a sarcinilor între amenințările interne la adresa securității naționale și amenințările externe (străine) la adresa securității naționale, ceea ce conduce, de asemenea, la responsabilități diferite, civile (Ministerul de Interne sau de Justiție) și militare (Ministerul Apărării). În trei state, diferitele structuri sunt integrate astfel încât să formeze un sistem de protecție care răspunde, în mod direct, în fața șefului guvernului (de exemplu, prim-ministrul).

Prelucrarea datelor cu caracter personal se bazează pe o lege adoptată la nivel național în statul membru în cauză, iar supravegherea se bazează fie pe legislația generală privind protecția datelor (denumită în continuare „LGPD"), fie pe una sau mai multe legi speciale care reglementează prelucrarea datelor cu caracter personal de către unul sau mai multe servicii de informații.

4.2. Rolul autorității naționale pentru supravegherea protecției datelor

Din evaluarea legislației naționale aplicabile reiese în mod clar faptul că LGPD din multe țări nu se aplică activităților desfășurate de serviciile de informații și că autoritatea pentru protecția datelor are un rol de supraveghere limitat sau, în unele cazuri, inexistent. Adesea, un regim specific de protecție a datelor este prevăzut de lege, însă acesta nu include în mod necesar o supraveghere specifică de către autoritatea pentru protecția datelor.

În cele două țări din afara UE care au răspuns cu amabilitate la chestionar[13], prelucrarea datelor cu caracter personal de către serviciile de informații este reglementată de LGPD. Acestea fac obiectul supravegherii de către autoritatea națională pentru protecția datelor pe baza dispozițiilor prevăzute în LGPD.

Atunci când este aplicabilă, LGPD prevede, în general, o serie de exceptări (derogări de la unul sau mai multe principii) pentru prelucrarea datelor cu caracter personal de către serviciile de informații. Exceptările se referă, în mod obișnuit, la atribuțiile de bază ale operatorilor de date și la drepturile persoanei vizate[14]. Limitările pot avea ca obiect restricționarea dreptului de a fi informat și a dreptului de acces al persoanei vizate care sunt, în general, exercitate prin intermediul autorității pentru protecția datelor.

În ceea ce privește supravegherea prelucrării datelor, numai în patru state membre se pare că legile naționale generale privind protecția datelor (sau legile prin care se instituie organismele generale de supraveghere a protecției datelor) prevăd, în principiu, aceleași competențe de supraveghere a serviciilor de informații ca și în cazul oricărui alt operator de date[15]. În treisprezece state membre, sfera de competență a autorității pentru protecția datelor include

[12] Irlanda.
[13] Serbia (un serviciu civil, două servicii militare), Elveția (un serviciu civil, un serviciu militar).
[14] De exemplu, Belgia, Bulgaria, Cipru, Germania, Ungaria, Grecia. Pentru unele state membre nu au putut fi stabilite informații privind exceptările.
[15] Bulgaria, Ungaria, Slovenia, Suedia.

serviciile naționale de securitate și de informații, însă, în unele cazuri, se aplică norme sau proceduri speciale în cazul supravegherii serviciilor de informații, fiind prevăzută și posibilitatea de a impune sancțiuni[16]. În nouă state membre, autoritatea pentru protecția datelor nu are competențe de supraveghere a serviciilor de informații care își desfășoară activitatea în calitate de operatori de date[17].

Doar în Suedia și în Slovenia, respectarea obligațiilor aplicabile în materie de protecție a datelor face obiectul unei supravegheri depline de către autoritatea pentru protecția datelor. În cazul în care alte autorități naționale pentru protecția datelor au competențe asupra activității serviciilor de informații, acestea controlează conformitatea cu LGPD aplicabilă și gestionează plângerile și exercitarea dreptului de acces de către persoana vizată. De asemenea, acestea au competența de a investiga cazuri, fie din proprie inițiativă, fie la cererea unei părți terțe, și de a efectua inspecții *in situ*. În unele state membre, pot exista unele limitări ale acestor competențe, de exemplu, prin impunerea respectării unor norme speciale de securitate în timpul investigațiilor, în scopul asigurării conformității cu cerințele privind secretul de stat.

4.3. Rolul altor mecanisme de supraveghere independente

Douăzeci de state membre au declarat că legislația lor prevede supravegherea și/sau controlul parlamentar asupra activităților serviciilor de informații, care se adaugă competențelor autorităților pentru protecția datelor în ceea ce privește prelucrarea datelor[18], precum și sisteme interne specifice de control[19]. În statele membre par însă să existe diferite interpretări ale controlului parlamentar, doar câteva dintre acestea putând fi considerate ca implicând existența unui organism de supraveghere a protecției datelor (inclusiv evaluarea drepturilor persoanei vizate și conformitatea cu dispozițiile prevăzute atât în LGPD, cât și în legislația specifică)[20].

Sistemele de supraveghere existente sunt extrem de diverse, cuprinzând după cum urmează:

- o comisie parlamentară, care poate avea sarcina amplă de a supraveghea autoritățile responsabile de asigurarea securității naționale și de activitatea de informații, în general, sau un serviciu de informații, în particular;

- activitatea de supraveghere și/sau control parlamentar se desfășoară în paralel cu activitatea altor organisme independente de supraveghere (altele decât autoritatea pentru protecția datelor). Modalitățile existente de control parlamentar iau forma unui ombudsman parlamentar, a unei delegații parlamentare sau a unei comisii parlamentare;

- o comisie parlamentară este singura autoritate de supraveghere în afara structurii puterii executive. În acest caz, sarcinile Parlamentului sunt formulate fie mai degrabă în mod general, fie fără să se prevadă accesul la cazurile pendinte;

[16] Austria, Belgia, Cipru, Estonia, Finlanda, Franța, Germania, Irlanda, Italia, Letonia, Luxemburg, Polonia, Suedia.
[17] Republica Cehă, Danemarca, Malta, Țările de Jos, Portugalia, România, Slovacia, Spania, Regatul Unit.
[18] De exemplu, în Finlanda, ombudsmanul parlamentar exercită această responsabilitate împreună cu autoritatea pentru protecția datelor, însă competențele sale se bazează pe legea specială privind serviciile de securitate și de informații.
[19] Cele douăzeci de state membre în cauză sunt: Austria, Bulgaria, Cipru, Republica Cehă, Estonia, Finlanda, Franța, Germania, Grecia, Ungaria, Italia, Letonia, Luxemburg, Polonia, Portugalia, România, Slovacia, Slovenia, Spania, Regatul Unit.
[20] Prezentul aviz nu analizează informațiile privind controlul administrativ (ministerial) și controlul politic general care au fost furnizate de mai multe state care au răspuns la chestionar.

- supravegherea este exercitată exclusiv de o autoritate specială. Cu toate acestea, competențele pot fi instituite de legislația în materie de protecție a datelor, însă a fost semnalat și un caz în care activitatea autorității respective a fost reglementată, până de curând, de instrumente juridice neobligatorii;

- supravegherea parlamentară generală se desfășoară în paralel cu un control judiciar specializat;

- există o autoritate generală pentru protecția datelor, precum și o comisie specializată de control mixt, exercitat de puterea executivă și de cea legislativă; comisia specializată este prezidată de un judecător, ceilalți membri provenind din diferite partide politice care sunt reprezentate sau care au fost reprezentate în Parlament. Sunt prevăzute proceduri de consultare cu autoritatea pentru protecția datelor;

- surse de inspirație în vederea îmbunătățirii elementelor de supraveghere pot fi găsite, de asemenea, în sistemele în care un organism special a fost creat în mod specific pentru a supraveghea protecția pe care o asigură datelor serviciile de informații: Comisia de supraveghere a datelor, formată din trei procurori, numiți de procurorul general, care supraveghează serviciile de informații împreună cu Consiliul de supraveghere parlamentară;

- deși autoritatea pentru protecția datelor poate fi sesizată cu scopul de a verifica dacă este implicată securitatea națională, din momentul stabilirii acestei implicări, autoritatea trebuie să înainteze cazul celor doi comisari independenți care sunt însărcinați cu supravegherea judiciară independentă a serviciilor naționale de informații și care, în calitate de secretari de stat, eliberează mandate pentru efectuarea operațiunilor secrete de supraveghere. Un tribunal special soluționează căile de atac introduse de persoanele vizate;

- legislația specializată prevede cooperarea dintre organismul special de supraveghere și autoritatea generală pentru protecția datelor: un comisar independent însărcinat cu protecția juridică trebuie să autorizeze desfășurarea anumitor operațiuni de către serviciile de informații (de exemplu, investigații sub acoperire, supravegherea video a anumitor persoane). Comisia pentru protecție juridică are, de asemenea, obligația de a depune o plângere la autoritatea pentru protecția datelor în cazul în care consideră că drepturile prevăzute în LGPD au fost încălcate.

Autoritatea pentru protecția datelor are competența de a supraveghea serviciile de informații, cu unele limitări, însă un organism parlamentar special este însărcinat cu supravegherea interceptării comunicațiilor și cu soluționarea plângerilor. Membrii comisiei respective sunt numiți de comisia de control parlamentar. Președintele trebuie să fie calificat să exercite o funcție judiciară.

5. Recomandări

A. O mai mare transparență

1. Este necesară o mai mare transparență cu privire la modul în care funcționează programele, precum și cu privire la acțiunile și la deciziile organismelor de supraveghere

Grupul de lucru consideră că este important ca statele membre să fie transparente în cea mai mare măsură posibilă cu privire la implicarea lor în programele de colectare și de schimb de date operative, de preferință în mod public, însă, dacă este necesar, cel puțin față de parlamentele lor naționale și de autoritățile de supraveghere competente. Se recomandă autorităților pentru protecția datelor să pună în comun expertiza de care dispun la nivel național pentru a restabili echilibrul între interesele de securitate națională și dreptul fundamental la respectarea vieții private a cetățenilor.

Ar trebui să se instituie anumite forme de raportare generală cu privire la activitățile de supraveghere în concordanță, de asemenea, cu obligația de transparență care revine statelor membre conform Curții Europene a Drepturilor Omului[21]. Orice ingerință în drepturile fundamentale trebuie să fie previzibilă și, prin urmare, aceste programe trebuie să se bazeze pe o legislație clară, specifică și accesibilă. Autoritățile naționale pentru protecția datelor sunt invitate să aducă această poziție la cunoștința guvernelor lor respective.

2. O mai mare transparență din partea operatorilor de date

Întreprinderile trebuie să fie cât se poate de transparente și să se asigure că persoanele vizate sunt informate că, din momentul în care datele lor cu caracter personal sunt transferate către țări terțe care nu asigură un nivel adecvat de protecție, pe baza instrumentelor disponibile pentru astfel de transferuri, datele respective ar putea face obiectul supravegherii de către autoritățile publice din țările terțe sau ar putea să fie accesate de autoritățile publice din țările terțe, în măsura în care astfel de derogări sunt prevăzute de instrumentele respective. Grupul de lucru este conștient de faptul că operatorii de date ar putea fi constrânși să nu informeze persoana vizată cu privire la ordinul pe care l-au primit de la o autoritate publică. Grupul de lucru salută eforturile recente de a furniza persoanei vizate informații mai fiabile și mai detaliate cu privire la solicitările primite și încurajează întreprinderile să-și îmbunătățească în continuare politicile de informare.

3. Maximizarea conștientizării publicului

Persoanele vizate trebuie să fie conștiente de consecințele pe care le poate avea utilizarea serviciilor de comunicații electronice online și offline, precum și de modul în care se pot apăra mai eficient. Aceasta este o responsabilitate comună a autorităților pentru protecția datelor, a altor autorități publice, a întreprinderilor, precum și a societății civile. În acest scop, Grupul de lucru intenționează să organizeze, în a doua jumătate a anului 2014, o conferință privind supravegherea care să reunească toate părțile interesate pentru a discuta o abordare posibilă.

[21] A se vedea, de asemenea, Curtea Europeană a Drepturilor Omului, cauza nr. 48135/06 — Youth Initiative for Human Rights/Serbia (25 iunie 2013), p. 6.

B. O supraveghere mai atentă

1. Menținerea unui sistem juridic coerent pentru serviciile de informații, inclusiv norme privind protecția datelor

Dezvăluirile făcute de Snowden au arătat în mod clar că serviciile de informații din statele membre ale Uniunii Europene prelucrează zilnic cantități mari de date cu caracter personal. Aceste date fac, de asemenea, obiectul unor schimburi cu alte servicii atât din interiorul, cât și din afara UE. Grupul de lucru consideră că este important ca statele membre să aibă un cadru juridic coerent pentru serviciile de informații care să includă norme privind prelucrarea datelor, în conformitate cu principiile de protecție a datelor, astfel cum sunt prevăzute în legislația europeană și în cea internațională. Drepturile persoanei vizate trebuie să fie garantate în cea mai mare măsură posibilă, protejând în același timp interesul public aflat în joc.

De asemenea, Grupul de lucru recomandă ca acest cadru juridic național să conțină norme clare privind cooperarea și schimbul de date cu caracter personal cu autoritățile de asigurare a respectării legii pentru prevenirea, combaterea și sancționarea infracțiunilor, inclusiv cu privire la transferul unor astfel de date către autorități din alte state membre ale UE și din țări terțe.

2. Asigurarea supravegherii eficace a serviciilor de informații

În cadrul juridic național privind serviciile de informații, ar trebui să se acorde o atenție deosebită mecanismelor de supraveghere în vigoare. O supraveghere adecvată, independentă și efectivă este de maximă importanță într-o societate democratică. Prin urmare, Grupul de lucru consideră că următoarele bune practici din cadrul diverselor mecanisme de supraveghere aflate în vigoare în prezent în statele membre ar trebui să facă parte din mecanismele de supraveghere în toate statele membre. Autoritățile naționale pentru protecția datelor sunt îndemnate să aducă aceste elemente în dezbaterea națională privind supravegherea serviciilor de informații:

- controale interne stricte pentru respectarea cadrului juridic național în vederea asigurării responsabilității și a transparenței;

- control parlamentar eficace exercitat în conformitate cu tradițiile parlamentare naționale. Autoritățile naționale pentru protecția datelor ar trebui să încurajeze parlamentele care dețin deja competențe de supraveghere a activității serviciilor de informații să-și îndeplinească în mod activ aceste sarcini;

- supraveghere externă eficace, solidă și independentă exercitată fie de un organism specific, cu implicarea autorităților pentru protecția datelor, fie de autoritatea pentru protecția datelor, care are competența de a accesa date și alte documente relevante în mod regulat și din proprie inițiativă (*ex officio*), precum și obligația de efectua investigații în urma plângerilor primite. Nu trebuie să fie necesară aprobarea prealabilă din partea serviciilor de informații care urmează să fie supravegheate.

C. Aplicarea efectivă a legislației în vigoare

1. Asigurarea respectării obligațiilor existente ale statelor membre ale UE și ale părților contractante la CEDO pentru protejarea drepturilor la respectarea vieții private și la protecția datelor cu caracter personal

Toate statele membre sunt părți la Convenția Europeană a Drepturilor Omului. Prin urmare, acestea trebuie să respecte condițiile prevăzute la articolele 7 și 8 din CEDO în ceea ce privește propriile lor programe de supraveghere. Obligațiile lor nu se opresc aici. Articolul 1 din CEDO obligă, de asemenea, părțile să garanteze tuturor persoanelor din jurisdicția lor drepturile și libertățile prevăzute în convenție. În ambele scenarii, statele membre ale UE, ca orice parte la CEDO, pot fi aduse în fața Curții Europene a Drepturilor Omului pentru o încălcare a dreptului la respectarea vieții private al subiecților de drept europeni.

2. Operatorii de date care fac obiectul jurisdicției UE trebuie să respecte legislația aplicabilă a UE în materie de protecție a datelor

Operatorii de date stabiliți în UE sau care utilizează echipamente într-un stat membru al UE trebuie să respecte obligațiile care le revin în temeiul legislației UE, inclusiv în cazul în care legislația din alte țări în care aceștia operează este în contradicție cu legislația UE. În acest sens, autoritățile pentru protecția datelor nu pot ignora faptul că este posibil să se efectueze transferuri de date care încalcă legislația UE. Prin urmare, Grupul de lucru reamintește faptul că autoritățile pentru protecția datelor pot suspenda, în conformitate cu dispozițiile stabilite la nivelul UE și la nivel național în ceea ce privește protecția datelor, fluxurile de date prevăzute în instrumentele de transfer atunci când există o probabilitate substanțială ca principiile de protecție a datelor să fie încălcate și când continuarea transferurilor ar crea un risc iminent de prejudiciere gravă a persoanelor vizate. Autoritățile naționale pentru protecția datelor ar trebui să decidă, în conformitate cu atribuțiile care le revin în temeiul legislației naționale, dacă într-o anumită situație se impun sancțiuni.

D. Îmbunătățirea protecției la nivel european

1. Adoptarea pachetului de reforme privind protecția datelor

Pentru a oferi o protecție solidă a datelor în Europa, finalizarea negocierilor cu privire la pachetul de reforme privind protecția datelor este de cea mai mare importanță. Noul Regulament general privind protecția datelor și Directiva privind protecția datelor în domeniul polițienesc și judiciar vizează nu doar o mai bună protecție a datelor pentru persoane. Acestea sunt menite, de asemenea, să clarifice domeniul lor de aplicare și să ofere autorităților pentru protecția datelor mai multe competențe în materie de asigurare a respectării legii. În special, posibilitatea de a impune sancțiuni (financiare) – ca măsură de ultim resort – ar trebui să asigure un control sporit asupra activității operatorilor de date. Grupul de lucru salută propunerea Parlamentului European de a prevedea informarea obligatorie a persoanelor în cazul în care, în ultimele douăsprezece luni, s-a permis unei autorități publice să aibă acces la date care le vizează. Transparența cu privire la aceste practici va spori în mod semnificativ încrederea. Prin urmare, Grupul de lucru îndeamnă

Consiliul și Parlamentul European să-și respecte calendarul convenit[22] și să se asigure că ambele instrumente pot fi adoptate în cursul anului 2014.

2. Clarificarea domeniului de aplicare a exceptării privind securitatea națională

Nu există în prezent nicio interpretare comună a ceea ce înseamnă securitatea națională. Nu există o definiție clară adoptată de legiuitorul european și nici jurisprudența instanțelor europene nu este concludentă în acest sens. Derogarea nu trebuie însă extinsă la prelucrarea datelor cu caracter personal în scopuri pentru care acestea nu pot fi utilizate în mod legal.

Un alt aspect al întrebării la care este necesar să se răspundă este în ce măsură o exceptare axată pe securitatea națională continuă să reflecte realitatea; în prezent, se pare că activitatea serviciilor de informații este, mai mult ca niciodată, strâns legată de activitatea autorităților de asigurare a respectării legii și urmărește mai multe scopuri diferite. Schimburi de date se efectuează în permanență și la nivel mondial, lăsând de o parte chestiunea privind securitatea cărei națiuni urmează să aibă de câștigat ca urmare a analizării datelor respective. Prin urmare, Grupul de lucru invită Consiliul, Comisia și Parlamentul să ajungă la un acord în vederea definirii principiului de securitate națională și să formuleze concluzii cu privire la ceea ce ar trebui să fie considerat ca fiind de domeniul exclusiv al statelor membre. În definirea principiului de securitate națională, trebuie să se acorde atenția cuvenită reflecțiilor Grupului de lucru, inclusiv celor formulate în prezentul aviz. Instituțiile UE sunt îndemnate să clarifice în pachetul de reforme privind protecția datelor faptul că, singură, protecția securității naționale a țărilor terțe nu poate să excludă aplicabilitatea dreptului UE.

E. Protecție internațională pentru rezidenții în UE

1. Insistarea asupra unor garanții adecvate pentru schimbul de date operative

Autoritățile publice ale țărilor terțe, în general, și serviciile de informații, în special, nu trebuie să aibă acces direct la datele din sectorul privat prelucrate în UE. Dacă solicită accesul la astfel de date într-o anumită situație pe baza unei suspiciuni rezonabile, după caz, acestea trebuie să depună o cerere în temeiul acordurilor internaționale, furnizând garanții adecvate privind protecția datelor. În ceea ce privește schimbul de informații operative, statele membre trebuie să se asigure că legislația națională prevede un temei juridic specific pentru astfel de transferuri, precum și garanții adecvate privind protecția datelor cu caracter personal. În opinia Grupului de lucru, acordurile de cooperare secrete între statele membre și/sau țările terțe nu îndeplinesc standardul Curții Europene a Drepturilor Omului referitor la un temei juridic clar și accesibil.

[22] http://euobserver.com/justice/122853.

2. Negocierea de acorduri internaționale în vederea acordării de garanții adecvate privind protecția datelor

Ideea unui așa-numit acord-cadru, care face în prezent obiectul unor negocieri între SUA și UE, este un pas în direcția cea bună. Cu toate acestea, este probabil ca un astfel de acord să prezinte două deficiențe: acesta va excepta cazurile referitoare la securitatea națională, cel puțin din perspectiva UE, întrucât este negociat ca un acord bazat doar pe legislația UE. De asemenea, structura acestuia sugerează că ar urma să se aplice doar datelor transferate între autoritățile publice din SUA și UE, nu și datelor colectate de entități private. Aceasta reiese, de asemenea, în mod clar, din raportul Grupului de contact la nivel înalt UE-SUA (GCNI) privind schimbul de informații și protecția vieții private și protecția datelor cu caracter personal[23], care constituie baza pentru negocierile privind acordul-cadru. Grupul de lucru subliniază că, în temeiul acordului-cadru, scopul prelucrării datelor transferate ar trebui să fie același atât în UE, cât și în SUA. Nu ar fi acceptabil ca datele provenite din aplicarea legislației UE să poată fi utilizate ulterior de serviciile de informații din SUA în scopuri de securitate națională dacă acest lucru nu este posibil, de asemenea, în UE.

Deoarece acordul-cadru nu va reuși să ofere o protecție totală tuturor cetățenilor, este nevoie de un acord internațional care să prevadă o protecție adecvată împotriva supravegherii nediscriminatorii. De asemenea, actualul conflict al jurisdicțiilor, care afectează o parte din activitățile de supraveghere divulgate, ar putea fi atenuat dacă un astfel de acord stabilește limite clare pentru activitățile de supraveghere. Cu toate acestea, acordul ar fi direct legat de exceptarea privind securitatea națională și, în consecință, nu ar intra în domeniul de aplicare a legislației UE. Prin urmare, statele membre sunt cele care trebuie să înceapă negocierile în mod coordonat. Ar trebui să se acorde atenția cuvenită identificării clare a activităților de supraveghere descrise care ar urma, într-adevăr, să se încadreze în sfera securității naționale și a activităților care sunt mai degrabă legate de scopuri de asigurare a respectării legii și de scopuri de politică externă, domenii care ar intra sub incidența dreptului Uniunii. Aceasta ar permite ca instituțiile UE să participe mai îndeaproape în cazul în care se iau măsuri în această direcție.

Noul acord nu trebuie să fie unul secret. Acesta trebuie să fie publicat și ar trebui să includă obligații ale părților contractante privind controlul necesar al programelor de supraveghere, transparența, tratamentul egal, cel puțin al cetățenilor tuturor părților la acord, mecanisme de exercitare a unor căi de atac și alte drepturi în materie de protecție a datelor. De asemenea, părțile implicate ar trebui să fie încurajate să se asigure că parlamentele lor naționale sunt informate în mod regulat cu privire la utilizarea și la valoarea acordului încheiat.

[23] Documentul nr. 15851/09 al Consiliului, 23 noiembrie 2009.

3. Dezvoltarea unui instrument aplicabil la nivel mondial de protecție a vieții private și a datelor cu caracter personal

Grupul de lucru sprijină, de asemenea, elaborarea unui instrument aplicabil la nivel mondial care să prevadă principii executorii pentru a se asigura un nivel ridicat de protecție a vieții private și a datelor, astfel cum s-a convenit în Declarația de la Madrid a Conferinței internaționale a comisarilor pentru protecția datelor și a vieții private[24]. În acest sens, s-ar putea avea în vedere adoptarea unui protocol adițional la articolul 17 din Pactul internațional al ONU cu privire la drepturile civile și politice. Într-un astfel de instrument internațional, trebuie să se asigure faptul că garanțiile oferite sunt aplicabile tuturor persoanelor vizate. De asemenea, este necesar să se ajungă la o interpretare generală a noțiunii de „prelucrare a datelor", întrucât există diferențe mari în ceea ce privește modul în care aceasta este înțeleasă la nivel mondial.

Grupul de lucru sprijină inițiativa luată de guvernul german și apelul lansat de Conferința internațională a comisarilor pentru protecția datelor și a vieții private[25,26]. De asemenea, Grupul de lucru continuă să sprijine aderarea țărilor terțe la Convenția 108 a Consiliului Europei.

[24] Standardele internaționale în materie de protecție a datelor cu caracter personal și a vieții private, adoptate de cea de a 31-a Conferință internațională a comisarilor pentru protecția datelor și a vieții private care s-a desfășurat la Madrid.
[25] http://www.bundesregierung.de/Content/EN/Artikel/2013/07/2013-07-19-bkin-nsa-sommerpk.html.
[26] Rezoluție privind ancorarea protecției datelor și a protecției vieții private în dreptul internațional, adoptată cu ocazia celei de a 35-a Conferințe internaționale a comisarilor pentru protecția datelor și a vieții private care s-a desfășurat la Varșovia.