РАБОТНА ГРУПА ЗА ЗАЩИТА НА ДАННИТЕ ПО ЧЛЕН 29

16/BG
WP 238

Становище 01/2016 относно проекта на решение относно адекватността на Щита на личните данни в отношенията между ЕС и САЩ

Прието на 13 април 2016 г.

РЕЗЮМЕ

На 29 февруари 2016 г. Европейската комисия публикува съобщение, както и проект на решение за адекватността с приложените към него текстове, които представляват нова рамка за трансатлантическия обмен на лични данни за търговски цели: т. нар. Щит за личните данни в отношенията между ЕС и САЩ (наричан по-долу „Щит за личните данни“). С това се цели замяна на предишното решение за „сфера на неприкосновеност на личния живот“ в отношенията със САЩ (U.S. Safe Harbour), обявено за невалидно от Съда на Европейския съюз (наричан по-долу „Съд на ЕС“) с решението по делото Schrems, постановено на 6 октомври 2015 г.

Съгласно член 30, параграф 1, буква в) от Директива 95/46/ЕО работната група по член 29 (наричана по-долу „РГ по член 29“) направи оценка на тези документи, за да даде становището си по проекта на решение за адекватността. РГ по член 29 прецени както търговските аспекти, така и възможните дерогации от принципите на Щита за личните данни за целите на националната сигурност, правоприлагането и обществения интерес.

РГ по член 29 взе под внимание установената с Директива 95/46/ЕО приложима правна уредба на ЕС за защита на личните данни, както и основните права на личен живот и защита на данните, както е посочено в член 8 от Европейската конвенция за правата на човека и членове 7 и 8 от Хартата за основните права на Европейския съюз. Тя взе под внимание също така правото на ефективни правни средства за защита и на справедлив съдебен процес, заложени в член 47 от Хартата, както и съдебната практика, свързана с различните основни права.

Освен това анализът отразява мотивите на Съда по делото Schrems относно свободата на преценка на Комисията при оценката на адекватността. Проверката и контролът на изискванията за адекватност трябва да се извършват стриктно, като се вземат предвид основните права на неприкосновеност на личния живот и на защита на данните и броят на потенциално засегнатите от предаването физически лица.

Щитът за личните данни трябва да се разглежда в настоящия международен контекст, като например появата на големи масиви от данни и нарастващата необходимост от сигурност. Обхватът и обемът на събиране и използване на лични данни се е увеличил драстично след публикуването на първоначалното решение за „сфера на неприкосновеност на личния живот“ през 2000 г. Европейските органи за защита на данните твърдо отстояват значението на принципите, които защитават.

РГ по член 29 приветства преди всичко значителните подобрения, внесени с Щита за личните данни, в сравнение с решението за „сфера на неприкосновеност на личния живот“. Групата отбелязва, че много от недостатъците на „сферата на

неприкосновеност на личния живот“, изтъкнати в нейното писмо до заместник-председател Рединг от 10 април 2014 г. са били взети предвид от преговарящите.

Фактът, че принципите и гаранциите, осигурявани от Щита за личните данни, са определени както в решението за адекватност, така и в приложенията към него, прави информацията трудна за намиране и понякога непоследователна. Това допринася за общата липса на яснота на новата рамка и затруднява достъпността ѝ за субектите на данни, организациите и органите за защита на данните. По същия начин липсва яснота и в използвания език. Поради това работната група по член 29 настоятелно призовава Комисията да направи новата рамка ясна и разбираема и от двете страни на Атлантическия океан.

Що се отнася до приложимото право, РГ по член 29 подчертава, че ако решението за адекватността на Щита за личните данни е прието въз основа на Директива 95/46/ЕО, то трябва да бъде в съответствие с правната уредба на ЕС за защита на данните както по отношение на обхвата, така и по отношение на терминологията. Работната група по член 29 счита, че непосредствено след започване на прилагането на Общия регламент относно защитата на данните трябва да се направи преглед, за да се гарантира, че решението за адекватност и приложенията към него следват високата степен на защита на данните, която се дава от регламента.

Относно търговските аспекти на Щита за личните данни

Основната цел на РГ по член 29 е да гарантира, че степента на защита, осигурявана на физическите лица, се запазва равностойна по същество, когато личните данни се обработват съгласно разпоредбите на Щита за личните данни. Въпреки че РГ по член 29 не очаква Щитът за личните данни да бъде обикновено и изчерпателно копие на правната уредба на ЕС, тя счита, че той следва да съдържа същността на основните принципи и в резултат на това да гарантира степен на защитата, която „по същество е равностойна“.

Независимо от предложените от Щита за личните данни подобрения, РГ по член 29 счита, че в проекта на решение за адекватността и в приложенията към него някои основни принципи за защита на данните, предвидени в европейското право, не са отразени или са били неадекватно заменени с алтернативни понятия.

Така например принципът за запазване на данните не е изрично упоменат и не може да бъде ясно обяснен от настоящата формулировка на принципа за цялост на данните и ограничаване в рамките на целта. Освен това липсва формулировка относно защитата, която трябва да бъде предоставена срещу отделните автоматизирани решения, основани единствено на автоматизирано обработване. Прилагането на принципа за ограничаване в рамките на целта при обработването на данни също е неясно. С цел да внесе повече яснота при използването на някои важни понятия, РГ по член 29 предлага между ЕС и САЩ да бъдат договорени ясни определения, които да са част от речник на термините, включен в раздела за често задавани въпроси на Щита за личните данни.

Тъй като Щитът за личните данни ще се използва и за предаване на данни извън САЩ, РГ по член 29 настоява, че при последващите предавания от субект — участник в Щита за личните данни, към получатели от трета държава следва да се осигурява същата степен на защита по отношение на всички аспекти на Щита (включително националната сигурност), като това последващо предаване не следва да води до занижаване или заобикаляне на принципите на ЕС за защита на данните. В случай че се предвижда последващо предаване към трета държава съгласно Щита за личните данни, всяка организация — участник в Щита за личните данни, следва да бъде задължена преди предаването да направи оценка на всички задължителни изисквания на националното законодателство на тази трета държава, приложими към вносителя на данните. Като цяло РГ по член 29 стига до заключението, че последващите предавания на лични данни на лица от ЕС не са достатъчно регламентирани, особено що се отнася до техния обхват, ограничаването в рамките на целта и гаранциите, които се прилагат за предавания на представители.

И накрая, въпреки че РГ по член 29 отбелязва наличието на допълнителните възможности, които са предоставени на физическите лица, за да упражняват правата си, тя се опасява, че новият механизъм за защита може да се окаже на практика твърде сложен, труден за използване от гражданите на ЕС и следователно неефективен. Поради това е необходимо допълнително разясняване на различните видове предприемани процедури; по-специално при желание органите на ЕС за защита на данните могат да се разглеждат като естествени звена за контакт на физическите лица от ЕС при различните процедури, с възможност да действат от тяхно име.

Дерогации за целите на националната сигурност

Що се отнася до достъпа до данни от страна на органите на публичната власт, както в ЕС, така и в трети държави, РГ по член 29 припомня своя анализ на съответните основни права, съдържащ се в работния документ относно обосновката за намеса в основните права на неприкосновеност на личния живот и защита на данните чрез мерки за наблюдение, когато се предават лични данни (Европейски основни гаранции) (WP237).

Голяма крачка напред в сравнение с Решението за „сфера на неприкосновеност на личния живот“ е това, че сега в проекта на решение за адекватността се разглежда подробно възможният достъп до данни, обработени съгласно Щита за личните данни, за целите на националната сигурност и правоприлагането. РГ по член 29 признава тази значителна крачка, както и предложената от администрацията на САЩ повишена прозрачност относно приложимото законодателство за събиране на разузнавателни данни (приложение VI).

Независимо от това РГ по член 29 отбелязва, че писмените изявления на Службата на директора на Националното разузнаване (ODNI) на САЩ не изключват масово и безразборно събиране на лични данни с произход от ЕС. РГ по член 29 припомня дългогодишната си позиция, че в едно демократично общество масовото и безразборно

наблюдение на физически лица никога не може да се разглежда като пропорционално и строго необходимо, както се изисква съгласно защитата, която приложимите основни права предоставят. Освен това осъществяването на цялостен надзор върху всички програми за наблюдение е от решаващо значение. Работната група по член 29 отбелязва, че с оглед на борбата срещу тероризма е налице тенденция все повече данни да се събират масово и безразборно. Предвид свързаните с това опасения относно защитата на основните права на неприкосновеност на личния живот и защита на данните, РГ по член 29 очаква предстоящите решения на Съда на ЕС по дела, свързани с масово и безразборно събиране на данни.

По отношение на правната защита РГ по член 29 приветства създаването на омбудсман, като нов механизъм за правна защита. Това може да представлява съществено подобрение за правата на физическите лица от ЕС във връзка с разузнавателните дейности на САЩ. РГ по член 29 се опасява обаче, че тази нова институция не е достатъчно независима и не разполага с подходящите правомощия за ефективно изпълнение на задълженията си, както и че не гарантира достатъчна защита в случай на несъгласие.

Съвместен преглед

Механизмът за годишен съвместен преглед, споменат в проекта на решение за адекватността, е ключов фактор за цялостната надеждност на Щита за личните данни и РГ по член 29 силно приветства възможността, която това дава, за да се прави преглед на решението за адекватността. Във връзка с това РГ по член 29 разбира, че нейните национални представители ще имат възможност пълноценно да участват в процеса на преразглеждане, но настоява за изясняване на точните договорености. Редът и условията (включително докладът от прегледа, публичното му оповестяване и възможните последици, както и финансиране) трябва да бъдат договорени достатъчно време преди провеждането на първия преглед.

Заключение

РГ по член 29 отбелязва значителните подобрения, предлагани от Щита за личните данни, в сравнение с обявеното за невалидно решение за „сфера на неприкосновеност на личния живот“. Предвид изразените опасения и поисканите разяснения РГ по член 29 настоятелно призовава Комисията да разреши тези проблеми, да предложи подходящи решения и да предостави исканите разяснения, с цел да се подобри проектът на решение за адекватността, както и да се гарантира, че защитата, предлагана от Щита за личните данни по същество е равностойна на тази в ЕС.

Съдържание

1. ВЪВЕДЕНИЕ

След постановеното на 6 октомври 2015 г. решение на Съда на Европейския съюз (наричан по-долу „Съд на ЕС“) по делото Schrems[1] работната група по член 29 (наричана по-долу „РГ по член 29“) отправи призив към държавите — членки на Европейския съюз (наричан по-долу „ЕС“), и другите европейски институции да започнат дискусии с органите на Съединените американски щати (наричани по-долу „САЩ“) с цел да намерят политически, законодателни и технически решения, позволяващи предаване на данни към територията на САЩ при зачитане на основните права.

На 2 февруари 2016 г. след повече от две години водене на преговори, Европейската комисия и Министерството на търговията на САЩ постигнаха политическо споразумение по *Нова рамка за трансатлантически обмен на лични данни за търговски цели: Щитът за личните данни в отношенията между ЕС и САЩ* (наричан по-долу „Щит за личните данни“), която цели да замести предишната „сфера на неприкосновеност на личния живот“.

На 29 февруари 2016 г. Комисията публикува Съобщение[2], проект на решение за адекватността и приложените към него текстове, които ще представляват Щита за личните данни. Съгласно член 30, параграф 1, буква в) от Директива 95/46/ЕО (наричана по-долу „Директивата“) работната група по член 29 проучи тези документи, за да даде становището си по проекта на решение за адекватността, изготвен от Комисията, включително основополагащите за Щита за личните данни документи. В оценката си РГ по член 29 е разделила работата си на оценка на търговската част на Щита за личните данни и анализ на гаранциите, въведени във връзка с дерогациите от Принципите на Щита за личните данни за целите на националната сигурност, правоприлагането и обществения интерес.

След решението по делото Schrems РГ по член 29 проведе няколко срещи с делегации от администрацията на САЩ, представители на организации на гражданското общество от ЕС и от САЩ и учени, с цел да изготви оценка на последствията от решението по делото Schrems. В хода на оценката на Щита за личните данни бяха проведени и други срещи с Европейската комисия и с представители на администрацията на Съединените щати. По време на тези срещи бяха предоставени някои разяснения, които също са взети предвид в настоящото становище. РГ по член 29 подчертава, че на сегашния етап това са само неофициални разяснения, които не могат да се считат за неразделна част от проекта на решение за адекватността, тъй като все още не са представени в писмен вид.

[1] Дело C-362/14 - Maximilian Schrems/Data Protection Commissioner, 6 октомври 2015 г. (наричано по-нататък „делото Schrems“).
[2] COM(2016) 117 final, 29 февруари 2016 г.

Въпреки това РГ по член 29 специално приветства поетия по време на тези срещи от Министерството на търговията на САЩ ангажимент за сътрудничество с органите за защита на данните от държавите — членки на ЕС, във връзка с прилагането на Щита за личните данни, както и за предоставяне на указания и правно тълкуване по отношение на прилагането на Щита за личните данни, които да бъдат публикувани на техните уебсайтове.

1.1 Общи бележки

1.1.1 Обхват на оценката на РГ по член 29

Преди всичко РГ по член 29 взе предвид приложимата правна уредба за защита на данните в държавите — членки на Европейския съюз, включително член 8 от Европейската конвенция за правата на човека (наричана по-долу „ЕКПЧ“), защитаваща правото на личен и семеен живот, както и членове 7, 8 и 47 от Хартата за основните права на Европейския съюз (наричана по-долу „Хартата“), защитаващи съответно правото на личен и семеен живот, правото на защита на личните данни и правото на ефективни правни средства за защита и на справедлив съдебен процес. Групата взе под внимание също така съответната съдебна практика, както и изискванията на Директивата.

Изискването за това трета държава да гарантира достатъчна степен на защита на данните беше определено допълнително от Съда с решението по делото Schrems. Съдът не само обясни, че разпоредбите на Директивата трябва да се тълкуват „с оглед на основните права, гарантирани с Хартата“[3], и по-специално правата по членове 7 и 8. Той също така посочи, че формулировката „достатъчна степен на защита“ трябва да се разбира в смисъл, че „от съответната трета страна се изисква ефективно да гарантира, по силата на вътрешното си законодателство или на международните си споразумения, степен на защита на основните права и свободи, която по същество е равностойна на гарантираната в Съюза по силата на Директива 95/46, разглеждана във връзка с Хартата“[4]. Подобна преценка никога не е правена в достатъчно обстойна степен по отношение на предишното решение относно „сферата на неприкосновеност на личния живот“. Поради това РГ по член 29 извърши преценка на проекта на решение за адекватността като взе предвид изискването за изготвяне на анализ на степента на защита на основните права и свободи, която следва да е *равностойна по същество* на гарантираната в ЕС. РГ по член 29 подчертава, че в това становище се съдържат основните ѝ опасения, но предвид ограниченото време, с което е разполагала след публикуването на проекта на решение за адекватността, на по-късен етап може да се открият още проблеми.

РГ по член 29 признава, че с определянето на думата „достатъчна“, употребена в член 25, параграф 6 от Директивата, като „равностойна по същество“, в решението по делото Schrems Съдът на ЕС е описал по-подробно адекватността. Съдът е подчертал,

[3] Решение по делото Schrems, точка 38.
[4] Решение по делото Schrems, точка 73.

че макар терминът „достатъчна степен на защита“ да не изисква от съответната трета държава да гарантира защита, която е идентична на гарантираната в правния ред на ЕС, той трябва да се разбира в смисъл, че от съответната трета държава се изисква ефективно да гарантира, по силата на вътрешното си законодателство или на международните си споразумения, степен на защита на основните права и свободи, която по *същество е равностойна* на гарантираната в Европейския съюз по силата на Директивата, разглеждана във връзка с Хартата.

1.1.2 Оценката на търговската част от проекта на решение за адекватността

В изготвения от нея работен документ 12 „Предаване на лични данни на трети държави: прилагане на членове 25 и 26 от директивата на ЕС за защита на данните“[5] РГ по член 29 вече обясни начина, по който прилага основните принципи на ЕС за защита на данните спрямо предаването на лични данни на трети държави. РГ по член 29 се опита да намери равностойни гаранции, които осигуряват степен на защита, равностойна на гарантираните в Директивата Принципи, главно по отношение на ограничаването в рамките на целта, качеството и пропорционалността на данните, прозрачността, сигурността, правата на достъп, коригиране и противопоставяне, запазването на данните и ограниченията по отношение на последващите предавания. Подобен метод беше използван в становищата, изготвени от РГ по член 29, при преценката на първоначалното решение за адекватността на „сферата за неприкосновеност на личния живот“[6], както и в препоръките, отправени от работната група в нейното писмо до предишния заместник-председател и комисар на ЕС по въпросите на правосъдието, Вивиан Рединг, публикувано на 10 април 2014 г.[7]

1.1.3 Преценка на дерогациите за достъп на публичните органи и свързаните с тях гаранции

Преценката на дерогациите за достъпа на публичните органи до лични данни, обхванати от Щита за личните данни, е сложна, особено като се отчита повишаването на осведомеността на органите за защита на данните и обществеността относно програмите за наблюдение на САЩ след разкритията на Сноудън. Работната група признава и приветства усилията на администрацията на САЩ да увеличи прозрачността относно програмите за наблюдение и нейната готовност в Щита за личните данни да бъдат включени допълнителни гаранции. В същото време РГ по член 29 подчертава, че в едно демократично общество всяка намеса, засягаща основните права на личен живот и защита на данните, трябва да бъде обоснована. Съдът на ЕС отправи критики относно факта, че в Решението за „сферата на неприкосновеност на личния живот“ не се съдържат каквито и да било констатации относно наличието в Съединените щати на правила с етичен характер, предназначени

[5] Прието от РГ по член 29 на 24 юли 1998 г., вж. по-специално стр. 6.
[6] Вж. становища WP62, WP32, WP27, WP23, WP21, WP19, WP15 и WP7.
[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf

за ограничаване на евентуална намеса. Във въпросното решение не се отбелязва и наличието на ефективна правна защита срещу този вид намеса[8].

Поради това РГ по член 29 анализира настоящата правна уредба на САЩ и практиките на разузнавателните агенции на САЩ, както са описани в приложенията към проекта на решението, както и условията, съгласно които те позволяват намеса в основните права за зачитане на личния живот и за защита на данните, защитавани от европейската правна уредба.

За да се прецени дали в едно демократично общество би била обоснована каквато и да е намеса, бе изготвена оценка с оглед на европейската съдебна практика относно основните права, която определя четири основни гаранции[9] за извършване на разузнавателни дейности:

А. Обработката следва да е в съответствие със закона и да се основава на ясни, точни и приемливи правила: това означава, че всеки, който е информиран в разумни граници, следва да бъде в състояние да предвиди какво би могло да се случи с неговите данни там, където те бъдат предадени;
Б. Трябва да бъдат доказани необходимостта и пропорционалността по отношение на преследваните легитимни цели: трябва да се намери баланс между целта, за която са събрани и достъпни данните, и правата на физическите лица;
В. Следва да има независим механизъм за надзор, който да е едновременно ефективен и безпристрастен: това може да бъде съд или друг независим орган, стига той да разполага с достатъчно възможности да извършва необходимите проверки;
Г. На всяко физическо лице трябва да се предоставят ефективни правни средства за защита: всеки следва да има правото да защити правата си пред независим орган.

1.2 Проект на решение за адекватността

РГ по член 29 приветства преди всичко факта, че е възможно стартирането на нова процедура за оценка на адекватността, по-малко от шест месеца след като Съдът на ЕС обяви решението за „сфера на неприкосновеност на личния живот“ за невалидно. Предвид количеството на предаванията на данни, които се осъществяват ежедневно между ЕС и САЩ и които се признават от РГ по член 29 за жизненоважна част на икономиката от двете страни на Атлантическия океан, е необходимо да не се отлага правната яснота по този въпрос.

РГ по член 29 изразява съжаление обаче, че публикуваният от Комисията проект на решение за адекватността не включва цялостна оценка на националното законодателство и международните ангажименти на САЩ под формата на доклад за адекватността, което в миналото е било обичайна практика при подобни процедури и е

[8] Решение по делото Schrems, точки 87—88.
[9] Европейските основни гаранции се основават на съдебната практика на Съда на ЕС и на Европейския съд по правата на човека и са доразвити в Работен документ WP237 на работната група по член 29, публикуван на 13 април 2016 г.

в съответствие с член 25 от Директивата. Това не позволява на РГ по член 29 да извърши пълен анализ на правния контекст, в границите на който ще функционира Щитът за личните данни. Тя забелязва например, че настоящият проект на решение за адекватността не включва констатации относно съществуващото в САЩ законодателство за защита на неприкосновеността на личния живот и на данните както на федерално, така и на щатско равнище, включително секторното законодателство, нито относно законодателството, позволяващо форми на публичен достъп, които не са свързани с наблюдение. Също така не е определена връзката между предаванията на данни съгласно Щита за личните данни и съгласно други съществуващи констатации за адекватността, като например Споразумението относно резервационните данни на пътниците (PNR) между ЕС и САЩ и Споразумението относно програмата за проследяване на финансирането на тероризма (TFTP).

1.2.1 Обхват на прилагане на правната уредба на ЕС за защита на данните, и по-специално на принципите на Директива 95/46/ЕО

РГ по член 29 припомня, че съгласно правната уредба на ЕС за защита на данните, и по-специално съгласно Директивата (член 4, параграф 1), законите на държавите членки се прилагат не само по отношение на операциите по обработката, извършвани от администратори на данни, установени на тяхна територия, но и когато администраторите на данни (макар и неустановени в ЕС) използват оборудването, разположено на територията на ЕС, по-специално за събиране на лични данни. Вследствие на това правото на държава — членка на ЕС, се прилага по отношение на всяка обработка, която се извършва преди предаването на САЩ, независимо дали в рамките на дейностите на организация, установена в ЕС, или чрез използването на оборудване, разположено в ЕС и използвано от организация, която не е установена в ЕС. РГ по член 29 изисква това да е изрично посочено в проекта на решение за адекватността.

Следва бъде обяснено обаче, че Принципите на Щита за личните данни ще се прилагат от момента на извършване на предаването на данни. Освен това РГ по член 29 припомня, че администраторите на данни, установени в ЕС и предаващи данни на обработващ данни в САЩ, продължават да бъдат задължени да спазват правото на ЕС за защита на данните.

1.2.2 Липса на яснота в документите, които са част от Щита за личните данни

Фактът, че осигуряваните от Щита за личните данни принципи и гаранции, са определени както в решението за адекватността, така и в приложенията към него, прави информацията трудна за намиране и понякога непоследователна. Това допринася за общата липса на яснота на новата рамка, както и затруднява достъпността ѝ за субектите на данни, организациите и органите за защита на данните. Също така липсва яснота и в използвания език. Поради това работната група по член 29 настоятелно призовава Комисията да направи новата рамка ясна и разбираема и от двете страни на Атлантическия океан.

РГ по член 29 предлага да се включи отделно приложение, в което да са представят определени основни термини, които се използват в документите към Щита за личните данни. Общото и недвусмислено разбиране на задълженията, налагани с решението за адекватността на Щита за личните данни, е от съществено значение за ефективното му функциониране и от двете страни на Атлантическия океан и в тази връзка РГ по член 29 е загрижена, че поради многобройните препратки и неуеднаквени формулировки, както и поради сложността на рамковите документи, ще са налице трудности по отношение на съгласуваността, разбираемостта и яснотата на прилагането на Щита за личните данни.

Още по-важно е, че документите към Щита за личните данни използват терминология, която не е в съответствие с обичайно използвания в ЕС речник, когато става дума за защита на данните. Това може и да не е проблем, доколкото е ясно каква би била съответната терминология съгласно правото на ЕС (и съгласно правото на САЩ). РГ по член 29 отбелязва със съжаление обаче, че случаят не е такъв, включително в проекта на решение за адекватността. Така например думата „достъп“ е използвана в глава 3 от проекта на решение за адекватността в смисъл, който предполага събиране на лични данни, вместо предоставяне на възможност на някого да разгледа вече събрани данни. Достъпът на дружествата до данни и правото на достъп на физическите лица са две отделни понятия, които не трябва да се бъркат.

РГ по член 29 подчертава, че терминологията следва да се използва последователно в целия документ, включително в проекта на решение за адекватността. В момента случаят не е такъв, например по отношение на понятията „обработка“ и „лични данни“. По принцип и двете са добре определени в приложение II, но не се прилагат последователно в целия документ, което води до появата на пропуски в защитата[10,11].

РГ по член 29 приветства това, че определенията на някои от използваните термини са били включени в документите, съставляващи Щита за личните данни. Случаят обаче не

[10] В някои от клаузите се изброяват единствено определени видове операции за обработка на данни, вместо да се използва терминът „обработка“. Резултатът от това е появата на пропуски в защитата. Напр. съгласно формулировката на приложение II, раздел III, точка 6, буква е), Принципите на Щита за личните данни ще се прилагат само когато организацията „съхранява, използва или разкрива“ получените данни (т.е. не за други операции, обхванати от термина „обработка“, като събиране, записване, промяна, извличане, консултиране, изтриване). Сигурността на данните ще се налага само за „създаване, поддържане, използване или разпространение“ на лична информация (приложение II, раздел II, точка 4). Определението за лични данни също е ограничено до „получени“ и „записани“ данни. Като допълнителен пример, принципът на уведомяването (приложение II, раздел II, точка 1, буква а), подточка iv) гласи, че една сертифицирана организация трябва да информира физическите лица за целите, за които „събира и използва“ данни за тях. В приложение II, раздел III, точка 9, буква а), подточка 11) само се споменават данни, които са „предавани“ или „оценени“. Дори и да изглежда, че в повечето такива случаи намерението не е да се ограничи обхватът на Принципите или да се създадат пропуски в защитата, тази противоречива терминология поражда риск от такива пропуски. Тъй като терминът „обработка“ е определен в Принципите, от съществено значение е да бъде използван последователно, с цел да се избегнат съществуващите в момента пропуски. В противен случай ще са налице твърде много възможности за вероятно непреднамерено тълкуване, което иначе би довело до погрешно тълкуване на формулировката на решението.

[11] Определението за „лични данни“, включено в приложение II, раздел I, точка 8, буква а), се отнася до „данни относно идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано“. Допълнителен принцип обаче гласи, че във връзка с данните относно човешките ресурси Принципите ще се прилагат само в случай на „предаване или на достъп до конкретна информация“. РГ по член 29 счита, че това открива възможност за обработка на лични данни по начин, който не е съвместим с принципите за защита на данните съгласно правото на ЕС, нито с общото определение за лични данни съгласно Щита за личните данни.

е такъв по отношение на редица други важни термини, включително „представител“ или „ обработващ данни“, „данни, кодирани с ключ“, „анонимни данни“ и „физическо лице от ЕС“, които по мнение на РГ по член 29 се нуждаят от ясно определение, с което да са съгласни и САЩ, и ЕС, с цел да се избегне объркване на по-късен етап, както за администраторите на данни, така и за обработващите данни, които използват Щита за личните данни, за надзорните органи и за обществото. Лесно решение би било към раздела с често задавани въпроси на Щита за личните данни да се добави речник на термините.

РГ по член 29 посочва също така законните основания за обработка на чувствителни данни, посочени в допълнителен принцип 1 (приложение II, раздел III, точка 1), в случаите, когато дадена организация не е необходимо да получи изрично съгласие (право на изрично съгласие (opt-in). Този допълнителен принцип 1 може да се разбира като подробно описание на законните основания за събирането на данни в ЕС, тъй като този списък е подобен на изброеното в член 8 от Директивата. РГ по член 29 би искала да припомни, че всяко обработване (включително събиране и предаване) на чувствителни данни, които са предмет на правото на ЕС, трябва да се извършва въз основа на законни основания съгласно член 8 от Директивата. Щитът за личните данни не може да се тълкува в смисъл, че предоставя алтернативни основания за такова обработване. Така например според РГ по член 29 не е възможно организация от САЩ да събира данни, за които се прилага правото на ЕС, въз основа на трудовото право на САЩ (вж. приложение II, раздел III, точка 1, буква а), подточка v). Поради това РГ по член 29 подчертава, че всяко тълкуване на допълнителен принцип 1 може да води само до прилагането му спрямо чувствителни данни, които вече са предадени, след като са събрани в ЕС въз основа на законни основания, предвидени в член 8 от Директивата.

И накрая, РГ по член 29 отбелязва липсата на яснота по въпроса кой може да се счита за физическо лице от ЕС и следователно да се ползва от защита съгласно Щита за личните данни: всички граждани на ЕС или лица, пребиваващи в ЕС. Това е от особено значение във връзка с правото на правна защита, включително достъпа до механизма на омбудсмана. Освен това решението за адекватността следва да разглежда въпроса за степента, в която Щитът за личните данни ще се прилага и за граждани/жители на държавите от ЕИП и Швейцария, които в миналото са били обхванати от схемата за „сфера на неприкосновеност на личния живот“.

1.2.3 Съвместен преглед и суспендиране

РГ по член 29 приветства факта, че Европейската комисия и администрацията на Съединените щати са се договорили за периодични прегледи на практическото приложение на Щита за личните данни. Този съвместен преглед е известна практика от много години в общността на работещите в областта на защитата на данните в ЕС, особено във връзка със споразуменията относно обмена на резервационни данни на пътниците (PNR данни) с трети държави и споразумението относно проследяване на финансирането на тероризма (TFTP). РГ по член 29 приветства също така факта, че в

тези съвместни прегледи от страна на органите за защита на данните могат да участват неопределен брой представители.

Предвид своя опит със съвместните прегледи през последните години РГ по член 29 би желала да изясни, че очаква съвместният преглед на Щита за личните данни да бъде по-цялостен, отколкото съвместните прегледи за PNR и TFTP. По-специално желателно е съвместният преглед да включва не само срещи с представители на агенциите, организациите и бизнеса на САЩ, но и проверки на място на определени елементи на Щита за личните данни. Представителите на органите за защита на данните (ОЗД), участващи в съвместния преглед, следва да могат да отправят предложения за такива проверки на място.

РГ по член 29 счита, че съвместният преглед изисква съвместна преценка на констатациите. До този момент резултатите от съвместните прегледи са представяни в работен документ на службите на Комисията, за което не се изискваше одобрението на членовете на екипа за съвместен преглед, които не работят в Комисията. Що се отнася до съвместния преглед на Щита за личните данни, РГ по член 29 би се радвала, ако докладът за констатациите може наистина да бъде споделен резултат. Като алтернатива може да се разгледа и публикуването на отделен доклад за съвместния преглед с ОЗД.

И накрая, що се отнася до съвместния преглед, РГ по член 29 припомня обещанието на Комисията, че разходите, направени от представителите на РГ по член 29 по време на съвместните прегледи, ще се възстановяват от Комисията. Работната група предполага, че това ще се прилага и по отношение на съвместния преглед на Щита за личните данни, във всеки случай за приемлив брой представители на ОЗД.

РГ по член 29 препоръчва редът и условията за съвместния преглед да се договорят между Комисията, администрацията на САЩ и РГ по член 29 поне три месеца преди извършването на първия съвместен преглед на Щита за личните данни и да се изготвят в писмен вид.

1.2.4 Правна уредба на ЕС в процес на преразглеждане

Решението за адекватността на Щита за личните данни е първото решение за адекватност, изготвено съгласно принципното споразумение за текста на Общия регламент относно защитата на данните. РГ по член 29 обаче установи, че Щитът за личните данни все още не отразява бъдещата ситуация. Така например важни нови понятия като правото на преносимост на данните и допълнителни задължения относно администраторите на данни, включително необходимостта да се извършва оценка на въздействието върху защитата на данните и да се спазват принципите на защита на личния живот още при проектирането и по подразбиране, не са включени в Щита за личните данни. Ето защо РГ по член 29 би желала да предложи Щитът за личните данни, заедно с всички съществуващи решения относно адекватността, да се преразгледат скоро след като Общият регламент относно защитата на данните започне

да се прилага. Би било добре в окончателното решение за адекватността да се направи изрично позоваване на този процес на преразглеждане.

2. ОЦЕНКА НА ТЪРГОВСКАТА ЧАСТ ОТ ПРОЕКТА НА РЕШЕНИЕ ЗА АДЕКВАТНОСТТА

2.1 Общи бележки

2.1.1 Подобрения

РГ по член 29 приветства внесените от Щита за личните данни подобрения и желанието от страна на преговарящите по него да се опитат и да отстранят подчертаните от нея недостатъци в „сферата на неприкосновеност на личния живот“. По-специално подобрения в сравнение със „сферата на неприкосновеност на личния живот“ могат да се забележат по отношение на следните елементи: включването на някои ключови определения като например „лични данни“, „обработка“ и „администратор“, механизмите, въведени за гарантиране на надзора на списъка към Щита за личните данни, и вече задължителните външни или вътрешни прегледи на спазването. Подобрения са направени и по отношение на принципа на достъп, като РГ по член 29 отбелязва, че сега се предоставят права на коригиране и заличаване, когато данните се използват по начин, който е несъвместим с Принципите на Щита за личните данни. Освен това вече е ясно, че физическото лице трябва да получи както потвърждение, че по отношение на него се обработват данни, така и съобщение за обработените данни.

РГ по член 29 приветства също така засилването на правните гаранции, приложими при последващи предавания, както и ангажиментите на Министерството на търговията на САЩ и на Федералната търговска комисия (ФТК) да осигуряват изпълнението на задълженията, предвидени в Щита за личните данни.

2.1.2 Прилагане на Щита за личните данни по отношение на организации, изпълняващи функциите на обработващ данни (представител)

За съжаление, степента, в която Принципите на Щита за личните данни се прилагат по отношение на сертифицирани организации, получаващи лични данни от ЕС просто с цел обработване (посочени като „представители“ или „обработващи данни“), остава неясна. Въпреки че в разпоредбите, съдържащи се в приложение II, раздел III, точка 10, буква а) наистина се посочва предаване на данни на сертифицирани организации за такива цели, т.е. посочване на изискването за сключване на договор, в тях липсва указание за това как Принципите на Щита за личните данни се прилагат по отношение на обработващите данни (представители). Това поражда несигурност както за сертифицирани организации от САЩ, получаващи данни за целите на обработването и за дружества, установени в ЕС, извършващи предаване на данни на сертифицирани организации, изпълняващи функциите на обработващи данни, така и за физическите лица, чиито данни се обработват. В резултат на това ще бъде трудно да се определи кои задължения всъщност са приложими по отношение на организациите — участници в

Щита, обработващи лични данни, получени от ЕС, при изпълнение на функциите им на обработващи данни. Ето защо със сигурност се изисква разясняване.

Трябва да се вземе под внимание и фактът, че няколко от задълженията, включени в Принципите, не са подходящи за лицата, обработващи данни, тъй като администраторите винаги са тези, които определят целите и средствата за обработването на данните (вж. определението за „администратор“ съгласно приложение II, раздел I, точка 8, буква в). Поради тази причина някои задължения, включени в Принципите, прилагани по отношение на организация, изпълняваща функцията на представител, може да са в противоречие с договора за обработването на данни, изискван съгласно правото на ЕС (договорът, посочен в приложение II, раздел III, точка 10, буква а). Така например договорът за обработване на данни по принцип няма да дава право на обработващия данни (представител) да извършва последващо предаване на данни на трета страна — администратор, дори при обстоятелствата, посочени в приложение II, раздел II, точка 3, буква а). Последващите предавания на представители на трета страна следва да се разрешават само след предварително одобрение от страна на администратора на данни. Освен това, съгласно изискванията на правото на ЕС, обработващ данни (представител) няма да бъде в състояние да извършва пълно уведомяване на физическите лица, както би следвало съгласно принципа за уведомяване (приложение II, раздел II, точка 1), например поради това, че тази организация не определя целите на обработването.

Поради това е от съществено значение в Принципите да се изясни, че в случай на такова противоречие, ще надделеят разпоредбите на договора за обработване на данни, и по-специално указанията на организацията, извършваща предаването на данните извън ЕС. Без подобно разяснение Принципите могат да бъдат тълкувани и прилагани по начин, който предлага твърде големи правомощия за контрол на представителя към Щита, а това ще изложи износителя на данни от ЕС на риск от нарушаване на задълженията му като администратор на данни съгласно закона за защита на данните на ЕС, приложим спрямо него при предаването на данни на организация — участник в Щита, изпълняваща функциите на представител. Освен това липсата на яснота създава впечатлението, че обработващият данни може според желанието си да използва повторно данните.

Освен това следва да се установят конкретни правила за случаите, в които една организация изпълнява функциите на обработващ данни (представител), за да се гарантира, че тази организация зачита указанията на администратора на данни. Следва да се поясни, че организациите от САЩ, получаващи данни просто с цел обработване, не могат да решат да обработват данните от свое име. При липсата на конкретни правила, приложими по отношение на организациите, действащи като обработващи данни, е трудно да се определи съгласно какви правила обработващият данни (представител) ще бъде в състояние да се самосертифицира.

2.1.3 Ограничения на задължението за придържане към Принципите

Приложение II, раздел I, точка 5 предвижда, наред с другото, изключения от Принципите, когато данни, обхванати от Щита за личните данни, се използват за целите на националната сигурност[12], обществения интерес, правоприлагането или следват законови, подзаконови нормативни актове, или съдебна практика, които пораждат взаимнопротиворечиви задължения или предвиждат изрични разрешителни. За РГ по член 29 е трудно да прецени, без да познава напълно законодателството на САЩ на федерално и щатско равнище, обхвата на това изключение и да реши дали тези ограничения са обосновани в едно демократично общество. От съществено значение е Европейската комисия да включи в своя проект на решение за адекватността и анализ на степента на защита, предоставяна в случаите, когато тези изключения са приложими. РГ по член 29 призовава Комисията да гарантира, че ЕС ще бъде информиран за всички законови или подзаконови нормативни актове, които могат да засегнат спазването на принципите, както приложимите понастоящем, така и приетите впоследствие, към момента на влизане в сила на новите закони или подзаконови актове в САЩ.

2.1.4 Липса на принцип за ограничаване на запазването на данни

Принципът за ограничаване на запазването на данни (член 6, параграф 1, буква д) от Директивата) е основен принцип в правото на ЕС за защита на данните, който налага личните данни да се пазят за срок, не по-дълъг от необходимия за постигането на целта, за която тези данни са събрани или обработени допълнително.

РГ по член 29 обаче не може да намери в документите, съставляващи Щита за личните данни, каквото и да е позоваване на необходимостта, администраторите на данни да гарантират, че данните се заличават, след като целта, за която тези данни са събрани или обработени допълнително, вече не е актуална. Следователно изглежда, че Принципите не налагат на сертифицираните организации ограничение за периода на съхранение на данните, сравнимо с това, наложено от принципа за ограничаване на запазването на данните съгласно правото на ЕС.

Формулировката на принципа „Цялост на данните и ограничаване в рамките на целта“ (приложение II, раздел II, точка 5) в никакъв случай не може да се счита за създаване на задължение за организация, изпълняваща функциите на администратор, да заличи данни, след като вече не са необходими за целите, за които са събрани или допълнително обработени, или за организация, изпълняваща функциите на обработващ данни, да заличи данни след прекратяването на споразумението за услуги.

Работната група подчертава, че липсата на разпоредби, налагащи ограничение върху запазването на данни съгласно Щита за личните данни, предоставя на организациите възможността да пазят данни за какъвто поискат срок, дори и след напускане на Щита

[12] Вж. глава 3 за повече коментари относно използването на лични данни, обхванати от Щита за личните данни за целите на националната сигурност и глава 4 за целите на правоприлагането.

за личните данни, което не е в съответствие с основния принцип за ограничаване на запазването на данни.

2.1.5 Липса на гаранции при автоматизирани решения, които имат правни последици или засягат съществено физическото лице

Щитът за личните данни не предоставя правни гаранции, когато физическите лица са обект на решение, което има правни последици за тях или ги засяга съществено, и което се основава единствено на автоматизираната обработка на данни, имащи за цел да се оценяват някои лични аспекти, свързани с тях, като представянето им на работното място, кредитоспособност, надеждност, поведение, и т.н.

Необходимостта от предвиждане на правни гаранции за автоматизирани решения (които имат правни последици или засягат съществено физическите лица), с цел да се предостави достатъчна степен на защита, е вече подчертана от РГ по член 29 в нейния работен документ 12.

Тази необходимост е от все по-голямо значение, тъй като непрекъснатото развитие на новите технологии позволява на повече дружества да обмислят прилагането на автоматизирана система за вземане на решения, което може са доведе до отслабване на позицията на физическите лица, оставени без право на защита срещу взетите по компютърен път решения. Когато решения, които са изцяло дело на автоматизирани системи, оказват влияние върху правното положение на физическите лица или ги засягат съществено (като например ги включват в черен списък и по този начин ги лишават от техните права), е от съществено значение да се осигурят достатъчно гаранции, включително правото да се познава използваната логика и да се поиска преразглеждане, което да не е автоматизирано.

2.1.6 Междинен период за съществуващи търговски взаимоотношения

Щитът за личните данни предвижда Принципите да се прилагат незабавно след сертифициране. Въпреки това организациите, които ще се сертифицират в рамките на първите два месеца след датата, на която рамката на Щита за личните данни се прилага ефективно, ще трябва да приведат съществуващите си търговски взаимоотношения с трети страни в съответствие с принципа за отчетност за последващото предаване във възможно най-кратък срок . Във всички случаи те следва да го направят не по-късно от девет месеца, след като са се сертифицирали съгласно Щита за личните данни.

Това означава, че съществуващите договори трябва в необходимата степен да бъдат приведени в съответствие с принципите между два и девет месеца след сертифицирането. В рамките на този междинен период са достатъчни принципите на уведомяването и на избора. РГ по член 29 набляга на факта, че предаванията могат да се извършват въз основа на Щита за личните данни само тогава, когато организацията може напълно да отговори на изискванията на Щита. Възможността в рамките на междинния период да се изпращат данни не може да се счита за отговаряща на

условията за законово предаване, и следователно не е приемлива, без получателят напълно да отговаря на принципите на Щита.

2.2. Специални коментари

2.2.1 Прозрачност

а) Общи бележки относно уведомяването

РГ по член 29 приветства по-всеобхватните и подробни изисквания, определени съгласно принципа „Уведомяване“, и по-специално това, че уведомяването трябва да включва връзка към или уеб адрес на списъка към Щита за личните данни, както и да се позовава на правото на достъп на физическите лица и на механизмите за алтернативно разрешаване на спорове[13]. РГ по член 29 предлага обаче те да бъдат по-ясни по отношение на други права (да коригират, заличават, когато има неточност или когато обработването е в нарушение на Принципите), които са обхванати.

Документите, съставляващи Щита за личните данни, пораждат опасения по отношение на момента, в който организация — участник в Щита за личните данни, трябва да предостави уведомяване на физическо лице. Приложение II, раздел II, точка 1, буква б) гласи, че „уведомяването трябва да бъде направено (...), когато физическите лица бъдат поканени за първи път да предоставят лична информация на организацията или веднага след като стане възможно, но във всеки случай, преди тези данни да бъдат използвани от организацията за цел, различна от тази, за която са били първоначално събрани или обработени от организацията, която извършва предаването или разкриването им за първи път на трета страна“. РГ по член 29 счита, че в много ситуации организацията — участник в Щита за личните данни, няма да събира данни директно от субекта на данни, а времето на уведомяването следва да бъде към момента, в който данните се записват от организация — участник в Щита.

РГ по член 29 отбелязва, че действителното прилагане на изискванията по отношение на принципа на уведомяването и политиката в областта на неприкосновеността на личния живот следва да бъдат оценени при първия годишен преглед на Щита за личните данни.

б) Публична достъпност на политиката в областта на неприкосновеността на личния живот

РГ по член 29 приветства факта, че вече е изрично определено, че Министерството на търговията на САЩ ще проверява дали дружествата, които имат публични уебсайтове, са публикували политиката си в областта на неприкосновеността на личния живот на

[13] Приложение II, раздел II, точка 1: РГ по член 29 се позовава на втората препоръка на Европейската комисия в Съобщение COM(2103)847, както и на писмото на РГ по член 29 до заместник-председател Рединг от 10 април2014 г., и по-специално точка 4 към „Прозрачност“.

този уебсайт, или къде е оповестена публично политиката им в областта на неприкосновеността на личния живот в случаите, когато нямат публични уебсайтове[14].

в) Публикуване на условията за поверителност на договори с обработващи данни

Наред с условията, съгласно които организациите — участници в Щита за личните данни, могат да предават данни на обработващ данни (представител), Щитът за личните данни предвижда задължение за самосертифицираните организации „при поискване да предоставят на министерството обобщение или представително копие на съответните разпоредби във връзка с неприкосновеността на личния живот от договора с представителя“ (вж. приложение II, раздел II, точка 3, буква б), подточка v). Работната група приветства това изискване за прозрачност към Министерството на търговията на САЩ.

2.2.2 Избор

Щитът за личните данни предвижда право на клауза за неучастие („opt out“) по отношение на разкриването на лична информация на трета страна или по отношение на използването на лична информация за несъвместима по същество цел[15] (приложение II, раздел II, точка 2). Освен това физическите лица се ползват във всеки един момент от правото си на клауза за неучастие при използването на лична информация за целите на директния маркетинг (приложение II, раздел III, точка 12, буква а)[16].

С изключение на контекста за целите на директния маркетинг, не са предоставени подробности за начина и момента на упражняване на клаузата за неучастие. Работната група по член 29 счита, че простото позоваване на съществуването на това право в политиката в областта на неприкосновеността на личния живот не може да бъде достатъчно, а следва да се предложи *индивидуализирана* възможност за упражняване на това право *преди* разкриването или повторната употреба на лична информация.

Освен това РГ по член 29 подчертава, че в Щита за личните данни следва да се предложи общо право на възражение (въз основа на първостепенни съображения, свързани с конкретната ситуация за субекта на данни), което се разбира като право да се поиска преустановяване на обработката по отношение на нечии данни, когато физическото лице има убедителни законни основания, свързани с конкретната за него ситуация.[17] РГ по член 29 изрично препоръчва в проекта на решение за адекватността да се разяснява, че правото на възражение следва да е налице във всеки един момент и

[14] Вж. първата препоръка на Европейската комисия в Съобщение COM(2013)847 и писмото на работната група по член 29 до заместник-председател Рединг, 10 април 2014 г., и по-специално точка 3 към „Прозрачност“.
[15] Допълнителен принцип 14, буква в), подточка I) предвижда правото на оттегляне от клинично изпитване, което може да се разглежда като право на възражение или оттегляне на съгласие.
[16] Това е идентично с предвижданото в схемата за „сфера на неприкосновеност на личния живот“ (често задаван въпрос 12), като в тази връзка не са правени промени.

че това възражение не е ограничено до използването на данните за директен маркетинг[18].

РГ по член 29 изразява опасенията си, че липсата на определение за това, какво трябва да се счита за „несъвместима по същество“ цел, ще доведе до объркване и правна несигурност. Следва да се уточни, че в никакъв случай, принципът „Избор“ не може да се използва за заобикаляне на принципа на ограничаване в рамките на целта[19]. Принципът на избора трябва да се прилага единствено когато целта се различава съществено, но все още е съвместима, тъй като обработването за несъвместима цел е забранено (приложение II, раздел II, точка 5, буква а). Трябва да се разясни, че правото на клауза за неучастие не може да дава право на организацията да използва данни за несъвместими цели. Поради това тя препоръчва хармонизиране на свързаните формулировки, като се използва една-единствена и определена формулировка (напр. „се различава съществено от — но все пак е съвместима със“).

Разясняването ще помогне да се определи кога решение за обработка на данни за друга цел или за разкриване на информация попада в обхвата на правото на ЕС. В тази ситуация обичайните правни условия на ЕС по отношение на тази обработка (като забраната за обработване за несъвместими цели, за предоставяне на законно основание за обработването и необходимостта да се информира лицето) ще се прилагат директно, включително по отношение на организация от САЩ, попадаща в обхвата на правото на ЕС. Това означава, че на практика износителят на данни от ЕС е този, който ще трябва да вземе такова решение, за да гарантира прозрачността и законността на обработката съгласно правото на ЕС. Поради това принципът „Избор“ ще се прилага само когато решението е взето изключително от организация — участник в Щита, от САЩ, без да се отнася до правото на ЕС.

2.2.3 Последващи предавания

а) Обхват

РГ по член 29 изразява загриженост във връзка със ситуацията, в която последващите предавания на лични данни се извършват от сертифицирана организация — участник в Щита за личните данни, в САЩ, към получател в трета държава.

Щитът следва да се разглежда не само като инструмент за предаване на данни на ЕС от ЕС към САЩ, но и като инструмент, който да се използва за предаване на данни от САЩ към трети държави. Ето защо разпоредбите относно последващите предавания са важен елемент на Щита, който следва да осигурява достатъчно гаранции и достатъчна степен на защита, когато се извършва последващо предаване на данни извън територията на САЩ. Един конкретен проблем е свързан с националната сигурност и правоприлагането.

[18] Виж писмото на РГ по член 29 до заместник-председателя Рединг, под „Избор“.

[19] Конкретен пример за по-нататъшно несъвместимо обработване одобрено съгласно принципа на избора е предоставен в допълнителен принцип 9, буква б), подточка i) (вж. коментара на РГ по член 29 за това под точката, свързана с данните за човешките ресурси).

Принципът на Щита за личните данни за отчетност за последващото предаване не е ограничен до администратори на лични данни, обработващи данни или представители на установен в САЩ получател. Следователно последващите предавания на трета държава могат да се извършват въз основа на Щита за личните данни дори в случаите, когато третата държава има закони, които предвиждат обществен достъп до лични данни, например с цел наблюдение. Това поражда риск за данните от ЕС от неоправдана намеса в защитата на основните права.

Във всеки случай на последващо предаване на трета държава, всяка организация — участник в Щита за личните данни, е задължена преди предаването да оценява задължителните изисквания на националното законодателство на третата държава, приложими към вносителя на данни. Ако е установен риск от съществени отрицателни последици за гаранциите, задълженията и степента на защита, предоставяни от Щита за личните данни, организацията — участник в Щита за личните данни, изпълняваща функциите на обработващ данни (представител), незабавно уведомява администратора на данни от ЕС, преди да извърши каквото и да е последващо предаване. В тези случаи износителят на данни има право да преустанови предаването на данни и/или да прекрати договора. Когато е налице риск от съществени неблагоприятни последици, организацията — участник в Щита, изпълняваща функциите на администратор, няма да има право на последващо предаване на данни, тъй като това би нарушило задължението ѝ в случай на последващо предаване да осигури същата степен на защита, която се осигурява от Принципите (вж. приложение II, раздел II, точка 3, буква а).

По подобен начин при промяна в законодателството на трета държава, която е вероятно да доведе до съществени неблагоприятни последици за гаранциите, задълженията и степента на защита, предоставяни от Щита за личните данни, организация — участник в Щита за личните данни, която изпълнява функциите на обработващ данни (представител), е длъжна, съгласно Щита за личните данни, да уведоми износителя на данни за тази промяна веднага след като разбере за нея, като в този случай износителят на данни има право да преустанови предаването на данни и/или да прекрати договора. Съответно организация — участник в Щита, изпълняваща функцията на администратор, няма да има право на последващо предаване, тъй като има задължение да предоставя същата степен на защита, която се осигурява от Принципите (вж. приложение II, раздел II, точка 3, буква а).

РГ по член 29 припомня позицията си за това, че ако администратор на данни от ЕС знае за последващо предаване на трета държава извън САЩ дори преди да се извърши предаването към САЩ, или ако администратор на данни в ЕС носи съвместна отговорност за решението да се позволи последващо предаване, последното следва да се счита за директно предаване от ЕС на трета държава извън територията на САЩ. Това означава, че по отношение на предаването са приложими членове 25 и 26 от Директивата, вместо принципа за предаване на данни на Щита за личните данни.

б) Предавания на данни от организация — участник в Щита за личните данни, на администратор на трета страна

РГ по член 29 приветства задължението за въвеждане на договори (приложение II, раздел II, точка 3, буква а), които да гарантират, че трета страна администратор ще осигури най-малко същата степен на защита на неприкосновеността на личния живот, която се изисква от Принципите на Щита за личните данни. Целта е да се гарантира, че личните данни продължават да бъдат адекватно защитавани дори и след като е извършено последващо предаване. РГ по член 29 обаче има някои забележки относно предложените условия.

Липса на позоваване на принципа на ограничаване в рамките на целта

РГ по член 29 препоръчва също така включването на ясно позоваване на принципа на ограничаване в рамките на целта (приложение II, раздел II, точка 5) в условията за последващите предавания на администратор на трета страна (приложение II, раздел II, точка 3, буква а). Това ще поясни, че последващи предавания не могат да се извършват, когато администраторът на трета страна ще обработва данните с несъвместима цел.

Изключение от необходимостта от договор за вътрешно-групови предавания между администратори

Изключение от необходимостта от договор се предвижда за вътрешно-групови предавания между администратори. В този случай Принципите гласят, че непрекъснатостта на защитата може да се предлага от задължителни фирмени правила (ЗФП) или „други вътрешно-групови инструменти (напр. програми за спазване и контрол)“ (приложение II, раздел III, точка 10, буква б). РГ по член 29 счита, че позоваването на „други вътрешно-групови инструменти“ не гарантира правно обвързващи ангажименти, поети от другите членове на групата. Тъй като РГ по член 29 и законодателството на ЕС[20] предпочитат като цяло задължителните ангажименти за очертаване на рамката на вътрешно-груповите предавания, е важно да се избягва използването на Щита за личните данни по начин, който заобикаля това изискване. РГ по член 29 припомня, че във всеки случай последващите предавания от САЩ на трета държава, планирани дори преди да се извърши предаването на САЩ, или които са предмет на съвместно администриране с администратор на данни от ЕС[21], трябва да се разглеждат като пряко предаване от ЕС на трета държава извън САЩ. Следователно по отношение на предаването са приложими членове 25 и 26 от Директивата.

в) Предавания от организация — участник в Щита за личните данни, на обработващ данни (представител) на трета страна

РГ по член 29 приветства факта, че сега договорът за последващо предаване е задължителен за получаващите субекти, които изпълняват функциите на обработващи данни (представители), независимо от тяхното участие в Щита за личните данни или ако се ползват от друго решение за установяване на адекватността. РГ по член 29

[20] В ОРЗД се подчертава и необходимостта от задължителни и изпълними ангажименти, когато се използва инструментът (ЗПЗ, договорни клаузи, кодекси за поведение или сертификация).
[21] Например за данните за човешките ресурси.

приветства допълнителните гаранции, разграничаващи тези последващи предавания (приложение II, раздел II, точка 3, буква а), подточка i); раздел II, точка 3, буква а), подточка iii); раздел II, точка 3, буква а), подточка iv); раздел II, точка 3, буква а), подточка v); раздел II, точка 7, буква г). Последната точка (приложение II, раздел II, точка 7, буква г) засяга задължението носенето на отговорност да продължи, когато данните се разкриват на представител. Изглежда обаче, че тази гаранция няма да се прилага, в случай че дадена организация е избрала да си сътрудничи с ОЗД (вж. приложение II, раздел III, точка 5, буква а накратко). РГ по член 29 не разбира мотива за такова изключение и счита, че отговорността следва да се прилага дори и в този случай.

Липса на позоваване на принципа за ограничаване в рамките на целта

РГ по член 29 отбелязва, че по отношение на принципа на отчетност за последващото предаване (приложение II, раздел II, точка 3) се обяснява, че личните данни могат да се предават на трета страна, която изпълнява функциите на представител, само за ограничени и конкретни цели, но не се твърди изрично, че тези ограничени и конкретни цели трябва да са съвместими с първоначалните цели, за които са събрани данните, както и с указанията на администратора. По този въпрос е необходима повече яснота. Поради това РГ по член 29 предлага да се гарантира, че решението за адекватността предоставя повече подробности, например като в рамките на принципа за последващо предаване се въведе (освен принципа за клаузата за неучастие) ясно позоваване на принципа на ограничаване в рамките на целта (приложение II, раздел II, точка 5), съгласно който данни не могат да се обработват (включително разкриват) с несъвместими цели.

Необходимост от повече допълнителни задължения за организациите — участници в Щита за личните данни, които изпълняват функциите на обработващи (представители), относно предавани данни към друг обработващ (представител)

Липсата на ясни правила в случаите, когато организация — участник в Щита, изпълнява функциите на представител (т.е. от името на администратор от ЕС), предполага появата на пропуск и може да попречи на администратора от ЕС да продължи да упражнява контрол. Организация — участник в Щита, получаваща данните като представител на администратор от ЕС, трябва да спазва указанията на администратора от ЕС. Това следва да е изрично посочено в Принципите, за да се гарантира, че неспазването на тези указания води не само до нарушаване на договора (приложение II, раздел III, точка 10, буква а), подточка ii), но и до нарушаване на принципите на Щита за личните данни.

Възможността организация — участник в Щита, която изпълнява функцията на представител, да извършва последващо предаване на данни на трета страна представител, трябва да бъде прозрачна за администратора и да подлежи на предварителното му одобрение. Поради това следва да е ясно посочено, че договорът, подписан между представителя и администратора от ЕС (посочен в често задаваните

въпроси, точка 10, като „договор по член 17“), е този, който определя дали последващото предаване е разрешено[22].

Настоящите условия, приложими към последващото предаване на представител, се основават на предположението, че организацията — участник в Щита, действа като администратор, и следователно може сама да вземе решение относно възможната намеса на трета страна представител. Това обаче не би трябвало да е възможно, когато организация — участник в Щита, изпълнява функциите на представител. В противен случай администраторът от ЕС ще бъде лишен от правомощията си за контрол.

Съответните разпоредби на договора, сключен с трета страна представител, свързани с неприкосновеността на личния живот, трябва да са достъпни за администратора и също така трябва да гарантират поне същата степен на защита, която се осигурява от договора, подписан с администратора на данни.

2.2.4 Цялост на данните и ограничаване в рамките на целта

а) Пропорционалност

По второстепенна точка РГ по член 29 се позовава на писмото си до заместник-председателя Рединг, в което пише, че „обработка на лични данни може, дори при пълно зачитане на уведомяването и на избора, да не е пропорционална по отношение на правата, свързани с интересите и свободите на субекта на данни или обществото. Принципът на пропорционалност или разумност трябва да се зачита на всички етапи от обработката и следва да се прилага в допълнение към принципите на уведомяването и на избора“[23].

Щитът за личните данни (приложение II, раздел II, точка 5, буква а) гласи, че информацията трябва да бъде ограничена до необходимата за целите на обработването. РГ по член 29 предпочита тази формулировка да бъде заменена в окончателното решение за адекватността, тъй като самият факт, че данните са подходящи за обработване, не е достатъчен обработването да е пропорционално. За да отговаря на принципа на пропорционалност, обработването следва да бъде ограничено до данните, които са необходими за самата обработка.

б) Точност

Принципът за цялост на данните и ограничаване в рамките на целта (приложение II, раздел II, точка 5) също гласи: „Доколкото е необходимо за тези цели, всяка организация трябва да вземе подходящи мерки, за да гарантира надеждността на личните данни по отношение на предвиденото им използване, както и тяхната точност, пълнота и актуалност“. РГ по член 29 отбелязва, че това е точно същата формулировка, като използваната в договорността за „сфера на неприкосновеност на личния живот“.

[22] Вж. писмото на РГ по член 29 до заместник-председателя Рединг от 10 април 2014 г., точка 4 към Последващо предаване.
[23] Вж. писмото на РГ по член 29 до заместник-председателя Рединг, 10 април 2014 г., точка 8.

РГ по член 29 се съмнява, че формулировката „доколкото е необходимо за тези цели“ ще бъде включена, тъй като по нейно мнение точността на данните не следва да зависи от целта на обработката. РГ по член 29 би предпочела в окончателното решение за адекватността да не се прави такава връзка.

в) Ограничаване в рамките на целта

Когато лични данни се предават на организация от САЩ от администратор на данни, установен в ЕС, износителят на данни следва изрично да уведоми организацията от САЩ за целите, с които първоначално са събрани данните. Това е от съществено значение, за да се определи дали след предаването настъпва промяна на целта, като по този начин се задействат принципите на уведомяването и на избора, а това ще допринесе за разпределяне на риска и отговорността.

Принципът „Цялост на данните и ограничаване в рамките на целта“ (приложение II, раздел II, точка 5) гласи, че организация не може да обработва лична информация по начин, несъвместим с целите, за които тя е била събрана или за които по-късно е дадено разрешение от физическото лице. Принципът на избора (приложение II, раздел II, точка 2) обаче предвижда изрично съгласие за „използването“ на чувствителна информация (т.е. лична информация, свързана с медицинското или здравословното състояние, с произход — раса или етнически произход, политически възгледи, вероизповедание или философски убеждения, членство в синдикат или сексуални предпочитания, както и данни относно съдебни досиета) с цели, несъвместими по същество с предназначението, с които е била първоначално събрана или за които по-късно е дадено разрешение от физическото лице. Това изрично съгласие не се изисква в ситуациите, посочени в Допълнителен принцип 1, буква а) (приложение II, раздел III, точка 1, буква а). По отношение на нечувствителната лична информация се предвижда режим на клауза за неучастие.

РГ по член 29 посочва, че обхватът на принципа за ограничаване в рамките на целта е различен в рамките на принципите на уведомяването, на избора и на цялост на данните и ограничаване в рамките на целта. Всъщност термините „несъвместима цел“ и „несъвместима по същество цел“ се използват в рамките на един и същ текст, без тези две понятия да са ясно разграничени[24].

РГ по член 29 има сериозни опасения поради факта, че такова несъответствие може да доведе до големи затруднение да се съчетаят принципите на цялост и на ограничаване в рамките на целта (приложение II, раздел II, точка 5) и принципа на избора (приложение II, раздел II, точка 2), тъй като единият гласи, че данните не могат да се обработват по начин, който е несъвместим с целите, с които са събрани, докато другият

[24] РГ по член 29 отбеляза, че са използвани и някои други изрази: „тази употреба не е съвместима с“ (приложение II, раздел III, точка 14, буква б), подточка ii) и „използва за други цели“ (приложение II, раздел III точка 9, буква б), подточка i) , „използвани (...) за цел, различна от тази, за която са били първоначално събрани“ (приложение II, раздел II, точка 1, буква б). Тази несигурност може да доведе до липсата на достатъчно гаранции по отношение на принципа на ограничаване в рамките на целта.

предвижда механизъм за клауза на неучастие в случай, че данните са обработени с цел, която е несъвместима по същество с първоначалната цел.

Поради това принципът на избор може да се разбира като разрешаване на бъдещо несъвместимо обработване[25]. Според РГ по член 29 трябва изрично да се посочи, че организацията не трябва да бъде упълномощена да обработва данни с несъвместима по същество цел, когато тази цел е несъвместима съгласно принципа за ограничаване в рамките на целта. С други думи, трябва да е ясно, че принципът на избор не е изключение от принципа за ограничаване в рамките на целта.

Също, във всеки случай, ако последващото обработване може да се разглежда като съвместимо, то тогава следва да се прилагат и принципите на уведомяването и на избора.

2.2.5 Изключения за журналистически цели

Изключенията за журналистически цели по отношение на обработването на лични данни са обхванати в допълнителен принцип 2 (приложение II, раздел III, точка 2). Разбираемо е, че тези разпоредби отразяват предвидената в Конституцията на САЩ защита на свободата на словото. Поради това документите към Щита за личните данни гласят, че „личната информация […], която е била публикувана преди това, след което е била архивирана, не е предмет на изискванията съгласно Принципите на Щита за личните данни“ (приложение II, раздел III, точка 2, буква б). Това изключение изглежда включва всяко последващо обработване от всеки администратор или обработващ данни, т.е. не трябва да се ограничава до последващо обработване за журналистически цели. Както вече бе посочено в писмото до заместник-председателя Рединг от 10 април 2014 г., РГ по член 29 би предпочела да види по-ограничен подход по отношение на изключенията за журналистически цели, който в по-голяма степен съответства на принципа, прилаган в ЕС, както и на правото на изключване от списък след случая с Google Испания[26].

2.2.5 Право на достъп, коригиране и заличаване за субектите на данни

Съгласно Щита за личните данни, физическите лица имат правото да получат *потвърждение* за това дали техните данни се обработват от организацията и тези данни да *им бъдат съобщени* (приложение II, раздел III, точка 8, буква а), подточка i). Задължението за организациите обаче да отговорят на искания на физически лица относно целите на обработването, категориите съответни лични данни, за които то се отнася, и получателите или категориите получатели, на които се разкриват личните данни, е доста слабо. РГ по член 29 счита, че подробностите, които трябва да се

[25] Вж. също така коментара в рамките на принципа на избора. РГ по член 29 счита, че фактът, че правилата за последващо предаване (приложение II, раздел II, точка 3) се отнасят само до принципа на избора, но не и до принципа за ограничение в рамките на целта, увеличава риска от такова разбиране.
[26] Решение от 13 май 2014 г. по дело C-131/12, Google Spain/Agencia Española de Protección de Datos и Mario Costeja González.

предоставят на субекта на данните, следва да са посочени в основната част на текста, вместо в бележките под линия и трябва да са представени като ясно задължение (свързано с приложение II, раздел III, точка 8, буква а, подточка i), буква l).

Съгласно допълнителен принцип 8 „достъпът се осигурява само в рамките на личната информация, която организацията съхранява“ (приложение II, раздел III, точка 8, буква г), подточка ii.) Това правило не трябва да се тълкува ограничително в смисъл, че достъпът по принцип трябва да бъде предоставен до данни, обработени по какъвто и да е начин от дадена организация, а не само съхранявани. Поради това за целите на ефективността на правото на достъп е важно да се поясни, че „съхранява“ означава „обработва“ по смисъла на предоставеното в приложение II, раздел I, точка 8, буква б) определение. Прилагането на това правило ще бъде разгледано по алтернативен начин в рамките на съвместния преглед на Щита за личните данни.

Запазват се опасенията и по отношение на списъка с изключенията, предоставен в приложение II, раздел III, точка 8, буква д), подточка i), който е подобен на този, представен във въпрос 8 от често задаваните въпроси към решението за сфера на неприкосновеност на личния живот и който има тенденция да се наклони балансът в посока към интересите на организациите. В този смисъл на физическите лица няма да бъде предоставен достъп до техните собствени лични данни по следните причини: „нарушаване на […] професионално задължение или привилегия“ (приложение II, раздел III, точка 8, буква д), подточка 3), „нарушаване на разследвания на служители по отношение на сигурността или относно оплаквания, или във връзка с планиране на нови назначения и реорганизации на дружествата“ (приложение II, раздел III, точка 8, буква д), подточка 4) и „нарушаване на поверителността, необходима при извършване на мониторинг, инспекции или изпълнение на регулаторни функции във връзка с доброто управление, или при бъдещи или текущи преговори, в които организацията участва“ (приложение II, раздел III, точка 8, буква д), подточка 5). Тези причини следва да се разглеждат в допълнение към общото изключение относно поверителната търговска информация, включено в приложение II, раздел III, точка 8, буква в). Ето защо физическо лице никога няма да има достъп до своите данни в изброените по-горе ситуации, без да има баланс между правата и интересите на лицето и тези на организацията, която трябва да вземе решение по отправеното към нея искане за достъп.

РГ по член 29 припомня, че правото на достъп до собствените данни се предоставя на физическите лица по член 8, параграф 2 от Хартата. Въпреки че това не е абсолютно право, то е основно за правото да защита на личните данни, тъй като улеснява упражняването на други права на субекта на данни, като коригиране или заличаване.

Що се отнася до правата на коригиране и заличаване, РГ по член 29 приветства значителното подобрение, внесено от Принципите на Щита за личните данни в сравнение с принципите на „сферата на неприкосновеност на личния живот“, което предвижда тези права да се предоставят не само в ситуации, в които данните са

неточни, но и когато данните се обработват в нарушение на Принципите (приложение II, раздел II, точка 6).

2.2.6 Защита, прилагане и отговорност за причинени вреди (механизми за правна защита)

а) Ефективно прилагане на правото на правна защита на физическите лица от ЕС

РГ по член 29 признава ангажиментите на органите на САЩ по отношение на различни етапи от механизма за правна защита. Предвид сложността и липсата на яснота относно общата архитектура на механизма обаче РГ по член 29 се опасява, че на практика ефективното упражняване на правото на субекта на данните може да бъде подкопано. РГ по член 29 посочва, че качеството на механизма за правна защита следва да има предимство пред количеството на механизмите, които са достъпни за гражданите на ЕС. Налице са и опасения, че по-голямата част от механизмите за защита, ако не и всички, предвиждат процедура в САЩ и по този начин усложняват наблюдението на процедурата от ОЗД от ЕС.

Всъщност предвиденият в Щита за личните данни механизъм за защита е съсредоточен най-напред върху възможността за субекта на данни да „отстоява правата си и да разследва случаи на неспазване на Щита за личните данни чрез директни контакти със самосертифицирано дружество от САЩ“[27]. Освен това организациите трябва да определят един независим орган за решаване на спорове, който да разследва и разглежда жалби на физически лица. РГ по член 29 приветства факта, че това ще бъде организирано, без да се заплаща от лицето.

Като алтернатива, жалби могат да се подават директно пред Федералната търговска комисия дори и ако тя не е задължена да ги разглежда. ОЗД също може да подаде жалба, като Министерството на търговията на САЩ е задължено да я разгледа и да положи всички възможни усилия да съдейства за разрешаването на жалби (приложение I), които Федералната търговска комисия (ФТК) ще разглежда с предимство (приложение II, раздел III, точка 7, буква д). Разглеждането на жалбите от ФТК с предимство обаче не гарантира на субекта на данни, че жалбите му ще бъдат разгледани.

Като последна мярка физическите лица ще имат възможност да поискат въпросът да бъде решен чрез правно обвързващ арбитраж. В САЩ ще бъде установена специалната група по арбитража, която ще подлежи на контрол от съдилищата на САЩ.

Щитът за личните данни също така предлага за организацията възможност да избира сътрудничество с ОЗД от ЕС (приложение II, раздел III, точка 5, буква а). Това е дори задължително за данните за човешките ресурси, събрани в рамките на трудови правоотношения (приложение II, раздел III, точка 9, буква г), подточка ii). В този случай няма да се прилага алтернативното разрешаване на спорове (АРС)

[27] Европейска комисия, проект на решение за адекватността, параграф 30.

(приложение II, раздел III, точка 5, буква а). Щитът за личните данни не определя ясно как ще се организира на практика сътрудничеството с ОЗД от ЕС. Не е ясно по-специално дали групата ще разглежда всички случаи, или всеки различен случай ще се разглежда от отделна група.

РГ по член 29 счита, че в решението за адекватността са необходими повече подробности, когато се разглежда компетентността на ОЗД да разглежда жалби. Това очевидно зависи от квалификацията на организацията, но не е ясно по какъв начин.

Когато организацията изпълнява функциите на представител от името на администратор от ЕС, физическите лица ще имат във всеки случай възможност да подадат оплакване пред компетентната ОЗД от ЕС. Ситуацията ще бъде подобна по отношение обработването на данни за човешките ресурси и за обработването на други търговски данни

Когато организация — участник в Щита за личните данни, изпълнява функциите на администратор на данни, компетентността на ОЗД да разглежда жалби ще бъде ограничена до обработване съгласно правото на ЕС (обработване в рамките на отговорността на администратор от ЕС, включително съвместен контрол с организация от САЩ, или когато спрямо организация — участник в Щита за личните данни, правото на ЕС ще е пряко приложимо, например при използване на оборудване в ЕС). За обработването на данни, което се извършва единствено съгласно правото на САЩ обаче, ще се прилагат изключително механизмите на Щита за личните данни. За да се преодолеят езиковите бариери и липсата на знания за правната система на САЩ, би било полезно, ако ОЗД от ЕС има право да действа като посредник за жалби на физически лица или да им помага в рамките на производство за АРС с организации от САЩ, или по време на техни договори с органите на САЩ, ако ОЗД прецени, че е целесъобразно.

РГ по член 29 подчертава, че разяснението в Щита за личните данни механизъм не следва по-ранната препоръка, съгласно която физически лица от ЕС следва „да могат да подават жалби за нанесени щети в Европейския съюз“, както и „да им се предостави право на подават жалби пред компетентния национален съд в ЕС“[28]. Би било добре, организациите — участници в Щита за личните данни, да включат такава възможност в политиката си в областта на неприкосновеността на личния живот.

С цел да се гарантира ефективност, РГ по член 29 препоръчва системата да позволява на ОЗД от ЕС да представлява субекта на данни и да действа от негово име или да действа като посредник. Като алтернатива, тя следва да съдържа специфични клаузи, свързани с компетентността, позволяващи на субектите на данни да упражняват правата си в Европа.

б) Арбитраж

[28] Виж писмото на РГ по член 29 до заместник-председателя Рединг, 10 април 2014 г.

Окончателните арбитражни процедури все още не са финализирани, което усложнява оценката на РГ по член 29. Тъй като изглежда, че схемата за арбитраж ще се осъществява съгласно правото на САЩ и единственият език, на който ще се води арбитражното дело, ще бъде английският, ОЗД от ЕС могат да поискат да имат право да подпомагат физически лица по време на процеса.

Освен това арбитражната процедура е въведена поради факта, че не е налице гаранция, че жалбата ще бъде разгледана, тъй като ФТК не е задължена да разглежда всяка подадена жалба. РГ по член 29 отбелязва, че ако физическо лице от ЕС реши, че има нужда да бъде подпомагано от адвокат, трябва да поеме за своя сметка разходите за хонорара на своя адвокат, което може да попречи на физическите лица да подадат жалбите си за арбитражна процедура.

в) Надзор, прилагане и ефективност на механизмите за правна защита

Условия за допускане в Щита

Съгласно Съда на ЕС „надеждността на такава система […] почива основно на въвеждането на ефективни механизми за откриване и контрол, позволяващи установяване и санкциониране в практиката на евентуалните нарушения на правилата, гарантиращи защитата на основните права […].“[29]

РГ по член 29 отбелязва, че изглежда, че по отношение на Щита за личните данни ролята на Министерството на търговията на САЩ в процеса на сертифициране се свежда просто до проверка на пълнотата на документите. Въпреки че РГ по член 29 признава, че самосертифицирането не предполага системна предварителна проверка на прилагането на политиките в областта на неприкосновеността на личния живот, Министерството на търговията следва най-малкото да се ангажира системно да извършва проверка дали политиките в областта на неприкосновеността на личния живот включват принципите на Щита за личните данни. Такъв ангажимент е посочен в проекта на решение за адекватността, но не може да бъде ясно определен в представителното писмо на Министерството на търговията[30].

Нарушението на принципите на Щита за личните данни може да остане незабелязано за дълъг период от време и да бъде установено само след нанасяне на сериозна вреда на основните права на субекта на данни, вероятно непоправима. Ето защо този подход може да противоречи на европейския принцип на предпазливост.

Прозрачност посредством списъка към Щита за личните данни и регистър на организациите, заличени от списъка

Във връзка с прозрачността по отношение на субекта на данните са направени значителни подобрения. Освен всички организации в САЩ, които са се

[29] Решение по делото Schrems, точка 81.
[30] Европейска комисия, проект на решение за адекватността, точка 34.

самосертифицирали пред Министерството на търговията, новият списък към Щита за личните данни ще съдържа също регистър на всички организации, заличени от списъка към Щита за личните данни, включително причината, поради която дадена организация е заличена[31]. Уебсайтът на Щита за личните данни на Министерството на търговията на САЩ ще продължи да поставя по-голям акцент върху целевите групи по начин, който ще улесни проверката на вида на информацията, която е включена в самосертифицирането на организацията, както и политиката в областта на неприкосновеността на личния живот, която се прилага по отношение на включената информация, и метода, който организацията използва за проверка на спазването на принципите[32]. РГ по член 29 приветства факта, че вече изрично е посочено, че Министерството на търговията на САЩ ще проверява дали дружествата, които имат публичен уебсайт, са публикували политиката си в областта на неприкосновеността на личния живот на този уебсайт, или къде е оповестена публично политиката им в областта на неприкосновеността на личния живот в случаите, когато нямат публични уебсайтове[33]. Документите също така са по-информативни по отношение на съдържанието на политиката в областта на неприкосновеността на личния живот[34].

РГ по член 29 счита, че е възможно да възникне проблем, ако организация, която вече е включена в списъка към Щита за личните данни, впоследствие разшири обхвата на сертификацията си с други категории данни. В тези случаи списъкът няма да отразява различните периоди на приложимост на Принципите към различните категории данни. Това поражда риск от невъзможност за физическите лица и предприятията в ЕС да преценят напълно дали определен набор от данни действително подлежи на Принципите на Щита за личните данни, и ако е така, откога. За да се избегне този недостатък, работната група препоръчва регистърът на организациите в списъка към Щита за личните данни да уточнява, поотделно за всяка категория лични данни, датата на влизане в сила на самосертифицирането.

РГ по член 29 приветства факта, че Министерството на правосъдието на САЩ ще поддържа регистър на организациите, които са били заличени от списъка към Щита за личните данни, и че този регистър ще включва обяснение, разясняващо че тези организации вече не се ползват с предимствата на Щита за личните данни, но трябва да продължат да прилагат Принципите по отношение на личните данни, които са получили, докато са били сертифицирани организации по Щита за личните данни, за времето през което продължават да съхраняват тези данни (приложение I, точка 3). Обаче тъй като някои от организациите, които са били заличени от списъка към Щита за личните данни, могат да изберат да върнат или да заличат данните, получени

[31] Приложение I, точка 5 и приложение II, раздел II, точка 1; РГ по член 29 се позовава и на четвъртата препоръка на Европейската комисия в Съобщение COM(2013)847, както и на писмото на РГ по член 29 до заместник-председател Рединг, 10 април 2014 г., и по-специално точка 5 към „Прозрачност“.

[32] Приложение I, точка 8; РГ по член 29 се позовава също така и на писмото си до заместник-председател Рединг, 10 април 2014 г., и по-специално точка 2 към „Прозрачност“.

[33] Приложение I, точки 3 и 4: РГ по член 29 се позовава също така първата препоръка на Комисията в Съобщение COM(2013)847, както и на писмото на РГ по член 29 до заместник-председател Рединг, 10 април 2014 г., и по-специално точка 3 към „Прозрачност“.

[34] Приложение I, точки 5 и 6 и приложение II, раздел III, точка 6.

съгласно Щита за личните данни, докато други организации ще запазят данните, които са получили съгласно Щита, важно е да се осигури по-голяма прозрачност по тези въпроси за физическите лица. Следователно регистърът на дружествата, поддържан от Министерството на търговията на САЩ, следва да посочва дали организацията все още съхранява лични данни, получени съгласно Щита за личните данни, или е върнала, или заличила тези данни. Ако организацията все още съхранява тези данни, регистърът следва изрично да указва, че организацията трябва да продължи да прилага Принципите по отношение на тези данни.

Освен това, в регистъра поддържан от Министерството на търговията на САЩ, следва да се посочва, че тези организации вече не се ползват от предимствата на Щита за личните данни за ново предаване, което означава, че организацията вече няма право да получава лични данни от ЕС съгласно Принципите.

Процедури за проверка

За да удостоверят, че самосертифицирането е ефективно на практика, организациите могат да извършват самооценка или външни прегледи на спазването. РГ по член 29 изразява съжаление, че обучение на служителите се изисква само когато организацията избере проверка чрез самооценки (приложение II, раздел III, точка 7, буква в). Също така изглежда, че необходимостта от проверка на това дали политиките са точни, пълни, поставени на видно място, прилагани изцяло и достъпни, се изисква само ако организацията избере варианта за вътрешен преглед (самооценки), и прегледът чрез външен механизъм е ограничен само до спазването на политиката на организацията за неприкосновеност на личния живот.

A posteriori

РГ по член 29 приветства факта, че ФТК и Министерството на търговията на САЩ притежават разследващи правомощия в случаи на подаване на жалби. Освен това РГ по член 29 отбелязва, че Министерството на търговията ще има възможност да извършва служебни проверки, по-специално чрез изпращане на въпросници. РГ по член 29 обаче би искала да се увери, че този подход е достатъчен, за да се изпълнят изискванията на Съда на ЕС за ефективни механизми за откриване и надзор на нарушения. В действителност РГ по член 29 все още има въпроси относно точните правомощия на правоприлагащите органи на САЩ за извършване на проверки на място на помещения на самосертифицирани организации за разследване на нарушения на Щита за личните данни относно това, как на територията на САЩ може да се получи *екзекватура* на решение на орган от ЕС и дали санкциите съгласно Щита за личните данни са възпиращи на практика.

2.2.7 Обработване на данни за човешките ресурси

Обхват

Допълнителен принцип 9 (приложение II, раздел III, точка 9) се прилага за лична информация относно служител (бивш и настоящ), събирана в рамките на трудовите правоотношения. Според формулировката на допълнителен принцип 9, буква а), подточка ii) Принципите на Щита за личните данни се прилагат само в случай на „предаване или осигуряване на достъп до конкретна информация“. Терминът „конкретна информация“ не е в съответствие с определението за „лични данни“ съгласно приложение II, раздел I, точка 8, буква а), което включва данни относно идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано, и следователно не е в съответствие с определението, използвано в Директивата[35].

Допълнителен принцип 9, буква а), подточка ii) гласи, че „статистическата информация, основаваща се на общи данни за заетостта, без да съдържа лични данни, или използването на анонимизирани данни, не поражда загриженост за неприкосновеността на личния живот“. Това изявление противоречи на редица становища, изготвени от РГ по член 29. РГ по член 29 би искала да подчертае, че общите данни все още могат да бъде повторно идентифицирани, и следователно следва да се разглеждат като лични данни[36].

Уведомяване, избор и ограничаване в рамките на целта

В допълнителен принцип 9, буква б), подточка i) се предоставя пример за прилагането на принципите на уведомяването и на избора, когато данните за човешките ресурси се използват с различна цел. Примерът е свързан с организация в САЩ, която „възнамерява да използва личната информация, събрана в рамките на трудови правоотношения, за цели, които не са свързани с трудовите правоотношения — например маркетингови съобщения“. В този случай промяната на целта е одобрена, при условие че се зачита принципът на уведомяването и на избора. Според РГ по член 29 по-нататъшното обработване на данните за човешки ресурси за целите на директния маркетинг в повечето случаи ще трябва да се разглежда като несъвместима цел, и следователно ще противоречи на принципа за ограничаване в рамките на целта (приложение II, раздел II, точка 5, буква а). Освен това РГ по член 29 счита, че изборът не може да бъде за служителя подходящо основание да се съгласи (клауза за неучастие) с промяна на целта в контекста на заетостта, когато такова съгласие може да не е напълно свободно.

РГ по член 29 има сериозни съмнения, че основният акцент на Щита за личните данни по отношение на принципа на избора като условие за по-нататъшно използване на данни за друга цел отговаря на Насоките на Организацията за икономическо сътрудничество и развитие (ОИСР) за неприкосновеността на личния живот, поради липсата на достатъчно гаранции за предотвратяване на използването на този механизъм

[35] Както вече бе подчертано, ограничаването до информация, която се предава или до която се осигурява достъп, също не е в съответствие с термина "обработване" (приложение II, раздел I, точка 8, буква б).
[36] Вж. становище 4/2007 относно понятието лични данни, както и становище 05/2014 относно техниките за анонимизиране.

за неучастие за последващо обработване за несъвместимо обработване. С допълнителен принцип 9, буква б), подточка iv) се предоставя широко и изрично изключение от принципите на уведомяването и на избора „в рамките на необходимото и за срока, необходим, за да се избегне накърняването на законните права на организацията да извършва повишаване в длъжност, назначения или вземането на други подобни решения в областта на трудовите правоотношения“. На първо място използването на данни за човешките ресурси за такива цели следва да бъде изрично заявено при събирането на данните. Освен това формулировката „други подобни решения в областта на трудовите правоотношения“ е твърде неопределена и всеобхватна. Вследствие на това данните за човешките ресурси ще бъдат напълно изключени от принципа на уведомяването и на избора, когато се обработват в рамките на трудови правоотношения. Ако терминът е толкова всеобхватен, той не позволява да се направи оценка на това, дали бъдещата му употреба е съвместима с първоначалната цел. РГ по член 29 препоръчва заличаването на това изключение.

Право на достъп

В допълнителен принцип 9, буква д), подточка i) се предвижда също така изключение от прилагането на принципа за достъп или от сключването на договор с трета страна администратор на данни за човешки ресурси, когато това е свързано със случайна, свързана с трудовите правоотношения операция, като резервиране на полет, хотелска стая или застрахователно покритие, предавания на лични данни за малък брой служители и при условие че са спазени принципите на уведомяването и на избора. РГ по член 29 не вижда разумна обосновка за такова изключение и препоръчва този параграф да се заличи.

2.2.8 Фармацевтични и медицински продукти

Обхват

Съгласно Щита за личните данни предаванията на данни, кодирани с ключ, от Европейския съюз на Съединените щати в контекста на фармацевтичните и медицинските продукти, не представляват предавания, които ще бъдат предмет на Щита за личните данни (приложение II, раздел III, точка 14, буква ж), подточка i). Предаването на данни, кодирани с ключ, обаче е защитено съгласно европейското право за защита на данните. Това на практика означава, че Щитът за личните данни не може да обхваща такива видове предаване. РГ по член 29 призовава Комисията на ЕС да се предвиди изрично, че проектът на решение за адекватността няма да обхваща предаването на кодирани с ключ данни за фармацевтични или медицински цели и вследствие на това такива предавания трябва да се обхващат от други гаранции като стандартни договорни клаузи (наричани по-долу „СДК“) или ЗФП. РГ по член 29 предлага в окончателното решение за адекватността това да бъде изяснено.

Предавания на данни за регулаторни и надзорни цели (приложение II, раздел III, точка 14, буква г)

РГ по член 29 е загрижена, че съгласно тези разпоредби, лични данни, които поради медицинското си естество са предимно чувствителни, могат да бъдат предадени на регулаторните органи в САЩ. Тъй като Щитът за личните данни е предназначен за предаване на данни между частни субекти, се оказва, че публичен орган, като регулаторни органи в САЩ няма право на самосертифициране съгласно Щита за личните данни, което повдига въпроса за адекватната защита на данните за такива предавания. Ако подобни предавания трябва да се администрират за регулаторни цели, трябва да се вземат подходящи мерки, за да се гарантира продължителна защита на основните права на субектите на данни от ЕС. РГ по член 29 подчертава факта, че проектът на решение за адекватността не предоставя каквито и да било констатации по този въпрос. Поради това РГ по член 29 няма никакви гаранции, че в рамките на този контекст чувствителните данни за субекти на данни от ЕС ще имат адекватна защита.

Освен това РГ по член 29 отбелязва, че не разбира защо целта за „маркетинг“ е включена като пример за обработване за бъдещи научни изследвания. Също така не е ясна и причината за въвеждане на последващи предавания на обекти на дружеството на друго място и други изследователи (приложение II, раздел III, точка 14, буква г) под заглавието „Предавания на данни за регулаторни и надзорни цели“. Тези въпроси изискват изясняване в окончателното решение за адекватността.

Контрол на безопасността и ефикасността на продуктите (включително докладване на правителствени агенции) и проследяване на пациенти, използващи определени лекарствени продукти или медицински изделия

В Щита за личните данни се предвижда изключение от принципите на уведомяването, избора, последващото предаване и достъпа до степен, при която придържането към Принципа е в противоречие със спазването на нормативните изисквания. Проектът на решение за адекватността не предвижда никакви констатации по отношение на ситуацията, в която принципите на Щита за личните данни са в противоречие със спазването на нормативните изисквания. Дори РГ по член 29 да разбира, че разследвания на правителствата могат да обосноват ограничения на уведомяването и правото на достъп, за да се защитят разследванията, групата не вижда причините, с които може да се обоснове такова голямо изключение, при което обработването се извършва от организацията или от трета страна в частния сектор. Така например, тъй като лечението на пациентите е все по-индивидуално, такова широко изключение от принципите на неприкосновеност на личния живот в случай на проследяване на пациенти, използващи определени лекарствени средства или медицински изделия, е неприемливо, тъй като този вид грижа ще стане обичаен. Това също е приложимо и когато фармацевтичните компании използват данни за контрол на безопасността и ефикасността на продуктите (изпитване или продажба на нови лекарства).

2.2.9 Информация, достъпна за широката общественост

Изключението от правото на достъп в случай на достъпна за широката общественост информация и информация за публичните регистри (приложение II, раздел III, точка 15,

букви г) и д) поражда опасения, доколко физическо лице е заинтересовано да разбере, когато упражнява правото си на достъп, дали конкретен администратор обработва данни за него и какви данни се обработват, за да може да упражнява контрол върху обработването на своите данни. РГ по член 29 многократно е завявала, че съгласно правото на ЕС, субектите на данни винаги имат право на достъп до своите данни и когато е необходимо, право да поискат коригиране или заличаване на данните, ако те не са били обработени законосъобразно или ако са непълни или неточни, независимо от това дали личните данни са били публикувани или не[37]. Ако искане на физическо лице за достъп е отхвърлено въз основа на това, че данните са придобити от публично достъпни източници или публични регистри, лицето ще загуби правото си да упражнява контрол върху точността на данните и върху това, дали данните са оповестени законно публично още в самото начало.

Щитът за личните данни обаче изключва публичните регистри и публично достъпната информация от принципите на уведомяването, на избора, на достъпа и на отчетността за последващото предаване (приложение II, раздел II, точка 15, буква б). Тези изключения изглеждат доста обширни в сравнение с директивата и пораждат опасения, тъй като, наред с другото, те влошават възможностите на лицата да контролират точността на своите данни и да ограничават тяхното разпространение.

2.3 Заключения

РГ по член 29 признава, че органите на САЩ и Европейската комисия са въвели значителни подобрения по отношение на търговските аспекти за предаване на данни между двата континента. Като взема под внимание посочения по-горе анализ, РГ по член 29 обаче счита, че търговската част от Щита за личните данни се нуждае от допълнително разяснение по много точки. Така например липсата на изричен принцип за запазване на данните е причина за безпокойство. Поради това РГ по член 29 има сериозни опасения, дали Щитът за личните данни може да гарантира степен за защита, която да е равностойна по същество на тази в ЕС.

В решението за адекватността трябва допълнително да се изяснят принципите за ограничаване в рамките на целта и на избора. Все още е налице и рискът от появата на пропуски по отношение на няколко принципа, свързани главно с последващите предавания, механизма за разглеждане на жалби и обработването на данни за човешките ресурси или на фармацевтични данни. Освен това начинът, по който трябва да се прилагат принципите на Щита за личните данни по отношение на обработващите данни (представители), изисква допълнително разработване и специално внимание, за да се гарантира ясно и недвусмислено прилагане на терминологията.

[37] Вж. WP20, точка 4.

3. Оценка на гаранциите за националната сигурност съгласно проекта на решение за адекватността

3.1 Гаранции и ограничения, които се прилагат за органите за национална сигурност на САЩ

Намесите в основните права на личен живот и защита на данните могат да бъдат допустими, при условие че такива намеси са обосновани в едно демократичното общество. Това означава, че принципите на неприкосновеност на личния живот не са абсолютни и че са възможни дерогации, но само ако са спазени приложимите (съществени) гаранции. Съгласно целта за по-голяма защита на личния живот, освен това организациите следва да се стремят да прилагат Принципите изцяло и прозрачно, включително като посочват в своите политики в областта на неприкосновеността на личния живот и къде ще се прилагат редовно изключения от принципите, предвидени в законодателната уредба на Съединените щати. По същата причина, когато Принципите и/или законодателството на САЩ позволяват на организациите да направят избор, от тях се изисква да изберат, когато е възможно, по-висока степен на защита.

Точка 5 от приложение II, раздел I, гласи, че „придържането към тези Принципи може да бъде ограничено: а) до необходимата степен, с оглед спазване изискванията за националната сигурност, обществения интерес или изискванията на правоприлагането; б) със закон, правителствено регулиране или съдебна практика, които пораждат взаимнопротиворечиви задължения или предвиждат изрични разрешителни, при положение че дадена организация, която е поискала подобно разрешително, може да докаже, че неспазването на принципите е ограничено до необходимата степен за гарантиране на първостепенните законово предвидени интереси, за които е поискано разрешителното; или в) ако действието на Директивата или на законодателството на държавата членка предвижда изключения или дерогации, при условие че тези изключения или дерогации се прилагат в сравними контексти.“

Въпросът е дали посочените в приложение II дерогации са обосновани в едно демократично общество. Съгласно проекта на решение за адекватността на Щита за личните данни Комисията счита, че „в Съединените американски щати има установени правила, предназначени да ограничат всяка намеса за целите на националната сигурност в основните права на физическите лица, чиито лични данни се предават от Съюза към Съединените американски щати съгласно Щита за личните данни в отношенията между ЕС и САЩ, като тази намеса се ограничава до строго необходимото за постигането на посочената легитимна цел“[38].

Като използва рамката, определена в раздел 1.2 от настоящото становище, и като взе под внимание писмените изявления на органите на САЩ и констатациите на Комисията, РГ по член 29 изготви оценка на настоящата правна уредба на САЩ и

[38] Проект на решение на Комисията съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета относно адекватността на защитата, осигурявана от Щита за личните данни в отношенията между ЕС и САЩ, параграф 88.

практиките на разузнавателните агенции на САЩ, както и условията, съгласно които те допускат всякаква намеса в основните права за защита на личния живот и защита на данните, защитени съгласно европейската правна уредба. Тази оценка се основава на анализа на Президентска изпълнителна директива 28 (ПИД-28), Изпълнителен декрет 12333 (ИД 12333) и на различните правни основания, установени от Закона на САЩ за надзор върху външното разузнаване (FISA — раздел 104, раздел 402, раздел 215, раздел 501 и раздел 702). РГ по член 29 разчита на приложение VI от Щита за личните данни, което включва изготвено от Службата на директора на Националното разузнаване (ODNI) писмо относно гаранциите и ограниченията, които се прилагат за органите на националната сигурност на САЩ, и обобщава предоставената от Европейската комисия информация относно дейностите на САЩ по събирането на радиоелектронна разузнавателна информация.

3.2 Гаранция А — Обработването следва да е законосъобразно и да се основава на ясни, точни и приемливи правила

Съгласно европейското право намесата трябва да е в съответствие със законите, въведените политики и процедури, както и да бъде достатъчно ясна и достъпна (в рамките на свободата на преценка, предоставена на отделни държави), за да даде на гражданите в достатъчна степен представа при какви обстоятелства и условия оправомощава публичните органи да прибягват до мерки за наблюдение[39].

РГ по член 29 отбелязва, че дейностите за радиоелектронно разузнаване се извършват въз основа на достъпна правна уредба. Всички закони, посочени в приложение VI (ПИД-28, FISA, Закона за свободата в САЩ, Закона за свобода на информацията (FOIA), са достъпни за широката общественост онлайн (в рамките на САЩ и извън тях). В приложение VI се представя резюме на приложимата правна уредба, ограниченията за събиране, за запазване и разпространение, спазване и надзор, прозрачност и правна защита. Правната система на САЩ за разузнавателните дейности съдържа редица различни документи, включително доклади на отделните агенции, политики и процедури, които трябва да бъдат анализирани, за да се придобие по-добра представа как тези дейности се извършват на теория и на практика. Във връзка с това РГ по член 29 е насочила вниманието си върху ограничен брой точки, които счита са особено важни.

[39] Европейски съд по правата на човека, делото Zakharov, точка 247 „Съдът вече е постановил, че изискването за „предвидимост“ на закона не стига чак дотам, да принуждава държавите да предвидят правни разпоредби, в които подробно е описано всяко поведение, което може да е съпроводено с решение за подлагане на физическо лице на тайно наблюдение на основание националната сигурност“. Поради характера на нещата, заплахите за националната сигурност могат да имат различен характер и могат да бъдат неочаквани или трудни за предварително откриване (вж. делото Kennedy, посочено по-горе, точка 159). В същото време Съдът подчертава, че по въпроси, засягащи основните права, би било в противоречие с върховенството на закона, един от основните принципи на демократичното общество, залегнал в Конвенцията, за правото на преценка, предоставено на изпълнителната власт в сферата на националната сигурност, да е изричен по отношение на неограничена власт. Следователно в закона трябва да се посочва достатъчно ясно обхватът на такова право на преценка, поверено на компетентните органи, както и начинът на упражняването му, като се има предвид легитимната цел на въпросната мярка, за предоставяне на адекватна защита за физическото лице срещу произволна намеса“.

3.2.1 Изпълнителен декрет 12333 и Президентска изпълнителна директива 28

Обхватът на Изпълнителен декрет 12333 е широк. По принцип всяко събиране на данни от външното разузнаване може да се извърши по преценка на Президента на САЩ въз основа на този указ. Твърди се обаче, че след въвеждането на FISA, ИД 12333 може да се използва само за събирането на данни извън територията на САЩ. РГ по член 29 отбелязва, че ИД 12333 не предоставя много данни относно географския си обхват, степента, в която данните могат да бъдат събирани, запазвани или допълнително разпространявани, нито относно характера на нарушенията, които могат да доведат до наблюдение, или вида информация, която може да бъде събирана или използвана.

Според РГ по член 29 основната цел на Президентска изпълнителна директива 28 (ПИД-28) е да се определят границите за събиране и обработване на лични данни, независимо от използваната програма за наблюдение и начина на получаване на данните.

ПИД-28 е директива на президента на Съединените американски щати, в която са заложени принципите на съответствие, съгласно които ще бъде разрешено и ще се извършва събирането на радиоелектронна разузнавателна информация, но ПИД-28 не е правно основание за събиране. ПИД-28 е ефективна, като налага тези принципи на органите на разузнавателните структури, които трябва да ги прилагат в своите политики и процедури. Директивата се прилага за дейности за радиоелектронно разузнаване, независимо от местонахождението на данните към момента на събиране, в рамките на САЩ или извън тях. Тя също така се прилага и по отношение на данни, събрани за целите на радиоелектронното разузнаване, когато те се предават от ЕС на САЩ.

По-специално ПИД-28 гласи, че радиоелектронните разузнавателни дейности са съобразени с конкретния случай, доколкото това е практически възможно[40]. По отношение на използването на данните, в нея се определят процедури за свеждане до минимум на данните (включително условия за запазване и разпространение на данни), за сигурността на данните и достъпа на съответните служители [т.е. правила, включващи гаранции за ограничаване на рисковете от злоупотреба и неправилно използване], качеството на данните и надзора. Тези гаранции се прилагат независимо от националността на субектите на данните, т.е. по отношение на лица, които са граждани на САЩ, и лица, които не са американски граждани.

По време на предаването на данни на САЩ се прилагат и гаранциите, установени в ПИД-28. В приложение VI се съдържа ангажимент по отношение на ODNI, съгласно който, ако разузнавателните структури на САЩ съберат данни при предаването им към Съединените щати по трансатлантически кабелни връзки, „това би ставало под

[40] „Радиоелектронните разузнавателни дейности са съобразени с конкретния случай, доколкото това е практически възможно. Когато определят дали да събират радиоелектронна разузнавателна информация, разузнавателните структури трябва да вземат предвид наличието на друга информация, включително от дипломатически или публични източници. На такива уместни и практически възможни алтернативни варианти на дейностите на радиоелектронното разузнаване следва да се отдава предпочитание.“ (раздел 1, буква г).

условията на ограниченията и гаранциите, разгледани в настоящия документ, включително в съответствие с изискванията на ПИД-28.“[41] РГ по член 29 отбелязва, че все още няма установена съдебна практика, определяща законосъобразността на прихващането на кабелни връзки, ако трябва да се извършва от всяка държава. В този случай САЩ нито потвърждават, нито отричат, че използват прихващане на кабелни връзки като средство за събиране на разузнавателни данни.

Понятието „радиоелектронно разузнаване“ не е определено в ПИД-28, нито в някой друг от приложимите текстове.

3.2.2 Закон за надзор върху външното разузнаване (Foreign Intelligence Surveillance Act — FISA)

Като цяло текстът на FISA очевидно е по-ясен и по-точен. Тълкуването на много разпоредби с оглед на ПИД-28 обаче, както и тяхното практическо приложение, зависят до голяма степен от прилагането ѝ от различните агенции. Въпреки че все още не е изготвен пълен доклад относно прилагането на новите гаранции, делегатите от САЩ са информирали представителите на РГ по член 29, че прилагането на гаранциите на ПИД-28 действително е приключило и се извършва по подобен начин във всички разузнавателни структури на САЩ.

По-точно, раздел 501 е относително ясен относно вида на разузнавателните операции, за които може да се получи разрешение: „производството на всякакви материални вещи (включително книги, записи, хартиени носители, документи и други вещи)“. Следва да се отбележи обаче, че фактът, че определението за „всякакви материални вещи“ включва „други вещи“, прави обхвата на този орган доста широк.

В раздел 702, в който се позволява данни да бъдат събирани от лица, които не са граждани на САЩ, за които има разумни основания да се счита, че се намират извън територията на Съединените щати, с цел събиране на външноразузнавателна информация[42] не се предоставя същото ниво на детайлност, както в раздел 501. По отношение на обхвата си, раздел 702 е насочен към доставчици на електронни съобщителни услуги, установени в САЩ за събиране на външноразузнавателна информация за физически лица, живеещи извън територията на САЩ. Понятието „външноразузнавателна информация“ е доста обширно. То включва, наред с другото, „информация по отношение на чужда сила или чужда територия, която е свързана с провеждането на политиката на външните работи на Съединените американски щати“[43], което поражда определена несигурност относно вида на информацията, която може да бъде събирана на практика.

[41] Приложение VI към Щита за личните данни, писмо на Службата на директора на Националното разузнаване (ODNI) относно гаранциите и ограниченията, които се прилагат за органите за национална сигурност на САЩ, точка 2.
[42] Дял 50 от Сборника на федералните закони на САЩ, параграф 1881a, буква Г), точка 1).
[43] Дял 50 от Сборника на федералните закони на САЩ, параграф 1881, буква д), точка 2).

Въпреки разсекретяването на документи, доклади до Конгреса и доклади за надзора на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи (наричан по-долу „PCLOB“), прилагането на FISA, включително обхватът и използването на конкретни критерии за избор, остава неясно и объркващо. Използването на конкретни критерии за избор („критерии за подбор“) се посочва в доклада на PCLOB[44], но според РГ по член 29 това не отговаря на правилата за целево събиране съгласно раздел 702[45]. Те не са упоменати в общодостъпните правила, доколкото РГ по член 29 е в състояние да потвърди това.

3.2.3 Заключение

Като цяло, РГ по член 29 отбелязва, че приложимите текстове, свързани с разузнавателните дейности, са достъпни онлайн и че органите на САЩ са предприели редица важни стъпки към прозрачност.

РГ по член 29 признава, че от 2013 г. насам са публикувани редица документи като политики, процедури, решения на FISC и други разсекретени документи. Освен това PCLOB е изготвил важни доклади относно дейностите, извършвани въз основа на раздел 702 и Закона за свободата в САЩ. Подобен доклад се очаква и относно дейностите съгласно ИД 12333.

Няколко законодателни приложения, които могат да хвърлят светлина върху последиците от изпълнителния указ относно физически лица извън Съединените щати и всички приложими гаранции, са класифицирани и като такива не са достъпни за обществеността или за физическите лица, които вероятно са засегнати от тяхното прилагане. Когато се разсекретяват текстове, те само предоставят ограничена стойност и информация относно разузнавателните дейности.

Въпреки положените усилия да се обясни функционирането на ИД 12333 след разкритията на Сноудън, по-специално чрез приемането на ПИД-28, настоящото практическо приложение на ИД 12333 продължава да бъде неясно. РГ по член 29 отбелязва, че приложение VI от Щита за личните данни не предоставя подробна информация относно функционирането на ИД 12333.

Въпреки че РГ по член 29 приветства ограниченията, обхванати от ПИД-28, трудно е да се прецени дали правната уредба на САЩ, посветена на наблюдението, е достатъчно предвидима, т.е. съдържа „ясни указания при какви обстоятелства и условия публичните органи са оправомощени да прибягват до такива мерки“, като се очаква допълнително разясняване, включително публикуването в рамките на ИД 12333 на доклад на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи.

[44] Доклад на PCLOB относно програмата за наблюдение действаща съгласно раздел 702 от FISA, точка 32.
[45] Дял 50 от Сборника на федералните закони на САЩ, параграф 1881а, буква Г).

3.3 Гаранция Б — Трябва да бъдат доказани необходимостта и пропорционалността спрямо преследваните легитимни цели

3.3.1 Президентска изпълнителна директива 28

С ПИД-28 се въвеждат ограничения относно целите, за които могат да се използват лични данни, и относно условията, съгласно които те могат да бъдат разпространявани и да въздействат върху събирането на радиоелектронна разузнавателна информация, независимо от използваното правно основание.

По-специално раздел 1 от ПИД-28 предвижда, че дейностите за радиоелектронно разузнаване на САЩ трябва винаги да са „съобразени с конкретния случай, доколкото това е практически възможно“. Въпреки че това ограничение се признава, е трудно да се определи дали „съобразени с конкретния случай, доколкото това е практически възможно“ означава, че всяко събиране на данни е необходимо и пропорционално.

В ПИД-28 е предвидено, че събирането на масиви от данни продължава да бъде разрешено, „за да бъдат идентифицирани нови или възникващи заплахи и друга информация, която е от критично значение за националната сигурност, които често остават скрити в голямата и сложна съобщителна система в съвременния свят“[46]. РГ по член 29 отбелязва, че ПИД-28 гласи, че „събрани „масиви“ от радиоелектронни разузнавателни данни означава разрешено събиране на големи количества радиоелектронни разузнавателни данни, което по технически или оперативни съображения се извършва, без да се използват разграничителни критерии (напр. конкретни идентификатори, критерии за избор и т.н.)“.

ПИД-28 налага ограничения върху използването на събраните масиви от радиоелектронни разузнавателни данни по отношение на целта на използване. Има шест цели, за които могат да бъдат събирани данни в „масиви“, включително борба срещу тероризма и други форми на сериозни (транснационални) престъпления. Анализът на РГ по член 29 предполага, че ограничаването в рамките на целта е по-скоро широко формулирано (и вероятно твърде широко), за да се разглежда като целево.

ПИД-28 не премахва възможността за безразборно събиране на лични данни в масиви, както и това, че мащабът на такива възможности за събиране продължава да бъде неясен и потенциално широк. Във връзка с това РГ по член 29 отбелязва, че в приложение VI ODNI потвърждава, че „всички дейности по събиране на масиви от данни по отношение на съобщения в интернет, които разузнавателните структури на САЩ извършват при радиоелектронното разузнаване, се осъществяват в малка част от

[46] ПИУ-28, раздел 2 и приложение VI към Щита за личните данни, писмо на Службата на директора на Националното разузнаване (ODNI) относно гаранциите и ограниченията, които се прилагат за органите за национална сигурност на САЩ, точка 3.

интернет“[47], и следователно ще оцени допълнителни доказателства, предоставени чрез мерки за прозрачност.

3.3.2 Закон за надзор върху външното разузнаване

Процедурите за свеждане до минимум в раздел 215 и раздел 702 от FISA са въведени, с цел да се защитят гражданите на САЩ от широкообхватния достъп на правителството до техните данни. Тези ограничения не се прилагат официално за чужденци, въпреки че властите на САЩ са заявили многократно на публични и частни срещи с представителите на РГ по член 29, че обхватът на прилагане на процедурите за свеждане до минимум на практика е увеличен, за да обхване всички лица, независимо от тяхната националност или обичайно пребиваване.

В раздел 702 се определя, че разрешеното придобиване „ще се осъществява по начин, съвместим с четвъртата поправка на Конституцията на Съединените щати, ограничаваща събирането на данни до това, което се счита за съвместимо с принципа на разумно търсене“. В тази връзка не се прави разлика между дружества от САЩ и дружества, които не са от САЩ“. С други думи, съгласно условието, че четвъртата поправка се отнася до всички видове събрани данни в САЩ, събиране в „масиви“, което се извършва на територията на САЩ, би било „необосновано“ и следователно противоконституционно.

РГ по член 29 приветства констатациите в доклада на PCLOB, че „на практика лицата, които не са американски граждани, също се възползват от достъпа и ограниченията за запазване, изисквани от процедурите за свеждане до минимум и/или за целево събиране на различните агенции, поради разходите и затрудненията за установяване и премахване на лична информация на граждани на САЩ, тъй като по-голям обем данни означава, че обикновено целият набор от данни се обработва в съответствие с по-високите стандарти за данните на САЩ“.

РГ по член 29 отбелязва също така, че съгласно констатациите на PCLOB „програмата не функционира чрез събиране на съобщения в масиви от данни“. Докладът за прозрачността на статистическата информация от 2014 г., издаден от ODNI, потвърждава тази констатация. Освен това, съгласно доклада на PCLOB, за насочване на наблюдението се използват „критерии за подбор“ като адрес на електронната поща или телефонен номер[48].

Съответните налични публични правила, свързани с целевото събиране, не предоставят обаче такива целенасочени правила, а целят единствено избягването на целево събиране за граждани на САЩ или за лица, пребиваващи в САЩ. Освен това ползите,

[47] Писмо на Службата на директора на Националното разузнаване (ODNI) относно гаранциите и ограниченията, които се прилагат за органите за национална сигурност на САЩ , точка 4. РГ по член 29 припомня в тази връзка доклада относно констатациите, направени от съпредседателите от ЕС на Работна група *ad hoc* ЕС — САЩ по защита на данните, който гласи, че „Съобщителните данни съставляват една много малка част от световния интернет трафик“, предвид факта, че „по-голямата част от световния интернет трафик се състои от стрийминг с голям обем и изтегляния, като телевизионни сериали, филми и спорт (параграф 3.1.2 от доклада)“.
[48] Доклад на PCLOB относно програмата за наблюдение, действаща съгласно раздел 702 от FISA, точка 32.

които според PCLOB се прилагат по отношение на лица, които не са граждани на САЩ, на практика не са правно обвързващи или създадени със закон, тъй като съществуващото законодателство, свързано с целевото събиране, не предвижда такива правила за определяне на обектите на разследване, а цели единствено избягването на целево събиране на данни за граждани на САЩ или за лица, пребиваващи в САЩ.

Освен това РГ по член 29 припомня, че за целите на раздел 702,лица са не само физически лица, но и групи, субекти, асоциации, дружества или чужди сили. Освен това фактът, че събирането се обосновава от „значима цел на придобиването е получаването на външноразузнавателна информация“ оставя известна несигурност по отношение на неговите цели и необходимост. РГ по член 29 приветства обаче информацията, предоставена в приложение VI, че общият брой на физическите лица, които са били обект на целево разследване съгласно раздел 702 през 2014 г., е приблизително 90 000[49]. Първият преглед на Щита за личните данни ще предостави възможност за демонстриране на допълнителни доказателства за правилата за определяне на обектите на разследване.

До момента липсва убедителна съдебна практика относно законността на масовото и безразборно събиране на данни и последващото използване на личните данни за целите на борбата с престъпността, включително относно въпроса при какви обстоятелства може да се извърши такова събиране и използване на лични данни. Очаква се през 2016 г. Съдът на ЕС да разреши този въпрос поне до известна степен в съединени дела Tele2 Sverige AB/Post- och telestyrelsen и Държавен секретар по вътрешните работи/Davis и други[50], както и да даде съвети относно валидността на канадското споразумение за PNR[51]. Междувременно РГ по член 29 припомня, че последователно е считала, че масовото и безразборно събиране на данни в никакъв случай не може да се приеме за пропорционално[52].

3.3.3 Заключение

Въпреки приетите ограничения след въвеждането на ПИД-28, опасенията на РГ по член 29, по-специално по отношение на пропорционалността на събирането на данни, продължават да са налице. На първо място, има признаци, че САЩ продължават да събират масово и безразборно данни или поне не изключват, че е възможно да го правят и в бъдеще. РГ по член 29 продължава да твърди, че такова събиране на данни не е в съответствие с правото на ЕС, и следователно е неприемливо.

На второ място, РГ по член 29 отбелязва, че целевото обработване на данни или обработване, което е „съобразено с конкретния случай, доколкото това е практически възможно“, също може да се счита за масово. Независимо от това, дали такова масово събиране на данни следва да бъде одобрено или не, понастоящем е предмет на

[49] Приложение VII, точка 11.
[50] Съд на ЕС, съединени дела C-203/15 и C-698/15.
[51] Съд на ЕС, дело A-1/15.
[52] WP215 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

производство пред Съда на ЕС. Поради тази причини РГ по член 29 няма да изготви окончателна оценка по отношение на законността на целенасочената, но масова обработка на данни. Тя обаче подчертава, че ако целенасочената, но масова обработка на данни бъде позволена, Принципите за определяне на обектите на разследване следва да се прилагат както към събирането, така и към последващото използване на данните, и не могат да се ограничат само до употребата. Във всеки случай е необходимо разяснение на проекта на решение за адекватността във връзка с шестте цели, посочени в ПИД-28, за които данните могат да се събират „като масиви“. На този етап РГ по член 29 не е убедена, че тези цели са достатъчно ограничаващи, за да се гарантира, че събирането на данни е наистина ограничено до това, което е необходимо и пропорционално.

3.4 Гаранция B — Трябва да съществува независим механизъм за надзор

САЩ не разполагат само с един-единствен надзорен орган на федерално равнище, натоварен със задачата да упражнява надзор върху последиците от програмите за разузнаване и наблюдение за неприкосновеността на личния живот и защитата на личните данни. По-скоро разузнавателните дейности на САЩ са предмет на многостепенен процес на надзор: може да се направи разграничение между вътрешен и външен надзор. РГ по член 29 признава, че практиката за докладване на надзорните органи на САЩ е много подробна и предимно публична.

3.4.1 Вътрешен надзор

Всички разузнавателни агенции и агенции по сигурността разполагат със служители, които са отговорни за гарантиране спазването на техните законодателни рамки, включително главни инспектори, чиято главна задача е да оценяват общото спазване на законодателството при работата на агенциите, включително, но не ограничено до законите, свързани с неприкосновеността на личния живот и защитата на данните. Главните инспектори се определят със закон и всички се назначават (или скоро ще бъдат назначавани) от Президента след одобрението на Сената, в опит да се гарантира, че ще бъдат организационно независими и ще докладват на Конгреса. РГ по член 29 счита, че поради това главните инспектори вероятно ще отговарят на критериите за организационна независимост, определени от Съда на ЕС и от Европейския съд по правата на човека (ЕСПЧ), поне от момента на прилагане на новия процес за номиниране по отношение на всички тях. Понастоящем продължават да са налице определени опасения по отношение на главните инспектори, които все още се назначават от Директора на агенцията, върху която упражняват надзор.

Главните инспектори могат да отправят препоръки, които впоследствие да бъдат препратени на Министерството на правосъдието и на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи (PCLOB) или дори на комисии на Конгреса, които могат да наложат спазването на препоръките. Ако главният инспектор открие нарушение, то може да се разгледа чрез вътрешни мерки и

мерки на политиката и да се докладва на Конгреса. Главният инспектор има правомощието да извършва както одити, така и проверки.

РГ по член 29 отбелязва, че докладите на главния инспектор могат да не бъдат предоставени на обществеността, като на него може също така да му бъде попречено да докладва, ако проверяваната информация е класифицирана. Докладите обаче ще подлежат винаги на надзор от страна на надзорните комисии в Конгреса, което представлява съществена гаранция дори когато не предоставя основания за индивидуална правна защита.

Всички агенции разполагат със служители по въпросите на неприкосновеността на личния живот и гражданските свободи, които съдействат чрез система за задължително самостоятелно докладване, с надзор от страна на Конгреса.

Като цяло, въведените механизми за вътрешен надзор могат да се считат много стабилни; за да се оправдае обаче намесата в основното право на неприкосновеността на личния живот и защита на данните, е необходимо надзорът да бъде напълно независим. Въпреки че РГ по член 29 уважава и зачита работата на различните служители по въпросите на неприкосновеността на личния живот и гражданските свободи, тя не може да заключи, че те отговарят на изискваното ниво на независимост, за да действат като независим надзор.

3.4.2 Външен надзор

Външният надзор включва редица различни механизми: съдебен надзор съгласно раздели 501 и 702, гарантиран от Съда за наблюдение на външното разузнаване (наричан по-долу „FISC“), надзор от страна на избрани в Конгреса комисии по въпросите на разузнаването и задачите, изпълнявани от PCLOB.

РГ по член 29 припомня, че в идеалния случай, както е заявено и от Съда на ЕС, и Европейския съд по правата на човека, надзорът следва да се извършва от съдия с цел да се гарантира независимостта и безпристрастността на процедурата. До скоро процедурата пред FISC беше едностранна процедура, без възможност съответните физически лица да бъдат изслушани или дори да бъдат уведомени за делото. Към момента процедурата пред FISC продължава да е едностранна, но след приемането на Закона за свободата в САЩ, към FISC са определени *amici curiae*. *Amici curiae* действат независимо, но не са създадени да защитават конкретни физически лица, които могат да участва в делото.

Със Закона за свободата в САЩ се създава група от *amici curiae*, които да информират FISC относно важни дела. Съдът е избрал петима адвокати, които са получили подходящи разрешения за достъп до класифицирана информация и предоставят технически консултации, присъстват на изслушванията на FISC и изготвят кратки изложения, както и разглеждат даден случай по същество от гледна точка на

неприкосновеността на личния живот и гражданските права. Те обаче ще извършват тези дейности само във важни случаи или когато възникнат нови правни въпроси[53].

Раздел 215 подлежи почти напълно на предварителен (но не и последващ) съдебен надзор, тъй като всички програми, използващи раздел 215, като основа за събиране, са предмет на одобрение от страна на FISC. Докладът на PCLOB определя, че „Раздел 702 се различава от тази традиционна рамка за електронно наблюдение на FISA както по отношение на прилаганите стандарти, така и по отношение на липсата на индивидуализирани определения от FISC. Съгласно закона главният прокурор и директорът на националното разузнаване извършват годишни сертифицирания, които позволяват за обект на разследване да се определят лица, които не са граждани на САЩ и за които има разумни основания да се счита, че се намират извън територията на Съединените американски щати, с цел събиране на външноразузнавателна информация, без да посочва на FISC конкретното лице, което не е гражданин на САЩ, което ще бъде обект на събирането. […] Също така не е налице изискване, правителството да посочва правдоподобна причина, поради която счита, че целта на разследване по раздел 702 е чужда сила или представител на чужда сила, както се изисква съгласно традиционния FISA.“[54]

В рамките на Конгреса избраните комисии по въпросите на разузнаването също упражняват надзор, като одобряват разузнавателните дейности, по-специално чрез гласуване на бюджета. Комисиите по въпросите на разузнаването в Сената и Камарата получават класифицирани брифинги относно разузнавателните дейности. На всеки шест месеца главният прокурор трябва да докладва на тези комисии за електронното наблюдение по FISA. За РГ по член 29 не става ясно до каква степен те имат право да обсъждат обработката на лични данни на физически лица, особено на лица, които не са граждани на САЩ.

Надзорният орган по въпросите на неприкосновеността на личния живот и гражданските свободи (PCLOB) е независим орган от изпълнителната власт на правителството на САЩ, на който са възложени две основни правомощия: 1) да преглежда и анализира действията, които изпълнителната власт предприема, за да защити нацията [САЩ] от тероризъм, като гарантира, че необходимостта от такива действия е балансирана с необходимостта от защита на неприкосновеността на личния живот и гражданските свободи, и 2) да гарантира, че въпросните свободи са подходящо разгледани при разработването и прилагането на закони, регламенти и политики, свързани с усилията за защита на нацията от тероризъм. РГ по член 29 отбелязва, че PCLOB разполага с правомощието да издава призовки, и с достъп до класифицирана информация. При изпълнение на задачите си той също така се опитва да провери ефикасността на програмите. Упражняваният от него надзор не се осъществява преди, а след събитието. PCLOB показва независимите си правомощия, като не се съгласява с Президента на Съединените щати по правни въпроси. По-специално той счита, че

[53] Закон за свободата РАЗДЕЛ IV — РЕФОРМИ НА СЪДА ЗА НАДЗОР НАД ВЪНШНОТО РАЗУЗНАВАНЕ раздел 401. Определяне на *amici curiae*.
[54] Доклад на PCLOB относно програмата за наблюдение съгласно раздел 702 от FISA, точки 24 и 25.

програмата за телефонни метаданни от раздел 215 не е законно разрешена, и стига до заключението, че тя не е ефективна, тъй като липсват сведения за разрушителни атаки. PCLOB извършва също така едногодишно проучване на програмата по раздел 702 и установява, че тя е законна и напълно одобрена по закон, както и че раздел 702 се е доказал като много ефективен, включително по въпроси, свързани с тероризма. И накрая, той действа въз основа на изискването за прозрачност и счита, че редица класифицирани факти не трябва да бъдат класифицирани. Разбира се, че в близко бъдеще PCLOB ще докладва относно прилагането на ПИД-28. Във връзка с това той счита, че за да се задържи информация относно чужденец, не е достатъчен фактът, че лицето е чужденец.

Накрая РГ по член 29 отбелязва, че ИД 12333 не предвижда съдебен контрол, надзор или механизми за правна защита за програмите за наблюдение, изпълнявани въз основа на него.

3.4.3 Заключение

Проектът на решение за адекватността показва, че в САЩ е въведен многостранен подход от механизми за вътрешен и външен надзор. Въпреки че работата на механизмите за надзор може да е обърквaща, РГ по член 29 е удовлетворена, че като цяло са въведени достатъчно механизми за вътрешен надзор. РГ по член 29 се опасява обаче, че липсва достатъчно надзор на програмите за наблюдение, предприети въз основа на ИД 12333.

РГ по член 29 отбелязва, че по-рано проявената от нея критичност относно това, че процедурите пред FISC не са състезателни, е смекчена само до определена степен чрез въвеждането на *amici curiae*, на които е възложено да „увеличат защитата на неприкосновеността на личния живот и гражданските свободи на физическите лица“. Освен това FISC не осигурява ефективен съдебен контрол върху целевото събиране от лица, които не са граждани на САЩ. Запазват се и някои съмнения по отношение на способността на FISC да оценява ефективно процедурите за целево събиране и свеждане до минимум, както е посочено и от PCLOB[55].

3.5 Гаранция Г — Физическите лица трябва да разполагат с ефективни правни средства за защита

3.5.1 Средства за съдебна защита

3.5.1.1 Изискване за основателност

Системата на САЩ, свързана със средствата за правна защита, включва важно ограничение: Конституцията на САЩ изисква физическото лице да докаже, че има основание: „изискването, ищците да са претърпели или ще претърпят преки щети или вреди и тези вреди да подлежат на обезщетение. На федерално равнище правните

[55] Доклад на PCLOB относно програмата за наблюдение, действаща съгласно раздел 702 от FISA, точка 11.

действия не могат да бъдат предприемани само въз основа на факта, че физическо лице или група е недоволна от действие или закон на правителството“[56]. Такова изискване вероятно ще бъде анулирано, поради липсата на уведомяване на физическите лица, подложени на наблюдение, дори и след приключването на тези мерки. Съдът на ЕС и Европейския съд по правата на човека нееднократно са заявявали, че физическите лица трябва да могат да получат достъп до административна или съдебна защита. В решението си по делото Zakharov Европейският съд по правата на човека потвърди, че въз основа на съдебната практика всеки може да се обърне към съда, ако има законно основание да предполага намеса в своите основните права[57].

Освен това за чужденците, които живеят извън САЩ, не се предвижда цялостна конституционна защита в рамките на САЩ съгласно съдебната практика на Върховния съд на Съединените щати[58]. Това по-специално е така във връзка с четвъртата поправка, която защитава гражданите на САЩ, но не и лицата, които не са граждани на САЩ, срещу необосновани претърсвания и изземвания, и от която произлиза голяма част от правото на неприкосновеност на личния живот в САЩ. Европейските граждани и други лица от Европа, живеещи извън САЩ, просто са изключени от защитата, която се предоставя съгласно четвъртата поправка[59].

Ограниченото прилагане на Закона за съдебната защита (както по отношение на съдържанието, тъй като изключва националната сигурност, така и във връзка с лица, които могат да разчитат на закона), многото изключения и правната несигурност във връзка с агенциите, по отношение на които ще се прилага Законът за съдебната защита, не удовлетворяват изискването за предлагане на ефективен механизъм за правна защита за всички физически лица, засегнати в случаи на наблюдение от разузнаването във връзка с националната сигурност.

3.5.1.2 Президентска изпълнителна директива 28

РГ по член 29 отбелязва, че ПИД-28 е само директива и следователно не може да поражда права за физическите лица. Това може да става единствено чрез законодателството. Поради това физическите лица не могат да се обърнат към съда въз основа на предполагаемо нарушение на гаранциите по силата на ПИД-28.

3.5.1.3 Закон за надзор върху външното разузнаване (FISA)

Съгласно FISA са налице някои правни средства за защита за физическите лица в случай на незаконно наблюдение. Според FISA „засегнато лице, различно от чужда сила или съответно служител на чужда сила [...], което е било подложено на електронно наблюдение или за което е била разкрита, или използвана информация, получена в

[56] https://www.law.cornell.edu/wex/standing; https://www.law.cornell.edu/wex/standinghttps://www.law.cornell.edu/wex/standing; Clapper / Амнести интернашънъл САЩ
[57] Европейски съд по правата на човека, Zakharov, точка 171.
[58] Решение по дело САЩ/Verdugo - Urquidez , точки 264—266.
[59] Доклад на съпредседателите на ЕС, раздел 2.

резултат на електронно наблюдение на такова лице, в нарушение на раздел 1809 от това право, има причина предприеме действия срещу всяко лице, което е извършило такова нарушение“. Това обаче изрично изключва чуждата сила или служител на чуждата сила, която е била подложена на мярката. Въпреки това, както вече бе посочено, ищецът трябва да докаже, че има основание, което на практика няма да бъде възможно.

Със Закона за свободата в САЩ е създадена консултативна група *Amicus Curie* към Съда за надзор върху външното разузнаване, която да предоставя (факултативно) консултации в случай на значимо ново правно тълкуване. Тяхната задача обаче е да предоставят безпристрастен съвет, а не да защитават интересите на конкретно физическо лице по негово искане.

3.5.2 Административни средства за защита

3.5.2.1 Главни инспектори

Друга възможност за правна защита е чрез главния инспектор, до когото могат да се подават жалби. Главните инспектори обаче нямат никакви задължения да разглеждат всяка отделна жалба: не е налице право на изслушване, а по-скоро дискреционни правомощия. Главният инспектор може също така да изготви доклади с констатации за нарушения, когато информацията е разсекретена. В случай че физическо лице може да предположи, че докладът го засяга, то тогава вероятно ще може да заведе дело пред съда въз основа на констатацията за нарушение на закона.

3.5.2.2 Закон за свобода на информацията

Средство за защита, достъпно за всички лица, е подаването на искане за свобода на информацията, което се основава на Закона за свобода на информацията (FOIA). Съгласно правителството на САЩ, искане по FOIA може да бъде отправено изобщо от всяко лице — гражданин на САЩ или не — което просто подаде искане до всеки регистър на агенция. Това включва регистри на физическите лица, въпреки че в този случай се изисква предоставяне на документ за самоличност. Ако обаче дадена информация е класифицирана, с цел да се защити националната сигурност, е малко вероятно да бъде уважено искане по FOIA, тъй като се прилага изключение: агенциите не са длъжни да предоставят достъп до класифицирана информация, включително ако тази информация е свързана с лицето, което е подало искането. От исканията по FOIA напълно се изключва информацията от текущите разследвания в областта на правоприлагането. И накрая, според РГ по член 29, искане по FOIA не предоставя право на проверка от независим орган на законността на обработването.

3.5.3 Омбудсман към Щита за личните данни

3.5.3.1 Създаване на омбудсман

Щитът за личните данни създава нов механизъм „за физическите лица от ЕС“ за подаване на искания по отношение на „радиоелектронното разузнаване на САЩ“ до

новосъздадения омбудсман към Щита за личните данни. Както е посочено в Меморандума, приложен към писмото на Държавния секретар на САЩ Джон Кери, от 22 февруари 2016 г., позицията на омбудсман ще бъде заета от заместник-държавния секретар С. Новели. Тя ще заема тази длъжност в допълнение към функциите си на старши координатор на международната дипломация в областта на информационните технологии — длъжност, създадена съгласно раздел 4, буква г) от ПИД-28. В писмото и в Меморандума се подчертава, че „заместник-държавният секретар е пряко подчинен на Държавния секретар и е независим от разузнавателните структури“.

Въпреки наименованието му, в Меморандума се обяснява, че омбудсманът към Щита за личните данни ще разглежда искания, свързани не само с достъп от националната сигурност до предадени от ЕС към САЩ данни съгласно Щита за личните данни, но и такива, в които данните са предавани съгласно стандартни договорни клаузи, задължителни фирмени правила, дерогации (съгласно член 26 от Директива 95/46/ЕО) или „възможни бъдещи дерогации“, както е определено в бележка под линия 2 от Меморандума.

Начинът, по който би трябвало да работи механизмът, е обобщен така: Физическо лице от ЕС подава искане до компетентния орган на държава членка за надзор на националните служби за сигурност или до централизиран „орган на ЕС за разглеждане на жалби на физическите лица“, в случай че последният бъде създаден или посочен. Органът, който препраща искането до Омбудсмана, ще трябва първо да провери дали искането е пълно, съгласно член 3, буква б) от писмото[60]. След като бъде предадено на омбудсмана към Щита за личните данни и той реши, че е в съответствие с член 3, буква б), омбудсманът към Щита за личните данни ще предостави отговор, което означава, че той в крайна сметка ще потвърди, че „i) оплакването е надлежно разгледано и ii) са спазени правото на САЩ, законите, декретите, президентските укази и политиките на институциите, които предвиждат ограничения и гаранции, както е разгледано в писмото на Службата на директора на Националното разузнаване, или ако не са спазени, че това неспазване е било отстранено“[61]. Отговорът „нито потвърждава, нито отрича, че се извършва целево наблюдение на физическото лице, както и не потвърждава конкретната корективна мярка, която е приложена“[62]. Що се отнася до въпроса как се провежда разследването на омбудсмана, обяснено е, че омбудсманът

[60] б) Органът на ЕС за разглеждане на жалби на физическите лица ще осигурява искането да бъде пълно, като се съобразява със следните действия:
i) проверка за самоличността на физическото лице и дали то действа от собствено име, а не като представител на правителствена или международна организация.
ii) осигуряване искането да бъде оформено писмено и да съдържа следната основна информация:
• информацията, която съставлява основанието за искането,
• характера на исканата информация или исканото решение,
• правителствените институции на Съединените щати, за които се смята, че се отнася искането, ако има такива, и
• други мерки, които са били приложени, за да бъде получена исканата информация или исканото решение и получен резултат чрез тях.
iii) проверка дали искането се отнася за данни, за които има основания да се счита, че са предадени от ЕС на Съединените щати съгласно Щита за личните данни, стандартни договорни клаузи, задължителни фирмени правила, дерогации или възможни бъдещи дерогации
iv) първоначално определяне дали искането не е несериозно, злонамерено или недобросъвестно.
[61] Приложение III към Щита за личните данни, раздел 4, буква е).
[62] Приложение III към Щита за личните данни, раздел 4, буква е).

към Щита за личните данни „ще работи в тясно сътрудничество с други длъжностни лица от правителството на Съединените щати, включително със съответните независими надзорни органи“[63], и по-специално „ще може, според случая, да работи в тясна координация със Службата на директора на Националното разузнаване, Министерството на правосъдието и други министерства и агенции, свързани с националната сигурност на Съединените щати, както и с главните инспектори, служителите по Закона за свобода на информацията и служителите по въпросите на гражданските свободи и неприкосновеността на личния живот“[64]. Тази координация ще бъда такава, че да гарантира, че омбудсманът към Щита за личните данни може да изпраща отговор, включително потвърждения, както е посочено по-горе.

3.5.3.2 Оценка на новия Механизъм на омбудсмана

Работната група признава усилията, положени от Европейската комисия и правителството на САЩ, за въвеждане на нов механизъм в оглед на подобряването на възможностите за съдебна защита относно дейностите на САЩ по наблюдение. Тя разбира, че оценката на този механизъм, като нововъведение в международните отношения относно радиоелектронното разузнаване или националната сигурност, е от съществено значение.

В този раздел РГ по член 29 ще оцени как създаването на омбудсмана към Щита за личните данни се свързва с необходимите изисквания за физическите лица да търсят съдебна защита, както е посочено в Хартата, ЕКПЧ и съдебната практика на европейските съдилища.

3.5.3.3 Възможно ли е създаването на омбудсман да е достатъчно само по себе си?

Като за начало следва да се постави въпросът дали изобщо може да се счита, че създаването на „омбудсман“ е в съответствие с член 47 от Хартата, в която се посочва ефективно правно средство за защита пред безпристрастен съд[65], ако не е налице друга възможност за търсене на ефективна правна защита. Това е важно, тъй като в своето важно съображение 95 в рамките на делото Schrems Съдът на ЕС се позовава на член 47 от Хартата, и го прави, без да посочва, че се предполага член 47 да се разбира с модификации в контекста на мерките за наблюдение. Точно обратното, Съдът на ЕС вече приложи член 47 от Хартата по делото Kadi II[66] към мерките за наблюдение, свързани с националната и съответно с международната сигурност[67].

[63] Приложение III към Щита за личните данни, раздел 2, буква а).
[64] Приложение III към Щита за личните данни, раздел 2, буква а).
[65] В разясненията във връзка с Хартата на основните права се завява освен това, че член 47 следва да се тълкува като предоставяне на гаранция към правото на ефективна защита пред съда (обяснение, свързано с Хартата на основните права, обяснение по член 47 (2007/C/ 303/02).
[66] Съединени дела C-584/10 P, C-593/10 P и C-595/10 P, Европейска комисия и Обединеното кралство / Kadi, 18 юли 2013 г.
[67] Kadi II, точки 97 и 100: всички актове на Съюза, включително тези, които имат за цел прилагането на резолюции, приети от Съвета за сигурност на основание глава VII от Устава на Обединените нации, подлежат на контрол за законосъобразността от съдилищата на Европейския съюз (глава VII е свързана с действия в случай на заплахи срещу мира, нарушения на мира и актове на агресия).

Съдебната практика на Европейския съд по правата на човека обяснява много точно, че правните средства за защита пред обикновените съдилища не са условие схемите за наблюдение да се разглеждат като съвместими с член 8 (и член 13 от ЕКПЧ)[68]. По-скоро Съдът е развил, съгласно член 8, като необходима гаранция за дейностите по наблюдение, тезата, че правната защита пред другите органи е допустима. Независимо от това Европейският съд по правата на човека има големи очаквания към други органи, предоставящи ефективни средства за защита, като твърди, че такъв орган трябва да бъде „независим от органите, които извършват наблюдението, и има достатъчни правомощия и компетентност да упражнява ефективен и продължителен контрол“[69].

В рамките на делото Kennedy и делото Klass Европейският съд по правата на човека представя по-задълбочен анализ на това, какво могат да означават тези очаквания в контекста на тайното наблюдение, когато субектът на данните не е уведомен за обработването на своите данни. И в двете решения органите са разглеждани като независими от Европейския съд по правата човека, специално независими от органите, извършващи наблюдението, но и независими от указанията[70] от всеки друг орган. По-специално по делото Kennedy съдът одобри независим и безпристрастен орган, който е приел собствени процедурни правила и се състои от членове, които заемат или са заемали високопоставени съдебни длъжности или са опитни адвокати[71].

При извършването на проверката на жалби, подадени от физически лица, органите и по двете решения са имали освен това достъп до цялата съответна информация, включително приключени материали. И накрая, и двата органа разполагат с правомощията да предприемат корективни мерки срещу неспазването[72].

Освен това на въпроса, дали омбудсманът може да се счита за „съд“, прилагането на член 47, параграф 2 от Хартата предполага допълнително предизвикателство, тъй като той предвижда, че правораздавателният орган трябва да бъде „създаден със закон“. Под въпрос е обаче дали един Меморандум, който определя работата на нов механизъм, може да се счита за „закон“.

В резултат на това, като се отчита принципът на равностойност по същество, работната група реши вместо да преценява дали Омбудсманът може да се счита официално за съд, създаден със закон, да доразвие нюансите на съдебната практика по отношение на специфичните изисквания, необходими „правни средства за защита“ и „правна защита“ да се считат за съвместими с основните права по смисъла на членове 7, 8 и 47 от

[68] Член 13 от ЕКПЧ задължава държавите членки да гарантират, че „всички, чиито права и свободи (...) са нарушени, трябва да разполагат с ефикасни вътрешноправни средства за своята защита от съответната национална институция“. Това не е необходимо да бъде съдебен орган, както пояснява Европейският съд по правата на човека в делото Klass, точки 56 и 67.
[69] Решение по делото Klass, точки 56 и 67.
[70] Европейски съд по правата на човека, Решение по делото Klass, точки 21 и 53.
[71] Комисията G 10 (към момента на решението) се състои от трима членове, като председателят ѝ трябва да бъде квалифициран да заема съдебна длъжност, Решение по делото Klass, точки 21 и 53.
[72] Европейски съд по правата на човека, Решение по делото Kennedy, точка 167; Решение по делото Klass, точки 21 и 53.

Хартата и член 8 (и 13) от ЕКПЧ. В по-нататъшния си анализ при обсъждане на обхвата на прилагане на новия механизъм работната група ще се съсредоточи върху следните критерии: изискването за подаване на искане до омбудсмана и за получаване на отговор („основателност“), независимостта на омбудсмана, неговите разследващи правомощия за достъп до необходимите материали, включително класифицирани документи, и за искане за помощ от други агенции, и накрая — неговите правомощия за предприемане на корективни мерки срещу неспазването.

3.5.3.4 Обхват на прилагането на Механизма на омбудсмана

Що се отнася до достъпа до Механизма на омбудсмана, РГ по член 29 счита, че всички субекти на правото на ЕС следва да бъдат обхванати от гаранциите съгласно Щита за личните данни. Не би било приемливо да се прави разграничение, основано на националност, особено предвид факта, че основните права в ЕС се прилагат по отношение на всеки, а не само на тези, които притежават европейски паспорти. Приложение III се позовава на „физическо лице от ЕС“, без допълнително да се определя кое е то. Работната група изразява съжаление за тази несигурност и предлага да се предвиди разяснение, чийто смисъл е, че всички субекти на правото на ЕС имат правото да отправят искането си до омбудсмана, което да бъде обработено съгласно условията на Меморандума. Освен това Комисията и САЩ следва да разгледат въпроса за степента, в която Щитът за личните данни ще се прилага и по отношение на граждани/жители на държавите от ЕИП и Швейцария, които в миналото са били обхванати от схемата за сфера на неприкосновеност на личния живот.

Освен това РГ по член 29 отбелязва определена несигурност по отношение на обхвата на прилагането на Механизма на омбудсмана. Като се има предвид, че Меморандумът предвижда, че на омбудсмана е поверена обработката на искания, свързани с националната сигурност по отношение на предадени от ЕС до САЩ данни, съобразно с всички инструменти за предаване съгласно правото на ЕС, в него е също толкова ясно, че той установява механизъм „относно радиоелектронното разузнаване“. Последният термин предполага, че когато данните са събрани чрез радиоелектронно разузнаване, се обхващат само такива предавания на данни, което повдига въпроса, дали събирането на данни съгласно FISA се счита например за „радиоелектронното разузнаване“. Очевидно такъв е случаят по отношение на раздел 702, както е обяснено в изявлението на ODNI, точка 10[73]. РГ по член 29 обаче изказва съжаление, че използването на термина „радиоелектронно разузнаване“ създава ненужна несигурност в този контекст.

Като друга последица от това, работната група счита, че Механизмът на омбудсмана не обхваща искания, свързани с достъп от правоприлагащи агенции[74]. Ако е така, това би оставило неизяснено дали исканията от някои агенции, главно ЦРУ, ще бъдат обхванати от механизма.

[73] Приложение VI към Щита за личните данни, точка 10.
[74] Меморандум относно създаването на омбудсман, точка 1 .

3.5.3.5 „Основателност“ и процедура по подаване на искането

Образуването на съдебно производство срещу мерки за наблюдение, предприети от правителството на САЩ пред обикновени съдилища в Съединените щати, е много трудно. Работната група е наясно, че Върховният съд е отхвърлил основателността при дела, свързани с разузнаването, в които заявителят не е бил в състояние да докаже „определено, конкретизирано и действително или предстоящо нараняване“ на физическо лице[75]. В това отношение създаването Механизма на омбудсмана е важна стъпка, тъй като добавя възможност за определена форма на правна защита, която в противен случай не би съществувала. Поради това работната група приветства разяснението в раздел 3, буква в). Въз основа на този раздел, за да се подаде искане съгласно новия механизъм, не е необходимо да се доказва, че до данните на заявителя е бил осъществен достъп чрез дейности за радиоелектронно разузнаване.

Работната група подкрепя до голяма степен процедурата за идентифициране на жалбоподателя съгласно Механизма на омбудсмана. Напълно разумно е тази идентификация да става на територията на ЕС, какъвто е случаят и с механизма за достъп съгласно споразумението TFTP2 между ЕС и САЩ. Работната група не разбира обаче защо проверката в ЕС следва да се извършва от „компетентни органи на държавите членки за надзор на националните служби за сигурност“. На първо място, съгласно член 4, параграф 2 от Договора за Европейския съюз, изглежда малко вероятно Европейската комисия да е в състояние да определя задачите на тези органи, които явно попадат в рамките на компетентността на държавите членки.

Освен това, предвид разнообразието от механизми за надзор на националните служби за сигурност в държавите членки, участието на съответните органи може сериозно да засегне ефективността на система за гражданите в държавите членки. Така например в случаи, когато има няколко органа, отговарящи за надзора на националните служби за сигурността и за физическото лице би било трудно да определи съответния, когато приложимите национални законови правила не предвиждат възможност за физическите лица да се свържат със съответния надзорен орган или когато тези органи не са създадени по начин, който ги прави подходящи да изпълняват задачите, наложени им в проекта на решение за адекватността[76]. Като се взема предвид участието на ОЗД в прилагането на Щита за личните данни и надзора върху него, както и тяхната подобна роля съгласно споразумението TFTP2, е по-разумно тази задача да се отреди на националните органи за защита на личните данни на държавите членки. Работната група подчертава, че счита, че е малко вероятно класифицираната информация да бъде обработвана като част от процедура пред омбудсмана към Щита за личните данни, тъй като всеки отговор ще бъде само „спазена или неспазена, но коригирана“.

[75] Решение по дело Clapper/ Amnesty International USA, 568 U.S. ___ (2013) II. точка 10.
[76] Така например в някои държави — членки на ЕС, физическите лица могат да получат достъп до информация, съхранявана от националните служби за сигурност само чрез искане до Върховния съд.

3.5.3.6 Независимост

В писмените изявления на Държавния секретар се посочва ясно, че длъжността на омбудсмана ще се изпълнява от заместник-държавния секретар. Той се номинира от Президента и изисква потвърждение от Сената. Длъжността на омбудсмана не изисква допълнително потвърждение; достатъчно е да се посочи кой изпълнява длъжността на омбудсман. Заместник-секретарят се номинира от Президента на Съединените американски щати, назначава се от Държавния секретар като омбудсман и получава потвърждение на Сената на Съединените щати за длъжността на заместник-секретар. Както се подчертава в направените изявления в писмото и Меморандума, омбудсманът е „независим от разузнавателните структури на САЩ“. РГ по член 29 поставя обаче въпроса, дали омбудсманът е създаден в рамките на най-подходящото министерство. Очевидно, за да може да се изпълнява ефективно ролята на омбудсман се изискват определени знания и познаване на работата на разузнавателните структури, докато в същото време наистина е необходима достатъчна отдалеченост от разузнавателните структури, за да може да се действа независимо.

Щитът за личните данни не определя специфични критерии за освобождаването на омбудсмана. Поради това работната група счита, че омбудсманът може да бъде освободен от длъжността по същия начин, по който може да бъде освободен от длъжността като заместник-секретар на Държавния департамент, което вероятно може да урони независимостта на позицията на омбудсмана.

Предвид същността на длъжността, назначаването на заместник-секретар на Държавния департамент за омбудсман е очевидно различно по отношение на независимостта от установената компетентност на обикновения съд за правна защита на физическите лица. Поради това се повдига въпросът, дали по отношение на независимостта омбудсманът може да се разглежда като равен на останалите независими надзорни органи, за които е установено, че отговарят на изискванията. В контекста на надзора тези органи биха били по-специално Трибуналът с разследващи правомощия (IPT) в Обединеното кралство и Комисията G10 в Германия.

За да се разбере дали това е така, трябва да се извърши допълнителна оценка чрез анализиране на правомощията, предоставени на „независимия орган“.

3.5.3.7. Правомощия за провеждане на разследвания

В рамките на делото Kadi II Съдът на Европейския съюз постановява във връзка с член 47 от Хартата, че изисква „заинтересованото лице да може да се запознае с мотивите за взетото по отношение на него решение посредством прочита на самото решение или чрез изпращането на мотивите му по искане на това лице, без да се засяга правомощието на компетентния съд да изиска изпращането им от съответния орган, за да може то да защити правата си при възможно най-добрите условия“[77]. Съдилищата на Европейския съюз трябва да гарантират, че решението се взема върху достатъчно

[77] Решение по делото Kadi II, точка 100.

стабилна фактологична основа[78]. Той заявява ясно, че „не може да бъде противопоставена тайната или поверителността на тези [...] данни или доказателства“, поне не пред Съдилищата на ЕС[79]. Поради това Работната група заключава, че на омбудсмана трябва да се предоставят информация и данни, които подкрепят мотивите, изтъкнати за провеждането на мярка, за да отговори на изискванията на Съда на Европейския съюз[80].

Още не е ясно обаче какви ще бъдат правомощията за разследване на омбудсмана. Проекторешението на Комисията и приложение III на Държавния департамент не са достатъчно ясни по този въпрос. Доколкото Работната група разбира, омбудсманът следва да получава достатъчно информация, за да бъде в състояние да посочи дали дадена операция по обработката на данни от службите за сигурност се извършва в съответствие със закона, и ако не, да гарантира, че ситуацията на неспазване е преодоляна. Нито в писмото от Държавния департамент, нито в проекторешението на Комисията се определя обаче дали омбудсманът ще има директен достъп до данните, които са налични за съответното физическо лице, и следователно ще може да проведе разследването си или може да разчита единствено на докладите на службите на правителството на САЩ.

3.5.3.8 Правомощия за защита

В Меморандума остава по-скоро неясно по какъв начин омбудсманът може да разпореди неспазването да бъде отстранено. В съчетание с липсата на яснота относно правомощията за разследване все още е неясно и до каква степен омбудсманът като такъв ще бъде в състояние ефективно да разпорежда неспазването да бъде отстранено, както и какъв ще бъде резултатът от такова действие. Означава ли това, че данни, получени по несъвместим начин (т.е. незаконосъобразно), не могат да се използват повече в която и да е процедура и трябва да бъдат заличени?

Освен това според работната група Щитът за личните данни не трябва да предвижда обжалване на решение на омбудсмана или негово преразглеждане.

И накрая, когато става въпрос за съобщението на омбудсмана до жалбоподателя след разглеждането от негова страна на жалбата, омбудсманът не трябва да разкрива, ако е било налице незаконосъобразно поведение от страна на разузнавателната структура. Предоставеният отговор ще бъде винаги един и същ и ще е неопределен. В делото Kadi II Съдът на ЕС постановява, че компетентният орган (в ролята си на надзорен орган) е длъжен да посочи мотивите си, които включват всички обстоятелства, въпреки че съгласно член 296 от ДФЕС не се изискват подробни мотиви[81].

[78] Решение по делото Kadi II, точка 119.
[79] Решение по делото Kadi II, точка 125.
[80] Решение по делото Kadi II, точка 122; въпреки че съответният орган не трябва да осигурява цялата информация и данни, които са в основата на мотивите за мярката.
[81] Решение по делото Kadi II, точка 116.

3.5.4 В заключение

Съществуването на ефективни правни средства за защита за физически лица продължава да предизвиква безпокойство в РГ по член 29. На първо място проектът на решение за адекватността не предоставя точен отговор на въпроса, в какви ситуации и при какви предпоставки физическите лица могат да заведат дело, за да определят правата си.

РГ по член 29 признава и приветства въвеждането на алтернативен механизъм за защита в лицето на Омбудсмана, което е единствено по рода си развитие в отношенията между ЕС и трета държава. Освен посочената по-рано необходимост от разясняване на термина „физически лица от ЕС“, механизмът създава допълнителна възможност за тях да търсят защита от администрацията на САЩ, за да се гарантира, че всички лични данни на жалбоподателя се обработват в съответствие с правото на САЩ.

В същото време РГ по член 29 отбелязва значителни недостатъци при оценяването на механизма на Омбудсмана спрямо стандартите за независим съд по смисъла на член 47 от Хартата и изискванията, които Съдът на ЕС и Европейският съд по правата на човека са въвели в съдебната си практика при случаи на наблюдение. На първо място, налице е опасението относно това, дали омбудсманът може да се счита (официално и напълно) за независим, особено поради относителната лекота, с която лица с политически назначения могат да бъдат освобождавани. На второ място, продължават да са налице опасения и относно правомощията на Омбудсмана за упражняване на ефективен и непрекъснат контрол. Въз основа на наличната в приложение III информация РГ по член 29 не може да стигне до заключението, че омбудсманът ще има по всяко време директен достъп до цялата необходима информация, файлове и ИТ системи, за да изготви оценката си, нито че наистина може да принуди отговорните разузнавателни агенции да преустановят всяко несъвместимо обработване на данни, особено в случай на неразбирателство по въпроса, дали обработването на данните е в съответствие със закона или не. Възможно е по-нататъшно разяснение на позицията и правомощията на омбудсмана да могат да разсеят опасенията на РГ по член 29.

3.6 Заключителни бележки относно гаранциите и ограниченията, които се прилагат за органите за национална сигурност на САЩ

Преди всичко РГ по член 29 приветства Комисията и органите на САЩ за всички положени от тях усилия за увеличаване на прозрачността относно последиците, които разузнавателните програми на САЩ могат да имат върху предадените данни съгласно Щита за личните данни или всеки друг инструмент за предаване, свързан с това. След разкритията на Сноудън през юни 2013 г. са предприети значителни стъпки. Въпреки това РГ по член 29 отбелязва, че все още са налице опасения. Най-малкото се изискват допълни обяснения и разяснения относно правата и задълженията съгласно Щита за личните данни.

Двете основни опасения на РГ по член 29 са свързани с факта, че масовото и безразборно събиране на данни не е напълно изключено от органите на САЩ и че правомощията и позицията на омбудсмана не са обяснени достатъчно подробно. Освен това за започване на процедура пред омбудсмана от името на физическо лице следва да бъдат компетентни националните ОЗД, вместо надзорните органи на разузнавателните агенции. Освен това, въпреки че РГ по член 29 определено признава опитите да се отговори на опасенията, изразени от ОЗД, ще бъдат приветствани и допълнителни гаранции, с цел да се гарантира, че всяка намеса, която може да е в резултат на програмите за наблюдение на САЩ, е необходима в едно демократично общество.

4. Оценка на гаранциите в областта на правоприлагането, които се предоставят от Щита за личните данни

4.1 Въведение

Що се отнася до публичния достъп до лични данни за целите на правоприлагането, РГ по член 29 отбелязва, че Принципите на неприкосновеност на личните данни в приложение II от Щита за личните данни включват дерогация, която е идентична с дерогацията, заложена в принципите за „сфера на неприкосновеност на личния живот“. От това следва, че общият характер на дерогацията се запазва, което означава, че новите Принципи на Щита за личните данни правят възможна намесата в основните права на лицата, чиито лични данни се предават от ЕС на САЩ „въз основа на изисквания, свързани с националната сигурност и с обществения интерес, или въз основа на вътрешното законодателство на САЩ“[82].

Една от основните критики, отправени от Съда по отношение на решението за „сфера на неприкосновеност на личния живот“ в делото Schrems, обаче е, че то „не съдържа каквато и да било констатация относно наличието в Съединените щати на правила с етичен характер, предназначени за ограничаване на евентуалната намеса, засягаща основните права на лицата, чиито данни се прехвърлят от Съюза към Съединените щати“.

Поради това РГ по член 29 приветства усилията на администрацията на САЩ да предостави повече информация за правната уредба относно намесата, засягаща личните данни, предадени съгласно Щита за личните данни в отношенията между ЕС и САЩ, за целите на правоприлагането, включително прилагането на ограничения и гаранции. В същото време, РГ по член 29 подчертава, че разглежда въпроса за публичния достъп, като отчита факта, че всяка намеса в основните права на личен живот и защита на данните трябва да бъде обоснована в едно демократично общество. Поради това РГ по член 29 анализира гаранциите в областта на правоприлагането на Щита за личните данни, като използва рамката, определена в раздел 1.2. от настоящото становище.

[82] Решение по делото Schrems, точка 87.

4.2 Прилагане на европейските основни гаранции спрямо достъпа на правоприлагащите органи до данни, с които разполагат дружествата

4.2.1 Достъпът от страна на правоприлагащите органи до лични данни следва да се извършва законосъобразно и въз основа на ясни, точни и приемливи правила

Приложение VII към Щита за личните данни съдържа писмо от Министерството на правосъдието на САЩ, в което „е направен кратък преглед на основните средства за разследване, използвани за получаването на търговска информация и други справочни данни от дружествата в Съединените щати за целите на правоприлагането в наказателната сфера или в сферата на обществените интереси (гражданскоправната и регулаторната сфера), включително ограниченията за достъпа, определени в тези законови разпоредби“.

Всички процедури, посочени в приложение VII, произтичат пряко от Конституцията на САЩ (четвъртата поправка), от писаните закони и процесуалното право, или от Насоките и политиките на Министерството на правосъдието. Приложение VII обаче не се отнася конкретно до всички закони, които предвиждат тези процедури, а вместо това се съсредоточава върху кратко описание на самите процедури. В приложение VII се посочва също, че „съществуват и други правни основания за оспорване от страна на дружествата на искания за информация от административни институции, според конкретната стопанска дейност и вида на данните, с които разполагат“, като се дават няколко неизчерпателни примера като Закона за банковата тайна, Закона за оповестяване на информация за кредити, Закона за правото на неприкосновеност на личните финанси.

Работната група по член 29 отбелязва, че рамката на законите, процедурите и политиките е фрагментирана и че приложимото правно основание за определено искане за достъп ще зависи от характера на търсените данни, характера на дружеството, характера на правните процедури (наказателни, административни, свързани с други обществени интереси) и характера на искащия достъп субект.

Тъй като всички приложими правила за ограничаване на достъпа на правоприлагащите органи до данни, които се предават съгласно Щита за личните данни, се основават на Конституцията, писаните закони и политиките за прозрачност на Министерството на правосъдието, РГ по член 29 отчита презумпцията за достъпност на тези правила. Яснотата и точността на правилата обаче могат да бъдат оценени само в рамките на всеки отделен вид процедура и искане за достъп. Поради това РГ по член 29 изразява съжаление, че въз основа на наличните подробности в приложение VII към Щита за личните данни и констатациите в проекта на решение в момента не може да се извърши подобна оценка.

4.2.2 Трябва да бъдат доказани необходимостта и пропорционалността по отношение на преследваните легитимни цели

РГ по член 29 отбелязва надлежно, че искането на достъп до данни за целите на правоприлагането може да се счита за преследване на легитимна цел. Така например член 8, параграф 2 от ЕКПЧ приема намесата в правото на защита на личния живот от страна на публичен орган „в интерес на (...) обществената сигурност (...) за предотвратяване на безредици или престъпления“. Такава намеса е приемлива обаче само когато е необходима и пропорционална[83].

Съгласно установената съдебна практика на Съда на ЕС, принципът на пропорционалност изисква законодателните мерки, предлагащи намеса в правото на личен живот и защита на личните данни, да „са годни да постигнат легитимните цели, преследвани от *разглежданата правна уредба,* и да не надхвърлят границите на подходящото и необходимото, за постигането на тези цели“[84] (акцентирането с курсив е направено от нас). Следователно оценката на необходимостта и пропорционалността се извършва винаги във връзка със специфични мерки, предвидени от законодателството.

В приложение VII органите на САЩ уточняват, че федералните прокурори и федералните следователи са в състояние да получат от организациите достъп до документи и друга регистрирана информация чрез „няколко вида процеси за задължително призоваване, включително призовки на „голямото жури“, административни разпореждания и заповеди за обиск, и могат да придобиват друг вид съобщителна информация “съгласно правомощията си за подслушване и използване на устройства за регистриране за целите на федерални наказателни разследвания“.[85] Освен това агенциите с граждански и регулаторни отговорности могат да издават призовки на организации за „търговска информация, данни, съхранени по електронен път, или други материали“[86]. В приложение VII се пояснява допълнително, че тези производства се използват като цяло за получаване на информация от „дружества“ в САЩ, независимо от това, дали те са сертифицирани или не в рамките на Щита за личните данни, и „независимо от гражданството на субекта на данните“. С други думи, изглежда, че субектите на тези защити са организациите, а не самите физически лица.

В допълнение към приложение VII, проекторешението, което се основава на Принципите на Щита за личните данни, съдържа констатации на Комисията относно съществуването в САЩ на правила за ограничаване на намесата в основните права на лицата, чиито лични данни се предават от ЕС на САЩ съгласно Щита за личните данни.

[83] Вж. работен документ относно Европейските основни гаранции, точки 7—9 За обща оценка на концепциите за необходимост и пропорционалност, вж. Становище 01/2014 на работната група за защита на личните данни по член 29 относно прилагането на концепциите за необходимост и пропорционалност и защитата на данните в сектора на правоприлагането.
[84] Решение по делото Digital Rights Ireland, точка 46 и цитираната в нея съдебна практика.
[85] Приложение VII, точка 2.
[86] Приложение VII, точка 4.

По-специално констатациите в проекторешението се отнасят до приложимите ограничения и гаранции съгласно четвъртата поправка в Конституцията на САЩ, съгласно която за претърсвания и изземвания от правоприлагащите органите по принцип се изисква съдебна заповед, издадена след като бъде доказано наличието на правдоподобна причина[87]. Констатациите са отнасят и до факта, че в изключителни случаи, когато не се прилага изискването за съдебна заповед, при правоприлагането се извършва тест за основателност[88].

Въпреки това констатациите не разясняват как тези гаранции се прилагат за лица, които не са граждани на САЩ. В действителност в едно от съображенията на проекторешението се признава, че „защитата съгласно четвъртата поправка не се прилага за лица, които не са американски граждани и не пребивават в Съединените американски щати“[89]. В същите параграфи на проекторешението се посочва също така, че лицата, които не са граждани на САЩ, „се ползват непряко чрез защитата, предоставена на дружества на САЩ, които пазят личните данни и които са получатели на исканията в областта на правоприлагането“. РГ по член 29 изразява обаче съжаление, че тази констатация не се позовава на източник на правото, нито в писаните закони, нито в съдебната практика.

Като цяло, РГ по член 29 отбелязва, че системата от средства за разследване, използвани за получаване на търговска информация и други справочни данни от дружествата в Съединените Щати за целите на правоприлагането в наказателната сфера или в сферата на обществените интереси, включително ограниченията за достъпа и гаранциите, представлява сложна среда от мерки. Към момента тази система не може да бъде оценена като цяло въз основа на наличната информация. За да се изготви действителна оценка на необходимостта и пропорционалността на мерките за разследване в областта на правоприлагането във връзка с основните права на личен живот и защита на данните, е необходима специфична оценка в отделните случаи.

4.2.3 Трябва да съществува независим механизъм за надзор

РГ по член 29 надлежно отбелязва факта, че повечето от процедурите, описани в приложение VII, предполагат наличието на решение на съда, преди органите да получат достъп до данните (напр. съдебни разпореждания за устройства за регистриране и проследяване, съдебни разпореждания за наблюдение съгласно Федералния закон за подслушванията, заповеди за претърсване — правило 41). Изглежда обаче, че не за всички от тях се изисква предварително участие на съд. Така например гражданските и регулаторни органи могат да издават разпореждане[90]. В тези случаи е налице възможност за последващ съдебен контрол на основателността на

[87] Проект на решение за адекватността, параграф 107.
[88] Щит за личните данни, параграф 107.
[89] Проект на решение за адекватността, параграф 108.
[90] Приложение VII, точка 4.

разпореждането, като „получателят на административното разпореждане може да оспори изпълнението му в съда“[91].

Въз основа на наличната информация РГ по член 29 отбелязва, че по отношение на достъпа на правоприлагащите органи до данни, съхранявани от дружествата в САЩ, следва да се въведе сравнително стабилен независим механизъм за надзор.

4.2.4 Физическите лица трябва да разполагат с ефективни правни средства за защита

Както бе посочено по-горе, „защитата съгласно четвъртата поправка не се прилага за лица, които не са американски граждани и не пребивават в Съединените американски щати“[92]. Това означава, че лице, което не е гражданин на САЩ, няма да бъде в състояние да оспори заповеди или разпореждания в Съда, като се позовава на четвъртата поправка. В проекта на решение за адекватността се посочва, че лицата, които не са граждани на САЩ, се ползват непряко чрез защитата, предоставена на дружествата в САЩ, които пазят личните данни и които са и получатели на исканията в областта на правоприлагането. РГ по член 29 посочва обаче, че дори тази защита да е ефективна, това не означава, че на физическите лица са предоставени ефективни правни средства за защита, тъй като изглежда, че в този случай субект на правото на ефективна правна защита е дружеството, което е получило искането за достъп, а не физическото лице, чиито данни се разглеждат.

В приложение VII не е включена допълнителна информация по отношение на възможните, произтичащи от писаните закони правни средства за защита, достъпни за лица, които не са граждани на САЩ в случаите, когато органите или дружествата предоставят или получават незаконосъобразно достъп до съдържанието на техните данни.

РГ по член 29 приветства факта, че в наскоро приетият Закон за съдебната защита[93] се предвижда правото на съдебна защита за лица, който не са граждани на САЩ. Тези права обаче са ограничени до ясно определени причини за действие: правото на получаване на коригиране и достъп до данни и адвокатски такси, когато „определена федерална агенция или структура“ отрича изменението на данните или отказва достъпа до такива данни, и правото на гражданскоправни средства за защита в случай на оповестяване на данни, което е „преднамерено или умишлено“.

Освен това съдебната практика на САЩ, която се посочва в бележките под линия на съответните съображения на проекторешението, по-специално решенията по дела City of Ontario/Quon[94], Мериленд/King[95] и Samson/Калифорния[96], не се отнася до оценката

[91] Приложение VII, точка 4.
[92] Проект на решение за адекватността, параграф 108
[93] Закон за съдебната защита от 2015 г., H.R. 1428.
[94] Решение по дело *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010).
[95] Решение по дело *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013).
[96] Решение по дело *Samson v. California*, 547 U.S. 843, 848 (2006).

на това дали лица, които не са граждани на САЩ, могат да подадат жалба пред съда, за да обжалват законосъобразността на намесата в неприкосновеността на личния им живот[97]. Всички случаи се отнасят до правото на личен живот на лицата в САЩ и всички от тях включват решения на Върховния съд на САЩ, които всъщност ограничават прилагането на четвъртата поправка.

Като цяло, РГ по член 29 одобрява и приветства приемането на Закона за съдебната защита, но все още има съмнения относно това дали действително са налични ефективни правни средства за защита за физически лица субекти на данни.

4.3 Заключителни бележки

РГ по член 29 приветства и признава усилията на администрацията на САЩ да предостави повече информация за правната уредба относно намесата, засягаща личните данни, предадени съгласно Щита за личните данни в отношенията между ЕС и САЩ за целите на правоприлагането, включително прилагането на ограничения и гаранции.

РГ по член 29 отбелязва, че системата от средства за разследване на правоприлагащите органи, включително приложимите ограничения и гаранции, е както всеобхватна, така и сложна, докато включената в Щита за личните данни информация е кратка. Ето защо РГ по член 29 изразява съжаление, че поради ограничената информация (т.е. в приложение VII към Щита за личните данни и относно констатациите в проекторешението) няма възможност да предостави цялостна оценка относно достъпността, предвидимостта, както и необходимостта и пропорционалността на приложимите към момента правила. Независимо от другите констатации на РГ по член 29 относно Щита за личните данни в настоящото становище, такава оценка може да бъде част от годишния преглед на Щита за личните данни.

Що се отнася до достъпа от страна на правоприлагащите органи, РГ по член 29 отбелязва, че следва да бъде въведен сравнително стабилен независим механизъм за надзор. Освен това РГ по член 29 приветства приемането на Закон за съдебната защита, който гарантира правото на съдебна защита на всички лица, които не са граждани на САЩ. РГ по член 29 отбелязва обаче, че тези права са с ограничено естество. В допълнение към констатацията, че лице, което не е гражданин на САЩ, няма да има възможност да оспори заповеди или разпореждания в Съда, като се позовава на четвъртата поправка, е налице и опасението дали действително в областта на правоприлагането са достъпни ефективни правни средства за защита за физически лица, субекти на данни.

[97] По делото *Ontario v. Quon* Съдът постановява, че град Онтарио не нарушава правата на гражданите си съгласно четвъртата поправка, тъй като достъпът на града до съдържанието на частните съобщения на въпросните служители е основателен и е мотивиран от свързаната с работата законна цел и не е прекомерен по обхват. По делото *Samson v. California* Съдът постановява, че „четвъртата поправка не забранява на полицейските служители да извършват претърсвания на освободени по подозрение“. По делото *Maryland v. King* Съдът постановява, че когато служителите извършват арест, въз основа на вероятна причина за задържане на заподозрян в криминално деяние и го отвеждат до управлението, за да бъде задържан в ареста, вземането на ДНК проба от бузата на арестанта и анализирането ѝ е законна полицейска процедура, както снемането на отпечатъци или фотографирането, която е основателна съгласно четвъртата поправка.

5. ЗАКЛЮЧЕНИЯ И ПРЕПОРЪКИ

Работната група по член 29 приветства на първо място факта, че в рамките на пет месеца след отмяната на „сферата на неприкосновеността на личния живот“ е представен нов проект на решение за адекватността, съдържащ много подобрения в сравнение с предходния механизъм. Тя е особено удовлетворена от по-голямата прозрачност, която се постига посредством въвеждането на два списъка към Щита за личните данни на уебсайта на Министерството на търговията: един списък, съдържащ регистрите на тези организации, които се придържат към Щита за личните данни, и друг списък, съдържащ регистрите на тези организации, които са се придържали към Щита в миналото, но вече не се придържат. Приветства се и по-голямата прозрачност във връзка с публичния достъп до данни, които се предават съгласно Щита за личните данни или за целите на националната сигурност, или за целите на правоприлагането. И накрая, РГ по член 29 е много удовлетворена да научи, че всички предавания на данни до САЩ ще получат отсега нататък една и съща защита: не са въведени специфични правни разпоредби, които да предоставят предимство на един или на друг вид инструмент.

5.1 Три въпроса, предизвикващи безпокойство

Все още са налице обаче три основни въпроса, предизвикващи безпокойство, които според РГ по член 29 трябва да бъдат разгледани.

Първото опасение е свързано с това, че текстът, използван в проекта на решение за адекватността, не задължава организациите да заличават данни, ако те вече не са им необходими. Това е съществен елемент от правото на ЕС за защита на данните, който гарантира, че данни не се съхраняват по-дълго от необходимото за постигане на целта, за която са били събрани. На второ място, РГ по член 29 разбира от приложение VI, че администрацията на САЩ не изключва напълно продължаващото масово и безразборно събиране на данни. РГ по член 29 поддържа твърдението, че такова събиране на данни е неоправдана намеса в основните права на физическите лица. Третият момент, пораждащ безпокойство, е въвеждането на Механизма на омбудсмана. Въпреки че РГ по член 29 приветства тази безпрецедентна крачка за създаване на допълнителен механизъм за защита и надзор за физическите лица, все пак продължават да са налице опасения за това, дали омбудсманът разполага с достатъчно правомощия, за да изпълнява функциите си ефективно. Най-малкото трябва да бъдат изяснени правомощията и положението на омбудсмана, с цел да се докаже, че ролята му е действително независима и може да предложи ефективна правна защита относно обработка на данни, която се извършва в нарушение.

5.2 Препоръчвани разяснения

В допълнение към посочените по-горе въпроси РГ по член 29 отбелязва различни моменти в цялото становище, където е желателно допълнително разясняване на решението за адекватността. Още по-важно е, че това се отнася до необходимостта да

се гарантира, че ключови понятия за защита на данните, използвани в Щита за личните данни, се определят и прилагат последователно. В момента ситуацията не е такава. Подкрепя се идеята за въвеждането на речник на термините в раздела с често задавани въпроси на Щита за личните данни, в който да бъдат включени определения, които в най-добрия случай ще са изцяло договорени между ЕС и САЩ. РГ по член 29 достига също до заключението, че последващите предавания на лични данни от ЕС не са достатъчно регламентирани, особено по отношение на техния обхват, ограничаването в рамките на целта и гаранциите, които се прилагат за предаванията на представители. Що се отнася до достъпа според Щита до лични данни от страна на правоприлагането, особено относно предвидимостта на съответното законодателство, съществува безпокойство поради обширния и сложен характер на системата за правоприлагане на САЩ както на федерално, така и на щатско равнище, както и ограничената информация, включена в решението за адекватност.

Щитът за личните данни е първото решение за адекватността, изготвено след принципното договаряне на текстовете на ОРЗД. Въпреки това много от подобренията на равнището на защитата на данни, предлагани на физическите лица, не са отразени в Щита за личните данни. Поради това РГ по член 29 препоръчва, скоро след влизането в сила на ОРЗД да се направи преглед на това решение за адекватността, както и на решенията за адекватността, изготвени за други трети държави.

Последната препоръка, направена тук от РГ по член 29, се отнася до съвместния преглед. РГ по член 29 приветства факта, че решението за адекватността на Щита за личните данни наистина ще бъде преразглеждано всяка година с активното участие на ОЗД и други съответни страни. Тя ще подкрепи споразумение относно елементите на съвместните прегледи, включително относно изготвянето и представянето на доклада от прегледа от всички страни, което да е налице достатъчно време преди първия преглед.