ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 9.10.2024 г.
COM(2024) 451 final

ДОКЛАД НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

относно първия периодичен преглед на функционирането на решението относно адекватното ниво на защита на Рамката за защита на личните данни в отношенията между ЕС и САЩ

1. ПЪРВИ ПЕРИОДИЧЕН ПРЕГЛЕД — КОНТЕКСТ, ПОДГОТОВКА И ПРОЦЕС

В решението си от 10 юли 2023 г. („решението относно адекватното ниво на защита“) Комисията установи, че с Рамката за защита на личните данни в отношенията между ЕС и САЩ (РЗЛД) се осигурява адекватно ниво на защита на личните данни, предавани от Европейския съюз към организации в Съединените американски щати[1]. С решението относно адекватното ниво на защита от Комисията се изисква да извършва периодични прегледи, първият от които следва да се проведе в срок от 1 година от датата на нотифицирането на решението относно адекватното ниво на защита до държавите членки. Първият преглед завършва с настоящия доклад.

Както се изисква в съображение 211 от решението относно адекватното ниво на защита, този първи преглед, извършен след първата година на действие на новата рамка, беше съсредоточен върху проверката дали всички елементи, предвидени в рамката, са приложени и функционират ефективно. Прегледът обхвана всички аспекти на функционирането на рамката, включително с оглед на правните промени, настъпили след приемането на решението относно адекватното ниво на защита.

При подготовката за прегледа Комисията събра информация от съответните заинтересовани страни, по-специално от неправителствени организации (НПО) с опит в областта на цифровите права и правото на неприкосновеност на личния живот[2], организации, сертифицирани съгласно РЗЛД, чрез съответните им търговски асоциации[3], както и от органите на САЩ, участващи в прилагането на рамката. Освен това Комисията събра обратна информация и от широката общественост чрез специална покана за предоставяне на данни на портала „Споделете мнението си“[4].

---

[1] Решение за изпълнение (ЕС) 2023/1795 на Комисията от 10 юли 2023 г. съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно адекватното ниво на защита на личните данни в Рамката за защита на личните данни в отношенията между ЕС и САЩ.

[2] Комисията изпрати въпросник до девет неправителствени организации (Human Rights Watch, American Civil Liberties Union, Consumer Federation of America, Center for Digital Democracy, New America Open Technology Institute, Access Now, Electronic Frontier Foundation, Electronic Privacy Information Center, Center for Democracy and Technology), като се съсредоточи върху съответните промени в правната рамка на САЩ, механизмите за надзор и контрол на прилагането, както и функционирането на механизмите за правна защита. Службите на Комисията и представителите на ЕКЗД също се срещнаха онлайн с тези НПО на 9 юли 2024 г.

[3] Комисията изпрати въпросник до девет търговски асоциации (Software & Information Industry Association, U.S. Chamber of Commerce, Information Technology Industry Council, the Software Alliance, Centre for Information Policy Leadership, Interactive Advertising Bureau, United States Council for International Business, Computer and Communications Industry Association, Engine), като се съсредоточи върху опита на дружествата, сертифицирани съгласно РЗЛД, по-специално по отношение на процеса на сертифициране, предприетите стъпки за спазване на принципите на РЗЛД, механизмите за разглеждане на искания и жалби от физически лица и др.

[4] Получената обратна информация е достъпна на следния адрес: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-%D0%A0%D0%B0%D0%BC%D0%BA%D0%B0-%D0%B7%D0%B0-%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B0-%D0%BD%D0%B0-%D0%BB%D0%B8%D1%87%D0%BD%D0%B8%D1%82%D0%B5-%D0%B4%D0%B0%D0%BD%D0%BD%D0%B8-%D0%B2-%D0%BE%D1%82%D0%BD%D0%BE%D1%88%D0%B5%D0%BD%D0%B8%D1%8F%D1%82%D0%B0-%D0%BC%D0%B5%D0%B6%D0%B4%D1%83-%D0%95%D0%A1-%D0%B8-%D0%A1%D0%90%D0%A9-%D0%B4%D0%BE%D0%BA%D0%BB%D0%B0%D0%B4-%D0%BD%D0%B0-

На 18 и 19 юли 2024 г. във Вашингтон се проведе среща за преглед. Тя беше открита от европейския комисар по въпросите на правосъдието и потребителите Didier Reynders и министъра на търговията на САЩ Gina Raimondo.[5]

От страна на ЕС прегледът беше извършен от представители на Генерална дирекция „Правосъдие и потребители“ на Европейската комисия, заедно с петима представители, определени от Европейския комитет по защита на данните (ЕКЗД) и представляващи различни национални органи за защита на данните, и Европейския надзорен орган по защита на данните[6]. От страна на САЩ участваха представители на Министерството на търговията (Department of Commerce — DoC), Държавния департамент, Федералната търговска комисия (Federal Trade Commission — FTC), Министерството на транспорта (Department of Transportation — DoT), Службата на директора на Националното разузнаване (Office of the Director of National Intelligence — ODNI), Министерството на правосъдието (Department of Justice — DoJ), главният инспектор на разузнавателната общност, както и членове на Надзорния съвет по въпросите на неприкосновеността на личния живот и гражданските свободи (Privacy and Civil Liberties Oversight Board — PCLOB). По време на съответните сесии за преглед беше предоставена информация и от представители на организации, предлагащи независими услуги за разрешаване на спорове, и на Американската арбитражна асоциация. Освен това за прегледа беше използвана информация от презентации на организации, сертифицирани съгласно РЗЛД, относно начина, по който дружествата спазват изискванията на рамката.

За своите констатации Комисията използва и публично достъпни материали, като например съдебни решения, правила и процедури за прилагане на съответните органи на САЩ, доклади и проучвания на неправителствени организации, доклади за прозрачността, изготвени от дружества, сертифицирани съгласно РЗЛД, годишни доклади на независими надзорни органи, както и медийна информация.

2. КОНСТАТАЦИИ

2.1. Търговски аспекти

2.1.1. Процесът на сертифициране

За да може да получава лични данни, предавани от ЕС въз основа на РЗЛД, дадено американско дружество трябва да се сертифицира към DoC и след това ежегодно да подновява сертифицирането за спазване на специфичните изисквания за защита на

%D0%9A%D0%BE%D0%BC%D0%B8%D1%81%D0%B8%D1%8F%D1%82%D0%B0-%D0%BE%D1%82%D0%BD%D0%BE%D1%81%D0%BD%D0%BE-%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D0%BE%D0%BD%D0%B8%D1%80%D0%B0%D0%BD%D0%B5%D1%82%D0%BE-%D0%BD%D0%B0-%D1%80%D0%B0%D0%BC%D0%BA%D0%B0%D1%82%D0%B0_bg.

[5] Срещата за преглед беше организирана по теми, като всяка специална точка от дневния ред беше представена чрез кратка презентация от съответния орган на САЩ, представител на ЕС или организация, последвана от подробна сесия с въпроси и отговори. В рамките на първия ден бяха обхванати „търговските аспекти“ на рамката (т.е. прилагането и осигуряването на съблюдаването на изискванията, приложими към дружества, сертифицирани съгласно РЗЛД), а въпросите, свързани с достъпа на органи на публичната власт до лични данни, бяха обсъдени на втория ден.

[6] Комисията и представителите на ЕКЗД се срещнаха на 12 юни и 10 юли 2024 г., за да се подготвят за прегледа, да обсъдят получената информация и да определят по отношение на кои аспекти е необходимо допълнително събиране на информация и разяснения.

данните („принципите на РЗЛД”). За сертифицирането е необходимо дружеството да попада в обхвата на правомощията за разследване и правоприлагане на FTC или DoT, да обяви публично ангажимента си да спазва принципите на РЗЛД и да предостави за публичен достъп своята политика за защита на личните данни, както и да изпълнява тези изисквания в пълна степен[7]. Преди да завърши сертифицирането, DoC проверява дали дружеството е изпълнило всички изисквания за сертифициране[8].

На срещата за преглед DoC обясни, че през тази първа година на РЗЛД фокусът е бил върху въвеждането на процеса на сертифициране, включително разработване на специални ИТ инструменти, актуализиране на процедури, комуникация с дружествата и провеждане на други дейности за предоставяне на информация/повишаване на осведомеността. Към датата на срещата за преглед повече от 2 800 дружества са били сертифицирани съгласно РЗЛД. Това означава, че в сравнение с предишната рамка — Щита за личните данни, повече дружества са били сертифицирани съгласно РЗЛД през първата година от нейното функциониране[9]. Съгласно информацията, предоставена от DoC, 70 % от участниците са малки и средни предприятия и много от сертифицираните съгласно РЗЛД дружества (47 %) са в сектора на информационните и комуникационните технологии (ИКТ). Освен това 60 % от дружествата са сертифицирани изключително за данни, които не са свързани с човешките ресурси, 2,5 % са сертифицирани изключително за данни, свързани с човешките ресурси, а 37,5 % са сертифицирани както за данни, свързани с човешките ресурси, така и за други данни.

DoC е въвело необходимите процедури за разглеждане на заявления от страна на дружествата. Дружествата трябва да подадат своите заявления за сертифициране на уебсайта на DoC за РЗЛД (https://www.dataprivacyframework.gov/). Той съдържа информация за това как дадено дружество може да се присъедини към РЗЛД[10], както и за задълженията на дружеството съгласно рамката[11]. Специален екип на DoC, под ръководството на специален директор за Рамката за защита на личните данни, отговаря за всички аспекти, свързани с управлението и администрирането на РЗЛД, включително процеса на сертифициране и наблюдението на спазването. Всяко заявление се възлага на конкретен служител, който отговаря за съответното дружество през целия процес на сертифициране.

За да бъдат сертифицирани съгласно рамката, дружествата подават заявление, включително проект на политика за защита на личните данни. DoC проверява дали той отговаря на съответните изисквания по РЗЛД. Когато дадена организация иска да сертифицира различни субекти в рамките на корпоративна група (напр. различни дъщерни дружества), DoC изисква и преглежда или една цялостна политика за защита на личните данни, в която ясно са посочени всички субекти, които трябва да бъдат обхванати, или отделни политики за всеки субект. Освен това DoC проверява в посочения в заявлението независим механизъм за обжалване (НМО)[12] дали организацията действително се е регистрирала към него. За дружества, които са избрали групата на

[7] Раздел I.2 от приложение I към решението относно адекватното ниво на защита.
[8] Приложение III към решението относно адекватното ниво на защита.
[9] През същия период 2 400 дружества са били сертифицирани по Щита за личните данни.
[10] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931).
[11] https://www.dataprivacyframework.gov/key-requirements
[12] Механизми за разрешаване на спорове в частния сектор, чрез които жалбите и споровете на всяко физическо лице се разследват и разрешават бързо без разходи за лицето.

органите за защита на данните (напр. защото обработват данни, свързани с човешките ресурси), DoC проверява дали дружеството е заплатило необходимите такси, за да се възползва от групата. Когато е необходимо, DoC проверява също дали кандидатът попада в юрисдикцията на FTC или DoT (и следователно има право да се присъедини към РЗЛД).

Ако всички условия са изпълнени, DoC информира организацията, че може да публикува на своя уебсайт своята политика за защита на личните данни, в която се прави позоваване на РЗЛД. След като политиката за защита на личните данни стане публична, DoC потвърждава сертифицирането и включва дружеството в списъка към РЗЛД на своя уебсайт. След датата, на която DoC включи организацията в посочения списък, вече може да се разчита на РЗЛД за получаване на лични данни от ЕС[13].

Както беше обяснено по време на срещата за преглед, проверките, извършени от DoC до момента, са довели до отхвърляне на 33 заявления поради несъответствие с изискванията по РЗЛД. Като цяло DoC работи с дружествата за отстраняване на всички установени проблеми. Когато DoC установи някакви проблеми, то уведомява дружеството, че трябва да ги отстрани и че липсата на отговор в определен срок или неуспешното извършване на самосертифицирането в съответствие с процедурите на DoC ще доведе до това заявлението да се счита за отказано. Ако първоначалното сертифициране не бъде извършено/променено в рамките на 12 месеца, DoC го счита за отказано.

Крайният срок за ежегодното повторно сертифициране за всяко дружество е посочен в списъка към РЗЛД. За да напомни на дружествата за необходимостта да подадат заявление за повторно сертифициране, DoC създаде система с напомняния за предстоящо изтичане на срока на сертификата. Организациите получават напомняне един месец преди крайния срок, след това две седмици и накрая един ден преди него. Организациите, които оставят сертификата си да изтече, се премахват от списъка към РЗЛД. Както е описано в приложение III към решението относно адекватното ниво на защита, DoC разполага със специална секция на уебсайта си, в която са изброени организациите от САЩ, които вече не са активни участници, като се посочват причините (напр. изтичане или оттегляне) съответните дружества да бъдат премахнати от списъка („списък с неактивни участници“). Когато дадена организация е премахната от списъка към РЗЛД, тъй като е допуснала сертификатът ѝ да изтече, DoC се свързва с нея, за да потвърди дали желае да се оттегли или пък възнамерява да се сертифицира повторно и, ако последното е вярно, да провери дали в периода, през който сертификатът е бил изтекъл, организацията е прилагала принципите на РЗЛД по отношение на личните данни, получени съгласно РЗЛД, и да изясни какви стъпки ще предприеме организацията за справяне с неуредените въпроси, които са довели до забавяне на повторното ѝ сертифициране. Когато дадено дружество уведоми DoC, че желае да се оттегли от РЗЛД, DoC изисква от него да потвърди дали ще върне или ще заличи данните, получени съгласно РЗЛД; дали ще ги запази и ще продължи да прилага принципите на РЗЛД към тези данни (което трябва да се потвърждава ежегодно); или дали ще ги запази и ще въведе други мерки за защита (например стандартни договорни клаузи, приети от Европейската комисия).

Обратната информация, получена от търговските асоциации и дружествата, показва, че дружествата, сертифицирани съгласно РЗЛД, са предприели редица стъпки, за да

[13] Раздел I, параграф 3 от приложение I към решението относно адекватното ниво на защита.

гарантират спазването на принципите на РЗЛД. Например, за да спазят *принципа „Защита, прилагане и отговорност за причинени вреди“*, организациите извършват вътрешни проверки, проведени чрез самооценка или чрез външен преглед на спазването. Двата НМО от частния сектор, които участваха в срещата за преглед, обясниха, че предоставят също така услуги за външен преглед на спазването чрез преглед на политиките за защита на личните данни, а един от тези НМО обясни, че освен това предоставя одити и случайни проверки, като се съсредоточава например върху принципите *„Достъп“*, *„Избор“* и *„Последващо предаване“*. Освен това сертифицираните дружества са разработили вътрешни програми за спазването и механизми за надзор, обучили са служители, въвели са механизми, даващи възможност на лицата да упражняват правата си, извършили са оценки на въздействието върху правото на неприкосновеност на личния живот и са направили преглед на съществуващите договори.

2.1.2. Наблюдение на спазването, неверни твърдения за участие и правоприлагане

Съгласно РЗЛД DoC отговаря за наблюдението на спазването на принципите на РЗЛД, като използва различни инструменти, в това число служебни проверки (по собствена инициатива), *ad hoc* проверки на място и въпросници относно спазването. Това включва търсене и разглеждане на неверни твърдения за участие в рамката, например чрез търсене в интернет[14].

За да извършва наблюдение на спазването на принципите от страна на дружествата, сертифицирани съгласно РЗЛД, DoC разчита основно на *ad hoc* търсения в мрежата и проверки в медиите (социалните медии) през последната година. DoC съобщи, че не е открило проблеми във връзка със спазването на принципите на РЗЛД през тази първа година и че не е насочило нито едно дружество към FTC или DoT за евентуални действия по правоприлагане. Освен това е създало специално звено за контакт, за да улесни сътрудничеството с органите за защита на личните данни, както и да получава жалби от лица и насочвания от други органи (напр. ОЗД или FTC). През изминалата година обаче не са получени насочвания или жалби. Докато през тази първа година на функциониране на РЗЛД фокусът беше върху създаването на рамката и процеса на сертифициране, на срещата за преглед DoC обясни, че планира да извършва проверки на спазването чрез автоматизирани средства, така че те да бъдат по-систематични, и че в момента разработва необходимите ИТ инструменти за това.

Комисията признава, че през тази първа година DoC трябваше да съсредоточи усилията си върху създаването на рамката и процеса на сертифициране. Занапред е важно DoC да засили усилията си за наблюдение и проверка на спазването на принципите, което е необходимо, за да се гарантира постоянно високо ниво на спазване на рамката и за да се откриват случаи, при които се налагат по-нататъшни действия по правоприлагане, в това число евентуални неверни твърдения за участие в рамката от страна на дружества. В това отношение Комисията приветства факта, че DoC потвърди намерението си да разработи и използва (автоматизирани) инструменти за по-ефективно и систематично

[14]Вж. приложение III към решението относно адекватното ниво на защита. Например неверни твърдения могат да възникнат, когато дадено дружество твърди, че участва в РЗЛД, а никога не е започвало процеса на сертифициране или пък го е започнало, но не го е завършило, или е позволило сертификатът му да изтече.

идентифициране на проблеми, свързани със спазването и неверни твърдения, и е на мнение, че това следва да бъде част от по-мащабни усилия за по-широко използване на различните инструменти, с които разполага (напр. проверки на място, въпросници за преглед на спазването, искания за информация и т.н.), включително за проверка на спазването на специфични изисквания по РЗЛД[15].

Организациите, сертифицирани съгласно РЗЛД, попадат в юрисдикцията на FTC и DoT. По време на срещата за преглед DoT потвърди, че са въведени всички процеси за предприемане на подходящи действия по правоприлагане. Освен това обясни, че много малко дружества в неговата юрисдикция са се присъединили към РЗЛД (т.е. няколко агенции за продажба на билети, но нито една авиокомпания). FTC потвърди, че систематично проверява за нарушения на РЗЛД при всяко от своите разследвания във връзка със защитата на лични данни. Досега FTC не е получила насочвания от други органи. Получила е няколко жалби, в които става въпрос за РЗЛД, макар че две от тях се отнасят до дружества от „списъка с неактивни участници“, други две са за дружества, които не участват в рамката, а една не се отнася за лични данни, предавани от ЕС. Към момента на изготвяне на настоящия доклад FTC не е издала решения за прилагане на РЗЛД, въпреки че потвърди, че няколко дружества, които са сертифицирани съгласно РЗЛД, понастоящем подлежат на разследване.

Комисията приветства факта, че FTC систематично извършва проверки за нарушения на РЗЛД във всичките си разследвания във връзка с правото на неприкосновеност на личния живот. Тъй като дългосрочната ефективност на РЗЛД зависи от нейното стриктно прилагане, от FTC се очаква да продължи да упражнява разследващите си правомощия съгласно рамката, включително чрез проактивно извършване на проверки, съсредоточени върху спазването на специфични изисквания по РЗЛД и/или върху определени сектори.

2.1.3. Разглеждане на жалби

РЗЛД предоставя на лицата от ЕС различни възможности за обжалване в случаи на неспазване на принципите на РЗЛД от страна на сертифицирани организации[16]. Това включва търсене на решение чрез директен контакт със съответна организация, сертифицирана по РЗЛД, която трябва да предостави отговор на засегнатото лице в рамките на 45 дни. Освен това физическите лица могат да подадат жалба до НМО, определен от съответната организация да разследва и разрешава жалби. В зависимост от обстоятелствата това може да бъде алтернативен орган за разрешаване на спорове или ОЗД[17]. На последно място, в случай че нито едно от другите налични средства за правна защита не е довело до задоволително разрешаване на жалбата на субекта на данните, лицето може да задейства процедура по правно обвързващ арбитраж от панела по РЗЛД като последна възможност.

[15] Например при последващо предаване на данни, като се използва възможността съгласно принцип 3(б) от РЗЛД да се поиска резюме или представително копие на съответните разпоредби за защита на личните данни от договорите за последващо предаване.

[16] Вж. раздел 2.4 от решението относно адекватното ниво на защита.

[17] Организациите, сертифицирани съгласно РЗЛД, са длъжни да сътрудничат при разследването и разрешаването на жалба от ОЗД или когато става въпрос за обработването на данни за ЧР, събрани в рамките на трудово правоотношение, или когато съответната организация доброволно се е подложила на надзор от страна на органите за защита на данните.

2.1.3.1. Разглеждане на жалби от страна на дружества

Отговорите на търговските асоциации и дружествата на въпросниците, изпратени от Комисията, показват, че дружествата, сертифицирани съгласно РЗЛД, са получили много малко или не са получили никакви жалби от физически лица относно неспазване на принципите на РЗЛД. Същевременно дружествата са въвели различни механизми и инструменти, за да дадат възможност на лицата да упражняват правата си и да подават жалби, включително чрез уеб-базирани формуляри, имейл и телефон.

2.1.3.2. *Независими механизми за обжалване (НМО)*

Обратната информация, получена по време на срещата за преглед, и информацията, предоставена от търговските асоциации, показват, че има много малък брой жалби до независимите механизми за обжалване. Избраните от дружествата НМО включват BBB National Programs, JAMS, TRUSTe и VeraSafe. Съгласно РЗЛД от НМО се изисква да публикуват годишен доклад с обобщени статистически данни за използването на техните услуги за разрешаване на спорове. Към момента на приемане на настоящия доклад всички съответни НМО са публикували своите годишни доклади[18].

Освен това на срещата за преглед BBB и VeraSafe направиха подробни презентации за дейността си от миналата година. Те докладваха увеличение на броя на дружествата, които избират техните услуги, спрямо предишните рамки и съобщиха, че са получили няколко жалби, въпреки че по-голямата част от тях не отговарят на условията. Например BBB са получили 87 жалби от лица от ЕС, като само две от тях отговарят на условията за разрешаване. Въпреки че BBB обясни, че жалбите се разглеждат средно за 5 работни дни, тези две жалби в крайна сметка са били приключени поради липса на отговор от лицата. VeraSafe са получили 26 жалби, като шест от тях отговарят на условията за разрешаване. Две от жалбите, които са свързани с искания за достъп и заличаване, са били решени, две продължават да са в ход, а други две са били или оттеглени, или затворени поради липса на отговор от страна на лицата. И двата НМО обясниха, че целта им е да отговарят на жалбите, като използват езика на съответното физическо лице.

Сертифицираните съгласно РЗЛД дружества, които обработват данни за ЧР, предавани от ЕС, трябва да изберат ОЗД от ЕС като свой НМО за тези данни, а за други видове лични данни, предавани въз основа на РЗЛД, те могат доброволно да изберат ОЗД от ЕС като свой НМО. Всъщност към момента на изготвяне на прегледа повече от половината

[18] ANA – https://www.ana.net/content/show/id/accountability-dpf-consumers;
BBB National Programs — https://assets.bbbprograms.org/docs/default-source/eu-privacy-shield/dpf_periodicalreport_072024.pdf; ICDR — AAA — https://go.adr.org/rs/294-SFS-516/images/Data%20Privacy%20Framework%20IRM%20Program%20Report%202023-2024%20FINAL.pdf?version=0;
Insights association — https://www.insightsassociation.org/Portals/INSIGHTS/Insights%20Association%20DPF%20Services%20Program%202024%20Annual%20Report_Final_1.pdf;
JAMS — https://www.jamsadr.com/files/Uploads/Documents/2024-Annual-Report-DPF-Cases.pdf;
Privacy Trust DPF Services — https://privacytrust.com/fserve/PrivacyTrust_Dispute_Resolution_Report_2023_2024.pdf;
TRUSTe Dispute Resolution — https://trustarc.com/wp-content/uploads/2024/07/2024-Independent-Recourse-Mechanism-Annual-Report.pdf;
Verasafe — https://verasafe.com/wp-content/uploads/2020/06/VeraSafe-DPF-Dispute-Resolution-Program-Annual-Report-2024.pdf

дружества, сертифицирани по РЗЛД, са избрали да постъпят по този начин[19], и Комисията приветства това решение. След като беше прието решението относно адекватното ниво на защита, ЕКЗД прие правилника за дейността на „Неформалната група на ОЗД от ЕС“. Групата е компетентна да предоставя правно обвързващи препоръки на организациите в САЩ относно нерешени жалби по РЗЛД от физически лица във връзка с обработването на лични данни, които са били предадени от ЕС съгласно РЗЛД. Съгласно правилника за дейността групата е съставена от един ОЗД, действащ като водещ ОЗД, и други ОЗД, определени за съпроверяващи[20]. Тя предоставя правно обвързващи препоръки в рамките на 60 дни след получаване на жалба по РЗЛД. Освен това ЕКЗД публикува образец на формуляр за подаване на жалби до ОЗД[21], както и „Често задавани въпроси“ за лица[22] и за дружества от ЕС[23] във връзка с РЗЛД. Към момента на прегледа групата не е получила никакви жалби.

2.1.3.3. Механизмът за правно обвързващ арбитраж

Международният център за разрешаване на спорове (ICDR), който е международното подразделение на Американската арбитражна асоциация, беше избран от DoC да администрира механизма за правно обвързващ арбитраж. След приемането на решението относно адекватното ниво на защита DoC, заедно с Комисията, избра 11 арбитри с опит в областта на правото на неприкосновеност на личния живот от различни сфери, включително арбитража, съдебната система, академичните среди и гражданското общество[24]. Освен това бяха приети арбитражните правила[25] за панела по РЗЛД и кодекс за поведение на арбитрите[26], като всички те са достъпни на уебсайта на ICDR. Към момента на изготвяне на прегледа арбитражният механизъм все още не е бил задействан от нито едно лице в ЕС.

2.1.4. Насоки, сътрудничество и повишаване на осведомеността

От влизането в сила на РЗЛД DoC проведе различни дейности за повишаване на осведомеността чрез организиране на пътуващи кампании, уебинари и конференции; събития с търговски асоциации и директно взаимодействие с повече от 3 000 дружества с оглед предоставяне на информация за РЗЛД. Освен това публикува насоки, включително под формата на често задавани въпроси, насочени към физически лица и към предприятия от ЕС и САЩ[27]. На свой ред ЕКЗД разработи формуляри за жалби, както и често задавани въпроси, насочени към физически лица и предприятия.

[19] Малко след датата на провеждане на срещата за преглед на уебсайта на РЗЛД беше посочено, че 1 511 от 2 892 участници са избрали орган за защита на данните от ЕС като механизъм за обжалване.
[20] На 17 април 2024 г. ЕКЗД прие правилника за дейността на „Неформалната група на ОЗД от ЕС“ в съответствие с Рамката за защита на личните данни. Той е достъпен на следния адрес: https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf.
[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_bg.
[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_bg.
[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_bg.
[24] https://go.adr.org/DPF_Arbitrator_Bios.html.
[25] https://go.adr.org/rs/294-SFS-516/images/IC.DR-AAA_EU-US_DPF_AnnexI_Arbitration_Rules.pdf.
[26] https://go.adr.org/rs/294-SFS-516/images/Code_of_Conduct_for_Arbitrators_Appointed_to_EU-US_DPF_AnnexI_Arbitrations.pdf.
[27] Вж. напр. https://www.dataprivacyframework.gov/US-Businesses.

Комисията също публикува въпроси и отговори, както и информационен лист за РЗЛД при приемането на решението относно адекватното ниво на защита[28].

Същевременно на срещата за преглед стана ясно, че е необходима повече работа за повишаване на осведомеността сред физическите лица и предоставяне на насоки на дружествата. Информацията, получена от дружествата и от НМО, както и много ниският брой жалби сочат, че е възможно физическите лица невинаги да са наясно с правата си и/или механизма за упражняването им. По време на срещата за преглед DoC изрази интерес да работи съвместно с ОЗД на ЕС с оглед повишаване на осведомеността относно рамката сред физическите лица в ЕС. Комисията насърчава подобни инициативи и също така предприема стъпки за по-добро информиране на хората, включително чрез предоставяне на допълнителна информация за РЗЛД на своя уебсайт, например чрез включване на връзки и препратки към съответните документи с насоки, приети от ЕКЗД, DoC и други органи на САЩ.

Що се отнася до насоките относно принципите на РЗЛД, по време на срещата за преглед представителите на ЕКЗД се съгласиха да си сътрудничат през следващите месеци, за да предоставят допълнителни разяснения относно понятието „данни, свързани с човешките ресурси“ съгласно РЗЛД и специфичните задължения, които се прилагат за обработката на такива данни. Бяха проучени различни елементи, които да бъдат включени в тези насоки. Например насоките може да се отнасят до определени практически сценарии, при които данните на служителите се обработват съгласно РЗЛД (напр. от доставчик на компютърни услуги „в облак“), и да дават обяснение кои задължения по РЗЛД са целесъобразни при такива сценарии. Освен това в насоките може да се предложи на дружествата, получаващи данни за служители — физически лица от ЕС (без да е задължително да използват тези данни в контекста на трудово правоотношение), да изберат групата на ОЗД като свой НМО. Това би гарантирало, че тези лица могат да се обърнат към орган, който се намира близо до тях и който при необходимост е по-запознат с националните закони, приложими за данните, свързани с човешките ресурси.

Освен това един специфичен аспект, при който изглежда, че би било полезно да има повече насоки (също въз основа на информация, получена от търговските асоциации), се отнася до изискванията по РЗЛД за последващото предаване на данни. DoC посочи също, че би било важно да се проучи дали някои сектори може да имат полза от допълнителни насоки относно прилагането на принципите на РЗЛД към дейностите им, напр. при научните изследвания в областта на здравеопазването и финансовите услуги.

Комисията приветства готовността на двете страни да разработят такива насоки и очаква работата по горепосочените теми да започне скоро.

В по-общ план са създадени няколко механизма за осигуряване на обмен и сътрудничество между органите на САЩ и ОЗД, включително чрез определянето на специални звена за контакт в рамките на FTC и DoC за работа със запитвания и случаи на сезиране от ОЗД.

2.1.5. Съответни промени в правната система на САЩ

Откакто беше прието решението относно адекватното ниво на защита, има редица промени в правната рамка на САЩ в областта на правото на неприкосновеност на личния

[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_bg.

живот. Това включва законодателни, регулаторни и съдебни промени. Като цяло те сочат към повишено сближаване между подходите на ЕС и САЩ към определени предизвикателства във връзка с правото на неприкосновеност на личния живот, включително чрез използването на подобни правни концепции. Някои от тези промени са в ход и ще трябва да бъдат допълнително наблюдавани.

На федерално равнище президентът издаде няколко указа, които са от значение за използването на лични данни. По-специално с Указ 14117 от 28 февруари 2024 г.[29] се забраняват или ограничават сделките, включващи определени категории чувствителни лични данни (напр. здравни данни, биометрични идентификатори, човешки геномни данни), със субекти в някои „будещи загриженост държави "[30]. С този указ на главния прокурор се възлага да предложи наредби с оглед конкретизиране на неговото прилагане, които към момента на приемане на настоящия доклад все още не бяха приети. Освен това с Изпълнителен указ 14110 от 30 октомври 2023 г. относно изкуствения интелект[31] се поставя акцент върху разработването на безопасен, защитен и надежден изкуствен интелект. Съгласно този указ няколко федерални агенции трябва да разработят стандарти и насоки за безопасност, свързани с ИИ, включително относно специфични свързани с ИИ рискове по отношение на правото на неприкосновеност на личния живот и техники за неговото опазване.

По отношение на законодателната работа през последните години в Конгреса бяха внесени федерални законопроекти във връзка с правото на неприкосновеност на личния живот, а към юли 2024 г. 20 щата на САЩ са приели подробни закони за неприкосновеността на личния живот, от които осем са влезли в сила: Калифорния, Колорадо, Орегон, Вирджиния, Кънектикът, Юта, Тексас и Флорида. Освен това 17 щата на САЩ са приели законодателство, насочено към автоматизираната обработка на лични данни (или поне някои нейни форми), с което като цяло се дава възможност за отказ от определени видове вземане на решения въз основа на „профилиране"[32].

---

[29] https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

[30] Както бе предложено от главния прокурор в предварително известие за предложено нормотворчество, издадено на 3 май 2024 г., тези държави включват Китай, Куба, Хонконг и Макао, Иран, Северна Корея и Венесуела. Вж. https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and

[31] https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[32] Въпреки че между различните държави има разлики в значението на понятието „профилиране", то обикновено се определя като всяка форма на автоматизирано обработване на лични данни с цел да се оценят, анализират или предскажат лични аспекти, свързани с икономическото състояние, здравето, личните предпочитания, интересите, надеждността, поведението, местоположението или движенията на дадено идентифицирано или идентифицируемо физическо лице. Обикновено потребителите могат да се откажат от профилиране. Следните щати са разработили законодателство относно профилирането: Колорадо (Colo. Rev. Stat. Ann. § 6-1-1306), Кънектикът (Conn. Gen. Stat. Ann. § 42-518), Делауеър (Del. Code Ann. tit. 6, § 12D-104), Флорида (Fla. Stat. Ann. § 501.705), Индиана (Ind. Code Ann. § 24-15-3-1), Кентъки (Ky. Rev. Stat. Ann. § 367.3615), Мериленд (Maryland Online Data Privacy Act of 2024, влязъл в сила на 9 май 2024 г.), Минесота (Minn. Stat. Ann. § 325O.07), Монтана (Mont. Code Ann. § 30-14-2808), Небраска (Neb. Rev. Stat. Ann. § 87-1107), Ню Хемпшир (N.H. Rev. Stat. Ann. § 507-H:4), Ню Джърси (N.J. Stat. Ann. § 56:8-166.8), Орегон (Or. Rev. Stat. Ann. § 646A.574), Роуд Айланд (Rhode Island Data Transparency and Privacy Protection Act, влязъл в сила на 29 юни 2024 г.), Тенеси (Tenn. Code Ann. § 47-18-3304), Тексас (Tex. Bus. & Com. Code Ann. § 541.051) и Вирджиния (Va. Code Ann. § 59.1-577).

По отношение на развитието на съдебната практика няколко представители на гражданското общество посочиха неотдавнашното решение на Върховния съд по делото *Loper Bright Enterprises v. Raimondo* (от 28 юни 2024 г.). С това решение се отменя предишната съдебна практика относно доктрината *Chevron*, съгласно която съдилищата прилагат принципа на зачитане на разумното тълкуване на закона от страна на регулаторната агенция в случай на неяснота в закон, прилаган от тази агенция. По-специално някои неправителствени организации изразиха загриженост относно въздействието на това решение на Върховния съд върху правомощията на FTC за създаване на правила в областта на правото на неприкосновеност на личния живот, като същевременно признаха, че е възможно то да няма никакво въздействие или да има само ограничено въздействие върху нейните правомощия за правоприлагане. На срещата за преглед FTC информира, че все още е рано да се установят точните последици от това решение. Същевременно тя обясни, че регулаторните правомощия на FTC съгласно Закона за Федералната търговска комисия се различават от тези на други административни агенции и за тях доктрината *Chevron* е по-малко релевантна. Следователно това неотдавнашно решение може да има само ограничено въздействие в тази област.

Освен това FTC информира за последните промени в своя подход към автоматизираното обработване на лични данни и изкуствения интелект. Това включва приемането на съвместно изявление заедно с други правоприлагащи органи срещу дискриминацията и предубежденията в автоматизираните системи[33], както и няколко действия за правоприлагане, при които FTC се съсредоточи, наред с други неща, върху прозрачността, справедливостта на автоматизираната обработка и способността на лицата да оспорват резултатите. Най-значимият случай в това отношение е решението на FTC срещу *Rite Aid* от март 2024 г., с което беше наложена 5-годишна забрана върху използването на технология за лицево разпознаване за целите на сигурността от това дружество[34]. По-специално FTC установи, че *Rite Aid* не е предприело разумни мерки за предотвратяване на грешни резултати и за информиране на потребителите за използваната технология. По-общо на срещата за преглед FTC разгледа текущите си приоритети и по-специално областите, при които според нея е необходим по-проактивен подход към правоприлагането в бъдеще. Това включва защитата на чувствителни лични данни (напр. здравни данни, биометрични данни, геолокация)[35], защитата на деца[36] и ненавършилите пълнолетие в онлайн пространството и сигурността на данните[37].

---

[33] https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

[34] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v.

[35] Вж. напр. неотдавнашните решения на FTC срещу X-Mode за продажба и споделяне на чувствителна информация за местоположение (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) и срещу Monument относно разкриването на чувствителни здравни данни на трети страни за маркетингови цели (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] Например FTC наскоро обяви разследване, което доведе до съдебно дело срещу TikTok и неговото дружество майка Bytedance за предполагаемо нарушаване на закона за правото на неприкосновеност на личния живот на децата. Твърди се, че и двете дружества не са спазили изискването за уведомяване а родителите и получаване на родителско съгласие преди събирането и използването на лични данни на деца на възраст под 13 години (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

[37] Вж. преглед на последните дейности по правоприлагане в актуализацията на FTC по отношение на правото на неприкосновеност на личния живот и сигурността на данните за 2023 г.: https://ec.europa.eu/commission/presscorner/detail/bg/mex_24_1307.

Комисията ще продължи да следи отблизо тези и други промени в САЩ, по-специално всички по-нататъшни стъпки към цялостен федерален закон за правото на неприкосновеност на личния живот и възможното въздействие на неотдавнашната съдебна практика на Върховния съд върху ролята на FTC в областта на неприкосновеността на личния живот.

Комисията приветства информацията, предоставена от FTC относно неотдавнашните ѝ дейности по правоприлагане и настоящите приоритети, които до голяма степен съответстват на тенденциите и приоритетите в правоприлагането в областта на защитата на личните данни в Европа. FTC участва активно и в мрежата от държави, които имат ползи от решението на ЕС относно адекватното ниво на защита, стартирана от Комисията през март 2024 г.[38] Това засилено сближаване следва да насърчи и улесни по-тясното сътрудничество между органите за защита на личните данни от двете страни на Атлантическия океан, по-специално по въпроси, свързани с функционирането на РЗЛД.

2.2. Аспекти, свързани с достъпа и използването на лични данни, предадени съгласно Рамката за защита на личните данни в отношенията между ЕС и САЩ, от страна на публични органи на САЩ

Решението относно адекватното ниво на защита включва подробна оценка на правилата, уреждащи събирането и използването на лични данни, предавани от ЕС към дружества, сертифицирани съгласно РЗЛД, от страна на публични органи на САЩ, по-специално за целите на наказателното правоприлагане и националната сигурност. Както беше потвърдено от органите на САЩ по време на срещата за преглед, след приемането на решението относно адекватното ниво на защита през първата година на функциониране на РЗЛД не е имало съответни промени в правната рамка, която се прилага за достъпа до данни за целите на правоприлагането или за регулаторни цели. Поради тази причина констатациите по-долу се отнасят само за промените в областта на националната сигурност.

Заключенията, направени в решението относно адекватното ниво на защита по отношение на достъпа до данни от страна на разузнавателните агенции, се основават на анализа на условията и ограниченията, приложими към операциите за радиоелектронно разузнаване съгласно няколко съответни правни акта, по-специално раздел 702 от Закона за упражняване на надзор върху външното разузнаване (FISA) и Указ 12333[39], допълнен и подсилен от Указ 14086 за засилване на защитните мерки за дейностите по радиоелектронно разузнаване на САЩ (Указ 14086), приет от президента на САЩ на 7 октомври 2022 г. Предпазните мерки, посочени в Указ 14086, се прилагат за всички дейности на САЩ по радиоелектронно разузнаване, независимо от правните основания, на които се основават тези дейности, и мястото, където се извършват, и защитават

[38] Вж. https://ec.europa.eu/commission/presscorner/detail/bg/mex_24_1307. В резултат на срещата през март 2024 г. беше решено да се проведат поредица от тематични сесии. Първата от тях се проведе през юли 2024 г. и беше съсредоточена върху разработването на инструменти, с които може да се подкрепят малките и средните предприятия да спазват законите в областта на правото на неприкосновеност на личния живот.

[39] Други мерки, които могат да бъдат предприети съгласно FISA по отношение на данни, предадени от ЕС, включват индивидуално електронно наблюдение (раздел 105 от FISA), физическо претърсване (раздел 302 от FISA), използване на устройства за регистриране и проследяване (раздел 402 от FISA) и събиране на търговска информация от определени дружества (обществени превозвачи, обекти за обществено настаняване, обекти за отдаване под наем на превозни средства или физически съоръжения за складиране, раздел 501 от FISA). Тези различни правни основания са анализирани подробно в решението относно адекватното ниво на защита (съображения 142—152).

данните на лицата, които не са граждани на САЩ (в това число европейци)[40]. Освен това с Указ 14086 беше създаден нов механизъм за правна защита, чрез който тези правно обвързващи предпазни мерки могат да бъдат използвани и прилагани от физически лица в ЕС.

В следващите раздели се описват стъпките, предприети от органите на САЩ с оглед спазване на Указ 14086 след приемането на решението относно адекватното ниво на защита, както и съответните промени във връзка с гореспоменатата правна рамка.

2.2.1. Съответни промени по отношение на правната рамка на САЩ

2.2.1.1. Прилагане на Указ 14086 от разузнавателните агенции

Въведените с Указ 14086 ограничения и гаранции допълват тези, предвидени в член 702 от FISA и Указ 12333. Те са задължителни за всички разузнавателни агенции и бяха приведени в действие чрез политики и процедури, приети от всяка агенция.

Като част от първия преглед органите на САЩ потвърдиха, че не са внасяни промени в Указ 14086 след приемането му. Освен това беше изяснено, че президентът на САЩ не е използвал правомощията си за актуализиране на списъка на законните цели, за които може да се използва радиоелектронно разузнаване, или списъка с целите, за които могат да се използват събраните масиви от данни, предвидени в раздели 2(b)(i)(B) и 2(b)(ii)(C) от Указ 14086[41]. С Указ 14086 беше въведена специфична процедура за определяне на по-конкретни приоритети на разузнаването, за които действително може да се събира информация чрез радиоелектронно разузнаване. По-специално трябва да се направи консултация със служителя по защита на гражданските свободи към Службата на директора на Националното разузнаване (CLPO към ODNI), за да се прецени за всеки приоритет дали 1) служи за постигане на една или повече законни цели, посочени в указа; 2) не е разработен с цел събиране на информация чрез радиоелектронно разузнаване за забранена цел, посочена в указа, нито се очаква да доведе до това, и 3) е определен, след като надлежно са взети предвид правото на неприкосновеност на личния живот и гражданските свободи на всички физически лица[42]. По време на срещата за преглед CLPO към ODNI потвърди, че е прегледала приоритетите, предложени от директора на Националното разузнаване в рамката за приоритети на националното разузнаване за 2023 г., заключи, че те отговарят на горните изисквания, и сподели заключението си с директора на Националното разузнаване, който от своя страна представи приоритетите за утвърждаване от страна на президента. Освен това CLPO към ODNI проведе обучение относно изискванията съгласно Указ 14086 за членове на разузнавателната общност, които участваха в разработването на приоритетите в областта на разузнаването.

Освен това през изминалата година органите на САЩ предприеха допълнителни практически стъпки за прилагане на Указ 14086 във всекидневната си работа. По-специално разузнавателните агенции са въвели допълнителни вътрешни политики и насоки относно прилагането на указа, например вътрешни процеси (чрез вътрешни

[40] За допълнителна информация вж. раздел 3.2.1.2 от решението относно адекватното ниво на защита.

[41] Тези законни цели включват например защита срещу шпионаж, саботаж или убийство или други разузнавателни дейности, извършвани от чуждо правителство, организация или лице или от тяхно име или с тяхна помощ; защита срещу тероризъм, вземане на заложници и задържане на лица в плен, извършвано от чуждо правителство, организация или лице или от тяхно име или с тяхна помощ.

[42] Член 2(b)(iii) от Указ 14086.

изисквания за разрешение, документиран контрол на достъпа, така че само лицата, които са били надлежно обучени и отговарят на необходимите изисквания за мисията, да имат достъп до информацията и др.), за да се гарантира, че изискванията за необходимост и пропорционалност са спазени в контекста както на целенасоченото събиране, така и на събирането на масиви от данни[43]. Освен това е проведено обучение по Указ 14086 на служители на различни разузнавателни агенции (напр. АНС, ЦРУ, ФБР), в това число годишни и *ad hoc* обучителни сесии, организирани от CLPO към ODNI, и задължителни обучения за всички нови служители, които се присъединяват към ODNI.

Комисията приветства различните мерки, въведени за прилагане и гарантиране на спазването на Указ 14086. С натрупването на повече опит при практическото прилагане на предпазните мерки по указа Комисията би оценила възможността да обсъди конкретни примери за това как указът се прилага на практика (при спазване на приложимите съображения за поверителност) в рамките на бъдещи прегледи.

2.2.1.2. Повторно разрешение съгласно раздел 702 от FISA

Раздел 702 от FISA позволява за обект на разследване да се определят лица, които не са граждани на САЩ и за които има разумни основания да се счита, че са с местонахождение извън САЩ, с цел събиране на външноразузнавателна информация. Придобиването на информацията се извършва въз основа на годишни сертификати, представени и одобрени от Съда по надзора върху външното разузнаване (FISC). В тези сертификати се посочват конкретни категории външноразузнавателни данни, които трябва да бъдат събрани. На 21 юли 2023 г. ODNI обяви, че има три одобрени сертификата съгласно раздел 702 от FISA, обхващащи следните категории в областта на външното разузнаване: 1) чужди правителства и свързани образувания, 2) борба с тероризма и 3) борба с разпространението[44]. Освен това сертификатите трябва да включват процедури за насочване и минимизиране, които са одобрени от FISC[45]. По-специално насочването се извършва чрез искане американските дружества, попадащи в обхвата на определението на FISA за „доставчик на електронни съобщителни услуги“, да разкриват електронни данни за съобщения, изпратени до или от определени „селектори“, чрез които се идентифицира конкретен профил в съобщително средство, напр. телефонен номер или имейл адрес. Правителството на САЩ публикува редица материали относно раздел 702 от FISA, за да информира обществеността за функционирането на програмите за надзор, приложимите изисквания и защитата на правото на неприкосновеност на личния живот, както и ролята на FISC[46].

Съгласно клаузата за прекратяване на действието срокът на действие на раздел 702 от FISA трябваше да изтече в края на 2023 г., освен ако Конгресът не даде повторно разрешение. След като даде временно повторно разрешение без никакви промени, на 19 април 2024 г. Конгресът прие Закона за реформиране на разузнаването и за

[43] Вж. https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguardsin-executive-order-14086, публикувани на 3 юли 2023 г.

[44] https://www.intelligence.gov/ic-on-the-record-database/results/1307-release-of-documents-related-to-the-2023-fisa-section-702-certifications.

[45] С тези процедури се ограничава събирането на данни по отношение на конкретна цел на външното разузнаване, ограничава се достъпът до бази данни, в които се съхранява информация, придобита съгласно раздел 702 от FISA (включително чрез контрол на достъпа), и се налагат ограничения върху използването, запазването и разпространението на такава информация.

[46] https://www.intel.gov/foreign-intelligence-surveillance-act.

гарантиране на сигурността на Америка (Reforming Intelligence and Securing America Act — RISAA), с който беше дадено разрешение за подновяване на действието на раздел 702 от FISA за период от 2 години и бяха въведени няколко промени. Най-общо мерките могат да бъдат разделени на две категории: 1) промени в обхвата на дейностите по наблюдение, разрешени съгласно раздел 702 от FISA, и 2) институционални и процедурни промени.

Промени в обхвата на дейностите по наблюдение, разрешени съгласно раздел 702 от FISA

С RISAA бяха въведени три основни промени в обхвата на дейностите по наблюдение, които могат да се извършват съгласно раздел 702 от FISA.

На първо място, окончателно се забранява събирането на информация от вида „относно“[47]. Това се отнася до събирането на съобщения, в които селекторът съгласно раздел 702 (напр. имейл адрес) не попада в графа „до“ или „от“ на съобщението, а по-скоро съдържа препратка към този селектор в самото съобщение (напр. имейл съобщения, които не са изпратени до или от избрания имейл адрес, но съдържат избрания имейл адрес в текста на имейла). Въпреки че такова събиране на информация беше изключено още през 2018 г. след изменение на FISA, FISA продължаваше да дава възможност за повторно започване на събирането на информация от вида „относно“ в бъдеще след специална процедура за получаване на разрешение, включваща FISC и Конгреса. С последното изменение, въведено чрез RISAA, тази възможност беше премахната.

На второ място, определението за външноразузнавателна информация е разширено, за да включва информация, свързана с борбата с разпространението на наркотици[48]. По време на срещата за преглед органите на САЩ обясниха, че тази промяна беше въведена с оглед на текущата криза с фентанила и нарастващата заплаха за националната сигурност от международни трафиканти и производители на наркотици. В този контекст беше потвърдено, че това понятие попада в рамките на няколко от законните цели, посочени в Указ 14086, т.е. разбиране или оценка на способностите, намеренията или дейностите на чужди организации, които представляват текуща или потенциална заплаха за националната сигурност на САЩ или техните съюзници; разбиране или оценка на транснационални заплахи, които оказват влияние върху глобалната сигурност, в това число рискове за общественото здраве; и защита срещу транснационални престъпни заплахи[49].

На трето място, с RISAA беше разширено определението за „доставчик на електронни съобщителни услуги“ (electronic communication service provider — ECSP), като по този начин беше разширен обхватът на дружествата, които могат да бъдат принудени да предоставят информация съгласно раздел 702 от FISA[50]. Определението вече включва и други доставчици на услуги, които имат „достъп до оборудване, което се използва или може да се използва за предаване или съхраняване на съобщения, предавани по кабелен път, или електронни съобщения“, като от него изрично са изключени обектите за обществено настаняване, жилищата, обществените съоръжения и заведенията за

[47] Раздел 22 от RISAA.
[48] Раздел 23 от RISAA.
[49] Раздел 2(b)(ii)(A)(2), (3) и (10) от Указ 14086.
[50] Раздел 25 от RISAA.

хранене. В писмо до Конгреса DoJ посочи, че това изменение е техническа промяна, с която се цели да се обхванат „изключително малък“ брой технологични дружества, които съгласно последните решения на FISC и Апелативния съд за надзор на външното разузнаване (Foreign Intelligence Surveillance Court of Review — FISCR) не са попадали в обхвата на предишното определение за ECSP[51]. В същото писмо DoJ се ангажира да ограничи обхвата на определението, като го прилага изключително с цел да обхване типа доставчици на услуги, разглеждан в съдебния спор, довел до решението на FISC. В резултат на това съответните дружества са посочени в класифицирано приложение за Конгреса. Няколко неправителствени организации, включително тези, които дадоха обратна информация като част от прегледа, изразиха загриженост относно това разширяване на обхвата на определението, като се аргументираха, че то потенциално може да включва много дружества в САЩ (тъй като много от тях предоставят някакъв вид услуга и имат достъп до оборудване за предаване на съобщения). Предвид тези опасения с подкрепата на разузнавателната общност беше предложено допълнително изменение чрез законопроект за разрешение на разузнаването за фискалната 2025 г., който в момента се разглежда от Конгреса. В случай че бъде приета от Конгреса, тази промяна ще гарантира, че новите дружества, обхванати от определението за ECSP, ще бъдат само тези, които са посочени в гореспоменатите решения на FISC. Законопроектът също предвижда всяка директива, насочена към такова дружество, да бъде докладвана на FISC, за да се даде възможност на съда да прецени дали дружеството наистина попада в обхвата на определението. В писмото си до Конгреса DoJ се ангажира да докладва на Конгреса на всеки шест месеца относно всеки случай, в който се прилага актуализираното определение, за да даде възможност на Конгреса да упражни подходящия надзор по отношение на тясното прилагане на определението.

Важно е да се отбележи, че на срещата за преглед органите на САЩ и PCLOB потвърдиха, че всички предпазни мерки на Указ 14086 продължават да се прилагат изцяло за всяко събиране и използване на данни съгласно раздел 702 от FISA, включително след тези изменения. По този начин, макар и RISAA донякъде да разширява обхвата на дружествата, които могат да станат обект на решение от съда, с него не се ограничава възможността за упражняване на правата. Независимо от това ще бъде важно да се наблюдава по-нататъшното развитие (в областта на законодателството и докладването) и да се получава информация относно прилагането на тези нови правила в практиката. Това включва например въздействието на разширяването на определенията за външно разузнаване и ECSP върху броя на целите съгласно раздел 702 от FISA (както се съобщава ежегодно от ODNI, вж. информацията по-долу относно прозрачността). Предстоящият последващ доклад относно след последния доклад на PCLOB относно раздел 702 от FISA (вж. по-долу) следва да бъде особено информативен в това отношение.

Институционални и процедурни промени

По отношение на институционалните и процедурните промени в RISAA бяха вписани няколко процедури, които вече се следват в практиката, и бяха въведени нови предпазни мерки. Макар и някои от промените да се отнасят само за лица, които са граждани на

[51] https://www.justice.gov/opa/media/1348621/dl?inline. Вж. решението на FISC от 2022 г. (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) и решението на Апелативния съд за надзор на външното разузнаване, с което се потвърждава това решение (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

САЩ, с някои от тях се засилва защитата както за лица, които са граждани САЩ, така и за лица, които не са граждани на САЩ, чиито данни може да се събират съгласно раздел 702 от FISA[52] и следователно са от значение за функционирането на РЗЛД.

На първо място, бяха въведени редица допълнителни изисквания за отчетност, надзор и докладване. По-специално персоналът на ФБР понастоящем трябва да бъде обучаван ежегодно относно приложимите правила за търсене на информация, получена съгласно раздел 702 от FISA[53]. От ФБР също се изисква да докладва на Конгреса за дейностите си по търсене на информация (напр. броя на запитванията, при които са използвани „партидни технологии“, т.е. прилагане на множество термини като част от една заявка) и за мерките за отчетност, въведени с цел да се гарантира спазването на правните изисквания за търсене (раздели 11 и 12 от RISAA). Освен това на главния инспектор на DoJ е възложено да изготви доклад относно спазването на изискванията за търсене на информация от страна на ФБР (раздел 9 от RISAA). В по-общ план, за да се увеличи прозрачността на процедурите пред FISC, понастоящем ODNI и главният прокурор трябва да извършат преглед за разсекретяване на решенията на FISC в рамките на 180 дни (раздел 7 от RISAA). Също така преписите от всички изслушвания пред FISC и Апелативния съд за надзор на външното разузнаване (FISCR, като решенията на FISC могат да бъдат обжалвани) трябва да се съхраняват и предават на Конгреса (раздел 8 от RISAA).

На второ място, с RISAA бяха въведени допълнителни ограничения върху използването на данни, събрани съгласно раздел 702 от FISA, от страна на ФБР. Раздел 2(г) от RISAA предвижда, че запитване, при което се използва „партидна технология“, може да бъде направено само след получаване на одобрение от адвокат във ФБР, освен ако не са налице извънредни обстоятелства. Освен това на ФБР вече е забранено автоматично да проверява неминимизирана информация, придобита съгласно раздел 702 от FISA, а вместо това бюрото трябва да гарантира, че е необходимо анализаторите изрично да изберат търсене в тази информация. С RISAA също така беше забранено на ФБР да прави запитвания, чиято единствена цел е намирането и извличането на доказателства за престъпна дейност (освен ако има основателна увереност, че това може да спомогне за смекчаване или премахване на заплаха за живота или сериозни телесни повреди, или когато това е необходимо, за да се спазят задълженията за разкриване на информация при съдебни спорове)[54]. Освен това на ФБР е забранено да включва неминимизирани данни в аналитични хранилища, освен ако целевото лице не е от значение за съществуващо разследване в областта на националната сигурност[55].

[52] Освен това с RISAA бяха въведени някои промени по отношение на традиционното индивидуално електронно наблюдение съгласно раздел 105 от FISA (въз основа на издадена заповед на FISC, при условие че е изпълнен определен стандарт за обосновано предположение). При заявление от страна на разузнавателна агенция до главния прокурор за решение за провеждане на индивидуално електронно наблюдение вече се изисква клетвена декларация, обосноваваща убеждението, че са изпълнени условията съгласно раздел 105 от FISA (раздел 6(а) от RISAA). Възможната продължителност на електронното наблюдение по отношение на чужди сили или агенти на чужди сили е удължена от 120 дни на 1 година (раздел 6(ж) от RISAA).

[53] Раздел 2(г) от RISAA.

[54] Раздел 3(а) от RISAA.

[55] Раздел 3(б) от RISAA. При необходимост поради извънредни обстоятелства директорът на ФБР може да вземе решение за изключване от обхвата на тази разпоредба, за което трябва да уведоми Конгреса.

На трето място, бяха променени някои разпоредби, свързани със статута и ролята на *amici curiae* пред FISC[56]. *Amici* се определят като експерти, които подпомагат съда (и FISCR) по въпроси, свързани с правото на неприкосновеност на личния живот и гражданските свободи, или помагат за изясняване на технологични въпроси при работата с приложение на конкретно правителството. Докато преди съгласно FISA от *amici* се изискваше да имат опит в областта на правото на неприкосновеност на личния живот и гражданските свободи, събирането на разузнавателна информация, комуникационните технологии или други подходящи области, сега по принцип се изисква опит в правото на неприкосновеност на личния живот/гражданските свободи и събирането на разузнавателна информация. И досега съдът можеше да определя *amicus* винаги, когато счете за подходящо, и беше длъжен да го направи, когато става въпрос за ново или значително тълкуване на закона. След повторното разрешение FISC вече е длъжен да определя *amicus* винаги, когато от него се иска да одобри сертификати по раздел 702 от FISA и съпътстващи процедури (напр. процедури по целево събиране), освен ако не установи, че това не е подходящо или вероятно ще доведе до ненужно забавяне[57]. Освен това, вместо да определи само един *amicus*, понастоящем съдът може да реши да определи един или повече *amici*. Също така се пояснява, че информацията, предоставена от *amici*, трябва да бъде „ограничена до разглеждане на конкретните въпроси, идентифицирани от съда“, въпреки че областите, в които *amici* могат да се изказват, продължават да бъдат широки (т.е. правни аргументи и информация, свързана със защитата на правото на неприкосновеност на личния живот и гражданските свободи на лицата, граждани на Съединените щати, събирането на разузнавателна информация и комуникационните технологии или всяка друга подходяща област).

На последно място, съгласно раздел 18 от RISAA се създава Комисия за реформиране на FISA — състояща се между другото от членове на Конгреса, председателя на PCLOB, главния заместник-директор на Националното разузнаване и заместник-главния прокурор, както и допълнителни членове, които се назначават от Конгреса[58] — която да препоръчва допълнителни реформи на FISA.

Комисията ще следи отблизо по-нататъшното развитие във връзка с раздел 702 от FISA, включително в контекста на надзорните дейности на PCLOB (вж. по-долу), работата на Комисията за реформиране и предстоящия преглед на FISA след 2 години.

2.2.1.3. Дейности по наблюдение на практика: цифри и тенденции

Годишният статистически доклад за прозрачност на ODNI относно използването на органите за наблюдение на националната сигурност от страна на разузнавателната общност за календарната 2023 г. (публикуван през април 2024 г.)[59] показва, че броят на целите съгласно раздел 702 от FISA се е увеличил от 245 073 през календарната 2022 г. на 268 590 през календарната 2023 г. В доклада се обяснява, че разликите в броя на целите може да са свързани с различни причини, включително промени в оперативните приоритети, събития на световната сцена, техническите възможности, поведението на целите и промени в телекомуникационния сектор. Освен това в доклада се посочва, че

[56] От съображения за яснота тези изменения не засягат статута и ролята на специалните адвокати пред Апелативния съд в областта на защитата на личните данни (Data Protection Review Court — DPRC), както беше потвърдено от САЩ на срещата за преглед.
[57] Раздел 5(б) от RISAA.
[58] Съгласно раздел 18 изрично се изисква да има представители, които не са от Конгреса.
[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.

нито едно лице, което не е гражданин на САЩ (в сравнение с 1 лице през 2021 г. и 0 лица през 2022 г.), не е било цел на наблюдение съгласно раздел 402 от FISA (устройства за регистриране или проследяване), а съгласно раздел 501 от FISA (достъп до търговска информация на предоставящи общи превози превозвачи, обекти за отдаване под наем на превозни средства или физически съоръжения за складиране) бяха издадени шест решения (в сравнение с 11 решения през 2021 г. и 2022 г.) за шест цели (в сравнение с 13 през 2021 г. и 11 през 2022 г.), обхващащи 5 412 уникални идентификатора (в сравнение с 23 157 през 2021 г. и 55 431 през 2022 г.), използвани за предаване на информация, събрана съгласно такива решения.

Годишният доклад на DoJ за Закона за упражняване на надзор върху външното разузнаване към Конгреса показва, че през календарната 2023 г. към FISC са подадени 327 заявления за извършване на електронно наблюдение и/или физическо претърсване за целите на външното разузнаване съгласно раздел 105 и раздел 302 от FISA съответно[60]. Общият брой на лицата, които са били цел на наблюдение, е между 500 и 999.

Що се отнася до писмата във връзка с националната сигурност, в доклада се посочва, че са подадени 10 115 искания за информация за лица, които не са граждани на САЩ (което не включва искания изключително за информация за абонатите), с които е била искана информация, отнасяща се до 3 033 различни лица, които не са граждани на САЩ[61].

Няколко сертифицирани съгласно РЗЛД дружества (напр. Google и Meta) се възползват от предоставената от законодателството на САЩ възможност за публикуване на отчети за прозрачност, с които информират за броя на исканията за информация по FISA и чрез писма във връзка с националната сигурност, които са получили през даден период на докладване. Към момента на изготвяне на настоящия доклад статистическите данни за исканията за информация по FISA, получени след юли 2023 г. все още не бяха налични. Google например съобщи, че между юли и декември 2023 г. е получил между 500 и 999 искания за информация чрез писма във връзка с националната сигурност, засягащи между 2 000 и 2 499 профила[62]. Meta съобщи, че през същия период на докладване е получило между 0 и 499 искания за информация чрез писма във връзка с националната сигурност, засягащи между 500 и 999 акаунта[63]. През последните години броят им остава относително стабилен. За да засилят още повече прозрачността, някои дружества (напр. Google) проактивно публикуват писмата във връзка с националната сигурност, които са получили, след като бъдат премахнати ограниченията по отношение на разкриването на информация[64].

2.2.1.4. Други области на развитие

[60] https://www.justice.gov/nsd/media/1350236/dl?inline.

[61] Тези цифри са до голяма степен непроменени спрямо предходната година на докладване (2022 г.). За сравнение през 2022 г. е имало 317 окончателни заявления към FISC за извършване на електронно наблюдение и/или физическо претърсване за целите на външното разузнаване. Общият брой на лицата, за които са издадени решения за електронно наблюдение, е между 0 и 499. ФБР подаде 9 103 искания за информация чрез писма във връзка с националната сигурност за лица извън САЩ през 2022 г. (с изключение на искания за информация само за абонати). Източник: https://irp.fas.org/agency/doj/fisa/2022rept.pdf

[62] https://transparencyreport.google.com/user-data/us-national-security.

[63] https://transparency.meta.com/reports/government-data-requests/country/US/.

[64] https://transparencyreport.google.com/user-data/us-national-security.

В контекста на подготовката на прегледа няколко неправителствени организации повдигнаха въпроси относно новите форми на придобиване на данни от страна на разузнавателните агенции на САЩ чрез закупуване на данни от търговски субекти, по-специално от брокери на данни. Те обясниха, че макар и събраните по този начин данни все пак да трябва да се обработват в съответствие с други изисквания, в това число например Указ 12333[65], това придобиване се извършва извън рамката на FISA и Указ 14086.

В това отношение следва да се припомни, че всеки вид доброволно споделяне на данни с трети страни е предмет на няколко подробни условия съгласно РЗЛД. На първо място, сертифицираната организация не може да споделя данни с трета страна (която не действа като представител/обработващ лични данни), без да уведоми съответните лица и да им даде възможност за избор[66]. На второ място, в съответствие с принципа за отчетност за последващо предаване, последващо предаване може да се извършва само 1) за ограничени и конкретни цели, 2) въз основа на договор между сертифицирана по РЗЛД организация и третата страна и 3) само ако този договор изисква третата страна да осигури същото ниво на защита като гарантираното ниво на защита съгласно принципите на рамката[67].

Освен това, както беше обсъдено по време на срещата за преглед, FTC е предприела принудителни действия срещу брокери на данни, продаващи чувствителни данни на потребители. Например в дело срещу *X-Mode* и неговия правоприемник *Outlogic* на 9 януари 2024 г. FTC прие решение, с което на дружеството се забранява да продава данни за геолокация на трети страни и се задължава да изтрие данните, които е използвал и споделял незаконно. По време на разследването FTC установи, наред с други неща, че дружеството не е предоставило пълна информация на физическите лица за използването и продажбата на техните данни за геолокация, не е въвело мерки, даващи възможност на лицата да откажат проследяване, позволило е данните да бъдат използвани за потенциално дискриминационни цели и не е поставило ограничения за използването на тази информация от трети страни[68]. Комисията очаква същият подход да бъде възприет от FTC , ако сертифицирани съгласно РЗЛД дружества споделят данни в нарушение на гореспоменатите разпоредби.

На последно място, важно е да се спомене, че през май 2024 г. ODNI издаде Рамка на политиката на разузнавателната общност за информацията, налична на пазара[69]. С тази рамка се определят редица принципи и изисквания, които разузнавателните агенции следва да спазват, включително за минимизиране на рисковете по отношение на правото на неприкосновеност на личния живот и гражданските свободи, когато придобиват и използват информация в контекста на търговска сделка.

[65] Вж. например раздел 2.4 от Указ 12333 относно техниките за събиране на данни.
[66] Вж. съображение 40 от решението относно адекватното ниво на защита.
[67] Вж. съображение 38 от решението относно адекватното ниво на защита.
[68] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.
[69] https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf. От август 2024 г. разузнавателните агенции са длъжни да спазват Рамката.

2.2.2. Независим надзор

Дейностите на американските разузнавателни агенции подлежат на надзор от страна на различни органи, в това число служители по защита на личните данни и гражданските свободи, главни инспектори, Конгреса и PCLOB. По-специално с Указ 14086 от всяка разузнавателна агенция се изисква да разполага с висши служители в областта на правото, надзора и съответствието, които да гарантират спазването на приложимото законодателство на САЩ. Тази надзорна функция се изпълнява от служители, на които е възложено да отговарят за спазването, а също и от служителите по защита на личните данни и гражданските свободи, и от главните инспектори[70]. Те трябва да извършват периодичен надзор над дейностите по радиоелектронно разузнаване и да гарантират, че всяко несъответствие се отстранява. Разузнавателните служби трябва да осигурят на тези служители достъп до цялата необходима информация, за да могат да изпълняват надзорните си функции, и не могат да предприемат никакви действия за възпрепятстване или неправомерно влияние върху надзорните им дейности.

Главният юрисконсулт на Службата на главния инспектор на разузнавателната общност (Intelligence Community Inspector General — ICIG) към ODNI — който има всеобхватна юрисдикция над цялата разузнавателна общност и е упълномощен да разследва жалби или информация относно обвинения в незаконни действия или злоупотреба с власт — участва в срещата за преглед. Той потвърди, че ICIG систематично проверява спазването на Указ 14086 като част от своите надзорни дейности. Освен това се позова на неотдавнашните надзорни дейности на други главни инспектори на разузнавателната общност, както е описано подробно в периодичните доклади. Например в полугодишния си доклад до Конгреса за периода април—септември 2023 г.[71] главният инспектор на АНС информира за оценка на вътрешна рамка на АНС за контрол на целенасочеността на решенията и исканията. Той заключи, че тази рамка функционира правилно с оглед гарантиране на спазването на законите, директивите и политиките в защита на гражданските свободи и правото на неприкосновеност на личния живот. В същия доклад се споменава и за разследване, при което е разкрита злоупотреба с инструмент за радиоелектронно разузнаване за неразрешени цели от страна на служител на АНС.

[70] Всяка разузнавателна агенция разполага с главен инспектор, който е с независим статут и отговаря за провеждането на одити и разследвания, свързани с дейностите, извършвани от съответната агенция за целите на националната сигурност. Те имат достъп до всички съответни материали (в това число класифицирани материали), ако е необходимо чрез връчване на призовка, и могат да вземат показания. Главните инспектори предават на ръководителите на агенциите случаи на предполагаеми криминални нарушения с цел започване на наказателно преследване и отправят препоръки за корективни мерки към ръководителите им. Въпреки че техните препоръки не са обвързващи, докладите им, включително тези относно последващите действия (или липсата на такива), обикновено се оповестяват публично и се изпращат до Конгреса. В тази връзка вж. бележка под линия 136 от решението относно адекватното ниво на защита за ролята на главния инспектор.

[71] https://oig.nsa.gov/reports/Article/3609957/semiannual-report-to-congress-1-april-2023-to-30-september-2023/.

Съгласно Указ 14086 на PCLOB[72] са поверени специфични надзорни функции[73]. Председателят на PCLOB и неговите трима членове участваха в срещата за преглед и информираха, че през април 2023 г. PCLOB е предоставил съвети на разузнавателните агенции относно техните проекти на политики и процедури за прилагане на Указ 14086 и с него е проведена консултация относно номинирането на съдии и специални адвокати за Апелативния съд в областта на защитата на личните данни (DPRC). Освен това съветът стартира проект за надзор с цел провеждане на 1) преглед на прилагането на актуализираните политики и процедури, приети от разузнавателните агенции, за да се гарантира, че те са в съответствие с указа, и 2) годишен преглед на функционирането на новия механизъм за правна защита (вж. по-долу)[74]. Членовете на PCLOB потвърдиха, че съветът планира да извърши и двата прегледа в близко бъдеще. По отношение на правната защита те обясниха, че предвид липсата на жалби прегледът на PCLOB ще бъде съсредоточен върху политиките и процедурите, въведени за създаване на механизма.

По отношение на други надзорни дейности на 28 септември 2023 г. PCLOB издаде доклад относно раздел 702 от FISA[75]. Този доклад е продължение на по-ранен доклад от 2014 г. и съдържа актуализирана фактическа и правна информация относно действието на програмите за наблюдение съгласно раздел 702 на FISA. Освен това докладът съдържа препоръки относно спазването на приложимите изисквания от страна на разузнавателните агенции и предложения към Конгреса за по-нататъшно укрепване на няколко аспекта на раздел 702 от FISA в контекста на повторното разрешение (включително чрез въвеждане на законните цели за дейностите по наблюдение, посочени в Указ 14086)[76]. По време на срещата за преглед PCLOB информира, че очаква скоро да получи отговори от разузнавателните агенции относно изпълнението на неговите препоръки, които ще бъдат включени в бъдещ последващ доклад. Други текущи проекти за надзор включват проект за борба с вътрешния тероризъм и неговото въздействие върху правото на неприкосновеност на личния живот и гражданските свободи и събирането на данни от открити източници или данни, налични в търговската мрежа, от страна на ФБР[77].

На последно място, НПО, с които бяха проведени консултации в контекста на прегледа, изразиха загриженост, че мандатът на някои от членовете на PCLOB изтича в близко

[72] PCLOB е независима агенция, натоварена с отговорности в областта на политиките за борба с тероризма и тяхното прилагане с оглед на защитата на неприкосновеността на личния живот и гражданските свободи. Той има достъп до цялата съответна информация (в това число класифицирана информация), провежда интервюта и изслушва свидетелски показания. Той може да издава препоръки до правоприлагащите и разузнавателните органи и редовно докладва на Конгреса и на президента. Неговите доклади са публично достъпни във възможно най-голяма степен.

[73] https://documents.pclob.gov/prod/Documents/EventsAndPress/834a1977-f420-4b2a-ae93-8a522b2c7c74/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL)%20-%20Completed%20508%20-%2010202022.pdf.

[74] https://www.pclob.gov/OversightProjects/Details/1115.

[75] https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.

[76] Комисията отбелязва, че някои от тези препоръки са включени като част от RISAA, включително препоръката относно събирането на данни или препоръката за засилване на ролята на експертите на FISC (*amici*).

[77] https://www.pclob.gov/OversightProjects.

бъдеще, което може да доведе до липса на кворум в PCLOB. По-конкретно мандатът на председателя е изтекъл и периодът, през който тя може да продължи да изпълнява функциите си, докато бъде намерен заместник, приключва през януари 2025 г., като освен това има едно свободно място, а трето ще се освободи също през януари следващата година. По време на срещата за преглед членовете обясниха, че не очакват да има липса на кворум в PCLOB, тъй като вече е подадена номинация за мястото, което е свободно към момента (за която се очаква потвърждение от Сената)[78]. Освен това те подчертаха, че дори ако се стигне до липса кворум, това няма да повлияе на способността на съвета да продължава да изпълнява проекти за надзор. Независимо от това, като се има предвид важната роля на PCLOB за извършването на преглед на изпълнението на Указ 14086, Комисията ще следи отблизо свободните позиции и номинациите/назначенията в бъдеще.

2.2.3. Средства за правна защита

С Указ 14086, допълнен от наредба на главния прокурор, беше създаден нов механизъм за правна защита с цел разглеждане и разрешаване на отговарящи на условията жалби от страна на физически лица относно дейности на радиоелектронно разузнаване на САЩ[79]. Всяко физическо лице в ЕС има право да подаде жалба до механизма за правна защита относно предполагаемо нарушение на законодателството на САЩ, с което се уреждат дейностите по радиоелектронно разузнаване (напр. Указ 14086, раздел 702 от FISA или Указ 12333), по отношение на лични данни, предадени към САЩ, които засягат по неблагоприятен начин интересите му във връзка с неприкосновеността на личния живот и гражданските свободи. Физическите лица могат да подадат жалба към ОЗД в държава — членка на ЕС, която насочва, чрез секретариата на ЕКЗД, жалбата към механизма за правна защита. Механизмът се състои от две нива, като първоначалното разследване на жалби се извършва от CLPO към ODNI, а след това лицата имат възможност да обжалват решението на CLPO пред независим DPRC. След приключване на прегледа от страна на CLPO към ODNI или DPRC лицата са информирани чрез националния орган, че „при прегледа или не са установени никакви попадащи в приложното поле нарушения, или CLPO към ODNI/DPRC е издал решение, налагащо подходящи корективни мерки“. Решенията на CLPO към ODNI и DPRC са обвързващи за разузнавателните служби.

След приемането на решението относно адекватното ниво на защита бяха предприети допълнителни стъпки, за да може механизмът за правна защита да функционира пълноценно.

По отношение на създаването на DPRC на 14 ноември 2023 г. в съда бяха назначени осем съдии[80] (т.е. с двама повече от минималния брой, изискван съгласно Указ 14086, допълнен от разпоредбите на главния прокурор в 28 C.F.R. § 201.3(a)). Те бяха назначени въз основа на критериите, посочени в Указ 14086, и в съответствие с установената в него процедура, включително след консултация с PCLOB, наред с други органи[81]. Те включват бивши съдии от Федералния окръжен съд и Апелативния съд, бивш главен прокурор на

[78] https://documents.pclob.gov/prod/Documents/EventsAndPress/deb9cd13-12af-4250-998e-a520a2419a6b/PCLOB%20nominee%20press%20release%206-13-24.pdf.
[79] Съображения 176—194 от решението относно адекватното ниво на защита.
[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.
[81] Раздел 3(d)(v) от Указ 14086.

САЩ и бивш член на PCLOB. Както се изисква съгласно указа, поне половината от съдиите имат предишен съдебен опит. Освен това през април 2024 г. двама специални адвокати — практикуващи юристи с опит както в областта на правото на неприкосновеност на личния живот, така и на националната сигурност — бяха назначени да представляват интересите на лицата пред DPRC. На срещата за преглед беше потвърдено, че всички съдии и специални адвокати са получили най-високото разрешение за достъп и следователно могат да имат достъп до класифицирани материали за целите на работата си за DPRC. Освен това DPRC публикува поредица от често задавани въпроси, чрез които предоставя повече информация за своята роля, независимост и функциониране[82].

По отношение на разглеждането на жалби на 6 декември 2022 г. ODNI прие Директива 126 на разузнавателната общност, с която се регламентират подробно различни аспекти на процеса на разследване и произнасяне по жалби (чрез определяне на крайни срокове, създаване на защитено електронно хранилище и комуникационни канали, изискване елементите на CLPO и разузнавателната общност да си сътрудничат с PCLOB в контекста на годишния преглед на механизма за правна защита и др.)[83]. Тази директива е приложима за цялата разузнавателна общност на САЩ и е допълнена от други вътрешни процедури, приети от отделни разузнавателни агенции във връзка със сътрудничеството им с CLPO към ODNI в контекста на разглеждането на жалби (напр. разработване на защитено хранилище за споделяне на жалби и документи за отговор; и защитени съобщения между съответните агенции). Освен това през следващите месеци DPRC ще издаде по-подробни правила за разглеждане на жалби и други процедурни аспекти.

В Европейския съюз и Съединените щати бяха предприети редица допълнителни мерки за информиране на широката общественост, както и за улесняване на подаването и разглеждането на жалби. Това включва приемането от страна на ЕКЗД на информационна бележка относно новия механизъм за правна защита[84], образец на формуляр за жалба (който трябва да бъде преведен и публикуван от всички ОЗД на техните национални езици)[85] и процедурен правилник, с който се урежда сътрудничеството между националните надзорни органи и секретариата на ЕКЗД[86]. По подобен начин ODNI публикува често задавани въпроси и информационен лист за новия механизъм за правна защита и се ангажира с дейности за повишаване на осведомеността сред обществеността[87].

Освен това през последната година ЕКЗД и съответните органи на САЩ имаха тясно сътрудничество по няколко оперативни аспекта. По-специално, както беше потвърдено по време на срещата за преглед, те въведоха криптиран комуникационен канал за

[82] https://www.justice.gov/opcl/dprc-resources.
[83] https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf
[84] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_bg.
[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_bg.
[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_bg.
[87] https://www.dni.gov/files/CLPT/documents/Fact_Sheets/The_Role_of_the_ODNI_CLPO_FAQs.pdf и https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.

предаване на жалби от националните органи в ЕС до секретариата на ЕКЗД, от секретариата на ЕКЗД до CLPO към ODNI, както и до Службата за защита на неприкосновеността на личния живот и гражданските свободи на DoJ (Office of Privacy and Civil Liberties — OPCL) и между CLPO към ODNI и други органи на САЩ (напр. DPRC). Освен това CLPO към ODNI обясни, че са въведени допълнителни вътрешни процедури за сътрудничество на отделните разузнавателни агенции с CLPO към ODNI по отношение на разглеждането на жалби.

На последно място, OPCL, която предоставя административна подкрепа на DPRC, също информира, че DPRC работи със собствен бюджетен ред и разполага с необходимите съоръжения за изпълнение на задачите си, в това число защитени компютри и лаптопи, телефони и др. Освен това, както се изисква съгласно Указ 14086, DoC е предприело необходимите мерки, включително чрез създаване на криптиран комуникационен канал с CLPO към ODNI, за поддържане на регистър на всички получени жалби, които отговарят на условията. DoC периодично ще се свързва с CLPO към ODNI, за да разбере дали информацията, свързана с дадена жалба, е била разсекретена. В случай че е разсекретена, DoC ще уведоми съответното лице, за да му даде възможност да получи достъп до тази информация.

Към момента на провеждане на срещата за преглед не са получени жалби от страна на надзорните органи на ЕС и следователно новият механизъм за правна защита все още не е задействан.

3. ЗАКЛЮЧЕНИЕ

Въз основа на информацията, събрана по време на този първи преглед, Комисията заключава, че органите на САЩ са въвели необходимите структури и процедури, за да гарантират, че Рамката за защита на личните данни функционира ефективно. В този контекст Комисията високо оценява много доброто сътрудничество с органите на САЩ за целите на извършване на прегледа.

Въпреки че този пръв преглед естествено беше съсредоточен върху проверката на наличието на всички съставни елементи на рамката, опитът при практическото прилагане на предпазните мерки, приложими както към обработката на данни от страна на сертифицирани дружества, така и към достъпа до данни от страна на публичните органи, неизбежно е ограничен след само една година работа. Поради това Комисията ще следи отблизо съответното развитие през следващите месеци и години, като обръща специално внимание на 1) предстоящите доклади на PCLOB относно прилагането на Указ 14086 и функционирането на механизма за правна защита при радиоелектронно разузнаване, по-специално на DPRC; 2) евентуални допълнителни изменения на раздел 702 от FISA; и 3) номинирането и назначаването на членове на PCLOB с оглед запълване на бъдещи свободни позиции.

Освен това, за да се осигури непрекъснато и ефективно функциониране на рамката, Комисията счита за важно да отбележи следното:

— Както беше обявено на срещата за преглед, DoC използва по-пълноценно различните инструменти, предоставени по РЗЛД, с оглед на наблюдението на

спазването на принципите на рамката от страна на дружествата и откриването на неверни твърдения за участие.

— FTC допълнително развива своя проактивен подход към разследването и правоприлагането на спазването на принципите на РЗЛД от страна на сертифицираните дружества; както и

— DoC, FTC и органите за защита на личните данни на ЕС разработват общи инструменти за предоставяне на насоки относно ключови изисквания съгласно принципите на РЗЛД, напр. по отношение на данните, свързани с човешките ресурси, и последващото предаване на данни.

С оглед на тези резултати от прегледа и както е предвидено в съображение 211 от решението относно адекватното ниво на защита, Комисията счита за целесъобразно следващият периодичен преглед да бъде извършен след три години. Това следва да даде възможност да се натрупа повече опит при практическото прилагане на РЗЛД и да се вземат предвид гореспоменатите бъдещи промени. Поради това, в съответствие с член 3, параграф 4 от решението относно адекватното ниво на защита, Комисията ще се консултира с ЕКЗД и комитета, създаден съгласно член 93, параграф 1 от Общия регламент относно защитата на данните, във връзка с периодичността на бъдещите прегледи.