

Препоръки



Препоръки 2/2020 относно европейските основни гаранции при прилагане на мерки за наблюдение

Приети на 10 ноември 2020 г.

Съдържание

1. ВЪВЕДЕНИЕ.....	4
2. НАМЕСА В ОСНОВНИТЕ ПРАВА.....	7
3. ЕВРОПЕЙСКИ ОСНОВНИ ГАРАНЦИИ.....	8
Гаранция А — Обработването следва да се основава на ясни, точни и достъпни правила	9
Гаранция Б — Трябва да бъде доказана необходимост и пропорционалност по отношение на преследваните легитимни цели.....	10
Гаранция В — Механизъм за независим надзор	13
Гаранция Г — Физическите лица трябва да разполагат с ефективни средства за правна защита	14
4. ОКОНЧАТЕЛНИ ЗАБЕЛЕЖКИ	16

Европейският комитет по защита на данните,

Като взе предвид член 70, параграф 1, буква д) от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива и за отмяна на Директива 95/46/ЕО (по-нататък „ОРЗД“)¹,

Като взе предвид Споразумението за Европейското икономическо пространство и по-конкретно приложение XI и протокол 37 към него, изменени с Решение на Съвместния комитет на ЕИП № 154/2018 от 6 юли 2018 г.,²

Като взе предвид членове 12 и 22 от своя Правилник за дейността,

Като взе предвид работния документ на Работната група по член 29 относно основателността на намесата в основните права на неприкосновеност на личния живот и на защита на личните данни чрез мерки за наблюдение при предаването на лични данни („Европейски основни гаранции, наричани по-нататък „ОЕГ“), РД237,

ПРИЕ СЛЕДНИТЕ ПРЕПОРЪКИ:

1. ВЪВЕДЕНИЕ

1. След решението по делото Schrems I органите на ЕС за защита на данните, участващи в работната група по член 29, се позоваха на съдебната практика, за да определят европейските основни гаранции, които трябва да бъдат спазвани, за да се гарантира, че намесата в правото на неприкосновеност на личния живот и защитата на личните данни чрез мерки за наблюдение при предаването на лични данни не надхвърля това, което е необходимо, и пропорционално в едно демократично общество.

2. ЕКЗД би желал да подчертае, че европейските основни гаранции се основават на съдебната практика на Съда на Европейския съюз (наричан по-нататък Съда на ЕС) във връзка с членове 7, 8, 47 и 52 от Хартата на основните права на ЕС (наричана по-нататък Хартата) и, в зависимост от случая, на съдебната практика на Европейския съд по правата на човека (наричан по-нататък: ЕСПЧ), свързана с член 8 от Европейската конвенция за правата на човека и основните свободи

¹ В настоящия документ не се разглеждат ситуации на предаване или последващо споделяне, попадащи в обхвата на Директивата относно правоприлагането в областта на защитата на данните (Директива (ЕС) 2016/680).

² Позоваванията на „държави членки“ в настоящия документ следва да се разбират като позовавания на „държавите членки на ЕИП“.

(наричана по-нататък ЕКПЧ), която се занимава с въпроси, свързани с наблюдението в държавите, които са страни по ЕКПЧ³.

3. Актуализацията на настоящия документ има за цел да бъдат допълнително развити европейските основни гаранции, изготвени първоначално в отговор на решението по делото Schrems I,⁴ като бъдат отразени поясненията, предоставени от Съда на ЕС (и от ЕСПЧ) след първото му публикуване, по-специално, в неговото историческо решение по делото Schrems II.⁵

4. В решението си по делото Schrems II Съдът на ЕС заяви, че при разглеждането на Решение 2010/87/ЕС на Комисията относно общите договорни клаузи при предаването на лични данни на обработващи лични данни, установени в трети държави, от гледна точка на приложението на членове 7, 8 и 47 от Хартата, не се установяват обстоятелства, които могат да засегнат валидността на това решение, а е обезсилено Решението относно Щита за личните данни. Съдът на ЕС постанови, че решението относно Щита за личните данни е несъвместимо с член 45, параграф 1 от ОРЗД с оглед на членове 7, 8 и 47 от Хартата. Ето защо съдебното решение може да служи като пример, когато мерките за наблюдение в трета държава (в този случай САЩ, съгласно член 702 от ЗНВР и Изпълнителен декрет 12333 (Executive Order 12333) не са нито достатъчно ограничени, нито предмет на ефективна правна защита, достъпна за субектите на данни, за да упражнят правата си, както се изисква съгласно правото на ЕС, за да се счита, че нивото на защита в трета държава е „по същество равностойно“ на гарантираното в Европейския съюз по смисъла на член 45, параграф 1 от ОРЗД.

5. Причините за обявяването на Щита за личните данни за недействителен засягат и други инструменти за предаване на данни⁶. Въпреки че Съдът тълкува член 46, параграф 1 от ОРЗД във връзка с валидността на стандартните договорни клаузи (наричани по-нататък: СДК), неговото тълкуване се прилага за всяко предаване на трети държави, които разчитат на някой от инструментите, посочени в член 46 от ОРЗД⁷.

6. В крайна сметка Съдът на ЕС следва да прецени дали намесата в дадено основно право може да бъде оправдана. Въпреки това, при липса на такова решение и при прилагане на постоянната съдебна практика, от органите за защита на данните се изисква да оценяват отделни случаи *ex officio* или вследствие на жалба и да отнесат случая до национален съд, ако се съмняват, че предаването не е в съответствие с член 45, когато е налице решение относно адекватното ниво на защита, или да спрат или забранят предаването, ако установят, че член 46 от ОРЗД не може да бъде спазен, и защитата на предаваните данни, изисквана от правото на ЕС, не може да бъде гарантирана с други средства.

³ В настоящите препоръки терминът „основни права“ произтича от Хартата на основните права на ЕС. Но той се използва и за да бъдат обхванати „правата на човека“, включени в Европейската конвенция за правата на човека.

⁴ Решение на Съда на ЕС от 6 октомври 2015 г. по дело Maximillian Schrems/Data Protection Commissioner, C-362/14, EU:C:2015:650 (наричано по-нататък Schrems I).

⁵ Решение на Съда на ЕС от 16 юли 2020 г. по дело Data Protection Commissioner/Facebook Ireland Ltd, Maximillian Schrems, дело C-311/18, ECLI:EU:C:2020:559 (наричано по-нататък дело Schrems II).

⁶ Вж. точка 105 от дело Schrems II.

⁷ Вж. точка 92 от дело Schrems II.

7. Целта на актуализираните европейски основни гаранции е да се предоставят елементи, за да се установи, дали мерките за наблюдение, позволяващи достъп до лични данни от страна на публичните органи в трета държава, които са национални агенции за сигурност или правоприлагащи органи, могат да се разглеждат като оправдана намеса или не.

8. Всъщност европейските основни гаранции са част от оценката, която трябва да се извърши, за да се определи дали дадена трета държава осигурява ниво на защита, което по същество е равностойно на гарантираното в рамките на ЕС, но в тях не се определят всички елементи, които са необходими, за да се счита, че дадена трета държава предоставя такова ниво на защита в съответствие с член 45 от ОРЗД. По същия начин, няма за цел в гаранциите да бъдат определени всички елементи, които може да са необходими, за да се прецени, дали правният режим на трета държава възпрепятства износителя и вносителя на данни за осигуряването на подходящи гаранции в съответствие с член 46 от ОРЗД.

9. Ето защо елементите, предоставени в настоящия документ, следва да се разглеждат като основни гаранции, които следва да бъдат регламентирани в третата държава при извършване на оценка на намесата, произтичаща от въведените мерките за наблюдение в тази държава, заедно с правото на неприкосновеност на личния живот и на защита на данните, а не като списък с елементи, показващи, че правният режим на трета държава като цяло предоставя по същество еквивалентно ниво на защита.

10. В член 6, параграф 3 от Договора за Европейския съюз е заложено, че основните права, залегнали в ЕКПЧ, представляват общи принципи на правото на Съюза. Въпреки това, както припомня Съдът на ЕС в своята съдебна практика, докато Европейският съюз не е одобрил даден инструмент, той не представлява правен инструмент, формално включен в правото на ЕС⁸. Така изискването от член 46, параграф 1 от ОРЗД ниво на защита на основните права, трябва да се определи въз основа на разпоредбите на същия регламент, разглеждани от гледна точка на основните права, гарантирани от Хартата. При все това, съгласно член 52, параграф 3 от Хартата съдържашите се в нея права, които съответстват на права, гарантирани от ЕКПЧ, имат същия смисъл и обхват като дадените им в посочената конвенция и следователно, както припомня Съдът на ЕС, съдебната практика на ЕСПЧ относно правата, които също са предвидени в Хартата на основните права на ЕС, трябва да се вземе предвид като минимален праг на защита при тълкуването на съответните права в Хартата⁹. Съгласно последното изречение на член 52, параграф 3 от Хартата обаче „[Т]ази разпоредба не пречи правото на Съюза да предоставя по-широка защита.“

11. Поради това, основните гаранции ще продължат да се основават отчасти на съдебната практика на ЕСПЧ, доколкото Хартата, както се тълкува от Съда на ЕС, не предвижда по-високо равнище на защита, което да залага изисквания, различни от съдебната практика на ЕСПЧ.

12. В настоящия документ се обяснява същността на четирите европейски основни гаранции, като те се описват по-подробно.

⁸ Вж. точка 98 от дело Schrems II.

⁹ Вж. точка 124 от съединени дела C-511/18, C-512/18 и C-520/18, дело La Quadrature du Net и др. (наричани по-долу: Дело La Quadrature du Net и др.).

2. НАМЕСА В ОСНОВНИТЕ ПРАВА

13. Основните права на зачитане на личния и семейния живот, включително на тайната на съобщенията, и на защита на личните данни са установени в членове 7 и 8 от Хартата и се прилагат за всички. Освен това в член 8 се определят условията за законосъобразно обработване на личните данни и се признава правото на достъп и поправка, и се изисква тези правила да подлежат на контрол от независим орган.

14. „(О)перацията по предаване на лични данни от държава членка към трета държава сама по себе си представлява обработване на лични данни.“¹⁰ Така членове 7 и 8 от Хартата се прилагат по отношение на тази конкретна операция и тяхната защита обхваща и предаваните данни, поради което на субектите на данни, чиито лични данни се предават на трета държава, трябва да се осигури ниво на защита, което по същество е равностойно на гарантираното в рамките на Съюза.¹¹

15. Според Съда на ЕС, когато се засяга основното право на зачитане на личния живот, гарантирано в член 7 от Хартата, при обработването на личните данни на дадено лице се засяга и правото на защита на данните, тъй като такова обработване попада в приложното поле на член 8 от Хартата и следователно трябва задължително да отговаря на изискването за защита на данните, предвидено в този член.¹²

16. Следователно, що се отнася до евентуалната намеса в основните права съгласно правото на ЕС, задължението, наложено на доставчиците на електронни съобщителни услуги (...) да запазват данни за трафика с цел предоставянето им, ако е необходимо, на компетентните национални органи, повдига въпроси, засягащи съвместимостта с членове 7 и 8 от Хартата.¹³ Същото важи и за други видове обработване на данни, като например предаването на данни на лица, различни от ползвателите, или достъпа до тези данни с оглед на използването им,¹⁴ което води по този начин до намеса в тези основни права. Освен това съгласно установената съдебна практика достъпът на публичен орган до данните представлява допълнителна намеса.¹⁵

17. За да се установи намеса, няма значение „дали съответните данни за личния живот имат чувствителен характер и дали заинтересованите лица са претърпели евентуални неудобства поради тази намеса“.¹⁶ Съдът на ЕС също така подчерта, че не е от значение дали запазените данни са били използвани впоследствие¹⁷.

18. Членове 7 и 8 от Хартата обаче не представляват абсолютни права, а трябва да се разглеждат във връзка с функцията им в обществото.¹⁸

¹⁰ Съд на ЕС, дело Schrems II, точка 83.

¹¹ Съд на ЕС, дело Schrems II, точка 96.

¹² Съд на ЕС, дело Schrems II, точки 170—171.

¹³ Съд на ЕС, дело C-623/17, Privacy International (наричано по-нататък Privacy International), точка 60.

¹⁴ Съд на ЕС, Privacy International, точка 61.

¹⁵ ЕСПЧ, Leander, точка 48; ЕСПЧ, Rotaru точка 46; Съд на ЕС, Digital Rights Ireland, точка 35.

¹⁶ Съд на ЕС, дело Schrems II, точка 171, включително цитираната съдебна практика.

¹⁷ Съд на ЕС, дело Schrems II, точка 171, включително цитираната съдебна практика.

¹⁸ Съд на ЕС, Privacy International, точка 63.

19. Хартата включва проверка за необходимост и пропорционалност, за да се очертаят ограниченията на правата, които тя защитава. В член 52, параграф 1 от Хартата се уточнява обхватът на възможните ограничения на членове 7 и 8, като се посочва, че „Всяко ограничаване на упражняването на правата и свободите, признати от настоящата Харта, трябва да бъде предвидено в закон и да зачита основното съдържание на същите права и свободи. При спазване на принципа на пропорционалност ограничения могат да бъдат налагани, само ако са необходими и ако действително отговарят на признати от Съюза цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора.“

20. Съдът на ЕС потвърди, че законодателството на ЕС, което включва намеса в основните права, гарантирани от членове 7 и 8 от Хартата, „трябва да определя ясни и точни правила, които да уреждат обхвата и прилагането на разглежданата мярка и да установяват минимални гаранции, така че лицата, чиито лични данни са засегнати, да разполагат с достатъчни гаранции, че данните ще бъдат ефективно защитени срещу риск от злоупотреба“, по-специално, когато личните данни са обект на автоматична обработка и „когато съществува значителен риск от незаконен достъп до тях“.¹⁹

21. Според Съда на ЕС защитата на правото на неприкосновеност на личния живот изисква дерогациите и ограниченията на правото на защита на данните да „се прилагат, доколкото това е строго необходимо.“ Освен това всяка цел от общ интерес трябва да бъде съгласувана с основните права, засегнати от мярката, „чрез надлежно балансиране“ между тази цел и въпросните права.²⁰

22. Следователно достъпът, запазването и по-нататъшното използване на лични данни от публичните органи в рамките на мерките за наблюдение не трябва да надхвърля границите на строго необходимото, преценено съгласно Хартата, в противен случай „не може да се счита за обосновано в едно демократично общество.“²¹

23. Четирите основни европейски гаранции, както са разработени в следващата глава, имат за цел да уточнят допълнително, как да се оцени степента на намеса в основните права на неприкосновеност на личния живот и на защита на данните във връзка с мерките за наблюдение от страна на публичните органи в трета държава при предаването на лични данни, както и какви правни изисквания трябва да се прилагат, за да се прецени дали подобна намеса би била приемлива съгласно Хартата.

3. ЕВРОПЕЙСКИ ОСНОВНИ ГАРАНЦИИ

24. След анализа на съдебната практика ЕКЗД счита, че приложимите правни изисквания за обосноваване на ограниченията на защитата на данните и правата на неприкосновеност на личния живот, признати от Хартата, могат да бъдат обобщени в четири европейски основни гаранции:

A. Обработването следва да се основава на ясни, точни и достъпни правила.

¹⁹ Съд на ЕС, Privacy International, точка 68 и цитираната в нея съдебна практика.

²⁰ Съд на ЕС, Privacy International, точка 68 и цитираната в нея съдебна практика.

²¹ Съд на ЕС, Privacy International, точка 81.

- Б. Трябва да бъде доказана необходимост и пропорционалност по отношение на преследваните легитимни цели.
- В. Необходимо е да съществува механизъм за независим надзор.
- Г. Физическите лица трябва да разполагат с ефективни средства за правна защита.

25. Гаранциите се основават на основните права на неприкосновеност на личния живот и защита на данните, които се прилагат за всички, независимо от тяхната националност.

Гаранция А — Обработването следва да се основава на ясни, точни и достъпни правила

26. Съгласно член 8, параграф 2 от Хартата личните данни следва, наред с другото, да се обработват „за точно определени цели и въз основа на съгласието на заинтересованото лице или по силата на друго предвидено от закона легитимно основание“, ²² както Съдът на ЕС припомня в решението по дело Schrems II. В допълнение към това, съгласно член 52, параграф 1 от Хартата всяко ограничение на упражняването на правата и свободите, признати от Хартата в ЕС, трябва да бъде предвидено от закона. Следователно, всяка оправдана намеса трябва да бъде в съответствие със закона.

27. С това правно основание следва да бъдат установени ясни и точни правила, с които да се урежда обхватът и прилагането на въпросната мярка и да се налагат минимални гаранции. ²³ Освен това, Съдът припомни, че „законодателството трябва да бъде правно обвързващо съгласно националното право“. ²⁴ Във връзка с това Съдът на ЕС поясни, че оценката на приложимото право на трета държава следва да бъде съсредоточено върху това, дали физическите лица могат да се позовават на него и да изискват, то да бъде приложено от съд. ²⁵ Ето защо Съдът посочва, че правата, предоставени на субектите на данни, трябва да бъдат приложими; когато на физическите лица не са предоставени приложими права по отношение на публични органи, осигурената степен на защита не може да се счита по същество за равностойна на произтичащата от Хартата, в разрез с изискването, заложено в член 45, параграф 2, буква а) от ОРЗД. ²⁶

28. Освен това Съдът подчертава, че приложимото право трябва да посочва при какви обстоятелства и при какви условия може да бъде приета мярка, предвиждаща обработването на такива данни ²⁷ (вж. по-долу в гаранция Б връзката между тези изисквания и принципите на необходимост и пропорционалност).

²² Вж. точка 173 от Schrems II.

²³ Вж. точка 175 и точка 180 от дело Schrems II и Становище 1/15 (Споразумението PNR между ЕС и Канада) от 26 юли 2017 г., точка 139 и цитираната съдебна практика.

²⁴ Вж. точка 68 от Privacy International — Следва също така да бъде ясно, че във френската версия на решението Съдът използва думата „réglementation“, която е с по-широко значение от понятието „актове“ на Парламента.

²⁵ Вж. точка 181 от Schrems II, в тази точка Съдът на ЕС се позовава на Presidential Policy Directive 28 на САЩ (Президентска изпълнителна директива № 28).

²⁶ Вж. точка 181 от Schrems II.

²⁷ Вж. точка 68 от Privacy International във връзка с правото на държавите членки.

29. Освен това Съдът на ЕС също така е посочил, че „изискването, всяко ограничение на упражняването на основни права да бъде предвидено в закон, означава, че самото правно основание, позволяващо намеса в тези права, трябва да определя обхвата на ограничението при упражняване на съответното право“.²⁸

30. Накрая Европейският съд по правата на човека „не счита, че има основание да се прилагат различни принципи, обхващащи достъпността и яснотата на правилата, уреждащи прихващането на индивидуални съобщения, от една страна, и по-общите програми за наблюдение“.²⁹ ЕСПЧ също така поясни, че правното основание следва да включва поне определение на категориите лица, които могат да бъдат обект на наблюдение, ограничение на продължителността на мярката, процедурата, която трябва да се следва при разглеждане, използване и съхраняване на получените данни, както и предпазните мерки, които трябва да се вземат при съобщаване на данните на други страни.³⁰

31. На последно място намесата трябва да бъде предвидима по отношение на последиците от нея за лицето, за да му/й се предостави адекватна и ефективна защита срещу произволна намеса и риск от злоупотреби. В резултат на това, обработването трябва да се основава на точно, ясно, но също така достъпно (т.е. публично) правно основание.³¹ По отношение на този въпрос ЕСПЧ припомни в делото *Zakharov*, че „позоваването на „предвидимост“ в контекста на прихващането на съобщения не може да бъде същото както в много други области“. Уточнява се, че по отношение на тайните мерки за наблюдение, като например, прихващането на съобщения, „предвидимостта не може да означава, че трябва да се позволи на някого да предвиди дали и кога има опасност неговите съобщения да бъдат прихванати от органите, за да може да съобрази поведението си с това“. Като се има предвид обаче, че в този вид ситуация рисковете от произвол са очевидни „от съществено значение е наличието на ясни и подробни правила за прихващане на телефонни разговори, особено като се има предвид, че наличната за използване технология непрекъснато се усъвършенства. Националното право трябва да бъде достатъчно ясно, за да дава на гражданите ясни указания относно обстоятелствата и условията, при които публичните органи са оправомощени да прибегнат до такива мерки“.³²

Гаранция Б — Трябва да бъде доказана необходимост и пропорционалност по отношение на преследваните легитимни цели

32. Съгласно член 52, параграф 1, първо изречение от Хартата всяко ограничаване на упражняването на правата и свободите, признати от Хартата, трябва да зачита основното съдържание на същите права и свободи. Съгласно член 52, параграф 1, второ изречение от Хартата при спазване на принципа на пропорционалност ограничения могат да бъдат налагани, само ако са необходими и ако действително отговарят на, признати от Съюза, цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора.³³

²⁸ Вж. *Schrems II*, точка 175 и цитираната съдебна практика, както и *Privacy International*, точка 65.

²⁹ ЕКПЧ, *Liberty*, точка 63.

³⁰ ЕКПЧ, *Weber* и *Saravia*, точка 95.

³¹ ЕСПЧ, дело *Malone*, точки 65, 66.

³² ЕСПЧ, дело *Zakharov*, точка 229.

³³ *Schrems II*, точка 174.

33. Що се отнася до **принципа на пропорционалност**, Съдът приема, че предвид правото на държавите членки, въпросът дали ограничение на правата на неприкосновеност на личния живот и на защита на данните може да бъде оправдано, трябва да се преценява, от една страна, като се измери **тежестта на намесата**, до която води подобно ограничение,³⁴ и от друга страна чрез проверка, дали **значението на преследваната с това ограничение цел от обществен интерес** е пропорционално на тази тежест.³⁵

34. В делото *La Quadrature du net* и др. може да се отбележи, че Съдът на ЕС е постановил, като е взел предвид правото на държава членка, а не на правото на трета държава, че с оглед на опазване на националната сигурност, може да се обосноват мерки, водещи до по-сериозна намеса в основните права, отколкото мерките, които биха могли да бъдат приложени за други цели, като например борбата с престъпността. Той констатира обаче, че случаят е такъв, стига да са налице достатъчно солидни основания да се счита, че съответната държава е изправена пред сериозна заплаха за националната сигурност, за която е доказано, че е действителна и настояща или предвидима, и при условие че отговаря на останалите изисквания, предвидени в член 52, параграф 1 от Хартата.³⁶

35. В тази връзка дерогациите и ограниченията относно защитата на личните данни трябва да се прилагат само, доколкото това е строго необходимо³⁷ съгласно установената практика на Съда. За да изпълни това изискване, освен като установява ясни и точни правила, уреждащи обхвата и прилагането на въпросната мярка, съответното законодателство трябва да налага минимални мерки за защита, така че лицата, чиито данни са били предадени, да разполагат с достатъчно гаранции, за да защитят ефективно личните си данни срещу риска от злоупотреби. „В него трябва по-специално да се посочва при какви обстоятелства и при какви условия може да бъде приета мярка, предвиждаща обработването на такива данни, като по този начин се гарантира, че намесата е ограничена до строго необходимото. Необходимостта от такива гаранции е още по-голяма, когато личните данни подлежат на автоматизирано обработване“.³⁸

³⁴ В тази връзка Съдът отбелязва например, че „намесата, която представлява събирането в реално време на данни, което позволява да бъде установено местонахождението на крайните устройства, изглежда особено сериозна, тъй като тези данни предоставят на компетентните национални органи средство за точно и постоянно проследяване на движението на потребителите на мобилни телефони (...)“ (дело *La Quadrature du Net* и др., точка 187, включително цитираната съдебна практика).

³⁵ *La Quadrature du Net* и др., точка 131.

³⁶ Точки 136 и 137. Вж. също решение по дело *Privacy International*, като Съдът подчертава, че такива заплахи могат да бъдат разграничени по своето естество и особена сериозност от общия риск от възникване на напрежение или безредици, дори със сериозно естество, които засягат обществената сигурност. Точка 75. Например в решението по дело *La Quadrature du Net* и др. Съдът посочва, че автоматизираният анализ на данни за трафик и данни за местонахождение, които обхващат общо и безразборно данните на лицата, използващи електронни съобщителни системи, представлява особено сериозна намеса, така че такава мярка може да отговаря на изискването за пропорционалност само в случаите, когато съответната държава членка е изправена пред сериозна заплаха за националната сигурност, за която е доказано, че е действителна и настояща или предвидима, и наред с други условия, при условие че продължителността на запазването е ограничена до строго необходимото (точки 174—177).

³⁷ *Schrems II*, точка 176, включително цитираната съдебна практика.

³⁸ *Schrems II*, точка 175.

36. В решението по дело Schrems II Съдът на ЕС подчертава, че законодателството на трета държава, в което не се посочват никакви ограничения на съдържанието се в него оправомощаване за прилагането на програми за наблюдение за целите на външното разузнаване, не може да осигури ниво на защита, което по същество е равностойно на нивото, гарантирано от Хартата. Всъщност, съгласно съдебната практика, за да бъдат изпълнени изискванията на принципа на пропорционалност, самото правно основание, което позволява намеса в основните права, трябва да определя обхвата на ограничението при упражняване на съответното право.³⁹

37. Що се отнася до **принципа на необходимост**, Съдът на ЕС пояснява, че правна уредба, която „общо разрешава съхраняването на всички лични данни на всички лица, чиито данни са били прехвърлени от Съюза (...), без да въвежда никакво разграничаване, ограничаване или изключение с оглед на преследваната цел и без да предвижда обективен критерий, позволяващ да се ограничи достъпът на публичните органи до данните и тяхното последващо използване за конкретни цели, които са строго ограничени и могат да обосноват намесата, каквато съдържат достъпът и използването на тези данни“ не отговаря на този принцип.⁴⁰ Според Съда на ЕС правна уредба, която общо разрешава на публичните органи достъп до съдържанието на електронни съобщения, трябва да се счита за засягаща същността на основното право на зачитане на личния живот, гарантирано с член 7 от Хартата.⁴¹

38. По подобен начин, обаче този път, когато се прави оценка на правото на държава членка, а не на правото на трета държава, Съдът на ЕС постанови в решението по дело La Quadrature du Net и др., че „законодателството, изискващо запазване на лични данни, трябва винаги да отговаря на обективни критерии, които установяват връзка между запазените данни и преследваната цел“.⁴² По същия начин, в решението по дело Privacy International Съдът също така постанови, че законодателният орган „трябва да разчита на обективни критерии, за да определи

³⁹ Schrems II, точка 180.

⁴⁰ Schrems I, точка 93 с допълнителни препратки. Вж. обаче този път във връзка с правото на държава членка, а не на трета държава, решение по дело Privacy International, точка 71, включително цитираната съдебна практика. В този случай Съдът постанови, че законодателство на държава членка, което изисква от доставчиците на електронни съобщителни услуги да разкриват данни за трафик и данни за местонахождение пред службите за сигурност и разузнавателните служби чрез общо и безразборно предаване, надхвърля границите на строго необходимото и не може да се счита за оправдано в рамките на едно демократично общество, както се изисква от Директивата за правото на неприкосновеност на личния живот и електронни комуникации, разглеждана в светлината на Хартата (параграф 81).

⁴¹ Schrems I, точка 94.

⁴² Дело La Quadrature du Net и др., точка 133. В тази връзка Съдът потвърди, че в Директивата за неприкосновеността на личния живот и електронните съобщения, тълкувана съгласно Хартата, не се допускат законодателни мерки, които предвиждат превантивна мярка за общо и безразборно запазване на данни за трафик и данни за местонахождение. Съдът постанови обаче, че в ситуации на сериозна заплаха за националната сигурност, за която е доказано, че е действителна и настояща или предвидима, законодателният орган може да разреши, с цел опазване на националната сигурност, използването на указания, с които да се изисква от доставчиците на електронни съобщителни услуги да запазват общо и безразборно данни за трафик и данни за местонахождение. Тази мярка обаче трябва да отговаря на специфични условия. По-специално, инструкцията може да се дава само за период, ограничен във времето до строго необходимото, който може да бъде удължен, ако заплахата продължава (параграф 168).

обстоятелствата и условията, при които компетентните национални органи трябва да получат достъп до въпросните данни“.⁴³

Гаранция В — Механизъм за независим надзор

39. ЕКЗД припомня, че намесата се извършва в момента на събирането на данните, но също така и в момента, в който публичен орган получава достъп до данните за по-нататъшна обработка. ЕСПЧ многократно е посочвал, че всяка намеса в правото на неприкосновеност на личния живот и защита на данните следва да бъде обект на ефективна, независима, и безпристрастна система за надзор, която трябва да бъде предвидена от съдия или от друг независим орган⁴⁴ (например административен или парламентарен орган). Независимият надзор върху изпълнението на мерките за наблюдение беше взет предвид и от Съда на ЕС в решението по делото Schrems II.⁴⁵

40. ЕСПЧ уточнява, че макар предварителното (съдебно) разрешение за прилагане на мерки за наблюдение да е важна предпазна мярка срещу произвол, трябва да се обърне внимание и на действителното функциониране на системата за прихващане, включително на принципа на взаимозависимост и взаимоограничаване при упражняването на власт, както и на наличието или липсата на действителна злоупотреба.⁴⁶ В делото Schrems II Съдът на ЕС взе предвид и обхвата на механизма за надзор, който не включва мерките за наблюдение на физическите лица.⁴⁷

41. Що се отнася до правото на държавите членки, Съдът на ЕС установи редица мерки, които са в съответствие с правото на ЕС, само ако подлежат на ефективен контрол, извършван от съд или независим административен орган, чието решение е обвързващо. Целта на този контрол е да се провери дали е налице положение, при което мярката е обоснована, и дали са спазени условията и предпазните мерки, които трябва да бъдат определени.⁴⁸ За събирането в реално време на данни за трафика и местоположението, прегледът следва да позволява да се направи предварителна проверка, между другото, дали е разрешено само в рамките на строго необходимото. В надлежно обосновани спешни случаи мерките могат да се предприемат без такъв предварителен преглед; въпреки това, Съдът все пак изисква в кратък срок да се извърши последващ преглед.⁴⁹

42. Що се отнася до механизмите за независим надзор във връзка с наблюдението, могат да бъдат взети предвид констатациите на Съда на ЕС относно независимостта на даден орган по отношение на средствата за правна защита (вж. по-долу в раздел „Гаранция Г“). Освен това, съдебната практика на ЕСПЧ може да предложи допълнителни елементи. Съдът е изразил предпочитанието

43 Privacy International, точка 78, включително цитираната съдебна практика. В решение по дело Privacy International, що се отнася до достъпа на даден орган до лични данни, предоставен съгласно правото на държава членка, Съдът постанови, че „общият достъп до всички запазени данни, независимо дали има връзка, поне непряка, с преследваната цел, не може да се счита за ограничен до строго необходимото“ (точки 77—78).

⁴⁴ ЕСПЧ, Klass, точки 17, 51.

⁴⁵ Schrems II, точки 179, 183.

⁴⁶ ЕСПЧ, Big Brother Watch, обжалвано, точки 319—320.

⁴⁷ Schrems II, точка 179.

⁴⁸ Съд на ЕС, дело La Quadrature du Net и др., точки 168, 189.

⁴⁹ Съд на ЕС, дело La Quadrature du Net и др., точка 189.

си съдия да носи отговорност за провеждането на надзора. Но не е изключено друг орган да бъде отговорен, „при условие че е достатъчно независим от изпълнителната власт“⁵⁰ и „от органите, извършващи наблюдението, и [е] получил достатъчно правомощия и компетентност, за да упражнява ефективен и непрекъснат контрол“.⁵¹ ЕСПЧ добави, че „начинът на назначаване и правният статут на членовете на надзорния орган“⁵² трябва да се вземат предвид при оценката на независимостта. Това включва „лица, квалифицирани да заемат съдебни длъжности, назначени от парламента или от министър-председателя. За разлика от това е установено, че министър на вътрешните работи, който не само е назначен по политически съображения и е член на изпълнителната власт, но и е участвал пряко във възлагането на специални средства за наблюдение, не е достатъчно независим“.⁵³ ЕСПЧ също така „отбелязва, че е от съществено значение надзорният орган да има достъп до всички съответни документи, включително до класифицираните материали“.⁵⁴ Накрая, ЕСПЧ взема предвид „дали дейността на надзорния орган подлежи на обществен контрол“.⁵⁵

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

43. Последната европейска основна гаранция е свързана с правата на защита на физическите лица. Той/Тя трябва да разполага с ефективни правни средства за защита, за да защити правата си, когато счита, че те не се спазват или не са били спазени. Освен това, Съдът на ЕС обяснява в решението по делото Schrems I, че „правна уредба, в която не се предвижда никаква възможност правният субект да използва правни средства за защита, за да получи достъп до засягащи го лични данни или да поправи, или да заличи такива данни, не зачита същественото съдържание на основното право на ефективна съдебна защита, признато в член 47 от Хартата. Всъщност, в член 47, първа алинея от Хартата се изисква всеки, чиито права и свободи, гарантирани от правото на Съюза, са били нарушени, да има право на ефективни правни средства за защита пред съд в съответствие с предвидените в този член условия“.⁵⁶

44. При оценката на правната уредба на държава членка, която позволява събиране в реално време на данни за трафик и данни за местонахождение, Съдът счете, че уведомяването е необходимо, „за да се даде възможност на засегнатите лица да упражнят правата си съгласно членове 7 и 8 от Хартата да поискат достъп до личните си данни, които са били предмет на тези мерки, и когато е уместно, последните да бъдат поправени или заличени, както и да се възползват, в съответствие с член 47, първа алинея от Хартата, от ефективни правни средства за защита пред съд“.⁵⁷ Той обаче признава също, че уведомяването на лицата, чиито данни са били

⁵⁰ ЕСПЧ, дело Zakharov, точка 258, дело Iordachi и др./Молдова, точка 40 и точка 51 и дело Dumitru Popescu/Румъния, точки 70—73.

⁵¹ ЕСПЧ, дело Klass, точка 56 и дело Big Brother Watch, обжалвано, точка 318

⁵² ЕСПЧ, дело Zakharov, точка 278.

⁵³ ЕСПЧ, дело Zakharov, точка 278.

⁵⁴ ЕСПЧ, дело Zakharov, точка 281.

⁵⁵ ЕСПЧ, дело Zakharov, точка 283.

⁵⁶ Съд на ЕС, Schrems I, точка 95.

⁵⁷ Вж. точка 190 от дело La Quadrature du Net и др. и Съд на ЕС, Становище 1/15, точка 220.

събрани или анализирани, трябва да се извършва само, доколкото и веднага след като уведомяването вече не застрашава задачите, за които отговарят тези органи.⁵⁸

45. Според ЕСПЧ въпросът за ефективните правни средства за защита е неразривно свързан също така с уведомяването на лицето за използваната мярка за наблюдение след приключване на наблюдението. По-специално, Съдът установи, че „по принцип няма достатъчно възможности за сезиране на съдилищата от страна на засегнатото лице, освен ако то не е уведомено за взетите мерки и по този начин може да оспори тяхната законосъобразност ретроспективно или при условията на евентуалност, освен ако лице, което подозира, че неговите съобщения се прихващат или са били прихванати, може да се обърне към съда, така че компетентността на съдилищата да не зависи от уведомяването за прихващането, при условие че е извършено прихващане на неговите съобщения“.⁵⁹ Така ЕСПЧ призна, че в някои случаи може да няма уведомление, но трябва да се предостави ефективно средство за правна защита. В този случай Съдът е пояснил, например в делото *Kennedy*, че даден съд предоставя достатъчно възможности за правна защита, ако отговаря на редица критерии, а именно да е независим и безпристрастен орган, който е приел свой собствен процедурен правилник; да се състои от членове, които трябва да заемат или са заемали висша съдебна длъжност или да бъдат опитни юристи и да не съществува доказателствена тежест, която трябва да бъде преодоляна, за да бъде сезиран.⁶⁰ При разглеждането на жалби от физически лица съдът следва да има достъп до цялата необходима информация,⁶¹ включително до класифицираните материали. И на последно място той следва да разполага с правомощия за отстраняване на неспазването.⁶²

46. Член 47 от Хартата се отнася до трибунал, въпреки че на езиците, различни от английски език, се отдава предпочитание на думата „съд“,⁶³ докато в ЕКПЧ държавите членки само се задължават да гарантират, че „всеки, чиито права и свободи са нарушени, разполага с ефективни правни средства за защита пред национален орган“,⁶⁴ който не е задължително да бъде съдебен орган.⁶⁵

47. Съдът на ЕС, имайки предвид решението по делото *Schrems II*, при оценяване на адекватността на нивото на защита на трета държава, е потвърдил, че „правните субекти трябва да разполагат с възможността да използват правни средства за защита пред независим и безпристрастен съд, за да получат достъп до отнасящи се до тях лични данни или да поправят, или да заличат такива данни“.⁶⁶ По същия начин, Съдът на ЕС счита, че ефективна съдебна защита

⁵⁸ Вж. точка 191 от дело *La Quadrature du Net* и др.

⁵⁹ ЕСПЧ, дело *Zakharov*, точка 234.

⁶⁰ ЕСПЧ, дело *Kennedy*, точка 190.

⁶¹ ЕКЗД отбелязва, че комисарят на Съвета на Европа за правата на човека счита, че така нареченото правило „трети страни“ — съгласно което разузнавателните агенции в дадена държава, които предоставят данни на разузнавателните агенции в друга държава, могат да наложат задължение на приемащите агенции да не разкриват прехвърлените данни на трета страна — не трябва да се прилага за надзорните органи, за да не се подкопава възможността за ефективно средство за защита (Издание относно демократичния и ефективен надзор на службите за национална сигурност).

⁶² ЕСПЧ, дело *Kennedy*, точка 167.

⁶³ Например думата трибунал е преведена като „*Gericht*“ на немски и „*gerecht*“ на нидерландски.

⁶⁴ Член 13 от ЕКПЧ

⁶⁵ ЕСПЧ, *Klass*, точка 67.

⁶⁶ Вж. точка 194 от *Schrems II*.

срещу такава намеса може да бъде осигурена не само от съд, но и от орган,⁶⁷ който предлага гаранции, които по същество са равностойни на изискваните от член 47 от Хартата. В решението си по делото Schrems II Съдът на ЕС подчерта, че независимостта на съда или органа трябва да бъде гарантирана, особено по отношение на изпълнителната власт, с всички необходими гаранции, включително, свързани с условията за освобождаване или отмяна на назначението,⁶⁸ и че правомощията, които следва да бъдат предоставени на съда, трябва да отговарят на изискванията на член 47 от Хартата. Във връзка с това на органа⁶⁹ се предоставят правомощия да приема решения, които са задължителни за разузнавателните служби, в съответствие с правните гаранции, на които субектите на данни биха могли да разчитат.⁷⁰

4. ОКОНЧАТЕЛНИ ЗАБЕЛЕЖКИ

48. Четирите европейски основни гаранции трябва да се разглеждат като основни елементи, които трябва да съществуват при оценката на степента на намеса в основните права на неприкосновеност на личния живот и защита на данните. Те не следва да се оценяват независимо, тъй като са тясно свързани помежду си, а чрез тях следва да се извършва като цяло преглед на съответната правна уредба във връзка с мерките за наблюдение, минималното ниво на гаранции за защита на правата на субектите на данни и средствата за правна защита, предвидени в националното право на третата държава.

49. Тези гаранции изискват известна степен на тълкуване, по-специално, като се има предвид, че не е задължително правната уредба на третата държава да бъде идентична с правната рамка на ЕС.

50. Както посочва ЕСПЧ в решението по дело Kennedy, „тази преценка зависи от съвкупността от обстоятелствата по делото, например естество, обхват и продължителност на евентуалните мерки, необходими причини за тяхното постановяване, компетентни органи за тяхното разрешаване, изпълняване и контролиране, вид правна защита, предоставен от вътрешното право“.⁷¹

51. Следователно оценката на мерките за наблюдение на трети държави спрямо основните европейски гаранции (ОЕГ) може да доведе до две заключения:

-)] Въпросното законодателство на третата държава не гарантира изпълнение на изискванията за ОЕГ: в този случай законодателството на третата държава не би осигурило равнище на защита, което по същество е равностойно на гарантираното в рамките на ЕС.
-)] Въпросното законодателство на третата държава отговаря на ОЕГ.

⁶⁷ Вж. точка 197 от Schrems II, в която Съдът изрично използва тази дума.

⁶⁸ Вж. точка 195 от Schrems II.

⁶⁹ Вж. точка 197 от Schrems II, в която Съдът изрично използва тази дума.

⁷⁰ Вж. точка 196 от Schrems II.

⁷¹ ЕСПЧ, дело Kennedy, точка 153.

52. При оценката на адекватността на нивото на защита съгласно член 45 от ОРЗД Комисията ще трябва да прецени дали ОЕГ са изпълнени като част от елементите, за които се счита, че гарантират, че законодателството на третата държава като цяло предлага ниво на защита, което по същество е равностойно на гарантираното в рамките на ЕС.

53. Когато износителите на данни разчитат, заедно с вносителите на данни, на подходящи гаранции съгласно член 46 от ОРЗД, като се вземат предвид изискванията на законодателството на трета държава, приложимо специално за предаваните данни, те ще трябва да гарантират, че е постигнато ефективно и равностойно по същество ниво на защита. По-специално, когато правото на третата държава не отговаря на изискванията на ОЕГ, това би означавало да се гарантира, че въпросното законодателство няма да засегне гаранциите и мерките, свързани с прехвърлянето, за да може все още да се осигури равнище на защита, което по същество е равностойно на гарантираното в рамките на ЕС.

54. ЕКЗД издаде допълнителни насоки и препоръки, които трябва да бъдат взети предвид, за да се извърши оценка, в зависимост от инструмента за предаване, който ще се използва и на необходимостта да се осигурят подходящи гаранции, включително допълнителни мерки според случая.⁷²

55. Освен това следва да се отбележи, че европейските основни гаранции се основават на изискванията на закона. ЕКЗД подчертава, че ЕОГ се основават на основните права, които се прилагат за всички, независимо от тяхната националност.

56. ЕКЗД отново изтъква, че европейските основни гаранции са референтен стандарт при оценката на намесата, произтичаща от прилагането на мерките за наблюдение на трети държави при международното предаване на данни. Тези стандарти произтичат от правото на ЕС и от съдебната практика на Съда на ЕС и ЕСПЧ, която е задължителна за държавите членки.

⁷² Референтен документ относно адекватното ниво на защита, РД 254, ред. 01, преразгледан и приет на 6 февруари 2018 г.; Препоръки 1/2020 на ЕКЗД относно мерките, които допълват инструментите за прехвърляне, за да се гарантира съответствие с нивото на защита на личните данни в ЕС, 10 ноември 2020 г.