



Брюксел, 12 септември 2022 г.
(OR. en)

12302/22

LIMITE

JUR 579
TELECOM 364
COSI 217
JAI 1155
ENFOPOL 451

Междуинституционално досие:
2021/0106(COD)

СТАНОВИЩЕ НА ПРАВНАТА СЛУЖБА¹

От:	Правната служба
Относно:	Предложение за регламент на Европейския парламент и на Съвета за определяне на хармонизирани правила относно изкуствения интелект – Целесъобразност член 114 и член 16 от ДФЕС да бъдат използвани като правни основания във връзка с разпоредбите, приложими за правоприлагащите и съдебните органи

I. ВЪВЕДЕНИЕ

1. С предложения регламент се установяват хармонизирани правила за пускането на пазара и въвеждането в експлоатация на системи с изкуствен интелект („системи с ИИ“) в Съюза („предложения регламент“)².

¹ Настоящият документ съдържа правно становище, защитено по силата на член 4, параграф 2 от Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета от 30 май 2001 година относно публичния достъп до документи на Европейския парламент, на Съвета и на Комисията, и до което Съветът на Европейския съюз не предоставя публичен достъп. Съветът си запазва всички законни права по отношение на неразрешено публикуване.

² Док. 8115/21.

2. На заседанието на работна група „Телекомуникации и информационно общество“ от 7 април 2022 г. Правната служба на Съвета изложи становището си относно това доколко е целесъобразно две разпоредби (членове 16 и 114 от ДФЕС) да бъдат използвани като правно основание на предложения регламент относно системите с изкуствен интелект („системи с ИИ“). С разясненията беше потвърдено, че правилните правни основания за предложението са членове 16 и 114 от ДФЕС, както и че не е подходящо да се използва член 87, параграф 2 от ДФЕС вместо член 114 от ДФЕС. По искане на работната група настоящото становище излага и доразвива в писмен вид изказването на представителя на Правната служба на Съвета на посоченото заседание.
3. Определение на понятието „системи с ИИ“ се съдържа в член 3, параграф 1 от предложения регламент. Като цяло тези системи съответстват на определени видове софтуер. Предложеният регламент се прилага както за доставчиците, които пускат на пазара системи с ИИ, така и за доставчиците, които въвеждат в експлоатация такива системи. В допълнение предложеният регламент се прилага и за ползвателите. „Доставчик“ може да бъде физическо или юридическо лице или публичен орган/организация, които разработват система с ИИ или възлагат разработването на система с ИИ с цел пускането ѝ на пазара или въвеждането ѝ в експлоатация под собственото им име или търговска марка. „Ползвател“ може да бъде всяко физическо или юридическо лице, публичен орган, агенция или друга организация, които използват система с ИИ, по отношение на която имат правомощия.

4. Съгласно определенията в член 3 правоприлагащите и съдебните органи могат да бъдат квалифицирани като доставчици и/или като ползватели на система с ИИ. Системите с ИИ, които са предназначени, както е определено от доставчика, за използване в сферата на правоприлагането или правораздаването, са класифицирани като високорискови съгласно приложение III. Като такива те трябва да изпълняват съществени изисквания (управление на риска, изпитване, управление на данни, техническа документация, прозрачност, човешки надзор, точност, надеждност и киберсигурност) и задължения (като системи за управление на качеството, техническа документация, оценяване на съответствието, коригиращи действия, задължение за информиране, задължения на вносителите и дистрибуторите), както и стандарти и оценка на съответствието. Хармонизираните правила са в духа на правилата, които се прилагат по отношение на безопасността на продуктите в Директива 2006/42/ЕО (машини)³ и Регламент (ЕО) 2017/745 (медицински изделия)⁴.
5. Що се отнася до системите с ИИ, включващи използването на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места за целите на правоприлагането, те попадат в категорията на забранените системи с ИИ. Същевременно са предвидени изключения от забраната за използване на системи с ИИ. На практика държавите членки могат да разрешат или не използването на такива системи. Ако са разрешени, системите са обект на детайлно уредени ограничения и предпазни мерки, така че използването им да бъде ограничено до строго необходимото и за да се защити основното право на защита на личните данни. Тези ограничения и предпазни мерки са предвидени в предложения регламент на основание член 16 от Договора за функционирането на Европейския съюз („ДФЕС“) и трябва да бъдат допълнително уредени в националното право. Член 5, параграф 1, буква г) и параграфи 2, 3 и 4 от предложения регламент представляват *lex specialis* спрямо Директива 2016/680 (Директива за защита на данните в областта на правоприлагането), която беше приета на основание член 16, параграф 2 от ДФЕС.

³ Директива 2006/42/ЕО на Европейския парламент и на Съвета от 17 май 2006 г. относно машините и за изменение на Директива 95/16/ЕО, ОВ L 157, 9.6.2006 г., стр. 24—86.

⁴ Регламент (ЕС) 2017/745 на Европейския парламент и на Съвета от 5 април 2017 г. за медицинските изделия, за изменение на Директива 2001/83/ЕО, Регламент (ЕО) № 178/2002 и Регламент (ЕО) № 1223/2009 и за отмяна на директиви 90/385/ЕИО и 93/42/ЕИО на Съвета, ОВ L 117, 5.5.2017 г., стр. 1—175.

В съответствие с член 5, параграф 1, буква г) целите на тези системи са ограничени до:

- i) целево издирване на конкретни потенциални жертви на престъпления, включително изчезнали деца;
- ii) предотвратяване на конкретна, значителна и непосредствена заплаха за живота или физическата безопасност на физически лица или на терористично нападение;
- iii) откриване, локализиране, идентифициране или преследване на извършител или заподозрян в извършването на престъпление, посочено в член 2, параграф 2 от Рамковото решение относно европейската заповед за арест⁵ и наказуемо в съответната държава членка с лишаване от свобода или мярка за задържане с максимален срок не по-малко от 3 години, както е определено в законодателството на съответната държава членка.

Съгласно член 5, параграф 3 използването на такива технологии от правоприлагащите органи подлежи на предварително разрешение от съдебен или административен орган. При надлежно обосновани спешни случаи обаче използването на системата може да започне без разрешение, като разрешението може да се поиска по време на използването или впоследствие.

Съгласно член 5, параграф 4 държава членка може да реши да разреши използването на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места за целите на правоприлагането и да въведе необходимите подробни правила за подаване на искания, издаване и изпълнение на предварително разрешение, както и за престъпленията, по отношение на които се иска това.

6. Правните основания за предложения регламент са член 16 от ДФЕС (защита на личните данни) и член 114 от ДФЕС (функциониране на вътрешния пазар). Оттук възниква въпросът доколко е целесъобразно тези правни основания да се използват във връзка с хармонизираните правила, приложими за системите с ИИ, предоставяни или използвани от правоприлагащите и съдебните органи.

⁵ Рамково решение 2002/584/ПВР на Съвета от 13 юни 2002 г. относно европейската заповед за арест и процедурите за предаване между държавите членки, ОВ L 190, 18.7.2002 г., стр. 1.

7. Настоящото становище акцентира на първо място върху целесъобразността член 114 от ДФЕС да бъде използван като правно основание в конкретния контекст на правоприлагащите органи, които са посочени в няколко разпоредби на предложения регламент, т.е. по отношение на системите за дистанционна биометрична идентификация в реално време на обществено достъпни места и високорисковите системи с ИИ, посочени в точка 6 от приложение III. Следователно в него се разглежда въпросът дали член 87, параграф 2 от ДФЕС (полицейско сътрудничество) би бил подходящо правно основание, така че да се обхване предоставянето и използването на системи с ИИ от правоприлагащите органи, вместо член 114 от ДФЕС (раздел II). По аналогия заключението в настоящата бележка може да се приложи за съдебните органи, посочени в приложение III, относно високорисковите системи с ИИ.
8. Освен това в настоящата бележка се разглежда доколко е целесъобразно член 16 от ДФЕС да се използва като допълнително правно основание, както и въпросът за прилагането на протоколи 21 и 22 в контекста на използването на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места от правоприлагащите органи (раздел III).

II. ЦЕЛЕСЪОБРАЗНОСТ ЧЛЕН 114 ОТ ДФЕС ДА БЪДЕ ИЗПОЛЗВАН КАТО ПРАВНО ОСНОВАНИЕ

9. Според установената съдебна практика правното основание на даден акт на Съюза не зависи от убедеността на дадена институция, що се отнася до преследваната цел, а трябва да се определи по обективни критерии, които да могат да бъдат предмет на съдебен контрол, включително, по-специално, целта и съдържанието на мярката. Ако при разглеждането на мярката се установи, че тя има двойна цел или е съставена от две части, едната от които може да бъде определена като основна или преобладаваща, докато другата е само акцесорна, мярката трябва да има едно-единствено правно основание, а именно правното основание, което съответства на основната или преобладаващата цел или съставна част. Единствено по изключение и ако е установено, че актът има едновременно няколко цели, неделими една от друга, като никоя от тях не е вторична или косвена спрямо друга, този акт може да се базира на съответните различни правни основания, освен в случаите, когато тези правни основания предписват процедури, които са несъвместими помежду си. Следва също да се отбележи, че в първото изречение на член 114, параграф 1 от ДФЕС се пояснява, че разпоредбите на този член се прилагат „[о]свен ако в Договорите не е предвидено друго“. Следователно използването на член 114 от ДФЕС е обосновано само ако липсва по-конкретна разпоредба, която да може да послужи за приемането на въпросната мярка⁶. Ако в Договора съществува по-конкретна разпоредба, която може да бъде правно основание на съответната мярка, тази мярка трябва да се основава на тази разпоредба⁷.

⁶ Становище на Правната служба на Съвета от 17 май 2016 г., 9007/16, точка 6.

⁷ Решение на Съда от 29 април 2004 г., *Комисия/Съвет*, Дело C- 338/01, EU:C:2004:253, точка 60.

A. ЦЕЛ НА ПРЕДЛОЖЕНИЯ РЕГЛАМЕНТ

10. Предложеният регламент хармонизира пускането на пазара, въвеждането в експлоатация и използването на конкретен вид софтуер (системи с ИИ). Фактът, че публичните органи и частните оператори могат да бъдат доставчици или ползватели на такива системи с ИИ, сам по себе си не е несъвместим с правното основание на член 114 от ДФЕС⁸.
11. Освен това фактът, че правоприлагащите органи или онези, които действат от тяхно име, могат да бъдат сред доставчиците или ползвателите на такива системи с ИИ, не е достатъчен, за да обоснове използването на член 87 от ДФЕС като правно основание. За да се определи дали това е необходимо, трябва да се анализират целта и съдържанието на предложения регламент.
12. Като цяло предложеният регламент има за цел, включително по отношение на системите за дистанционна биометрична идентификация в реално време на обществено достъпни места и високорисковите системи с ИИ, да гарантира последователно и високо равнище на защита в целия Съюз, като същевременно се предотвратява възпрепятстването на свободното движение на системи с ИИ и свързани с тях продукти и услуги в рамките на вътрешния пазар. С него се установяват еднакви задължения за операторите и се гарантира еднаква защита на императивни съображения от обществен интерес и на правата на лицата в целия вътрешен пазар (съображение 2). Предложеният регламент определя по-специално правила, уреждащи пускането на пазара и въвеждането в експлоатация на определени системи с ИИ, като по този начин гарантира безпрепятственото функциониране на вътрешния пазар и дава възможност тези системи да се ползват от принципа на свободно движение на стоки и услуги (съображение 5). Като цяло предложението цели да бъде създаден още при проектирането надежден, приложим във всички области ИИ, с пълен набор от правила за разработването, предлагането на пазара и използването на основани на ИИ продукти, услуги и системи. Предвид факта, че ИИ вече се използва в огромен брой услуги и продукти и че това ще продължи и в бъдеще, предложението следва логиката на вътрешния пазар, като определя „рамка за безопасност на продуктите“, изградена около четири рискови категории. С него се налагат изисквания за навлизане на пазара и сертифициране на високорискови системи с ИИ чрез задължителна процедура за маркировка „СЕ“.

⁸ Вж. становището на Правната служба на Съвета (ST 11395/14, точки 39—41) и прецеденти като Директива (ЕС) 2016/2102, директиви 2014/24/ЕС, 2014/25/ЕС и 2014/23/ЕС.

13. Нито една от заявените цели на предложения регламент не се отнася до постигането на цели, свързани с обществената сигурност. Дори ако целите, свързани с обществената сигурност, трябва да бъдат постигнати непряко чрез процеса на хармонизиране на пускането на пазара/въвеждането в експлоатация/използването на системи с ИИ от правоприлагащите органи, при тълкуването на член 87, параграф 2 от ДФЕС в светлината на член 67 от ДФЕС Съдът⁹ заяви, че за да може даден акт на Съюза, предвид неговата цел и съдържание, да се основава на член 87, параграф 2 от ДФЕС, той трябва да бъде пряко свързан с целите, определени в член 67 от ДФЕС (т.е. в този случай — предотвратяване на престъпността и полицейско сътрудничество). В контекста на предложения регламент това е изключено, тъй като единствените хармонизирани правила за използването на такива системи от правоприлагащите органи са или (1) типовите правила за безопасност на продуктите, които се прилагат еднакво за всички доставчици и ползватели във връзка с пускането на пазара/въвеждането в експлоатация или използването на системите с ИИ, или (2) правилата за защита на личните данни, за които член 16 от ДФЕС е добавен като правно основание (вж. част III по-долу).
14. По друго дело¹⁰, въпреки че целта на изменението на Директивата за огнестрелните оръжия беше да се гарантира по-високо равнище на обществена сигурност по отношение на терористичната заплаха и други форми на престъпност, Съдът приема, че хармонизирането на аспектите, свързани с безопасността на стоките, е един от съществени елементи за правилното функциониране на вътрешния пазар, тъй като разнородните правила в тази област могат да създадат пречки пред търговията¹¹.

⁹ Решение от 6 май 2014 г., *Европейска комисия/Европейски парламент и Съвет на Европейския съюз*, C- 43/12, EU:C:2014:298.

¹⁰ Решение от 3 декември 2019 г., *Чешка република/Европейски парламент*, C-482/17, EU:C:2019:1035.

¹¹ Пак там, съображение 57: „Тъй като обаче, противно на твърдяното от Република Полша, особеността на огнестрелните оръжия е тяхната опасност не само за ползвателите, но и за широката общественост, както Съдът вече е отбелязал в точка 54 от решение от 23 януари 2018 г., *Buhagiar* и др. (C- 267/16, EU:C:2018:26), както се припомня в нето съображение от Директива 91/477, съображения за обществена сигурност са абсолютно необходими в рамките на правна уредба относно придобиването и притежаването на тези стоки“. Вж. също решението от 23 януари 2018 г., *Albert Buhagiar* и др./*Minister for Justice*, C-267/16, EU:C:2018:26, точка 54: „В това отношение е важно да се отбележи, че с оглед на риска за безопасността на хората, който представляват огнестрелните оръжия, тяхното свободно движение може да бъде постигнато само чрез стриктно регламентиране на условията за тяхното пренасяне между държави членки, сред които е принципът за предварителното разрешение, издавано от държавите членки, в които се пренасят такива стоки“.

15. Целите на предложения регламент, включително член 5, параграф 1, буква г), параграфи 2, 3 и 4 относно използването на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места за целите на правоприлагането и разпоредбите, свързани с високорисковите системи с ИИ, посочени в точка 6 от приложение III, не са пряко свързани с цел в областта на обществената сигурност. Напротив, предложението взема предвид основните опасения, свързани с начина, по който системите с ИИ засягат здравето, безопасността и основните права. Поради това съответните разпоредби са пряко свързани с целта за осигуряване на еднакви условия на конкуренция при пускането на пазара/въвеждането в експлоатация или използването на системи с ИИ на вътрешния пазар, като същевременно се защитават здравето, безопасността и основните права на ползвателите.
16. С оглед на гореизложеното основната цел на предложения регламент е да се подобри функционирането на вътрешния пазар по смисъла на член 114 от ДФЕС, а целите, посочени в член 67 от ДФЕС, са само непряко и акцесорно свързани с тази основна цел.

Б. СЪДЪРЖАНИЕ НА ПРЕДЛОЖЕНИЯ РЕГЛАМЕНТ

17. Предложеният регламент по същество съдържа правила за това какво е необходимо за пускането на конкретен продукт (софтуер с ИИ) на пазара (или за въвеждането му в експлоатация), за да се гарантира, че той е безопасен и спазва основните права. В него се определя пълен набор от правила за разработването, предлагането на пазара и използването на основани на ИИ продукти, услуги и системи. Предложеният регламент не задължава правоприлагащите органи да използват система с ИИ, която е пусната законосъобразно на пазара, нито урежда пряко начина, по който правоприлагащите органи следва да използват такава система с ИИ. Вместо това той ясно определя ситуациите, при които предвидената употреба се счита за високорискова просто защото дадена система с ИИ ще бъде използвана от правоприлагащите или от съдебните органи.

18. Освен това член 29 от предложения регламент съдържа правила относно условията за използване на високорискови системи с ИИ, но тази уредба не е специфична за сектора, има ограничен обхват (главно по отношение на инструкциите за употреба на продукта) и е неразривно свързана със задълженията, наложени на разработчиците на системи с ИИ съгласно предложения регламент. Той също така предоставя на държавите членки известна свобода на действие да въведат допълнителни правила относно използването на такива високорискови системи с ИИ. По отношение на системите за дистанционна биометрична идентификация в реално време на обществено достъпни места, използвани за целите на правоприлагането (член 5), предложеният регламент урежда частично използването на такива системи от гледна точка на защитата на данните въз основа на член 16 от ДФЕС (вж. част III по-долу).
19. Освен това само държавите членки могат да решат да предвидят възможност за пълно или частично разрешаване на използването на такива системи за дистанционна биометрична идентификация в реално време. Конкретните условия за това използване се определят в националното право, но трябва да са в унисон с общите критерии и предпазни мерки, определени в регламента: предварително съдебно или административно разрешение, искане, издаване и изпълнение на предварителното разрешение, както и посочване на престъпленията, във връзка с които могат да се използват тези системи.

20. Системите с ИИ са специфичен вид софтуер. Следователно хармонизираните правила, които се прилагат за пускането на пазара или въвеждането в експлоатация/използването на системи с ИИ, са сходни с хармонизираните правила за безопасност на продуктите. Те се прилагат по еднакъв начин, без да се прави разграничение между публични и частни ползватели. Съгласно съответните съображения от предложения регламент следва да се гарантира последователна и висока степен на защита в целия Съюз. Същевременно следва да се предотвратят различията, които възпрепятстват свободното движение на системите с ИИ и свързаните с тях продукти и услуги в рамките на вътрешния пазар. Това ще се постигне чрез установяване на еднакви задължения за операторите и осигуряване на еднаква защита на императивните съображения от обществен интерес и на правата на лицата в целия вътрешен пазар въз основа на член 114 от ДФЕС¹².
21. В приложение III относно високорисковите системи с ИИ предложеният регламент съдържа няколко позовавания на правоприлагането, управлението на граничния контрол и правораздаването (съответно точки 6, 7 и 8). Те включват подробно и изчерпателно изброяване, съответстващо на член 6, параграф 2, в допълнение към други високорискови системи във връзка с рисковете за безопасността на продуктите, посочени в член 6, параграф 1. Всъщност съгласно член 6, параграф 1 някои системи с ИИ трябва да се считат за високорискови по дефиниция поради очакваната им сериозност и високите рискове за основните права, здравето и безопасността. Други системи, считани за високорискови и изброени в приложение III, включват образование, управление на критични инфраструктури, заетост, биометрична идентификация и категоризация, както и достъп до основни обществени и частни услуги.

¹² Поради това е необходима правна рамка на Съюза, с която да се определят хармонизирани правила относно изкуствения интелект, за да се насърчи разработването, използването и навлизането на изкуствения интелект на вътрешния пазар, и която същевременно осигурява високо равнище на защита на въпросите от обществен интерес, като здравето и безопасността, и защитата на основните права, признати и защитени от правото на Съюза. За постигането на тази цел следва да бъдат установени правила относно пускането на пазара и въвеждането в експлоатация на някои системи с ИИ, като по този начин се гарантира безпрепятственото функциониране на вътрешния пазар и се даде възможност тези системи да се ползват от принципа на свободно движение на стоки и услуги (вж. съображения 2 и 5 от предложението).

22. Тези правила за високорисковите системи с ИИ обаче не указват дали правоприлагащите и съдебните органи (или тези в другите посочени области) следва или не следва да използват такива системи. Предложеният регламент ще окаже само косвено въздействие върху реалното развитие на системите с ИИ, които могат да се използват от правоприлагащите органи, и върху използваните понастоящем и в бъдеще системи с ИИ. Следователно правилата се отнасят до системи с ИИ, които са *„предназначени да се използват“* от такива органи (вж. например член 3, точка 12, член 8, параграф 2 и приложение III). Определянето на дадена система с ИИ като високорискова води до прилагането на специфичен набор от правила относно управлението на риска, управлението на данните и техническите спецификации. Ползвателите на такива високорискови системи с ИИ трябва да спазват инструкциите за употреба, да поддържат регистри и да извършват оценки на въздействието върху защитата на данните.
23. Освен това в правото на Съюза или в националното право могат да бъдат установени задължения на ползвателите, различни от задълженията, свързани с инструкциите за употреба, , без да се засяга правото на преценка на ползвателя при организирането на собствените му ресурси и дейности с цел изпълнение на мерките за човешки надзор, посочени от доставчика (член 29, параграф 2 от предложения регламент). Тези правила предвиждат допълнителни гаранции за основните права за високорисковите системи с ИИ.

24. С оглед на гореизложеното следва да се подчертае, че предложеният регламент не съдържа правила, които имат за цел да позволят или предотвратят използването от правоприлагащите органи на пусната на пазара високорискова система с ИИ. Съгласно предложените правила за система с ИИ, разработена или използвана от правоприлагащите органи в резултат на предвидената ѝ употреба, ще се прилага отделен етикет (за висок риск). Това използване ще се урежда от националното право и до известна степен ще се решава от самите правоприлагащи органи. Всъщност в член 29 от предложения регламент е установен минимум от условия за употреба (ограничени до инструкциите за употреба) за високорисковите системи с ИИ, включително изброените в точки 6, 7 и 8 от приложение III, които ще бъдат допълнително уредени в националното право. Ето защо в съответствие със съдебната практика на Съда следва да се внесе разграничение между, от една страна, планираната цел на предложения регламент, която не е да се регулира използването на системи с ИИ от правоприлагащите органи, и, от друга страна, въздействието, което то може да има непряко¹³, които не са от значение за анализа на целесъобразността на правното основание.
25. Точки 6, 7 и 8 (съответно относно правоприлагането, миграцията и правораздаването) не са преобладаващи сред високорисковите системи с ИИ. Всъщност съгласно предложения регламент високорискова система с ИИ не е непременно система, която е включена в списъка в приложение III. Повечето високорискови системи всъщност са изброените по общ начин в член 6, параграф 1, буква а) и б) от предложения регламент (във връзка с безопасността на продуктите). Други високорискови системи с ИИ са изброени в приложение III, съдържащо точки 1 (биометрична идентификация), 2 (критична инфраструктура), 3 (образование и професионално обучение) и 4 (заетост, управление на работниците и достъп до самостоятелна заетост), които се отнасят до области, различни от правосъдието и вътрешните работи (ПВР). Всички ползватели на такива високорискови системи с ИИ подлежат на единен режим, установен не с оглед на техния специфичен статут (например дали са икономически оператори или публични органи), а от гледна точка на защитата на здравето, безопасността и основните права.

¹³ Вж. решението на Съда от 21 юни 2018 г., *Република Полша/Европейски парламент, Съвет на Европейския съюз*, C-5/16, EU:C:2018:483, точки 63—68, и решението на Съда от 22 юни 2022 г., *Leistritz AG/LH*, C-534/20, EU:C:2022:495, точка 28.

26. Ето защо предложеният регламент съдържа хармонизирани правила относно пускането на пазара, въвеждането в експлоатация и използването на системи с ИИ, независимо дали те се използват от частни оператори или публични органи, включително, акцесорно¹⁴, от правоприлагащи и съдебни органи.
27. Като се остави настрана използването на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места за целите на правоприлагането, за което се прилагат специални правила относно обработването на лични данни (вж. част III по-долу), предложеният регламент не съдържа хармонизирани правила относно използването на високорискови системи с ИИ. Както е обяснено в точки 18 и 19 по-горе, позоваването на използването на високорискови системи с ИИ по същество се отнася до инструкциите за употреба на продукта (член 29) и е свързано със задълженията, наложени на разработчиците. Както е посочено в точка 22, решението дали правоприлагащите или съдебните органи могат да използват високорискова система с ИИ, която е законосъобразно пусната на пазара съгласно предложения регламент, се взема съгласно националното право и от националните органи.
28. Поради това член 87, параграф 2 от ДФЕС, и по-специално буква а) от него, не е подходящо правно основание за предложения регламент. Правилата в предложението нито насърчават, нито възпрепятстват събирането, съхранението, обработването, анализа и обмяна на съответната информация. Когато тези дейности се извършват от правоприлагащи органи, просто трябва да се спазват редица неспецифични хармонизирани условия с цел защита правата на потребителите. По подобен начин заявените цели на предложения регламент не включват разработването на общи техники за разследване. Предложените изисквания относно използването на високорискови системи с ИИ не са специфични за областта на ПВР и не се отнасят до полицейското сътрудничество в тесен смисъл, както е определено в ДФЕС.

¹⁴ Вж. становището на Съда относно *Истанбулската конвенция*, A-1/19, EU:C:2021:198, по-специално точки 298 и 301.

29. Съгласно разпоредбите на член 5, параграф 4 от предложението регламент дадена държава членка все пак може да реши да разреши използването на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места за целите на правоприлагането. В случай че вземе такова решение, държавата членка е длъжна да определи необходимите подробни правила за подаването на искане, издаването и изпълнението на предварителното разрешение, както и престъпленията, за чието разследване или наказателно преследване е разрешено използването¹⁵. В съответствие с резултатите от обсъжданията в рамките на Съвета предложените правила няма да доведат до предоставяне на нови правомощия на съответните национални органи. Вместо това използването на съществуващи или евентуални бъдещи механизми е ограничено, за да се гарантира защитата на правото на неприкосновеност на личния живот и на личните данни.
30. С оглед на гореизложеното член 114 от ДФЕС е единственото подходящо правно основание за хармонизирани правила относно високорисковите системи с ИИ, включително тези, които се използват от правоприлагащите и съдебните органи, а правното основание в областта на ПВР в част трета, дял V от ДФЕС, като например член 87 от ДФЕС по отношение на тези хармонизирани правила, не е нито обосновано, нито целесъобразно.

¹⁵ Следва да се отбележи, че член 5, параграф 4 от предложението има някои характеристики, подобни на тези на член 15, параграф 1 от Директива 2002/58 за електронната търговия. По-специално в него се предвижда възможност за държавите членки да дерогират от някои забрани, установени в правото на Съюза. Съгласно постоянната съдебна практика националните разпоредби, които имат за цел да дерогират от тази забрана, задължително попадат в обхвата на правото на Съюза, което от своя страна задейства прилагането на Хартата по отношение на тях.

III. ЦЕЛЕСЪОБРАЗНОСТ ЧЛЕН 16 ОТДФЕС ДА БЪДЕ ИЗПОЛЗВАН КАТО ДОПЪЛНИТЕЛНО ПРАВНО ОСНОВАНИЕ

31. Предложеният регламент включва като правно основание член 16 отДФЕС, като по отношение на обработването на лични данни в областта на правоприлагането в съображения 25 и 26 от него се съдържа позоваване на член 6а от Протокол № 21 и член 2а от Протокол № 22 относно обработването на лични данни в областта на предотвратяването на престъпността. Според Комисията член 16 отДФЕС има за цел да служи изключително като правно основание за разпоредбите, с които се въвеждат ограничения върху обработването на биометрични лични данни по допълващ начин в сравнение с Директива 2016/680 (Директива относно правоприлагането в областта на защитата на данните). Член 5, параграф 1, буква в) е формулиран като принципна забрана, от която се прилагат три изключения. По-конкретно, използването на системи за дистанционна биометрична идентификация в реално време на обществено достъпни места за целите на правоприлагането е забранено, освен ако то е строго необходимо за:
- а) целево издирване на потенциални жертви на престъпления, б) предотвратяване на непосредствено терористично нападение или атака срещу физическата безопасност/живота на физическо лице; в) локализиране, идентифициране или преследване на извършител или заподозрян в извършването на тежко престъпление (с позоваване на европейската заповед за арест). В член 5, параграфи 2, 3 и 4 се предвиждат допълнителни изисквания, свързани с това конкретно използване на системи с ИИ от правоприлагащите органи, по-специално оценка на необходимостта и пропорционалността, предварително разрешение (освен в извънредни ситуации) и решение на държавите членки дали да разрешат на национално равнище конкретното използване на инструменти с ИИ в такива ситуации.
32. Член 5 е подробна разпоредба, уреждаща конкретно използване на инструменти с ИИ, която не само има за цел да допълни съществуващата законодателна рамка на Съюза (Директивата относно правоприлагането в областта на защитата на данните, която се основава на член 16 отДФЕС), но изисква и национална рамка за изпълнение.

33. По същество, въпреки че е формулирано като забрана, специфичното правило в член 5 може да се опише като установяващо строга и извънредна рамка за широко разпространения мониторинг в реално време чрез инструменти с ИИ на физически лица на открито с оглед тяхното идентифициране. Забраната също така надхвърля обикновеното използване на камери за записване и се отнася до използването на инструменти с ИИ с цел автоматизирано разпознаване на човешки характеристики на обществено достъпни места (характеристики като лице, но и походка, пръстови отпечатъци, ДНК, глас, динамика при натискане на клавишите на клавиатура и други биометрични или поведенчески сигнали). Това предполага и съпътстващо снемане на данни за лицата и тяхното идентифициране чрез сравнителен анализ/проверка на данните. Освен това правилото трябва да се преценява и с оглед на факта, че идентифицирането в реално време от частни ползватели на обществени места също може да бъде разрешено (за събития като футболни срещи).
34. Направените от Комисията допълнителни разяснения показват, че понастоящем нито една или евентуално много малко държави членки са регламентирали този конкретен въпрос, с цел да се позволи на правоприлагащите органи да използват инструменти с ИИ за откриване в реално време на физически лица на обществени места. От практическа гледна точка обаче, въпреки че не бяха представени убедителни данни, доказващи, че съществуващите практики и инструменти ще трябва да се променят, изглежда ясно, че бъдещите техники за разследване, криминалистични методи и правила за събиране на доказателства ще трябва да интегрират този подход на забрана/изключения.
35. Що се отнася до правното основание, разпоредбите, с които се въвеждат ограничения върху обработването на биометрични лични данни по допълващ начин (в сравнение с Директивата относно правоприлагането в областта на защитата на данните), целят защита на личните данни чрез установяване на подходящи гаранции. Тази цел е неразривно свързана с целта на разпоредбите, попадащи в обхвата на член 114 от ДФЕС, без едната от тях да е второстепенна и косвена спрямо другата. Предложеният регламент има за цел да се определи обща рамка за системите с ИИ, като се следва основан на риска подход. В този контекст хоризонталното регулиране на системите с ИИ може да включва строги гаранции, приложими за тази конкретна система с ИИ за откриване в реално време. Следователно една такава специфична система с ИИ, съдържаща подходящи гаранции за защита на личните данни, е неразривно свързана с общата цел за подобряване на функционирането на вътрешния пазар и не е второстепенна или косвена по отношение на нея. Поради това предложеният регламент следва да има като правно основание две разпоредби в съответствие с приложимата съдебна практика (вж. точка 9 по-горе).

36. Остава обаче въпросът кое правно основание следва да се използва за регламентиране на обработването на лични данни за целите на използването на системите, посочени в член 5, параграф 1, буква в) — параграф 4 от предложения регламент. Всъщност член 87, параграф 2, буква а) от ДФЕС представлява правно основание за мерките, предприемани от правоприлагащите служби във връзка с предотвратяването, разкриването и разследването на престъпления, отнасящи се до събирането, съхранението, обработването, анализа и обмяна на съответната информация.
37. Както обаче посочва генералният адвокат в становището си относно споразумението с Канада относно резервационните данни на пътниците (A1/15), член 16 от ДФЕС, от една страна, и член 87, параграф 2, буква а) и член 82, параграф 1, буква г) от ДФЕС, от друга страна, не могат да имат йерархични отношения от вида „*lex generalis* — *lex specialis*“¹⁶. Член 16, параграф 2 от ДФЕС е единствената разпоредба, която се прилага към правилата, свързани със защитата на физическите лица по отношение на обработването на лични данни от правоприлагащите органи на държавите членки при извършването на дейности за предотвратяване на престъпления. Самият факт, че член 5 се позовава на списъка на тежките престъпления в Рамковото решение относно европейската заповед за арест не променя тази оценка: това позоваване не означава, че Рамковото решение се прилага¹⁷. Става въпрос единствено за законодателна техника, при която тежките престъпления се посочват, без да е необходимо да се създава отделно приложение.
38. Това не променя факта, че предвиденото в член 5 правило не е установено като средство за допълнително ограничаване на условията за прилагане на тези мерки, свързани с ПВР, а с цел да се гарантира, че в бъдеще всяко използване на биометричната идентификация в реално време от системите с ИИ ще отговаря адекватно на опасенията, свързани с основните права, и най-вече на необходимостта да се гарантира, че биометричните данни се събират и обработват при зачитане на правото на неприкосновеност на личния живот и на личните данни.

В това отношение регламентът няма за цел да установи нова, задължителна и специфична за ПВР процедура, а по-скоро се основава на изпитани и тествани процедурни средства, за да се гарантира зачитането на основните права.

¹⁶ Вж. становището на генералния адвокат P. Mengozzi от 8 септември 2016 г., *Проект за споразумение между Канада и Европейския съюз*, Становище 1/15, EU:C:2016:656, точки 112—120.

¹⁷ Що се отнася до прилагането на този списък с тежки престъпления от държавите членки, вж. решението на Съда от 21 юни 2022 г., *Луга за правата на човека/Съвет на министрите*, C-817/19, EU:C:2022:65, точки 150—152.

39. Ако член 16 от ДФЕС е подходящо допълнително правно основание, това повдига въпроси относно прилагането на членове 6а и 2а съответно от протоколи 21 и 22. Както е обяснено в съображения 25 и 26 от предложението, това означава, че когато правоприлагащите органи в Ирландия или Дания използват системи за дистанционна биометрична идентификация в реално време на обществено достъпни места с цел предотвратяване на престъпления и когато Ирландия или Дания не са обвързани от съответните правила за полицейско или съдебно сътрудничество по наказателноправни въпроси, тези две държави членки няма да бъдат обвързани от член 5, параграф 1, буква г) и параграфи 2 и 3 от предложения регламент. Това не означава, че член 5, параграф 1, буква г) и параграфи 2 и 3 съдържат правила относно полицейското сътрудничество, като например правила за обмен на информация между правоприлагащите органи. Това означава единствено, че член 5, параграф 1, буква г) и параграфи 2 и 3 от предложения регламент, подобно на Директива 2016/680 (Директива относно правоприлагането в областта на защитата на данните), която е *lex generalis*, приета въз основа на член 16 от ДФЕС, уреждат обработването на биометрични лични данни в специфичния контекст на системите за дистанционна биометрична идентификация в реално време на обществено достъпни места с цел предотвратяване на престъпления и нищо повече. В това отношение предложението на Комисията следва подхода, възприет от законодателя на Съюза за Директивата относно правоприлагането в областта на защитата на данните, с което се потвърждава, че използването на член 87, параграф 2 от ДФЕС в този контекст не е обосновано.
40. В конкретния случай добавянето на член 16 от ДФЕС към член 114 от ДФЕС е обосновано от факта, че член 5, параграф 1, буква г) и параграфи 2 и 3 са единствените разпоредби, уреждащи разрешени случаи за използването на система с ИИ, което нарушава правото на защита на личните данни, което пък представлява *lex specialis* по отношение на общата рамка за защита на данните. Тези специални правила за защита на данните, засягащи използването на такива чувствителни системи с ИИ, не могат да се считат за вторични или косвени по отношение на правното основание за вътрешния пазар. Поради това добавянето на член 16 от ДФЕС като правно основание е достатъчно обосновано в предложения регламент и използването на член 87, параграф 2, буква а) от ДФЕС не е целесъобразно.

IV. ЗАКЛЮЧЕНИЕ

41. Предвид изложеното по-горе Правната служба на Съвета смята, че:

- а) Използването на членове 16 и 114 от ДФЕС като правно основание за предложения регламент е обосновано и целесъобразно;
 - б) Използването на член 87, параграф 2 от ДФЕС или на друго правно основание в областта на ПВР не е обосновано, нито подходящо във връзка с хармонизираните правила, приложими за системите с ИИ, които могат да бъдат предоставяни или използвани от правоприлагащите или съдебните органи.
-