Насоки

Насоки № 05/2022 относно използването на технология за лицево разпознаване в областта на правоприлагането

Версия 2.0

Приети на 26 април 2023 г.

История на версиите

Версия 1.0	12 май 2022 г.	Приемане на насоките за обществена консултация
Версия 2.0	26 април 2023 г.	Приемане на насоките след обществена консултация

Съдържание

КРАТКО ИЗЛОЖЕНИЕ

Все повече правоприлагащи органи (ПО) прилагат или възнамеряват да прилагат технология за лицево разпознаване (ТЛР). Тя може да се използва за **удостоверяване на автентичността** или за **определяне на самоличността** на дадено лице и да се прилага върху видеоклипове (напр. CCTV) или снимки. Тя може да се използва за различни цели, включително за търсене на лица в списъците за наблюдение на полицията или за наблюдение на движението на дадено лице в публичното пространство.

ТЛР е изградена въз основа на обработването на **биометрични данни**, поради което обхваща обработването на специални категории лични данни. Често в ТЛР се използват компоненти на **изкуствен интелект** (ИИ) или машинно самообучение (МС). Макар че това дава възможност за широкомащабно обработване на данни, то също така поражда риск от дискриминация и неверни резултати. ТЛР може да се използва в контролирани ситуации на директен контакт, но също така и в огромни тълпи и важни транспортни центрове.

ТЛР е **чувствителен инструмент за правоприлагащите органи.** Правоприлагащите органи са изпълнителни органи и имат суверенни правомощия. ТЛР има склонност да засяга основните права — също и отвъд правото на защита на личните данни — и може да окаже влияние върху нашата социална и демократична политическа стабилност.

По отношение на защитата на личните данни в сферата на правоприлагането трябва да бъдат изпълнени **изискванията на Директивата относно правоприлагането в областта на защитата на данните (ДПЗД)**. В ДПЗД е предвидена определена рамка по отношение на използването на ТЛР, по-специално член 3, параграф 13 от ДПЗД (определение „биометрични данни“), член 4 (принципи, свързани с обработването на лични данни), член 8 (законосъобразност на обработването), член 10 (обработване на специални категории лични данни) и член 11 от ДПЗД (автоматизирано вземане на индивидуални решения).

Прилагането на ТЛР може да засегне и още няколко други основни права. Ето защо **Хартата на основните права на ЕС** („Хартата“) е от съществено значение за тълкуването на ДПЗД, по-специално правото на защита на личните данни по член 8 от Хартата, но и правото на неприкосновеност на личния живот, установено в член 7 от Хартата.

Законодателните мерки, които служат като правно основание за обработването на лични данни, засягат пряко правата, гарантирани с членове 7 и 8 от Хартата. Обработването на биометрични данни при всички обстоятелства само по себе си представлява сериозна намеса. Това не зависи от резултата, напр. положително съвпадение. Всяко ограничаване на упражняването на основните права и свободи трябва да бъде предвидено в правото и да зачита същността на тези права и свободи.

Правното основание трябва да бъде **достатъчно ясно** обяснено, за да дава на гражданите адекватна представа за условията и обстоятелствата, при които органите имат правото да прибягват до всякакви мерки за събиране на данни и тайно наблюдение. Само транспонирането в националното право на общата клауза на член 10 от ДПЗД не би било достатъчно прецизно и предвидимо.

Преди националният законодател да създаде ново правно основание за каквато и да е форма на обработване на биометрични данни с използване на лицево разпознаване, той следва да направи **консултация** с компетентния надзорен орган по защита на данните.

Законодателните мерки трябва да бъдат **подходящи** за постигане на легитимните цели, преследвани от въпросната правна уредба. Една **цел от общ интерес** — колкото и фундаментална да е тя — сама по себе си не оправдава ограничаването на основно право. Със законодателните мерки следва да се прави **разграничение** между лицата, които попадат в обхвата на директивата, с оглед на целта, например борба с конкретни тежки престъпления, и да са насочени към тях. Ако мярката обхваща всички лица по общ начин, без такова разграничение, ограничение или изключение, тя засилва намесата. Тя също така засилва намесата, ако обработването на данните обхваща значителна част от населението.

Данните трябва да се обработват по начин, който гарантира приложимостта и ефективността на правилата и принципите на ЕС за защита на данните. Въз основа на всяка ситуация с **оценката на необходимостта и пропорционалността** трябва също така да се определят и разглеждат всички възможни последици за други основни права. Ако данните се обработват систематично без знанието на субектите на данни, това вероятно ще породи **общо усещане за постоянно наблюдение**. Това може да доведе до възпиращ ефект по отношение на някои или всички засегнати основни права, например човешкото достойнство съгласно член 1 от Хартата, свободата на мисълта, съвестта и религията съгласно член 10 от Хартата, свободата на изразяване на мнение съгласно член 11 от Хартата, както и свободата на събранията и сдруженията съгласно член 12 от Хартата.

Обработването на специални категории данни, като например биометрични данни, може да се счита за **„строго необходимо“** (член 10 от ДПЗД) само ако намесата в защитата на личните данни и ограничаването ѝ са ограничени до абсолютно необходимото, т.е. незаменимото, и изключват всякакво обработване от общ или систематичен характер.

Фактът, че снимката **очевидно е направена обществено достояние** (член 10 от ДПЗД) от субекта на данните не предполага, че свързаните биометрични данни, които могат да бъдат извлечени от снимката чрез специални технически средства, се считат за очевидно направени обществено достояние. Настройките по подразбиране на дадена услуга, напр. предоставянето на публичен достъп до образци или липсата на избор, напр. образците се оповестяват публично, без потребителят да може да променя тази настройка, по никакъв начин не следва да се тълкуват като данни, които очевидно са направени обществено достояние.

С член 11 от ДПЗД се установява рамка за **автоматизирано вземане на индивидуални решения**. Използването на ТЛР води до използването на специални категории данни и може да доведе до профилиране в зависимост от начина и целта, за които се прилага ТЛР. При всички случаи, в съответствие с правото на Съюза и член 11, параграф 3 от ДПЗД, профилирането, което води до дискриминация на физически лица въз основа на специалните категории лични данни, е забранено.

Член 6 от ДПЗД се отнася до необходимостта да се **прави разграничение между различните категории субекти на данни**. Най-вероятно няма основание за намеса по отношение на субектите на данни, за които няма доказателства, които да подсказват, че между тяхното поведение може да има връзка, дори косвена или далечна, със законната цел съгласно ДПЗД.

Принципът за свеждане на данните до минимум (член 4, параграф 1, буква д) от ДПЗД) налага също така всеки видеоматериал, който не е от значение за целта на обработката, винаги да бъде премахван или анонимизиран (напр. чрез размазване без възможност за възстановяване на данните със задна дата) преди внедряването.

Администраторът трябва внимателно да обмисли как (или дали може) да изпълни изискванията, свързани с **правата на субекта на данни**, преди да започне каквото и да е обработване на данни с ТЛР, тъй като ТЛР често включва обработване на специални категории лични данни без каквото и да е очевидно взаимодействие с физическото лице.

Ефективното упражняване на правата на субектите на данни зависи от изпълнението от администратора на неговите **задължения за предоставяне на информация** (член 13 от ДПЗД). Когато се оценява дали е налице „конкретен случай“ съгласно член 13, параграф 2 от ДПЗД, трябва да се вземат предвид няколко фактора, включително дали личните данни се събират без знанието на субекта на данните, тъй като това би бил единственият начин да се даде възможност на физическите лица да упражняват ефективно правата си. Ако вземането на решения се извършва единствено въз основа на ТЛР, тогава субектите на данни трябва да бъдат информирани за характеристиките на автоматизираното вземане на решения.

Що се отнася до **исканията за достъп**, когато биометричните данни се съхраняват и са свързани с дадена самоличност също и чрез буквено-цифрови данни, в съответствие с принципа за свеждане на данните до минимум, това следва да позволи на компетентния орган да даде потвърждение на искане за достъп въз основа на търсене по тези буквено-цифрови данни и без да стартира по-нататъшно обработване на биометрични данни на други лица (т.е. чрез търсене с ТЛР в база данни).

Рисковете за субектите на данни са особено сериозни, ако в полицейска база данни се съхраняват и/или се споделят с други субекти неточни данни. Администраторът трябва съответно да **коригира** съхраняваните данни и системите за ТЛР (вж. също съображение 47 от ДПЗД).

Правото на **ограничаване** става особено важно, когато става въпрос за технология за лицево разпознаване (която се основава на алгоритъм(и) и следователно никога не показва окончателен резултат) в ситуации, в които се събират големи количества данни и точността, и качеството на идентифицирането могат да варират.

Оценката на въздействието върху защитата на данните (ОВЗД) преди използването на ТЛР е задължително изискване, вж. член 27 от ДПЗД. ЕКЗД препоръчва резултатите от такива оценки или поне основните констатации и заключения на ОВЗД да се оповестяват като мярка за повишаване на доверието и прозрачността.

За повечето случаи на внедряване и използване на ТЛР е присъщ висок риск за правата и свободите на субектите на данни. Поради това органът, който внедрява ТЛР, следва да се **консултира** с компетентния надзорен орган преди внедряването на системата.

Като се има предвид уникалният характер на биометричните данни, органът, който прилага и/или използва ТЛР, следва да обърне специално внимание на **сигурността на обработването**, в съответствие с член 29 от ДПЗД. По-специално, правоприлагащият орган следва да гарантира, че системата отговаря на съответните стандарти и прилага мерки за защита на биометричните образци. Принципите и гаранциите за защита на данните трябва да бъдат вградени в технологията преди началото на обработването на лични данни. Ето защо, дори когато ПО възнамерява да прилага и използва ТЛР от външни доставчици, той трябва да гарантира, напр. чрез процедурата за възлагане на обществена поръчка, че се използва само ТЛР, изградена на принципите на **защита на данните етапа на проектирането и по подразбиране**.

Воденето на записи (вж. член 25 от ДПЗД) е важна гаранция за проверка на законосъобразността на обработването, както на вътрешно равнище (т.е. самонаблюдение от страна на съответния администратор/обработващ лични данни), така и от външни надзорни органи. По отношение на системите за лицево разпознаване се препоръчва водене на записи и на промените в референтната база данни, и на опитите за идентифициране или проверка, включително оценката на потребителя, резултата и степента на доверие. **Воденето на записи** обаче е само един от основните елементи на цялостния **принцип на отчетност** (вж. член 4, параграф 4 от ДПЗД). Администраторът трябва да е в състояние да докаже съответствието на обработването с основните принципи за защита на данните, посочени в член 4, параграфи 1—3 от ДПЗД.

ЕКЗД припомня своя съвместен призив с ЕНОЗД **за забрана** на някои видове обработване във връзка с: 1) дистанционна биометрична идентификация на лица в публично достъпни пространства; 2) системи за лицево разпознаване с помощта на изкуствен интелект, които категоризират лицата въз основа на техните биометрични данни в групи според етническа принадлежност, пол, както и по политическа или сексуална ориентация или други основания за дискриминация 3) използване на технологии за лицево разпознаване или подобни технологии за извеждане на заключения относно емоциите на физическо лице; и 4) обработване на лични данни в сферата на правоприлагането, което би се основавало на база данни, попълнена чрез събиране на лични данни в масов мащаб и по безразборен начин, напр. чрез „събиране“ на достъпни онлайн снимки и изображения на лица.

Основна гаранция за засегнатите основни права е **ефективният надзор** от страна на компетентните надзорни органи за защита на данните. Поради това държавите членки трябва да гарантират, че ресурсите на надзорните органи са подходящи и достатъчни, за да могат те да изпълняват мандата си.

Настоящите **насоки са предназначени за** законодателите на европейско и национално равнище, както и за правоприлагащите органи и техните служители, които прилагат и използват системите за ТЛР. Предназначени са за физическите лица, доколкото те са заинтересовани като цяло, или в качеството им на субекти на данни, по-специално по отношение на правата на субектите на данни.

Насоките имат за цел да предоставят информация за специфичните характеристики на ТЛР и приложимата правна уредба в сферата на правоприлагането (по-специално на ДПЗД).

- Освен това те предоставят **инструмент, който да помогне при първото определяне на чувствителността на даден случай на употреба** (приложение I).
- Те съдържат и **практически насоки за правоприлагащите органи, които желаят да закупят и управляват система за ТЛР** (приложение II).
- В насоките също така са описани няколко типични случая на **употреба и са изброени множество съображения, които са от значение**, особено по отношение на проверката за необходимост и пропорционалност (приложение III).

1 ВЪВЕДЕНИЕ

1. Технологията за лицево разпознаване (ТЛР) може да се използва за автоматично разпознаване на хора въз основа на тяхното лице. Тя често се основава на изкуствен интелект, като например технологии за машинно самообучение. Приложенията на ТЛР все повече се изпитват и използват в различни области — от индивидуална употреба до употреба в частни организации и публична

администрация. Правоприлагащите органи (ПО) също очакват предимства от използването на технологията. Тя обещава решения на сравнително нови предизвикателства, например разследвания, включващи голям брой събрани доказателства, но също така и на известни проблеми, по-специално по отношение на недостига на персонал за задачи по наблюдение и търсене.

2. Голяма част от повишения интерес към ТЛР се дължи на ефективността и мащабируемостта ѝ. Едновременно с това се появяват недостатъците, присъщи на технологията и нейното приложение — също в голям мащаб. Макар че може хиляди набори от лични данни да се анализират с натискането на един бутон, дори само незначителните последици от алгоритмичната дискриминация или неправилната идентификация могат да доведат до голям брой лица, които са засегнати сериозно в поведението и ежедневието си. Самият размер на обработването на лични данни, и по-специално на биометрични данни, е друг ключов елемент на ТЛР, тъй като обработването на лични данни представлява намеса в основното право на защита на личните данни съгласно член 8 от Хартата на основните права на Европейския съюз (Хартата).

3. Прилагането на ТЛР от ПО ще има — и до известна степен вече има — значителни последици за отделни лица и за групи хора, включително малцинствата. Тези последици ще окажат значително влияние и върху начина, по който живеем заедно, и върху нашата социална и демократична политическа стабилност, и ще придадат голямо значение на плурализма и политическото противопоставяне. Правото на защита на личните данни често е ключово като предпоставка за гарантиране на други основни права. Прилагането на ТЛР има особено голяма склонност да оказва намеса в основните права извън правото на защита на личните данни.

4. Поради това ЕКЗД счита, че е важно да допринесе за продължаващото интегриране на ТЛР в областта на правоприлагането, обхванатa от Директивата за правоприлагането[1], съответно националните закони, които я транспонират, и да предостави настоящите насоки. Насоките имат за цел да предоставят съответната информация на законодателите на равнището на ЕС и на национално равнище, както и на правоприлагащите органи и техните служители при въвеждането и използването на системите за ТЛР. Обхватът на насоките е ограничен до ТЛР. Други форми на обработване на лични данни въз основа на биометрични данни от ПО, особено ако се обработват от разстояние, обаче могат да доведат до подобни или допълнителни рискове за физическите лица, групите и обществото. В зависимост от съответните обстоятелства някои аспекти на тези насоки може да послужат като полезен източник и в тези случаи. И накрая, физическите лица, които са заинтересовани като цяло или в качеството си на субекти на данни, също могат да намерят важна информация, по-специално по отношение на правата на субектите на данни.

5. Насоките се състоят от основния документ и три приложения. В основния документ са представени технологията и приложимата правна уредба. В приложение II може да бъде намерен образец, с който да се подпомогне установяването на някои от основните аспекти за класифициране на тежестта на намесата в основните права в дадена област на приложение. ПО, които желаят да осигурят и прилагат система за ТЛР, могат да намерят практически насоки в

[1] Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета.

приложение II. В зависимост от областта на приложение на ТЛР може да са от значение различни съображения. Набор от хипотетични сценарии и съответни съображения можете да намерите в приложение III.

2 ТЕХНОЛОГИЯ

2.1 Една биометрична технология, две различни функции

6. Разпознаването на лица е технология на вероятностите, способна автоматично да разпознава хора въз основа на тяхното лице, за да удостовери автентичността им или да ги идентифицира.

7. ТЛР попада в по-широката категория на биометричните технологии. Биометричните данни включват всички автоматизирани процеси, използвани за разпознаване на дадено лице чрез количествено определяне на физически, физиологични или поведенчески характеристики (пръстови отпечатъци, структура на ириса, глас, походка, модели на кръвоносни съдове и др.). Тези характеристики се определят като „биометрични данни“, тъй като позволяват или потвърждават уникалната идентификация на това лице.

8. Такъв е случаят с лицата на хората или по-специално техническото им обработване с устройства за лицево разпознаване: посредством заснемане на изображението на лице (снимка или видео), наречено биометрична „проба“, е възможно да се извлече цифрово представяне на отличителните характеристики на това лице (това се нарича „образец“).

9. Биометричният образец е цифрово представяне на уникалните характеристики, извлечени от биометрична проба, и може да се съхранява в биометрична база данни[2]. Този образец би трябвало да е уникален и специфичен за всеки човек и по принцип е постоянен[3]. На етапа на разпознаване устройството сравнява този образец с други образци, създадени преди това или изчислени директно от биометрични проби, като например лица, присъстващи на изображение, снимка или видеоклип. Следователно „разпознаването на лица“ е двуетапен процес: вземането на портретната снимка и преобразуването ѝ в образец, последвано от разпознаване на това лице чрез сравняване на съответния образец с един или повече други образци.

10. Както всеки биометричен процес разпознаването на лица може да изпълнява две различни функции:

- **удостоверяване на автентичността** на дадено лице с цел да се провери дали лицето е това, което той/тя твърди, че е. В този случай системата сравнява предварително записан биометричен образец или проба (напр. съхранявани в смарткарта или биометричен паспорт) с едно лице, например това на човек, който се явява на контролен пункт, за да провери дали това е едно и също лице. Следователно тази функционалност се основава на сравняването на два образеца. Това се нарича също „**проверка** 1 към 1“.

- **идентифициране** на лице с цел намиране на лице сред група хора в рамките на конкретна зона, изображение или база данни. В този случай системата трябва да обработи всяко заснето лице, за да генерира биометричен образец и след това да провери дали той съвпада с лице, което е познато на системата. Следователно тази функционалност се основава на сравняването на един образец с база данни от образци или проби (базова линия). Това се

[2] Насоки относно лицевото разпознаване, Консултативен комитет по Конвенция № 108, Конвенция за защита на лицата при автоматизираната обработка на лични данни, Съвет на Европа, юни 2021 г.
[3] Това може да зависи от вида на биометрията и възрастта на субекта на данните.

нарича още идентифициране 1 към много. При това идентифициране например може да се направи връзка между лично име (фамилно име, собствено име) с лице, ако сравнението се прави спрямо база данни със снимки, свързани с фамилни и собствени имена. Идентифицирането може да включва и проследяване на лице в тълпа, без непременно да се прави връзка с гражданската самоличност на лицето.

11. И в двата случая използваните техники за лицево разпознаване се основават на очаквано съвпадение между образците: сравнявания и базовата линия(и). От тази гледна точка случаите са вероятностни: при сравнението се прави извод за по-голяма или по-малка вероятност лицето действително да е това, чиято автентичност трябва да бъде удостоверена или което трябва да бъде идентифицирано; ако тази вероятност надвишава определен праг в системата, определен от потребителя или разработчика на системата, системата ще приеме, че е налице съвпадение.

12. Въпреки че двете функции — удостоверяване на автентичност и идентифициране — са различни, и двете са свързани с обработването на биометрични данни, свързани с идентифицирано или подлежащо на идентифициране физическо лице, и следователно представляват обработване на лични данни, и по-конкретно обработване на специални категории лични данни.

13. Разпознаването на лица е част от по-широк спектър от техники за обработка на видеоизображения. Някои видеокамери могат да заснемат хора в определена зона, по-специално техните лица, но сами по себе си не могат да се използват за автоматично разпознаване на отделни лица. Същото важи и за обикновената фотография: камерата не е система за лицево разпознаване, тъй като снимките на лицата трябва да се обработват по специален начин, за да се извлекат биометрични данни.

14. Простото откриване на лица от т.нар. „интелигентни“ камери също не представлява непременно система за лицево разпознаване. Макар че те също повдигат важни въпроси по отношение на етиката и ефективността, цифровите техники за откриване на необичайно поведение или случаи на насилие, или за разпознаване на емоциите на лицето или дори на силуети, не могат да се считат за биометрични системи, обработващи специални категории лични данни, при условие че нямат за цел уникално идентифициране на дадено лице и че съответното обработване на лични данни не включва други специални категории лични данни. Тези примери не са напълно несвързани с разпознаването на лица и все пак са предмет на правилата за защита на личните данни.[4] Освен това този тип система за разпознаване може да се използва в комбинация с други системи, целящи идентифицирането на лице, и следователно да се счита за технология за лицево разпознаване.

15. За разлика от системите за видеозаснемане и обработка например, за които е необходимо инсталирането на физически устройства, разпознаването на лица е софтуерна функционалност, която може да бъде внедрена в съществуващи системи (камери, бази данни с изображения и др.). Следователно, тази функционалност може да бъде свързана или да си взаимодейства с множество системи и да се комбинира с други функционалности. Подобно интегриране във вече съществуваща инфраструктура налага специално внимание, тъй като то води до рискове поради факта, че технологията за лицево разпознаване може да бъде неизтриваема и лесно скрита[5].

[4] Член 10 от ДПЗД (или член 9 от ОРЗД) обаче е приложим към системи, които се използват за категоризиране на лица въз основа на техните биометрични данни в групи според етническа принадлежност, както и политическа или сексуална ориентация, или други специални категории лични данни.

[5] При носените върху тялото камери например, които все по-често се използват на практика.

2.2 Голямо разнообразие от цели и приложения

16. Извън обхвата на настоящите насоки и на ДПЗД лицевото разпознаване може да се използва за широк кръг от цели — както за търговска употреба, така и за решаване на безпокойства, свързани с обществената безопасност или правоприлагането. То може да се прилага в много различни видове контекст: в личната връзка между потребителя и дадена услуга (достъп до приложение), за достъп до определено място (физическо филтриране) или без никакво конкретно ограничение в обществеото пространство (разпознаване на лица на живо). То може да се прилага за всякакъв вид субекти на данни: клиент на услуга, служител, случаен свидетел, издирвано лице или лице, замесено в съдебно или административно производство, и др. Някои употреби вече са обичайни и широко разпространени; други все още са на експериментален или спекулативен етап. Макар че в настоящите насоки няма да се разглеждат всички такива употреби и приложения, ЕКЗД припомня, че те може да се прилагат само ако са в съответствие с приложимата правна уредба, и по-специално с ОРЗД и съответните национални закони.[6] Дори в рамките на ДПЗД, в допълнение към функциите за удостоверяване на автентичността или идентифициране, данните, обработвани посредством технология за лицево разпознаване, могат да бъдат допълнително обработвани и за други цели, като например категоризация.

17. По-специално, скалата на потенциалните употреби може да се анализира в зависимост от степента на контрол, която хората имат върху своите лични данни, ефективните средства, с които разполагат за упражняване на този контрол, и правото им на инициатива за задействане и използване на тази технология, последиците за тях (в случай на разпознаване или неразпознаване) и мащаба на извършваното обработване. Разпознаването на лица въз основа на образец, съхраняван на лично устройство (смарткарта, смартфон и др.), принадлежащо на това лице, използвано за удостоверяване на автентичността и за строго лично ползване чрез специален интерфейс, не поражда същите рискове като например използването за целите на идентифицирането в неконтролирана среда, без активното участие на субектите на данни, когато образецът на всяко лице, влизащо в зоната за наблюдение, се сравнява с образци от широка част от населението, съхранявани в база данни. Между тези две крайности се намира много разнообразен спектър от употреби и свързани с тях въпроси относно защитата на личните данни.

18. За да се илюстрира допълнително контекстът, в който понастоящем се обсъждат или прилагат технологии за лицево разпознаване, било то за удостоверяване на автентичността или за идентифициране, ЕКЗД счита за подходящо да се посочат редица примери. Примерите по-долу са единствено с описателна цел и не следва да се разглеждат като предварителна оценка на съответствието им с достиженията на правото на ЕС в областта на защитата на данните.

Примери за удостоверяване на автентичността чрез лицево разпознаване

19. Удостоверяването на автентичността може да бъде проектирано така, че потребителите да имат пълен контрол върху него, например за да се даде възможност за достъп до услуги или приложения само в домашни условия. Като такова то се използва широко от собствениците на смартфони за отключване на тяхното устройство, вместо удостоверяване на автентичността с парола.

20. Удостоверяването на автентичността чрез лицево разпознаване може да се използва и за проверка на самоличността на лице, което желае да се възползва от публични или частни услуги

[6] За допълнителни насоки вж. също Насоки 3/2019 на ЕКЗД относно обработването на лични данни чрез видеоустройства, приети на 29 януари 2020 г.

на трети страни. Следователно, такива процеси предлагат начин за създаване на цифрова идентичност чрез използване на мобилно приложение (смартфон, таблет и др.), което след това може да се използва за достъп до онлайн административни услуги.

21. Освен това удостоверяването на автентичността чрез лицево разпознаване може да има за цел контролиране на физическия достъп до едно или повече предварително определени места, например входове на сгради или конкретни контролно-пропускателни пунктове. Тази функция например се прилага при определени видове обработване за целите на преминаване на границата, при което лицето на даден човек на граничния контролно-пропускателен пункт се сравнява с лицето, съхранено в неговия документ за самоличност (паспорт или разрешение за сигурно пребиваване).

Примери за идентифициране чрез лицево разпознаване

22. Идентификацията може да се прилага по много и дори още по-разнообразни начини. Те включват по-специално, но без да се ограничават до изброените по-долу употреби, които понастоящем са предмет на наблюдение, експериментиране или планиране в ЕС.

- търсене в база данни от снимки на самоличността на неидентифицирано лице (жертва, заподозрян и др.);
- наблюдение на движенията на дадено лице в публичното пространство. Лицето му/ѝ се сравнява с биометричните образци на лица, които пътуват или са пътували в наблюдаваната зона, например когато в нея е оставен багаж или след като е извършено престъпление;
- реконструиране на маршрута на дадено лице и последващите му взаимодействия с други лица чрез забавено сравнение на едни и същи елементи в опит да се установят например контактите му;
- дистанционна биометрична идентификация на издирвани лица на обществени места. Всички лица, заснети на живо от камери за видеозащита, се сравняват в реално време с база данни, съхранявана от силите за сигурност;
- автоматично разпознаване на хората в дадено изображение, за да се установят, например, връзките помежду им в дадена социална мрежа, която използва това разпознаване. Изображението се сравнява с образците на всички участници в мрежата, които са дали съгласие за тази функция, за да се предложи поименното идентифициране на тези връзки;
- достъп до услуги, като някои автоматични касови машини разпознават клиентите си, като сравняват лице, заснето от камера, с базата данни за портретни снимки, съхранявана от банката;
- проследяване на маршрута на пътник на определен етап от пътуването. Образецът, изчислен в реално време, на всяко лице, което се регистрира на изходите, разположени на определени етапи от пътуването (пунктове за предаване на багаж, изходи за извеждане към самолета и др.), се сравнява с образците на лицата, вече регистрирани в системата.

23. В допълнение към използването на ТЛР в областта на правоприлагането, широкият набор от наблюдавани приложения със сигурност налага всеобхватен дебат и политически подход, за да се гарантира съгласуваност и съответствие с достиженията на правото на ЕС в областта на защитата на данните.

2.3 Надеждност, точност и рискове за субектите на данни

24. Подобно на всяка технология, лицевото разпознаване също може да бъде предмет на предизвикателства, когато става дума за прилагането му, по-специално по отношение на неговата надеждност и ефикасност що се отнася до удостоверяването на автентичността или идентифицирането, както и на общия въпрос относно качеството и точността на „изходните“ данни и резултата от обработването чрез технологиите за лицево разпознаване.

25. Такива технологични предизвикателства пораждат особени рискове за засегнатите субекти на данни, които са още по-значими или сериозни в областта на правоприлагането, като се имат предвид възможните правни или други последици за физическите лица, които ги засягат по подобен начин. В този смисъл изглежда полезно да се подчертае и че последващото използване на ТЛР само по себе си не е по-безопасно, тъй като лицата може да бъдат проследявани във времето и на различни места. Следователно, последващото използване също крие специфични рискове, които трябва да се оценяват във всеки отделен случай.[7]

26. Както посочва Агенцията на ЕС за основните права в доклада си за 2019 г., „определянето на необходимото ниво на точност на софтуера за лицево разпознаване е предизвикателство: има много различни начини за оценка и преценка на точността, също и в зависимост от задачата, целта и контекста на използването му. При прилагането на технологията на места, посещавани от милиони хора, например железопътни гари или летища, относително малък дял грешки (напр. 0,01 %)[8] все пак означава, че стотици хора са погрешно обозначени. Освен това може да е по-вероятно да има грешни съвпадения при едни категории лица, отколкото при други, както е описано в раздел 3. Съществуват различни начини за изчисляване и тълкуване на процентите на грешка, поради което е необходима предпазливост. Освен това, що се отнася до точността и грешките, въпросите, свързани с това колко лесно може да бъде заблудена една система, например чрез фалшиви изображения на лица (т.нар. „фалшифициране на данни“), са важни, особено за целите на правоприлагането.“[9]

27. В тази връзка ЕКЗД счита, че е важно да се припомни, че ТЛР, независимо дали се използва за целите на удостоверяване на автентичността или идентифициране, не дава категоричен резултат, а разчита на вероятността две лица или изображения на лица да отговарят на едно и също лице.[10] Този резултат се влошава допълнително, когато качеството на биометричната проба, въведена във функцията за лицево разпознаване е ниско. Размазването на входящите изображения, ниската разделителна способност на камерата, движението и слабата светлина могат да бъдат фактори за ниско качество. Други аспекти, които оказват значително влияние върху резултатите, са разпространението и фалшифицирането, например, когато престъпниците се опитват да избегнат преминаването покрай камерите или да заблудят ТЛР. Многобройни проучвания също така подчертават, че подобни статистически резултати от алгоритмично обработване също може да са предмет на отклонения, особено в резултат на качеството на изходните данни, както и на базите данни за обучение, или на други фактори, като например избора на място за внедряване. Освен това следва да се подчертае въздействието на технологията за лицево разпознаване върху други основни права, като например зачитането на личния и семейния живот, свободата на изразяване на мнение и свободата на информация, свободата на събиране и сдружаване и др.

[7] Вж. примерите, представени в приложение III.

[8] Този процент на точност произтича от цитирания доклад и отразява процент, който е много по-добър от сегашните резултати на алгоритмите в приложенията на ТЛР.

[9] Технология за лицево разпознаване: съображения за основните права в контекста на правоприлагането, Агенция на ЕС за основните права, 21 ноември 2019 г.

[10] Тази вероятност се нарича „коефициент на увереност“.

28. Ето защо е от съществено значение надеждността и точността на технологията за лицево разпознаване да се вземат предвид като критерии за оценка на съответствието с основните принципи за защита на данните, както е посочено в член 4 от ДПЗД за защита на данните, и по-специално когато става въпрос за справедливост и точност.

29. Като подчертава, че висококачествените данни са от съществено значение за висококачествените алгоритми, ЕКЗД подчертава също така необходимостта администраторите на данни, като част от задължението си за отчетност, да извършват редовна и систематична оценка на алгоритмичното обработване, за да гарантират по-специално точността, справедливостта и надеждността на резултата от такова обработване на лични данни. Личните данни, използвани за целите на оценяването, обучението и по-нататъшното развитие на системите за ТЛР, могат да бъдат обработвани само въз основа на достатъчно правно основание и в съответствие с общите принципи за защита на данните.

3 ПРИЛОЖИМА ПРАВНА УРЕДБА

30. Използването на технологии за лицево разпознаване е неразривно свързано с обработването на лични данни, включително специални категории данни. Освен това то оказва пряко или косвено въздействие върху редица основни права, залегнали в Хартата на основните права на ЕС. Това е особено важно в областта на правоприлагането и наказателното правосъдие. Поради това всяко използване на технологии за лицево разпознаване следва да се извършва в строго съответствие с приложимата правна уредба.

31. Следната информация е предназначена да се използва при оценката на бъдещи законодателни и административни мерки, както и при прилагането на съществуващото законодателство за всеки отделен случай, който включва ТЛР. Значимостта на съответните изисквания варира в зависимост от конкретните обстоятелства. Тъй като не е възможно да се предвидят всички бъдещи обстоятелства, се счита, че това служи единствено за помощ, а не трябва да се тълкува като изчерпателно изброяване.

3.1 Обща правна уредба — Хартата на основните права на ЕС и Европейската конвенция за правата на човека (ЕКПЧ)

3.1.1 Анализ на Хартата

32. Хартата на основните права на ЕС (наричана по-нататък „Хартата“) е предназначена за институциите, органите, службите и агенциите на Съюза и за държавите членки, когато прилагат правото на Съюза.

33. Регламентирането на обработката на биометрични данни за целите на правоприлагането съгласно член 1, параграф 1 от ДПЗД неизбежно повдига въпроса за спазването на основните права, по-специално на зачитането на личния живот и съобщенията съгласно член 7 от Хартата и на правото на защита на личните данни съгласно член 8 от Хартата.

34. Събирането и анализът на видеозаписи на физически лица, включително на техните лица, предполага обработване на лични данни. При техническото обработване на изображението се обхващат и биометричните данни. Техническото обработване на данни, свързани с физическо лице, на информацията за времето и мястото дава възможност да се направят заключения относно личния живот на това лице. Тези заключения може да се отнасят до расовия или

етническия произход, здравето, религията, навиците в ежедневието, местата на постоянно или временно пребиваване, ежедневните или други движения, извършваните дейности, социалните връзки на тези лица и социалните кръгове, в които се движат. Големият обхват на информацията, която може да бъде разкрита чрез прилагането на ТЛР, ясно показва възможното въздействие върху правото на защита на личните данни, предвидено в член 8 от Хартата, но и върху правото на неприкосновеност на личния живот, предвидено в член 7 от Хартата.

35. При такива обстоятелства също не може да се изключи, че събирането, анализът и по-нататъшното обработване на въпросните биометрични (лицеви) данни може да окаже въздействие върху начина, по който хората чувстват, че имат свобода на действие, дори ако действието изцяло попада в обхвата на разбирането за свободно и отворено общество. То може също така да има сериозни последици за упражняването на основните им права, като например правото им на свобода на мисълта, съвестта и религията, на мирни събрания и на свободно сдружаване съгласно членове 1, 10, 11 и 12 от Хартата. Това обработване включва и други рискове, като например риск от злоупотреба с личната информация, събрана от съответните органи в резултат на незаконен достъп до личните данни и използването им, нарушение на сигурността и др. Рисковете често зависят от обработването и обстоятелствата около него, като например риска от незаконен достъп и използване от полицейски служители или от други неупълномощени страни. Някои рискове обаче просто са присъщи на уникалния характер на биометричните данни. За разлика от адреса или телефонния номер, субектът на данни не може да промени своите уникални характеристики, като например лицето или ириса си. В случай на неразрешен достъп или случайно публикуване на биометрични данни това би довело до компрометиране на данните при използването им като пароли или криптографски ключове или би могло да се използва за по-нататъшни неразрешени дейности по наблюдение в ущърб на физическото лице.

3.1.2 Намеса в правата, установени в Хартата

36. Обработването на биометрични данни при всички обстоятелства представлява сериозна намеса само по себе си. Това не зависи от резултата, напр. положително съвпадение. Обработването представлява намеса, дори ако биометричният образец е изтрит веднага след като съпоставката с полицейската база данни не е довела до положителен резултат.

37. Намесата в основните права на субектите на данни може да произтича от правен акт, който има за цел или води до ограничаване на съответното основно право[11]. Тя може да произтича и от акт на публичен орган със същата цел или действие или дори на частен субект, на който по закон е възложено да упражнява публична власт и публични правомощия.

38. Законодателна мярка, която служи за правно основание за обработването на лични данни, засяга пряко правата, гарантирани от членове 7 и 8 от Хартата[12].

39. Използването на биометрични данни и по-специално на ТЛР в много случаи също засяга правото на човешко достойнство, гарантирано от член 1 от Хартата. Човешкото достойнство изисква хората да не бъдат третирани просто като предмети. ТЛР изчислява екзистенциални и особено лични характеристики — лицевите характеристики — в машинночетима форма с цел използването ѝ като човешки регистрационен номер или лична карта, като по този начин третира лицето като предмет.

[11] Съд на ЕС, решение по дело C-219/91 — Ter Voort, RoC 1992 I-05485, т. 36е.; Съд на ЕС, решение по дело C-200/96 — Metronome, RoC 1998 I-1953, т 28.
[12] Съд на ЕС, решение по дело C-594/12, т. 36; Съд на ЕС, решение по дело C-291/12, т. 23 и следв.

40. Такова обработване може да засегне и други основни права, като например правата по членове 10, 11 и 12 от Хартата, доколкото възпиращите ефекти са предвидени или произтичат от съответното видеонаблюдение на правоприлагащите органи.

41. Освен това следва внимателно да се разгледат и потенциалните рискове, пораждани от използването на технологии за лицево разпознаване от страна на правоприлагащите органи по отношение на правото на справедлив съдебен процес и презумпцията за невиновност съгласно членове 47 и 48 от Хартата. Резултатът от прилагането на ТЛР, напр. съвпадение, може не само да доведе до това дадено лице да бъде подложено на допълнителни полицейски действия, но и да бъде решаващо доказателство в съдебни производства. Недостатъците на ТЛР, като например възможна пристрастност, дискриминация или неправилно идентифициране („фалшиво положително“), могат да доведат до сериозни последици и за наказателното производство. Освен това при оценката на доказателствата резултатът от прилагането на ТЛР може да бъде облагодетелстван, дори ако има противоречиви доказателства („предубеденост в полза на автоматизацията“).

3.1.3 Обосновка за намесата

42. Съгласно член 52, параграф 1 от Хартата всяко ограничаване на упражняването на основните права и свободи трябва да бъде предвидено в правото и да зачита същността на тези 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 Европейския съюз цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора.

3.1.3.1 Предвидено по закон

43. В член 52, параграф 1 от Хартата е определено изискването за конкретно правно основание. Това правно основание трябва да бъде достатъчно ясно в своите условия, за да дава на гражданите адекватна представа за условията и обстоятелствата, при които органите имат правото да прибягват до всякакви мерки за събиране на данни и тайно наблюдение[13]. То трябва да посочва с разумна яснота обхвата и начина на упражняване на съответната свобода на преценка, предоставена на публичните органи, така че да гарантира на лицата минималната степен на защита, която им се полага съгласно принципа на правовата държава в едно демократично общество[14]. Освен това за законосъобразността са необходими адекватни гаранции, за да се гарантира по-специално спазването на правото на дадено лице по член 8 от Хартата. Тези принципи се прилагат и за обработката на лични данни за целите на оценяването, обучението и по-нататъшното развитие на системите на ТЛР.

44. Като се има предвид, че биометричните данни, когато се обработват за целите на уникалното идентифициране на физическо лице, представляват специални категории данни, изброени в член 10 от ДПЗД, различните приложения на ТЛР в повечето случаи биха налагали специален закон, в който точно да бъде описано приложението и условията за използването ѝ. Това обхваща по-специално видовете престъпления и, ако е приложимо, подходящия праг на тежестта на тези престъпления, за да може, наред с другото, ефективно да се изключи дребното престъпление.[15]

[13] ЕСПЧ, Shimovolos с/у Русия, т.68; Vukota-Bojić с/у Швейцария.
[14] ЕСПЧ, Piechowicz с/у Полша, т. 212.
[15] Вж. напр. решенията на Съда на ЕС по дела C-817/19 Ligue des droits humains, т. 151e, C-207/16 Ministerio Fiscal, т. 56.

3.1.3.2 Същността на основното право на неприкосновеност на личния живот и на защита на личните данни, заложено в членове 7 и 8 от Хартата

45. Ограниченията на основните права, които са неизбежни за всяка ситуация, все пак трябва да са съобразени със същността на конкретното право, което трябва да се зачита. Същността се отнася до същината на това основно право[16]. Човешкото достойнство също трябва да се зачита, дори когато дадено право е ограничено[17].

46. Признаци за евентуално нарушение на неприкосновената същност са следните:

- Разпоредба, с която се налагат ограничения независимо от индивидуалното поведение на дадено лице или от изключителни обстоятелства[18].
- Прибягването до съд не е възможно или е възпрепятствано[19].
- Преди да се стигне до строго ограничение, обстоятелствата на съответното лице не се вземат предвид[20].
- С оглед на правата по членове 7 и 8 от Хартата: В допълнение към широкото събиране на метаданни за комуникацията, придобиването на информация за съдържанието на електронното съобщение би могло да наруши същността на тези права[21].
- С оглед на правата по членове 7, 8 и 11 от Хартата: Законодателство, което налага на доставчиците на достъп до публични онлайн комуникационни услуги и на доставчиците на хостинг услуги да съхраняват общи и неизбирателни, inter alia, лични данни, свързани с тези услуги[22].
- Във връзка с правата по член 8 от Хартата: Липсата на основни принципи за защита и сигурност на данните също би могла да наруши същността на правото[23].

3.1.3.3 Законосъобразна цел

47. Както вече беше обяснено в точка 3.1.3., ограниченията на основните права трябва действително да отговарят на целите от общ интерес, признати от Европейския съюз, или на необходимостта от защита на правата и свободите на други хора.

48. Признати от Съюза са както целите, посочени в член 3 от Договора за Европейския съюз, така и други интереси, защитени от специални разпоредби на Договорите[24], а именно, наред с другото, пространство на свобода, сигурност и правосъдие, предотвратяване и борба с престъпността. В отношенията си с останалия свят Съюзът следва да допринася за мира и сигурността и за защитата на правата на човека.

49. Необходимостта от защита на правата и свободите на други хора се отнася до правата на лицата, които са защитени от правото на Европейския съюз или на неговите държави членки. Оценката

[16] Съд на ЕС, решение по дело C-279/09, RoC 2010 I-13849, т. 60.
[17] Разяснения относно Хартата на основните права, дял I, Разяснение на член 1, ОВ C 303, 14.12.2007 г., стр. 17—35.
[18] Съд на ЕС, решение по дело C-601/15, т. 52.
[19] Съд на ЕС, решение по дело C-400/10, RoC 2010 I-08965, т. 55.
[20] Съд на ЕС, решение по дело C-408/03, RoC 2006 I-02647, т. 68.
[21] Съд на ЕС, решение по дело 203/15 — Tele2 Sverige, т. 101 — Съд на ЕС, решение по дела C-293/12 и C-594/12, т. 39.
[22] Съд на ЕС, решение по дело C-512/18, La Quadrature du Net, т. 209 и сл.
[23] Съд на ЕС, решение по дело C-594/12, т. 40.
[24] Разяснения относно Хартата на основните права, дял I, Разяснение на член 52, ОВ C 303, 14.12.2007 г., стр. 17—35.

трябва да се извърши с цел да се съгласуват изискванията за защита на съответните права и да се постигне справедлив баланс между тях[25].

3.1.3.4 Тест за необходимост и пропорционалност

50. Когато става въпрос за намеса в основните права, обхватът на правото на преценка на националния законодател и на законодателя на Съюза може да се окаже ограничен. Това зависи от редица фактори, включително съответната област, естеството на въпросното право, гарантирано от Хартата, естеството и сериозността на намесата и целта на намесата[26]. Законодателните мерки трябва да бъдат подходящи за постигане на легитимните цели, преследвани от разглежданата правна уредба. Освен това мярката не трябва да надхвърля границите на това, което е подходящо и необходимо за постигането на тези цели[27]. Една цел от общ интерес — колкото и фундаментална да е тя — сама по себе си не оправдава ограничаването на основно право[28].

51. Съгласно установената съдебна практика на Съда на ЕС дерогациите и ограниченията във връзка със защитата на личните данни трябва да се прилагат само доколкото това е строго необходимо[29]. Това също така означава, че за постигането на целта не съществуват средства, които предполагат по-малко намеса. Възможните алтернативи, например — в зависимост от дадената цел — допълнителен персонал, по-чести полицейски действия или допълнително улично осветление, трябва да бъдат внимателно идентифицирани и оценени. Със законодателните мерки следва да се прави разграничение и те следва да са насочени към лицата, попадащи в обхвата на тези мерки, с оглед например на целта за борба с тежката престъпност. Ако то обхваща всички лица по общ начин, без такова разграничение, ограничение или изключение, то засилва намесата[30]. То засилва намесата също и ако обработването на данните обхваща значителна част от населението[31].

52. Защитата на личните данни, произтичаща от изричното задължение, установено в член 8, параграф 1 от Хартата, е особено важна за правото на зачитане на личния живот, гарантирано в член 7 от Хартата[32]. В законодателството трябва да са предвидени ясни и точни правила, които определят обхвата и прилагането на въпросната мярка и налагат гаранции, така че лицата, чиито данни се обработват, да разполагат с достатъчно гаранции, за да защитят ефективно личните си данни срещу риска от злоупотреба и срещу всеки незаконен достъп или използване на тези данни[33]. Необходимостта от такива гаранции е още по-голяма, когато личните данни подлежат

---

[25] Jarass GrCh, 3. Aufl. 2016, EU-Grundrechte-Charta член 52 Rn. 31—32.

[26] Съд на ЕС, решение по дело C-594/12, т. 47 със следните източници: вж. по аналогия, що се отнася до член 8 от решение на Европейския съд по правата на човека, S. и Marper с/у Обединеното кралство [голям състав], №. 30562/04 и 30566/04, § 102, ECHR 2008-V.

[27] Решение на Съда на ЕС по дело C-594/12, т. 46, със следните източници: Решение по дело-343/09 Afton Chemical, EU:C:2010:419, т. 45; Решение по дело Volker und Markus Schecke и Eifert, EU:C:2010:662, т. 74; Решение по дела C-581/10 и C-629/10, Nelson и др. EU:C:2012:657, т. 71; Решение по дело Sky Österreich, C-283/11, EU:C:2013:28, т. 50; и Решение по дело C-101/12 Schaible EU:C:2013:661, т. 29.

[28] Решение на Съда на ЕС по дело C-594/12, т. 51.

[29] Решение на Съда на ЕС по дело C-594/12, т. 52, със следните източници: Решение по дело C-473/12 IPI, EU:C:2013:715, т. 39 и цитираната съдебна практика.

[30] Решение на Съда на ЕС по дело C-594/12, т. 57.

[31] Решение на Съда на ЕС по дело C-594/12, т. 56.

[32] Решение на Съда на ЕС по дело C-594/12, т. 53.

[33] Решение на Съда на ЕС по дело C-594/12, т. 54, със следните източници: вж. по аналогия, що се отнася до член 8 от Решение на Европейския съд по правата на човека от 1 юли 2008 г. по дело Liberty и други с/у Обединеното кралство № 58243/00, точки 62 и 63; решение по дело Rotaru с/у Румъния, точки 57—59 и решение по дело S. и Marper с/у Обединеното кралство, § 99.

на автоматична обработка и когато съществува значителен риск от незаконен достъп до данните[34]. Освен това вътрешно или външно, напр. съдебно, разрешение за внедряване на ТЛР също може да послужи за предпазна мярка и може да се окаже необходимо в някои случаи на сериозна намеса.[35]

53. Установените правила трябва да бъдат адаптирани към конкретната ситуация, например количеството обработени данни, естеството на данните[36] и риска от незаконен достъп до тях. За това са необходими правила, които по-специално да уреждат защитата и сигурността на въпросните данни по ясен и стриктен начин, за да се гарантира пълната им неприкосновеност и поверителност[37].

54. Що се отнася до отношенията между администратора и обработващия лични данни, на обработващите лични данни не следва да се позволява да вземат предвид само икономически съображения, когато определят нивото на сигурност, което те прилагат по отношение на личните данни; това може да застраши достатъчното високо ниво на защита[38].

55. В правния акт трябва да бъдат изложени материалноправни и процесуални условия и обективни критерии, чрез които да се определят границите на достъпа на компетентните органи до данните и последващото им използване. За целите на предотвратяването, разкриването или наказателното преследване съответните престъпления би трябвало да се считат за достатъчно сериозни, за да се обоснове степента и сериозността на тези намеси в основните права, заложени например в членове 7 и 8 от Хартата[39].

56. Данните трябва да се обработват по начин, който гарантира приложимостта и действието на правилата на ЕС за защита на данните; по-специално тези, предвидени в член 8 от Хартата, който гласи, че спазването на изискванията за защита и сигурност подлежи на контрол от независим орган. Географското място, където се извършва обработването, може да е от значение в такава ситуация[40].

57. По отношение на различните етапи на обработване на лични данни следва да се прави разграничение между категориите данни въз основа на тяхната възможна полезност за целите на преследваната цел или в зависимост от засегнатите лица[41]. Определянето на условията на обработването, например определянето на периода на съхранение, трябва да се основава на обективни критерии, за да се гарантира, че намесата е ограничена до строго необходимото[42].

58. Въз основа на всяка ситуация с оценката на необходимостта и пропорционалността трябва да се определят и вземат под внимание всички последици, които попадат в обхвата на други основни права, като човешкото достойнство в съответствие с член 1 от Хартата, свободата на мисълта, съвестта и религията в съответствие с член 10 от Хартата, свободата на изразяване на мнение в

[34] Решение на Съда на ЕС по дело C-594/12, т. 55, със следните източници: вж. по аналогия, що се отнася до член 8 от Решение на Европейския съд по правата на човека по дело S. и Marper с/у Обединеното кралство, т. 103 и Решение от 18 април 2013 г. по дело M. K. с/у Франция, № 19522/09, т. 35.

[35] Решение на ЕСПЧ по дело Szabó и Vissy с/у Унгария, точки 73—77.

[36] Вж. също повишените изисквания за технически и организационни мерки при обработването на специални категории данни, член 29, параграф 1. от ДПЗД.

[37] Решение на Съда на ЕС по дело C-594/12, т. 66.

[38] Решение на Съда на ЕС по дело C-594/12, т. 67.

[39] Решение на Съда на ЕС по дело C-594/12, точки 60 и 61.

[40] Решение на Съда на ЕС по дело C-594/12, т. 68.

[41] Решение на Съда на ЕС по дело C-594/12, т. 63.

[42] Решение на Съда на ЕС по дело C-594/12, т. 64.

съответствие с член 11 от Хартата, както и свободата на събранията и сдруженията в съответствие с член 12 от Хартата.

59. Освен това трябва да се счита за въпрос с голяма тежест това, че ако данните се обработват систематично без знанието на субектите на данни, това вероятно ще доведе до общо усещане за постоянно наблюдение[43]. Това може да доведе до възпиращ ефект по отношение на някои или всички засегнати основни права.

60. За да улеснят и извършат оценката на необходимостта и пропорционалността на законодателните мерки, свързани с лицевото разпознаване в областта на правоприлагането, националните законодатели и законодателите на Съюза биха могли да се възползват от наличните практически инструменти, специално разработени за тази задача. По-специално може да се използва инструментариумът за необходимост и пропорционалност[44], предоставен от Европейския надзорен орган по защита на данните.

3.1.3.5 Член 52, параграф 3 и член 53 от Хартата (ниво на защита, включително във връзка с това от ЕКПЧ)

61. Съгласно член 52, параграф 3 и член 53 от Хартата значението и обхватът на тези права от Хартата, които съответстват на правата, гарантирани от ЕКПЧ, трябва да бъдат същите като тези, определени от ЕКПЧ. Макар че по отношение по-специално на член 7 от Хартата в ЕКПЧ може да бъде намерена равностойна разпоредба, това не е така с член 8 от Хартата[45]. Член 52, параграф 3 от Хартата не възпрепятства правото на Съюза да предоставя по-широка защита. Тъй като ЕКПЧ не представлява правен инструмент, който да е официално включен в правото на ЕС, законодателството на ЕС трябва да се приема в светлината на основните права на Хартата[46].

62. Съгласно член 8 от ЕКПЧ публичните органи не се намесват в упражняването на това право на зачитане на личния и семейния живот, освен когато го налага законът и според необходимото в едно демократично общество в интерес на националната сигурност, обществената безопасност или икономическото благосъстояние на страната, за предотвратяване на безредици или престъпления, за защита на здравето и морала или за защита на правата и свободите на други лица.

63. ЕКПЧ също така определя стандарти по отношение на начина, по който могат да се предприемат ограничения. Едно от основните изисквания, освен върховенството на закона, е предвидимостта. За да се изпълни изискването за предвидимост, правото трябва да бъде достатъчно ясно в своите условия, за да дава на лицата адекватна представа за обстоятелствата и условията, при които органите са оправомощени да прибягват до такива мерки.[47] Това изискване се признава от Съда на ЕС и от законодателството на ЕС в областта на защитата на данните (вж. раздел 3.2.1.1).

---

[43] Решение на Съда на ЕС по дело C-594/12, т. 37.

[44] Европейски надзорен орган по защита на данните: Оценка на необходимостта от мерки, които ограничават основното право на защита на личните данни: набор от инструменти (11.4.2017 г.); Европейски надзорен орган по защита на данните: Насоки на ЕНОЗД за оценка на пропорционалността на мерките, които ограничават основните права на неприкосновеност на личния живот и на защита на личните данни (19.12.2019 г.).

[45] Решение на Съда на ЕС по дело C-203/15 — Tele2 Sverige, т. 129.

[46] Решение на Съда на ЕС по дело C-311/18, т. 99.

[47] Европейски съд по правата на човека, Решение по дело COPLAND с/у ОБЕДИНЕНОТО КРАЛСТВО, 3.4.2007 г., № 62617/00, т. 46.

64. В допълнение към правата по член 8 от ЕКПЧ трябва да се спазват изцяло и разпоредбите на Конвенцията за защита на лицата при автоматизирана обработка на лични данни[48]. Все пак трябва да се има предвид, че тези разпоредби представляват само минимален стандарт с оглед на преобладаващото право на Съюза.

3.2 Специфична правна уредба — Директивата относно правоприлагането

65. В ДПЗД е предвидена определена рамка за използването на ТЛР. На първо място, в член 3, параграф 13 от ДПЗД е дадено определение за понятието „биометрични данни“[49]. За подробности вж. раздел 2.1 по-горе. Второ, в член 8, параграф 2 се пояснява, че за да бъде всяко обработване законосъобразно, то трябва — освен да е необходимо за целите, посочени в член 1, параграф 1 от ДПЗД — да бъде регулирано в националното право, в което да са посочени най-малко целите на обработването, личните данни, които ще се обработват, и предназначението на обработването. Допълнителни разпоредби с особено значение във връзка с биометричните данни са членове 10 и 11 от ДПЗД. Член 10 трябва да се тълкува във връзка с член 8 от ДПЗД[50]. Винаги трябва да се спазват принципите за обработване на лични данни, определени в член 4 от ДПЗД, а всяка оценка на евентуално обработване на биометрични данни чрез ТЛР трябва да се ръководи от тях.

3.2.1 Обработване на специални категории данни за целите на правоприлагането

66. Съгласно член 10 от ДПЗД обработването на специални категории данни, като например биометрични данни, се разрешава само когато това е строго необходимо и при спазване на подходящи гаранции за правата и свободите на субекта на данните. В допълнение към това то се допуска само когато е разрешено от правото на Съюза или на държава членка, за да се защитят жизненоважните интереси на субекта на данните или на друго физическо лице, или когато такова обработване се отнася до данни, които очевидно са направени обществено достояние от субекта на данните. Тази обща клауза подчертава чувствителността на обработването на специални категории данни.

3.2.1.1 Разрешено от правото на Съюза или правото на държава членка

67. Що се отнася до необходимия вид законодателна мярка, в съображение 33 от ДПЗД се посочва, че „[к]огато в настоящата директива се прави позоваване на правото на държава членка, правно основание или законодателна мярка, това не налага непременно приемането на законодателен акт от парламент, без да се засягат изискванията съгласно конституционния ред на съответната държава членка.“[51]

68. Съгласно член 52, параграф 1 от Хартата всяко ограничение на упражняването на правата и свободите, признати от Хартата, е „предвидено в закон“. Това отразява формулировката „предвидени в закона“ в член 8, параграф 2 от ЕКПЧ, която означава не само спазване на

[48] ETS № 108.

[49] Член 3, параграф 13 от ДПЗД: „биометрични данни“ означава лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни.

[50] РД 258, Становище относно някои ключови въпроси във връзка с Директива (ЕС) 2016/680 относно правоприлагането (ЕС 2016/680), стр. 7.

[51] Видът на разглежданите законодателни мерки трябва да е в съответствие с правото на ЕС или с националното право. В зависимост от степента на намеса на ограничението може да се изисква конкретна законодателна мярка на национално равнище, като се вземе предвид нивото на нормата.

приложимото право, но се отнася и до качеството на това право, без да се засяга естеството на акта, налагайки то да бъде съобразено с принципите на правовата държава.

69. В съображение 33 от ДПЗД е посочено също така, че „[п]ри все това правото на държавата членка, правното основание или законодателната мярка обаче следва да бъдат ясни и точни и прилагането им да бъде предвидимо за правните субекти, както изисква съдебната практика на Съда и на Европейския съд по правата на човека. Правото на държава членка, уреждащо обработването на лични данни в рамките на обхвата на настоящата директива, следва да посочва най-малко общите цели на обработването, личните данни, които се обработват, конкретните цели на обработването, процедурите за опазване на цялостността и поверителността на личните данни и процедурите за тяхното унищожаване“.

70. Националното право трябва да бъде достатъчно ясно, за да дава на субектите на данни адекватни указания относно обстоятелствата и условията, при които администраторите са оправомощени да прибягнат до такива ограничения. Това включва възможни предварителни условия за обработване, като например специфични видове доказателства, както и необходимостта от съдебно или вътрешно разрешение. Съответното законодателство може да бъде технологично неутрално, доколкото специфичните рискове и характеристики на обработването на лични данни от системите за ТЛР са разгледани в достатъчна степен. В съответствие с ДПЗД и съдебната практика на Съда на Европейския съюз (Съда на ЕС) и на Европейския съд по правата на човека (ЕСПЧ) наистина е от съществено значение законодателните мерки, които имат за цел да осигурят правно основание за мярка за лицево разпознаване, да са предвидими за субектите на данни.

71. На законодателна мярка не може да се прави позоваване като на закон, който разрешава обработването на биометрични данни чрез ТЛР за целите на правоприлагането, ако с нея просто се транспонира общата клауза в член 10 от ДПЗД.

72. Освен биометричните данни член 10 от ДПЗД урежда обработването на други специални категории данни, като например сексуална ориентация, политически възгледи и религиозни убеждения, като по този начин обхваща широк спектър на обработване. Освен това в подобна разпоредба липсват конкретни изисквания, в които да се посочват обстоятелствата и условията, при които правоприлагащите органи ще бъдат оправомощени да прибягват до използването на технология за лицево разпознаване. Поради позоваването на други видове данни и изричната необходимост от специални гаранции без допълнителни спецификации, националната разпоредба за транспониране на член 10 от ДПЗД в националното право — със също толкова обща и абстрактна формулировка — не може да се използва като правно основание за обработването на биометрични данни, свързани с разпознаване на лица, тъй като би ѝ липсвала точност и предвидимост. В съответствие с член 28, параграф 2 или член 46, параграф 1, буква в) от ДПЗД, преди законодателят да създаде ново правно основание за всяка форма на обработване на биометрични данни чрез лицево разпознаване, следва да проведе консултация с националния надзорен орган за защита на данните.

3.2.1.2 Строго необходимо

73. Обработването може да се счита за „строго необходимо“ само ако намесата в защитата на личните данни и нейните ограничения са ограничени до абсолютно необходимото[52].

[52] Последователна съдебна практика относно основното право на зачитане на личния живот, вж. Решение на Съда на ЕС по дело C-73/07, т. 56 (Satakunnan Markkinapörssi и Satamedia); Решение на Съда на ЕС по дела C-92/09 и C-93/09, т. 77 (Schecke и Eifert); Решение на Съда на ЕС по дело C-594/12, т. 52 (Цифрови права); Решение на Съда на ЕС по дело C-362/14, т. 92 (Schrems).

Добавянето на термина „строго“ означава, че законодателят е възнамерявал обработването на специални категории данни да се извършва само при условия, които са дори по-строги от условията за необходимост (вж. точка 3.1.3.4 по-горе). Това изискване следва да се тълкува като абсолютно необходимо. То ограничава до абсолютен минимум свободата на преценка, с която правоприлагащият орган разполага при проверката за необходимост. В съответствие с установената съдебна практика на Съда на ЕС условието за „строга необходимост“ е тясно свързано и с изискването за обективни критерии, за да се определят обстоятелствата и условията, при които може да се извършва обработване, като по този начин се изключва всяко обработване от общ или систематичен характер[53].

3.2.1.3 Очевидно направени публично достояние

74. Когато се преценява дали обработването е свързано с данни, които очевидно са направени публично достояние от субекта на данните, следва да се припомни, че снимката сама по себе си не се счита систематично за биометрични данни[54]. Следователно фактът, че снимката очевидно е направена обществено достояние от субекта на данните, не означава, че свързаните биометрични данни, които могат да бъдат извлечени от снимката чрез специални технически средства, се считат за очевидно направени обществено достояние.

75. Що се отнася до личните данни като цяло, за да се счита, че биометричните данни са очевидно направени публично достояние от субекта на данните, той трябва умишлено да е направил биометричния образец (а не просто образа на лицето) свободно достъпен и публичен чрез отворен източник. Ако трета страна разкрива биометричните данни, не може да се счита, че данните са очевидно направени публично достояние от субекта на данните.

76. Освен това не е достатъчно да се тълкува поведението на физическо лице, за да се приеме, че биометричните данни са очевидно направени публично достояние. В случай на социални мрежи или онлайн платформи, например ЕКЗД счита, че фактът, че субектът на данните не е задействал или задал конкретни функции за защита на личните данни, не е достатъчен, за да се счита, че този субект на данни очевидно е направил публично достояние своите лични данни и че тези данни (напр. снимки) могат да бъдат обработвани в биометрични образци и използвани за целите на идентификацията без съгласието на лицето. В по-общ план настройките по подразбиране на дадена услуга, например предоставянето на публичен достъп до образците или липсата на избор, например образците се оповестяват публично, без потребителят да може да променя тази настройка, в никакъв случай не следва да се тълкуват в смисъл, че данните очевидно са направени обществено достояние.

3.2.2 Автоматизирано вземане на индивидуални решения, включително профилиране

77. В член 11, параграф 1 от ДПЗД е предвидено задължението на държавите членки на общо основание да забраняват решения, базиращи се единствено на автоматизирано обработване, включително профилиране, което поражда неблагоприятни правни последици за субекта на данните или го засяга в значителна степен. Като изключение от тази обща забрана такова обработване може да бъде възможно само ако е разрешено от правото на Съюза или правото на държава членка, което се прилага спрямо администратора и което предвижда подходящи

[53] Решение на Съда на ЕС по дело-623/17, т. 78.

[54] Вж. съображение 51 от ОРЗД: „[…] обработването на снимки не следва систематично да се счита за обработване на специални категории лични данни, тъй като снимките се обхващат от определението за биометрични данни единствено когато се обработват чрез специални технически средства, позволяващи уникална идентификация или удостоверяване на автентичността на дадено физическо лице. “

гаранции за правата и свободите на субекта на данните, най-малкото правото на получаване на човешка намеса от страна на администратора. То може да се използва само ограничително. Този праг се прилага за обикновени (т.е. не специални) категории лични данни. Още по-висок праг и по-ограничено използване се прилагат за изключението по член 11, параграф 2 от ДПЗД. В него отново се подчертава, че решенията по първата алинея не се основават на специални категории данни, т.е. по-специално биометрични данни за целите на уникалното идентифициране на физическо лице. Изключение може да се предвиди само ако са налице подходящи мерки за защита на правата и свободите на субекта на данни и законните интереси на съответното физическо лице. Това изключение трябва да се тълкува в допълнение към и в светлината на разпоредбите на член 10 от ДПЗД.

78. В зависимост от системата за ТЛР дори човешката намеса при оценяването на резултатите от ТЛР може сама по себе си да не осигури достатъчно гаранции за спазване на правата на лицата, и по-специално на правото на защита на личните данни, като се имат предвид възможните пристрастия и грешки, които могат да възникнат в резултат на самото обработване. Освен това човешката намеса може да се счита за предпазна мярка само ако лицето, което се намесва, може да оспори критично резултатите от ТЛР по време на човешката намеса. От решаващо значение е да се даде възможност на лицето да разбере системата за ТЛР и нейните ограничения, както и правилно да тълкува резултатите от нея. Необходимо е също така да се създаде работно място и организация, с които да се противодейства на последиците от предубедеността в полза на автоматизацията и да се избягва насърчаването на безкритично приемане на резултатите, напр. чрез кратки срокове, обременяващи процедури, потенциални неблагоприятни последици за кариерата и др.

79. Съгласно член 11, параграф 3 от ДПЗД профилирането, което води до дискриминация на физическите лица въз основа на специални категории лични данни, например биометрични данни, се забранява в съответствие с правото на Съюза. Съгласно член 3, параграф 4 от ДПЗД „профилиране“ означава всяка форма на автоматизирано обработване на лични данни, изразяващо се в използване на лични данни за оценяване на някои лични аспекти, свързани с дадено физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение. Когато се преценява дали са предвидени подходящи мерки за гарантиране на правата и свободите на субекта на данни и законните интереси на съответното физическо лице, трябва да се има предвид, че използването на ТЛР може да доведе до профилиране в зависимост от начина и целта, за която се прилага технологията. При всички случаи, в съответствие с правото на Съюза и член 11, параграф 3 от ДПЗД е забранено профилирането, което води до дискриминация на физически лица въз основа на специалните категории лични данни.

3.2.3 Категории субекти на данни

80. Член 6 от ДПЗД се отнася до необходимостта да се прави разграничение между различните категории субекти на данни. Това разграничение трябва да се прави, когато е приложимо и доколкото е възможно. То трябва да покаже въздействието върху начина, по който се обработват данните. От примерите, дадени в член 6 от ДПЗД, може да се заключи, че по правило обработването на лични данни трябва да отговаря на критериите за необходимост и пропорционалност също и по отношение на категорията на субектите на данни[55]. Освен това

[55] Вж. също Решение на Съда на ЕС по дело C-594/12, точки 56—59.

може да се заключи, че по отношение на субектите на данни, за които няма доказателства, които могат да наведат на мисълта, че поведението им може да има връзка, дори косвена или отдалечена, със законната цел според ДПЗД, най-вероятно няма основание за намеса[56]. Ако не е приложимо или не е възможно да се направи разграничение съгласно член 6 от ДПЗД, изключението от правилото на член 6 от ДПЗД трябва да се разгледа стриктно при оценката на необходимостта и пропорционалността на намесата. Разграничението между различните категории субекти на данни се явява съществено изискване, когато става въпрос за обработване на лични данни, включващо разпознаване на лица, като се имат предвид и възможните фалшиви положителни или фалшиви отрицателни резултати, които могат да имат значително въздействие върху физическите лица, както и в хода на разследването.

81. Както беше посочено, при прилагането на правото на Съюза трябва да се спазват разпоредбите на Хартата на основните права на Европейския съюз, вж. член 52 от Хартата. Следователно рамката и критериите, предоставени от ДПЗД, трябва да се тълкуват с оглед на Хартата. Правните актове на ЕС и неговите държави членки не трябва да спадат под тази мярка и трябва да гарантират пълното действие на Хартата.

3.2.4 Права на субекта на данни

82. ЕКЗД вече е предоставил насоки относно правата на субектите на данни съгласно ОРЗД в различни аспекти[57]. В ДПЗД са предвидени подобни права на субектите на данни, а общи насоки по този въпрос са предоставени в становище на Работната група по член 29, което е одобрено от ЕКЗД[58]. При определени обстоятелства ДПЗД позволява известни ограничения на тези права. Параметрите на тези ограничения ще бъдат разгледани по-подробно в раздел 3.2.4.6. „Законни ограничения на правата на субекта на данни“.

83. Въпреки че всички права на субектите на данни, изброени в глава III от ДПЗД, естествено се прилагат и към обработването на лични данни чрез технология за лицево разпознаване (ТЛР), следващата глава ще акцентира върху някои от правата и аспектите, във връзка с които може да има особен интерес от получаване на насоки. Освен това настоящата глава и нейният анализ зависят от това дали въпросното обработване с ТЛР изпълнява правните изисквания, описани в предходната глава.

84. Като се има предвид естеството на обработването на лични данни чрез ТЛР (обработване на специални категории лични данни често без очевидно взаимодействие със субекта на данните), администраторът трябва внимателно да прецени как (или дали може) да изпълни изискванията на ДПЗД, преди да започне обработването чрез ТЛР. По-специално чрез внимателен анализ на:

- това кои са субектите на данни (често повече от този(тези), който(които) е(са) основната цел за целите на обработването),
- по какъв начин субектите на данни са информирани за обработването чрез ТЛР (вж. раздел 3.2.4.1),
- как субектите на данни могат да упражняват правата си (в този случай както правата на информация и достъп, така и правата на коригиране или ограничаване могат да бъдат

[56] Вж. също Решение на Съда на ЕС по дело C-594/12, т. 58.
[57] Вж. например 1/2022 Насоки на ЕКЗД относно правата на субектите на данни — Право на достъп и 3/2019 Насоки на ЕКЗД относно обработването на лични данни чрез видеоустройства.
[58] РД 258, Становище относно някои ключови въпроси във връзка с Директива (ЕС) 2016/680 относно правоприлагането (ЕС 2016/680).

особено трудни за спазване, в случай че ТЛР се използва за всички проверки, с изключение на проверката 1 към 1 при пряк контакт с физическото лице).

3.2.4.1 Запознаване на субектите на данни с техните права и информация в кратка, разбираема и лесно достъпна форма

85. ТЛР води до предизвикателства, свързани с гарантирането на информирането на физическите лица относно обработването на техните биометрични данни. Особено трудно е, ако даден ПО анализира чрез ТЛР видеоматериал, който произхожда или е предоставен от трета страна, тъй като ПО има малка възможност, а в повечето случаи и никаква, да уведоми субекта на данните по време на събирането (напр. чрез знак на място). Всеки видеоматериал, който не е от значение за разследването (или целта на обработването), следва винаги да бъде премахван или анонимизиран (напр. чрез замъгляване без възможност за обратно възстановяване на данните), преди да се пристъпи към каквото и да е обработване на биометрични данни, за да се избегне рискът да не е изпълнен принципът за свеждане на данните до минимум, посочен в член 4, параграф 1, буква д) от ДПЗД, както и задълженията за предоставяне на информация, посочени в член 13, параграф 2 от ДПЗД. Отговорност на администратора е да прецени каква информация би била от значение за субекта на данните при упражняване на неговите права и да гарантира, че необходимата информация е предоставена. Ефективното упражняване на правата на субектите на данни зависи от изпълнението от страна на администратора на задълженията му за предоставяне на информация.

86. В член 13, параграф 1 от ДПЗД се посочва каква минимална информация трябва да се предоставя на субекта на данните като цяло. Тази информация може да бъде предоставена чрез уебсайта на администратора, в печатна форма (напр. брошура, достъпна при поискване) или леснодостъпни по друг начин източници за субекта на данни. Администраторът на данни трябва във всички случаи да гарантира, че информацията се предоставя ефективно поне по отношение на следните елементи:

- самоличност и данни за контакт на администратора, включително на длъжностното лице по защита на данните,
- целта на обработването и това, че то е обработване чрез ТЛР,
- правото на подаване на жалба до надзорен орган и данните за връзка с този орган,
- правото на искане на достъп до, коригиране или изтриване на личните данни и ограничаване на обработването на личните данни.

87. Освен това в конкретни случаи, определени в националното право, които следва да бъдат в съответствие с член 13, параграф 2 от ДПЗД[59], като например обработването чрез ТЛР, следната информация трябва да се предоставя пряко на субекта на данните:

- правното основание за обработването,
- информация за това къде са събрани личните данни без знанието на субекта на данните,
- срока, за който ще се съхраняват личните данни, или, когато това не е възможно, критериите, използвани за определяне на този срок,

[59] Например член 56, параграф 1 от Германския федерален закон за защита на данните, в който, наред с другото, се посочва каква информация трябва да се предоставя на субектите на данни при операции под прикритие

- ако е приложимо, категориите получатели на личните данни (включително трети държави или международни организации).

88. Въпреки че член 13, параграф 1 от ДПЗД съдържа обща информация за обществеността, член 13, параграф 2 от ДПЗД се отнася до допълнителната информация, която трябва да бъде предоставена на конкретен субект на данни в конкретни случаи, например когато данните се събират пряко от субекта на данните или косвено без знанието на субекта на данните[60]. В член 13, параграф 2 от ДПЗД няма ясно определение за това какво се има предвид под „конкретни случаи“. Той обаче се отнася до ситуации, в които физическите лица трябва да бъдат информирани за обработването, което се отнася конкретно до тях, и да им бъде предоставена подходяща информация, за да могат ефективно да упражняват правата си. ЕКЗД счита, че когато се преценява дали е налице „конкретен случай“, трябва да се вземат предвид няколко фактора, включително дали личните данни се събират без знанието на субекта на данните, тъй като това би бил единственият начин да се даде възможност на лицата да упражняват ефективно своите права. Други примери за „конкретни случаи“ биха могли да бъдат случаите, когато личните данни се обработват допълнително като обект на процедура за международно наказателно сътрудничество или в случай на обработване на лични данни в рамките на операции под прикритие, както е посочено в националното право. Освен това от съображение 38 от ДПЗД, че ако вземането на решения се извършва единствено въз основа на ТЛР, субектите на данни трябва да бъдат информирани за характеристиките на автоматизираното вземане на решения. Това би означавало също така, че това е специфичен случай, в който на субекта на данни следва да се предостави допълнителна информация в съответствие с член 13, параграф 2 от ДПЗД[61].

89. И накрая, следва да се отбележи, че съгласно член 13, параграф 3 от ДПЗД държавите членки могат да приемат законодателни мерки, които ограничават задължението за предоставяне на информация в конкретни случаи за определени цели. Това се прилага, доколкото и докато такава мярка представлява необходима и пропорционална мярка в едно демократично общество, като надлежно се вземат предвид основните права и законните интереси на субекта на данните.

3.2.4.2 Право на достъп

90. По принцип субектът на данните има право да получи положително или отрицателно потвърждение за всяко обработване на личните му данни и, ако отговорът е положителен, достъп до личните данни като такива, както и до допълнителна информация, както е посочено в член 14 от ДПЗД. Що се отнася до ТЛР, когато биометричните данни се съхраняват и са свързани с дадена самоличност и чрез буквено-цифрови данни, това следва да позволи на компетентния орган да потвърди искането за достъп въз основа на търсене по тези буквено-цифрови данни, без да започва по-нататъшно обработване на биометрични данни на други лица (т.е. чрез търсене с ТЛР в база данни). Трябва да се спазва принципът за свеждане на данните до минимум и да не се съхраняват повече данни, отколкото е необходимо с оглед на целта на обработката.

3.2.4.3 Право на коригиране на личните данни

91. Тъй като в ОРЗД не се предвижда абсолютна точност, от особена важност е администраторите да бъдат бдителни по отношение на исканията за коригиране на лични данни. Възможно е също

[60] РД 258, Становище относно някои ключови въпроси във връзка с Директивата относно правоприлагането (ЕС 2016/680), стр. 17—18.

[61] Следва да се отбележи също така разликата между „предоставя на субектите на данни“ съгласно член 13, параграф 1 от ДПЗД и „предоставя на субекта на данните“ съгласно член 13, параграф 2 от ДПЗД. Според член 13, параграф 2 от ДПЗД администраторът трябва да гарантира, че информацията достига до субекта на данните, когато публикуваната информация на даден уебсайт няма да бъде достатъчна.

така даден субект на данни въз основа на ТЛР да е бил поставен в неточна категория, напр. да е неправилно поставен в категорията на заподозрени лица въз основа на първоначално предположение за начина на действие във видеозапис. Рисковете за субектите на данни са особено сериозни, ако такива неточни данни се съхраняват в полицейска база данни и/или се споделят с други структури. Администраторът трябва да коригира съхраняваните данни и системите за ТЛР по подходящ начин, вж. съображение 47 от ДПЗД.

3.2.4.4 Право на изтриване

92. При повечето обстоятелства, в случай че не се използва за проверка/удостоверяване на автентичността 1 към 1, ТЛР ще представлява обработване на голям брой биометрични данни на субектите на данни. Поради това е важно администраторът предварително да прецени докъде стигат ограниченията на неговата цел и необходимост, така че искането за заличаване в съответствие с член 16 от ДПЗД да може да бъде разгледано без неоправдано забавяне (тъй като администраторът трябва, наред с другото, да заличи личните данни, които се обработват извън това, което приложимото законодателство позволява съгласно членове 4, 8 и 10 от ДПЗД).

3.2.4.5 Право на ограничаване

93. В случай че точността на данните се оспорва от субекта на данните и не може да бъде установена (или когато личните данни трябва да се съхраняват за целите на бъдещите доказателства), администраторът е длъжен да ограничи личните данни на това физическо лице в съответствие с член 16 от ДПЗД. Това е особено важно, когато става въпрос за технология за лицево разпознаване (основана на алгоритъм(ми), и следователно никога не показва окончателен резултат) в ситуации, в които се събират големи количества данни и точността, и качеството на идентифицирането могат да варират. При лошо качество на видеоматериалите (напр. от местопрестъпление) рискът от фалшиви положителни резултати се увеличава. Освен това, ако изображенията на лица в списъка за наблюдение не се актуализират редовно, това също ще увеличи риска от фалшиви положителни или фалшиви отрицателни резултати. В конкретни случаи, когато данните не могат да бъдат изтрити поради факта, че са налице разумни основания да се смята, че заличаването би могло да засегне законните интереси на субекта на данните, данните следва вместо това да бъдат ограничени и обработвани само за целта, която е попречила на изтриването им (вж. съображение 47 от ДПЗД).

3.2.4.6 Законни ограничения на правата на субекта на данни

94. Що се отнася до задълженията за предоставяне на информация на администратора и правото на достъп на субектите на данни, ограничения са разрешени само ако са предвидени в закона, който на свой ред трябва да представлява необходима и пропорционална мярка в едно демократично общество при надлежно зачитане на основните права и законните интереси на засегнатото физическо лице (вж. член 13, параграфи 3 и 4, член 15 и член 16, параграф 4 от ДПЗД). Когато ТЛР се използва за целите на правоприлагането, може да се очаква, че тя ще се използва при обстоятелства, при които това би било вредно за преследваната цел за информиране на субекта на данните или за даване на възможност за достъп до данните. Това би било така например при полицейско разследване на престъпление или с цел защита на националната или обществената сигурност.

95. Правото на достъп не означава автоматично достъп до цялата информация, напр. при наказателно дело, в което се съдържат лични данни. Валиден пример за това кога могат да бъдат разрешени ограничения на правото може да бъде в хода на наказателно разследване.

3.2.4.7 Упражняване на права чрез надзорния орган

96. В случаите, в които съществуват законни ограничения за упражняването на правата съгласно глава III от ДПЗД, субектът на данните може да поиска от органа за защита на данните да упражни правата му от негово име, като провери законосъобразността на обработването от администратора. Администраторът е длъжен да информира физическото лице за възможността да упражни правата си по този начин (вж. член 17 от и член 46, параграф 1, буква ж) от ДПЗД). За ТЛР това означава, че администраторът трябва да гарантира, че са налице подходящи мерки, за да може да бъде разгледано такова искане, напр. да се даде възможност за търсене в записани материали, при условие че субектът на данните предостави достатъчно информация, за да бъдат намерени личните му данни.

3.2.5 Други законови изисквания и предпазни мерки

3.2.5.1 Член 27 Оценка на въздействието върху защитата на данните

97. Оценката на въздействието върху защитата на данните (ОВЗД) преди използването на ТЛР е задължително изискване, тъй като по-специално видът на обработването, при което се използват нови технологии, и като се вземат предвид естеството, обхватът, контекстът и целите на обработването, вероятно ще доведе до висок риск за правата и свободите на физическите лица. Като се има предвид, че използването на този вид технологии предполага системно автоматично обработване на специални категории данни, може да се предположи, че в такива случаи администраторът по правило е задължен да извърши ОВЗД. ОВЗД следва да съдържа най-малко общо описание на предвидените операции по обработване, оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите, оценка на рисковете за правата и свободите на субектите на данни, мерките, предвидени за справяне с тези рискове, гаранции, мерки за сигурност и механизми за гарантиране на защитата на личните данни и доказване на съответствието. ЕКЗД препоръчва резултатите от такива оценки или поне основните констатации и заключения на ОВЗД да се оповестяват като мярка за повишаване на доверието и прозрачността[62].

3.2.5.2 Член 28 Предварителна консултация с надзорния орган

98. Съгласно член 28 от ДПЗД администраторът или обработващият лични данни трябва да се консултира с надзорния орган преди обработването, когато: а) оценката на въздействието върху защитата на данните показва, че обработването би довело до висок риск при липса на мерки, предприети от администратора за намаляване на риска; или б) видът на обработването, по-специално когато се използват нови технологии, механизми или процедури, е свързан с висок риск за правата и свободите на субектите на данни. Както вече беше обяснено в раздел 2.3. от настоящите насоки, ЕКЗД счита, че повечето случаи на внедряване и използване на ТЛР съдържат присъщ висок риск за правата и свободите на физическите лица. Следователно, в допълнение към оценката на въздействието върху защитата на данните, органът, който внедрява ТЛР, следва да се консултира с компетентния надзорен орган преди внедряването на системата.

3.2.5.3 Член 29 Сигурност на обработването

99. Уникалният характер на биометричните данни прави невъзможно за субекта на данни да ги промени, в случай че те са компрометирани, например в резултат на нарушение на сигурността на данните. Поради това компетентният орган, който прилага и/или използва ТЛР, следва да обърне специално внимание на сигурността на обработването, в съответствие с член 29 от ДПЗД. По-специално, правоприлагащият орган следва да гарантира, че системата отговаря на

[62] За повече информация вж. РД 248 ред.01 Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определянето на това дали съществува вероятност обработването „да породи висок риск“.

съответните стандарти, и да приложи мерки за защита на биометричните образци[63]. Това задължение е още по-важно, ако правоприлагащият орган използва доставчик на услуги от трета страна (обработващ данни).

3.2.5.4 Член 20 Защита на данните на етапа на проектирането и по подразбиране

100. Защитата на данните на етапа на проектирането и по подразбиране в съответствие с член 20 от ДПЗД има за цел да гарантира, че принципите и гаранциите за защита на данните, например свеждане до минимум на данните и ограничаване на съхранението, са вложени в технологията чрез подходящи технически и организационни мерки, като например псевдонимизация, още преди началото на обработването на лични данни и ще се прилагат през целия им жизнен цикъл. Като се има предвид присъщият висок риск за правата и свободите на физическите лица, изборът на такива мерки не следва да зависи единствено от икономически съображения,[64] а вместо това следва да е насочен към прилагане на най-съвременните технологии за защита на данните. В същия дух, ако ПО възнамерява да прилага и използва ТЛР от външни доставчици, той трябва да гарантира, например чрез процедура за възлагане на обществена поръчка, че се прилага единствено ТЛР, изградена въз основа на принципите за защита на данните на етапа на проектирането и по подразбиране[65]. Това също така означава, че прозрачността на функционирането на ТЛР не е ограничена от задължения за търговска тайна или права на интелектуална собственост.

3.2.5.5 Член 25 Водене на записи

101. В ДПЗД са предвидени различни методи за доказване от страна на администратора или обработващия лични данни на законосъобразността на обработването и за гарантиране на целостта и сигурността на данните. В това отношение регистрите на системите са много полезен инструмент и важна предпазна мярка за проверка на законосъобразността на обработването както на вътрешно равнище (т.е. самонаблюдение), така и от външни надзорни органи, като например органите за защита на данните. Съгласно член 25 от ДПЗД в системите за автоматизирано обработване следване да се съхраняват регистри най-малко за следните операции по обработване: събиране, промяна, консултиране, разкриване, включително предаване, комбиниране и заличаване. Освен това регистрите за справки и разкриване на данни следва да дават възможност да се установят основанието, датата и часът на тези операции и, доколкото е възможно, идентификацията на лицето, което е извършило справка или е разкрило лични данни, както и самоличността на получателите на тези лични данни. Освен това в рамките на системите за лицево разпознаване се препоръчва да се извърши водене на записи за следните допълнителни операции по обработване (отчасти извън обхвата на член 25 от ДПЗД):

- Промени в референтната база данни (добавяне, изтриване или актуализиране). В регистъра следва да се съхранява копие от съответното (добавено, изтрито или актуализирано) изображение, когато не е възможно по друг начин да се провери законосъобразността или резултатът от операциите по обработване.

- Опити за идентифициране или проверка, включително резултата и степента на доверие. Трябва да се прилага строг принцип на минимизиране, така че в регистрите да се съхранява

[63] Вж. например: ISO/IEC 24745 Информационна сигурност, киберсигурност и защита на неприкосновеността на личния живот — защита на биометричната информация.

[64] Вж. съображение 53 от ДПЗД.

[65] За повече информация вж. Насоки на ЕКЗД относно Защита на данните на етапа на проектирането и по подразбиране, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf .

само идентификаторът на изображението от референтната база данни, вместо самото референтно изображение. Воденето на записи за въведените биометрични данни трябва да се избягва, освен ако не е необходимо (напр. само в случаи на съвпадение)

- Самоличността на потребителя, който е поискал идентификацията или е извършил опит за проверка.

- Всички лични данни, съхранявани в регистрите на системите, подлежат на строги ограничения по отношение на целите (напр. одити) и не трябва да се използват за други цели (напр. за да може все пак да се извършва разпознаване/проверка, включително на изображение, което е било изтрито от референтните бази данни). Следва да се прилагат мерки за сигурност, за да се гарантира целостта на записите, като системите за автоматично наблюдение за откриване на злоупотреби с регистрационните файлове са силно препоръчителни. По отношение на регистрите на референтната база данни мерките за сигурност следва да бъдат еквивалентни на референтната база данни в случай на съхранение на портретни снимки. Също така следва да се въведат автоматични процеси, за да се гарантира прилагането на срока за съхранение на данните за регистрационните файлове.

3.2.5.6 Член 4, параграф 4 Отчетност

102. Администраторът трябва да е в състояние да докаже, че обработването отговаря на принципите, посочени в член 4, параграфи 1—3, вж. член 4, параграф 4 от ДПЗД. В това отношение от решаващо значение е системната и актуална документация на системата (включително актуализации, модернизации и алгоритмично обучение), техническите и организационните мерки (включително наблюдение на работата на системата и потенциална човешка намеса) и обработването на личните данни. За да се докаже законосъобразността на обработването на лични данни, особено важен елемент е воденето на записи на данни съгласно член 25 от ДПЗД (вж. раздел 3.2.5.5). Принципът на отчетност се отнася не само до системата и обработването, но и до документирането на процедурните гаранции, като например оценки на необходимостта и пропорционалността, ОВЗД, както и вътрешните консултации (напр. одобрение на проекта от ръководството или вътрешни решения относно стойностите на коефициента на доверие) и външните консултации (напр. органа за защита на данните). Приложение II включва редица елементи в това отношение.

3.2.5.7 Член 47 Ефективен надзор

103. Ефективният надзор от страна на компетентните органи за защита на данните е една от най-важните гаранции за основните права и свободи на физическите лица, засегнати от използването на ТЛР. В същото време осигуряването на всеки орган за защита на данните на необходимите човешки, технически и финансови ресурси, помещения и инфраструктура е предпоставка за ефективното изпълнение на техните задачи и упражняване на правомощията им[66]. Още по-важни от броя на наличните служители са уменията на експертите, които трябва да покриват много широк спектър от въпроси — от наказателни разследвания и полицейско сътрудничество до анализ на големи масиви от данни и изкуствен интелект. Поради това държавите членки следва да гарантират, че ресурсите на надзорните органи са подходящи и достатъчни, за да им

[66]Вж. Съобщение на Комисията „Първи доклад относно прилагането и функционирането на Директива (ЕС) 2016/680 защитата на данните в областта на правоприлагането („ДПЗД“)“, COM(2022) 364 final, стр. 3.4.1.

позволят да изпълняват мандата си за защита на правата на субектите на данни и да следят отблизо всички промени в това отношение.[67]

4 ЗАКЛЮЧЕНИЕ

104. Използването на технологии за лицево разпознаване е неразривно свързано с обработването на значителни количества лични данни, включително специални категории данни. Лицето и в по-общ план биометричните данни са трайно и неотменимо свързани със самоличността на дадено лице. Следователно използването на лицево разпознаване има пряко или косвено въздействие върху редица основни права и свободи, залегнали в Хартата на основните права на ЕС, които може да преминават границите неприкосновеността на личния живот и защитата на данните, като например човешкото достойнство, свободата на движение, свободата на събиране и други. Това е особено важно в областта на правоприлагането и наказателното правосъдие.

105. ЕКЗД разбира, че е необходимо правоприлагащите органи да се възползват от най-добрите възможни инструменти за бързо установяване на самоличността на извършителите на терористични актове и други тежки престъпления. Тези инструменти обаче следва да се използват при стриктно спазване на приложимата правна уредба и само в случаите, когато отговарят на изискванията за необходимост и пропорционалност, както е посочено в член 52, параграф 1 от Хартата. Освен това, макар че съвременните технологии могат да бъдат част от решението, те в никакъв случай не са панацея.

106. Съществуват определени случаи на използване на технологиите за лицево разпознаване, които представляват неприемливо висок риск за хората и обществото („червени зони“). Поради тези причини ЕКЗД и ЕНОЗД призоваха за тяхната обща забрана[68].

107. По-специално, дистанционната биометрична идентификация на физически лица в публично достъпни пространства представлява висок риск от намеса в личния живот на хората и няма място в едно демократично общество, тъй като по своята същност води до масово наблюдение. В същия дух ЕКЗД счита, че поддържаните от изкуствен интелект системи за лицево разпознаване, които категоризират лицата въз основа на техните биометрични данни в клъстери според етническата принадлежност, пола, както и политическата или сексуалната ориентация, не са съвместими с Хартата. Освен това ЕКЗД е убеден, че използването на лицево разпознаване или подобни технологии за определяне на емоциите на физическо лице е крайно нежелателно и следва да бъде забранено, евентуално с няколко надлежно обосновани изключения. Освен това ЕКЗД счита, че обработването на лични данни в рамките на правоприлагането, което ще се основава на база данни, попълнена чрез масово и безразборно събиране на лични данни, например чрез „събиране“ на достъпни онлайн снимки и портретни снимки, по-специално такива, които се предоставят чрез социалните мрежи, само по себе си не отговаря на изискването за строга необходимост, предвидено в правото на Съюза.

[67] Вж. Принос на ЕКЗД към оценката на Европейската комисия на Директива относно защитата на данните в областта на правоприлагането (ДПЗД) съгласно член 62, параграф 14, https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf

[68] Вж. Съвместното становище 5/2021 на ЕКЗД и ЕНОЗД относно предложението за Регламент на Европейския парламент и на Съвета за определяне на хармонизирани правила относно изкуствения интелект (Законодателен акт за изкуствения интелект) https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

5 ПРИЛОЖЕНИЯ

Приложение I: Модел на подпомагане

Приложение II: Практическо ръководство за управление на проекти за ТЛР в ПО

Приложение III: Практически примери

ПРИЛОЖЕНИЕ I — ОБРАЗЕЦ ЗА ОПИСАНИЕ НА СЦЕНАРИИТЕ

(С информационни карета за аспектите, разгледани в рамките на сценария)

Описание на обработването:

- Описание на обработването, контекст (връзка с престъплението), цел

Източник на информация:

- Видове субекти на данни: ☐ всички граждани ☐ осъдени лица ☐ заподозрени лица
  ☐ деца ☐ други уязвими субекти на данни
- Източник на изображението: ☐ публично достъпни пространства
  ☐ интернет
  ☐ частноправен субект ☐ други физически лица ☐ други .....
- Връзка с престъплението: ☐ Пряка времева ☐ Косвена времева
  ☐ Пряка географска ☐ Косвена географска
  ☐ Не е необходима
- Начин на събиране на информацията: ☐ дистанционно ☐ в кабина или в контролирана среда
- Контекст — засягане на други основни права:
  ☐ Не
  Да, а именно ☐ свобода на събранията
  ☐ свобода на словото
  ☐ различни:.....
- Възможности за допълнителни източници на информация относно субекта на данните:
  ☐ Документ за самоличност ☐използване на обществен телефон ☐ регистрационни номера на превозно средство
  ☐ други .....

Референтна база данни (с която се сравнява заснетата информация):

- Специфичност: ☐ бази данни с общо предназначение☐ специфични бази данни, свързани със сферата на престъплението
- Описание на начина на попълване на тези референтни бази данни (и правно основание)
- Промяна на предназначението на базата данни (напр. сигурността на частната собственост е основната цел): ☐ ДА
  ☐ НЕ

Алгоритъм:

- Вид на обработването: ☐ проверка 1 към 1 (удостоверяване на автентичността) ☐ идентифициране 1 към много
- Съображения за точност
- Технически предпазни мерки

Резултат:

- Въздействие ☐ Пряко (напр. субектът на данни може да бъде арестуван, разпитван, дискриминационно поведение)

  ☐ Косвено (използвани за статистически модели, няма сериозни правни действия срещу субектите на данни)

- Автоматизирано решение: ☐ ДА☐ НЕ
- Срок на съхранение

Правен анализ:

- Анализ на необходимостта и пропорционалността — цел/тежест на престъплението/брой на лицата, които не са замесени, но са засегнати от обработването
- Вид предварителна информация за субекта на данните: ☐ При влизане в конкретната зона

  ☐ На уебсайта на ПО като цяло

  ☐ На уебсайта на ПО за конкретното обработване

  ☐ Друго .....
- Приложима правна уредба:

  ☐ ДПЗД се копира предимно в националното законодателство

  ☐ Общо национално законодателство относно използването на биометрични данни от ПО

  ☐ Специално национално законодателство за това обработване (лицево разпознаване) за този компетентен орган

  ☐ Специално национално законодателство за това обработване (автоматизирано решение)

Заключение:

Общи съображения за това дали описаното обработване е вероятно да е съвместимо с правото на ЕС (и някои указания за правни предпоставки)

ПРИЛОЖЕНИЕ II — ПРАКТИЧЕСКИ НАСОКИ ЗА УПРАВЛЕНИЕ НА ПРОЕКТИ ЗА ТЛР В ПО

В настоящото приложение са предоставени някои допълнителни практически насоки за правоприлагащите органи („ПО“), които планират да стартират проект, включващ технология за лицево разпознаване („ТЛР“). Приложението съдържа повече информация за организационните и техническите мерки, които трябва да се вземат предвид по време на внедряването на проекта, и не следва да се разглежда като изчерпателен списък от стъпки/мерки, които трябва да се предприемат. То следва да се разглежда и във връзка с Насоки 3/2019 на ЕКЗД относно обработването на лични данни чрез видеоустройства[69] и всички регламенти на ЕС/ЕИП и насоки на ЕКЗД относно използването на изкуствен интелект.

В настоящото приложение са предоставени насоки въз основа на предположението, че ПО ще възлагат обществени поръчки за ТЛР (като готови за употреба продукти). Ако ПО планират да разработят (допълнително обучат) ТЛР, тогава се прилагат допълнителни изисквания за подбор на необходимите набори от данни за обучение, валидиране и изпитване, които да се използват по време на разработването, и ролите/мерките за средата за разработване. По подобен начин готов продукт може да се нуждае от допълнителни корекции за предвидената употреба, като в този случай трябва да се спазят горепосочените изисквания за избор на набори от данни за тестване, валидиране и обучение.

Принадлежността към един и същ ПО сама по себе си не осигурява пълен достъп до биометрични данни. Както при всички други категории лични данни, биометричните данни, събирани за определена цел на правоприлагането по силата на конкретно правно основание, не могат да се използват без подходящо правно основание за различна цел на правоприлагането (член 4, параграф 2 от Директива (ЕС) 2016/680 (ДПЗД). Освен това разработването/обучението за инструмент за управление на ТЛР се счита за различна цел и трябва да се прецени дали обработването на биометрични данни за измерване на ефективността/обучението по технологията, така че да се избегне въздействие върху субектите на данни поради ниска ефективност, е необходимо и пропорционално, като се вземе предвид първоначалната цел на обработването.

1. РОЛИ И ОТГОВОРНОСТИ

Когато ПО използва ТЛР за изпълнението на задачите си, попадащи в обхвата на ДПЗД (предотвратяване, разследване, разкриване или наказателно преследване на престъпления и др., съгласно член 3 от ДПЗД), той може да се счита за администратор на ТЛР. ПО обаче се състоят от няколко звена/отдели, които може да участват в това обработване или чрез определяне на процеса на прилагане на ТЛР, или чрез прилагането му на практика. Поради особеностите на тази технология може да е необходимо включването на различни единици или с цел подпомагане на измерването на нейната ефективност, или за допълнителното ѝ обучение.

[69] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

В проект, включващ ТЛР, има няколко заинтересовани страни[70] в рамките на ПО, чието участие може да бъде необходимо:

- Висше ръководство — за одобряване на проекта след балансиране на рисковете спрямо потенциалните ползи.
- Длъжностно лице по защита на данните (ДЛЗД) и/или правен отдел на ПО — за съдействие при оценката на законосъобразността на изпълнението на определен проект за ТЛР; при извършването на оценка на въздействието върху ОВЗД; при гарантиране на спазването и упражняването на правата на субектите на данни.
- Собственик на процеса — изпълнява роля на конкретно звено в рамките на съответния ПО за разработване на проекта, като взема решения относно елементите от проекта за ТЛР, включително изискванията за ефективност на системата; определя подходящ показател за справедливост; определя коефициента на доверие[71]; определя допустими прагове за пристрастност; определя потенциалните рискове, които проектът за ТЛР поражда за правата и свободите на физическите лица (чрез консултиране също и с ДЛЗД, и ИТ отдела с ИИ, и/или отдела за анализ на данните (вж. по-долу), и за представянето им на висшето ръководство. Собственикът на процеса ще се консултира и с ръководителя на референтната база данни, преди да вземе решение за елементите на проекта за ТЛР, за да разбере както целта на използване на референтната база данни, така и нейните технически характеристики. В случай на повторно обучение на съществуваща ТЛР, собственикът на процеса също ще отговаря за подбора на набора от данни за обучението. В качеството си на звеното, натоварено с разработването и определянето на елементите по проекта, собственикът на процеса отговаря за провеждането на ОВЗД.
- Отдел „Изкуствен интелект и/или анализ за данните“ — за подпомагане на извършването на оценка на въздействието върху защитата на данните; за разясняване на наличните показатели за измерване на ефективността на системата, справедливостта[72] и потенциалните предразсъдъци; за прилагане на технологиите и техническите предпазни мерки, за да се предотврати неразрешен достъп до събраните данни, кибератаки и др. В случай на повторно обучение на съществуваща ТЛР отделът за ИТ с ИИ или анализ на данните ще обучава системата въз основа на набора от данни за обучение, предоставен от собственика на процеса. Този отдел ще отговаря и за въвеждането на мерки за смекчаване на рисковете, установени съвместно от собствениците на процеса (напр. специфични за ИИ рискове, като например атаки за достигане до заключения чрез модели).
- Крайни потребители (например полицейски служители на терен или в криминалистични лаборатории) — за извършване на сравнения спрямо базата данни; за критичен преглед на резултатите, като се вземат предвид предишните доказателства, и за предоставяне на обратна информация на собственика на процеса за фалшиви положителни резултати и индикации за възможна дискриминация.

[70] Следните роли са показателни за различните заинтересовани страни и техните отговорности в проект за ТЛР. Въпреки че използваният за описание на ролите в настоящото приложение език не е категоричен, всеки ПО трябва да определи и възложи подобни роли в съответствие със своята организация. Възможно е дадена единица да натрупва повече от една роля, например отговорник за процесите и мениджър на референтна база данни или отговорник за процесите и отдел за ИТ с ИИ и/или отдел за анализ на данни (в случай че отделът на собственика на процеса разполага с всички необходими технически познания).

[71] Коефициентът на доверие е нивото на увереност в прогнозата (съвпадението) под формата на вероятност. Напр. при сравняване на два образеца има 90 % увереност, че те принадлежат на едно и също лице. Коефициентът на доверие е различен от ефективността на ТЛР, но влияе на ефективността. Колкото е по-висок прагът на доверие, толкова по-малко ще бъдат фалшивите положителни и повече фалшивите отрицателни резултати в резултатите от FRT.

[72] Справедливостта може да се определи като липсата на несправедлива, незаконна дискриминация, например полова или расова пристрастност.

- Управител на референтната база данни — специалното звено в рамките на компетентния ПО, което отговаря за попълването и управлението на референтната база данни, т.е. базата данни, с която ще се сравняват изображенията, включително изтриването на изображенията на лица след определения период на съхранение. Тази база данни може да бъде създадена специално за предвидения проект за ТЛР или да съществува предварително за съвместими цели. Управителят на референтната база данни отговаря за определянето на това кога и при какви обстоятелства могат да се съхраняват портретните снимки, както и за определянето на изискванията за запазване на данните (в съответствие с времето или други критерии).

Тъй като за повечето случаи на внедряване и използване на ТЛР е присъщ висок риск за правата и свободите на субектите на данни, надзорният орган по защита на данните също следва да бъде включен в рамките на предварителната консултация, изисквана съгласно член 28 от ДПЗД.

2. ВЪВЕЖДАНЕ В ЕКСПЛОАТАЦИЯ/ПРЕДИ ПРИДОБИВАНЕ НА СИСТЕМАТА ЗА ТЛР

Собственикът на процеса в дадена ПО трябва първо да има ясно разбиране за процеса(ите), който(ито) е(са) насочен(и) към използването на ТЛР (случай(и) на използване), и да се увери, че има правно основание, за да обоснове планирания случай на използване. Въз основа на това той трябва да:

- Опише официално случая на използване. Трябва да се опише проблемът, който трябва да се реши, и начинът, по който ТЛР ще осигури решение, както и общият преглед на процеса (задачата), в който ще се прилага. Във връзка с това правоприлагащите органи следва да документират най-малко[73]:
  - Категориите лични данни, записани в процеса
  - Целите и конкретните задачи, за които ще се използва ТЛР, включително потенциалните последици за субекта на данните след съвпадение.
  - Кога и как ще бъдат събирани портретните снимки (включително информация за начина на това събиране, например на входа на летището, видеозаписи от камери за сигурност извън магазин, в който е извършено престъпление, и др., както и категориите субекти на данни, чиито биометрични данни ще бъдат обработвани).
  - Базата данни, с която ще се сравняват изображенията (референтна база данни), както и информация за начина, по който е създадена, нейния размер и качеството на биометричните данни, които съдържа.
  - Участниците от ПО, които ще бъдат упълномощени да използват системата за ТЛР и да действат с нея в рамките на правоприлагането (техните профили и права на достъп трябва да бъдат определени от собственика на процеса).
  - Предвиденият срок на съхранение на входящите данни или моментът, който ще определи края на този срок (например приключването или прекратяването на наказателното производство в съответствие с националното процесуално право, за което данните първоначално са били събрани), както и всяко последващо действие (заличаване на тези данни, анонимизация и използване за статистически цели или за целите на научни изследвания и т.н.).
  - Водене на записи от прилагането и достъпност на водените регистри и записи.

[73] В приложение I е предоставен списък на елементите, които подпомагат администратора да опише случай на приложение на ТЛР.

- Показателите за ефективност (напр. точност, прецизност, припомняне, оценка F1) и техните минимално допустими прагове.[74]
- Оценка на броя на хората, които ще бъдат предмет на ТЛР в даден момент/случай.

- Извърши оценка на необходимостта и пропорционалността[75]. Фактът, че тази технология съществува, не следва да бъде факторът за нейното прилагане. Собственикът на процеса трябва първо да прецени дали съществува подходящо правно основание за предвиденото обработване. За тази цел трябва да се проведат консултации с ДЛЗД и правната служба. Движещата сила на внедряването на ТЛР трябва да бъде това, че тя е необходимо и пропорционално решение на конкретно определен проблем на ПО. Това трябва да се оценява в зависимост от целта/сериозността на престъплението/броя на лицата, които не са замесени, но са засегнати от системата за ТЛР. За целите на оценката на законосъобразността следва да се вземе предвид най-малко следното: ДПЗД[76], ОРЗД[77], [78] всяка съществуваща правна уредба за ИИ[79] и всички съпътстващи насоки, предоставени от надзорните органи за защита на данните (като например Насоките на ЕКЗД № 3/2019 относно обработването на лични данни чрез видеоустройства[80]). Тези законодателни актове на ЕС винаги трябва да бъдат съгласувани с приложимите национални изисквания, особено в областта на наказателнопроцесуалното право. В оценката на пропорционалността следва да се посочат основните права на субектите на данни, които могат да бъдат засегнати (освен неприкосновеността на личния живот и защитата на данните). В нея следва също така да се опишат и разгледат всички ограничения (или липсата на ограничения), наложени в случая на употреба на системата за ТЛР. Дали например системата ще работи постоянно или временно и дали ще бъде ограничена до определен географски район.

[74] Съществуват различни показатели за оценка на ефективността на системата за ТЛР. Всеки показател дава различен поглед върху резултатите от системата и нейният успех в предоставянето на адекватна картина на това дали системата за ТЛР функционира добре или не зависи от случая на използване на технологията. Ако акцентът е върху постигането на високи проценти на правилно съвпадение на лице, могат да се използват показатели като точност и припомняне. Тези показатели обаче не измерват доколко добре ТЛР се справя с отрицателните примери (за колко от тях системата е дала съвпадение). Собственикът на процеса, с помощта на отдела за ИТ с ИИ и анализ на данните, трябва да може да определи изискванията за производителност и да ги изрази в най-подходящите показатели според случая на използване на ТЛР.

[75] Може да се обмислят допълнителни стъпки, за да се гарантира необходимостта по отношение на адаптирането и използването на системата, така че описанието на случая на използване може също да бъде леко променено по време на оценката на необходимостта и пропорционалността.

[76] Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания.

[77] 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 данни.

[78] В случаите, когато в рамките на научен проект, насочен към проучване на използването на ТЛР, трябва да се обработват лични данни, но това обработване не попада в обхвата на член 4, параграф 3 от ДПЗД като цяло, ще бъде приложим ОРЗД (член 9, параграф 2 от ДПЗД). В случай на пилотни проекти, които ще бъдат последвани от операции по правоприлагане, ДПЗД все пак ще бъде приложима.

[79] Има например предложение за РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА ЗА ОПРЕДЕЛЯНЕ НА ХАРМОНИЗИРАНИ ПРАВИЛА ОТНОСНО ИЗКУСТВЕНИЯ ИНТЕЛЕКТ (ЗАКОНОДАТЕЛЕН АКТ ЗА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ) И ЗА ИЗМЕНЕНИЕ НА НЯКОИ ЗАКОНОДАТЕЛНИ АКТОВЕ НА СЪЮЗА, който обаче все още не е приет като регламент.

[80] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

- Извърши оценка на въздействието върху защитата на данните (ОВЗД) [81]. ОВЗД следва да се извърши, тъй като има вероятност внедряването на ТЛР в областта на правоприлагането да доведе до висок риск за правата и свободите на физическите лица[82]. ОВЗД следва да съдържа по-специално: общо описание на предвидените операции по обработване[83], оценка на рисковете за правата и свободите на субектите на данни[84], мерки, предвидени за справяне с тези рискове, гаранции, мерки за сигурност и механизми за гарантиране на защитата на личните данни и доказване на съответствие. ОВЗД е текущ процес, така че всички нови елементи на обработването следва да се добавят и оценката на риска следва да се актуализира на всеки етап от проекта.
- Получи одобрение от висшето ръководство, като разясни рисковете за правата и свободите на субектите на данни (от случая на употреба и технологията) и съответните планове за третиране на риска.

3. ПО ВРЕМЕ НА ВЪЗЛАГАНЕТО НА ОБЩЕСТВЕНИ ПОРЪЧКИ И ПРЕДИ ВНЕДРЯВАНЕТО НА ТЛР

- Определи критериите за избор на ТЛР (алгоритъм). Собственикът на процеса следва да определи критериите за избор на алгоритъм с помощта на отдела на ИТ с ИИ и/или анализ на данните. На практика те ще включват показатели за справедливост и производителност, определени в описанието на случая на използване. Тези критерии следва да включват и информация, свързана с данните, с които е бил обучен алгоритъмът. Наборът за обучение, тестване и валидиране трябва да включва в достатъчна степен проби от всички характеристики на субектите на данни, които ще бъдат обект на ТЛР (напр. възраст, пол и раса), за да се намалят отклоненията. Доставчикът на ТЛР трябва да предостави информация и показатели за наборите от данни за обучение, тестване и валидиране на ТЛР и да опише мерките, предприети за измерване и намаляване на потенциалната незаконна дискриминация и пристрастия. Когато е възможно, собственикът на процеса трябва да провери дали доставчикът е имал правно основание да използва този набор от данни за целите на обучението на алгоритмите (въз основа на информацията, която доставчикът ще предостави). Освен това собственикът на процеса следва да гарантира, че доставчикът на ТЛР прилага стандарти за сигурност, свързани с биометричните данни, като например ISO/IEC 24745, които предоставят насоки за защита на биометричната информация съгласно

[81] Допълнителни насоки относно ОВЗД могат да бъдат намерени на: Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679, РД 248 ред.01, достъпни на адрес: https://ec.europa.eu/newsroom/article29/items/611236 и инструментариума на ЕНОЗД „Отчетност на място“, част II, достъпен на адрес: https://edps.europa.eu/node/4582_en

[82] ТЛР, в зависимост от случая на употреба, може да попадне в обхвата на следните критерии, които задействат обработване с висок риск (от Насоки относно ОВЗД, РД 248 ред.01): Систематично наблюдение, обработване на данни в голям мащаб, съпоставяне или комбиниране на набори от данни, иновативно използване или прилагане на нови технологични или организационни решения.

[83] Описанието на обработването, както и оценката на необходимостта и пропорционалността, както вече е описано в горепосочените стъпки, също са част от ОВЗД, с изключение на оценката на риска. Ако е необходимо, в ОВЗД ще бъде представено по-подробно описание на потоците от лични данни.

[84] Анализът на рисковете за субектите на данни следва да включва рискове, свързани с мястото на сравняване на портретните снимки (на място/дистанционно), рискове, свързани с обработващи лични данни/подизпълнители, както и рискове, специфични за машинното самообучение, когато това е приложимо (напр. заразяване на данни, враждебни примери).

различни изисквания за поверителност, цялост и възможност за подновяване/отмяна по време на съхранение и предаване, както и изисквания и насоки за сигурното управление, и обработването на биометричната информация, които са в съответствие с изискванията за сигурност и неприкосновеност на личния живот.

- Повторно обучи алгоритъма (ако е необходимо). Собственикът на процеса следва да гарантира, че усъвършенстването на системата за ТЛР за постигане на по-голяма точност преди нейното използване също е част от възложените услуги. В случай че е необходимо допълнително обучение за придобитата система за ТЛР, за да се отговори на показателите за точност, освен да вземе решение за повторно обучение, собственикът на процеса трябва да вземе решение, с помощта на отдела ИТ с ИИ и/или анализ на данните относно подходящия представителен набор от данни, който да се използва, и да провери законосъобразността на данните за това използване.
- Създаде подходящи предпазни мерки за третиране на рисковете, свързани със сигурността, пристрастията и ниската ефективност. Това включва създаване на процес за наблюдение на ТЛР след използването му (водене на записи и обратна информация за точността и справедливостта на резултатите). Освен това трябва да се гарантира, че рисковете, които са специфични за някои системи за машинно обучение и ТЛР (напр. заразяване на данни, враждебни примери, обръщане на модела, заключения от бялата кутия), се установяват , измерват и намаляват. Собственикът на процеса трябва също така да определи подходящи предпазни мерки, за да гарантира, че изискванията за запазване на информация относно биометричните данни, включени в набора от данни за преквалификация, ще бъдат спазени.
- Документира системата за ТЛР. Това следва да включва общо описание на системата за ТЛР, подробно описание на елементите на системата за лицево разпознаване и на процеса на нейното създаване, подробна информация за наблюдението, функционирането и контрола върху системата и подробно описание на рисковете, и мерките за тяхното намаляване. Елементите, включени в тази документация, ще включват основните елементи на описанието на системата ТЛР от предходни фази (вж. по-горе), но те ще бъдат подкрепени с информация, свързана с наблюдението на ефективността и прилагането на промени в системата, включително евентуални актуализации на версиите и/или повторно обучение.
- Създаде ръководства за потребителя, които обясняват технологията и случаите на употреба. Те трябва да обясняват по ясен начин всички сценарии и предварителни условия, при които ще се използва системата за управление на риска.
- Обучи крайните потребители как да използват технологията. Такива обучения трябва да обясняват възможностите и ограниченията на технологията, така че потребителите да могат да разберат обстоятелствата, при които е необходимо да я прилагат, и случаите, в които тя може да бъде неточна. Такива обучения също така ще спомогнат за намаляване на рисковете, свързани с пропускане на проверката/критикуване на резултатите от алгоритъма.
- Да се консултира с надзорния орган за защита на данните съгласно член 28, параграф 1, буква б) от ДПЗД. Предостави информация съгласно член 13 от ДПЗД с цел информиране на субектите на данни относно обработването и техните права. Тези известия трябва да бъдат отправени до субектите на данни на подходящ език, така че те да са в състояние да разберат обработването и да обяснят основните елементи на технологията, включително степента на точност, наборите от данни за обучение и мерките, предприети за избягване на дискриминация и ниска точност на алгоритъма.

4. ПРЕПОРЪКИ СЛЕД ВНЕДРЯВАНЕТО НА ТЛР

- Да осигури човешка намеса и надзор на резултатите. Никога да не предприема мерки по отношение на дадено лице единствено въз основа на резултата от ТЛР (това би означавало нарушение на член 11 от ОРЗД — автоматизирано вземане на индивидуални решения с правни или други подобни последици за субекта на данните). Да гарантира, че служител на правоприлагащите органи преглежда резултатите от ТЛР. Също така да гарантира, че потребителите от ПО избягват предубеденост в полза на автоматизацията, като разследват противоречива информация и критично оспорват резултатите от технологията. За тази цел е важно да се осигури непрекъснато обучение и повишаване на осведомеността на крайните потребители, но висшето ръководство следва да гарантира, че са налице достатъчно човешки ресурси за извършване на ефективен надзор. Това означава, че на всеки служител се предоставя достатъчно време, за да оспори критично резултатите от технологията. Записва, измерва и оценява до каква степен човешкият надзор променя първоначалното решение за ТЛР.
- Проследява и разглежда отклоненията на модела на ТЛР (влошаване на ефективността), след като моделът е в експлоатация.
- Създава процес за постоянна преоценка на рисковете и на мерките за сигурност редовно и всеки път, когато технологията или случаят на използване претърпят промени.
- Документира всяка промяна в системата през целия ѝ жизнен цикъл (напр. надграждане, повторно обучение).
- Създава процес, както и съответните технически възможности за разглеждане на искания за достъп от субектите на данни. Трябва да е налице технически капацитет за извличане на данни, ако е необходимо те да бъдат предоставени на субектите на данни, преди да възникне каквото и да е искане.
- Гарантира, че са въведени процедури в случай на нарушаване на сигурността на данните. Ако настъпи нарушение на сигурността на личните данни, което включва биометрични данни, рисковете вероятно ще са високи. В този случай всички участващи потребители следва да са запознати със съответните процедури, които трябва да се следват, ДЛЗД и субектите на данни следва незабавно да бъдат информирани.

ПРИЛОЖЕНИЕ III — ПРАКТИЧЕСКИ ПРИМЕРИ

Съществуват много различни практически условия и цели на използването на лицево разпознаване, например в контролирана среда като пресичане на граници, кръстосана проверка с данни от полицейски бази данни или с лични данни, които очевидно са направени публично достояние от субекта на данните, данни от камери на живо (разпознаване на лица на място) и др. В резултат на това рисковете за защитата на личните данни и други основни права и свободи се различават значително в различните случаи на използване. С цел да се улесни оценката на необходимостта и пропорционалността, която следва да предшества решението за евентуално внедряване на лицево разпознаване, настоящите насоки предоставят неизчерпателен списък на възможните приложения на ТЛР в областта на правоприлагането.

Представените и оценени сценарии се основават на **хипотетични** ситуации и имат за цел да илюстрират някои конкретни употреби на ТЛР и да предоставят помощ при разглеждането на всеки отделен случай, както и да зададат обща рамка. Те нямат за цел да бъдат изчерпателни и не засягат текущи или бъдещи процедури, предприети от национален надзорен орган във връзка с проектирането, експериментирането или прилагането на технологии за лицево разпознаване. Представянето на тези сценарии следва да служи само за илюстриране на насоките за създателите на политики, законодателите и правоприлагащите органи, които вече са предоставени в настоящия документ, при разработването и предвиждането на прилагането на технологии за лицево разпознаване, за да се гарантира пълно съответствие с достиженията на правото на ЕС в областта на защитата на личните данни. В този смисъл следва да се има предвид, че дори в сходни ситуации на използване на ТЛР наличието или отсъствието на определени елементи може да доведе до различен резултат от оценката на необходимостта и пропорционалността.

1 СЦЕНАРИЙ 1

1.1. Описание

Автоматизирана система за граничен контрол, която позволява автоматизирано преминаване на границата чрез удостоверяване на автентичността на биометричното изображение, съхранено в електронния документ за пътуване на граждани на ЕС и други пътници, преминаващи през граничния пункт, и установяване, че пътникът е законният притежател на документа.

Тази проверка/удостоверяване на автентичността включва само индивидуално разпознаване на лица и се извършва в контролирана среда (напр. на електронните врати на летищата). Биометричните данни на пътника, преминаващ през граничния пункт, се заснемат, когато той е изрично приканен да погледне към камерата на електронната врата, и се сравняват с тези от представения документ (паспорт, лична карта и др.), който е издаден съгласно специфични технически изисквания.

В същото време, въпреки че обработването в такива случаи по принцип попада извън обхвата на ДПЗД, резултатът от проверката може да се използва и за съпоставяне на (буквено-цифрови) данни на лицето в базите данни на правоприлагащите органи като част от граничния контрол и поради това може да доведе до действия със значителни правни последици за субекта на данните, например арест в съответствие със сигнал в ШИС. При определени обстоятелства биометричните данни могат да се използват и за търсене на съвпадения в базите данни на

правоприлагащите органи (в такъв случай на тази стъпка се извършва идентификация по метода „1 към много“).

Резултатът от обработването на биометрични изображения оказва пряко въздействие върху субекта на данните: само в случай на успешна проверка позволява преминаване на границата. В случай на неуспешна идентификация граничните служители трябва да извършат втора проверка, за да се уверят, че субектът на данните е различен от този, който е посочен в документа за самоличност.

В случай че бъде установен сигнал в ШИС или национален сигнал, граничните служители трябва да извършат втора проверка и необходимите допълнителни проверки, а след това да предприемат всички необходими действия, например да арестуват лицето, да информират съответните органи.

Източник на информация:

- Видове субекти на данни: ☒ всички физически лица, които пресичат границите
- Източник на изображението: ☒ друг (документ за самоличност)
- Връзка с престъплението: ☒ Не е необходима
- Начин на събиране на информацията:☒ в кабина или в контролирана среда
- Контекст — засягане на други основни права: Да, а именно: ☒ Право на свободно движение ☒ Право на убежище

Референтна база данни (с която се сравнява заснетата информация):

- Специфичност: ☒ специфични бази данни, свързани с граничния контрол

Алгоритъм:

- Вид на проверката:☒ проверка 1 към 1 (удостоверяване на автентичността)

Резултат:

- Въздействие☒ Пряко (на субекта на данните е разрешено или отказано влизане)
- Автоматизирано решение:☒ Да

1.2. Приложима правна уредба

От 2004 г. насам, съгласно Регламент (ЕО) № 2252/2004 на Съвета[85], паспортите и другите документи за пътуване, издавани от държавите членки, трябва да съдържат биометрично изображение на лицето, съхранено в електронен чип, вграден в документа.

В Кодекса на шенгенските граници (КШГ)[86] са определени изискванията за граничните проверки на лица по външните граници. За гражданите на ЕС и други лица, които се ползват с право на свободно движение съгласно правото на Съюза, минималните проверки следва да се състоят от проверка на техните документи за пътуване, когато е целесъобразно, чрез използване на технически устройства. КШГ беше изменен впоследствие с Регламент (ЕС) 2017/2225[87], с който бяха въведени, *inter alia*, определения за „електронни врати“, „система за автоматизиран

[85] РЕГЛАМЕНТ (ЕО) № 2252/2004 НА СЪВЕТА от 13 декември 2004 г. относно стандартите за отличителните знаци за сигурност и биометричните данни в паспортите и документите за пътуване, издавани от държавите членки.

[86] РЕГЛАМЕНТ (ЕС) 2016/399 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 9 март 2016 г. относно Кодекс на Съюза за режима на движение на лица през границите (Кодекс на шенгенските граници).

[87] Регламент (ЕС) 2017/2225 на Европейския парламент и на Съвета от 30 ноември 2017 г. за изменение на Регламент (ЕС) 2016/399 във връзка с използването на Системата за влизане/излизане.

граничен контрол“ и „система за самообслужване“, както и възможността за обработване на биометрични данни с цел извършване на гранични проверки.

Следователно може да се приеме, че съществува ясно и предвидимо правно основание, което разрешава тази форма на обработване на лични данни. Освен това правната рамка е приета на равнището на Съюза и е пряко приложима за държавите членки.

1.3. Необходимост и пропорционалност — цел/сериозност на престъплението

Проверката на самоличността на гражданите на ЕС чрез автоматизиран граничен контрол, като се използва техният биометричен образ, е елемент от граничните проверки по външните граници на ЕС. Следователно тя е пряко свързана със сигурността на границите и служи на цел от общ интерес, призната от Съюза. Също така порталите за автоматизиран граничен контрол спомагат за ускоряване на обработването на пътниците и за намаляване на риска от човешки грешки. Освен това обхватът, степента и интензивността на намесата в този сценарий са много по-ограничени в сравнение с други форми на лицево разпознаване. Въпреки това обработването на биометрични данни създава допълнителни рискове за субектите на данни, които трябва да бъдат адекватно разгледани и ограничени от компетентния орган, който внедрява и управлява ТЛР.

1.4. Заключение

Проверката на самоличността на гражданите на ЕС в рамките на автоматизирания граничен контрол е необходима и пропорционална мярка, при условие че са налице подходящи гаранции, по-специално прилагането на принципите на ограничаване в рамките на целта, качество на данните, прозрачност и високо равнище на сигурност.

2 СЦЕНАРИЙ 2

2.1. Описание

ПО определят система за идентифициране на жертвите на отвличане на деца. Упълномощен полицейски служител може да извърши сравнение на биометричните данни на дете, за което се предполага, че е отвлечено, с база данни на жертви на отвличане на деца при строги условия, единствено с цел идентифициране на непълнолетни лица, които може да отговарят на описанието на изчезналото дете, за което е образувано разследване и е подаден сигнал.

Въпросното обработване би представлявало сравнение на лицето или изображението на физическо лице, което може да съответства на описанието на изчезнало дете, с изображенията, съхранявани в базата данни. Такова обработване ще се извършва в конкретни случаи, а не систематично.

Базата данни, спрямо която ще се прилага сравнението, се попълва със снимки на изчезнали деца, за които е докладвано за подозрение за отвличане на деца — заплаха за живота или физическата неприкосновеност на детето — и е образувано наказателно разследване към съдебен орган, и за които е издаден сигнал за отвличане на деца. Данните се събират в рамките на процедурите, установени от компетентния правоприлагащ орган, т.е. полицейски служители, оправомощени да изпълняват мисии на съдебната полиция. Категориите записани лични данни са:

- самоличност, прякор, псевдоним, родство, националност, адреси, електронни адреси, телефонни номера;

- дата и място на раждане;
- информация за произход;
- снимка с технически характеристики, позволяващи използването на устройство за лицево разпознаване, и други снимки.

Резултатите от сравнението трябва също да бъдат прегледани и проверени от упълномощен служител, за да се потвърдят предишните доказателства с резултата от сравнението и да се изключат евентуални фалшиви положителни резултати.

Снимките и личните данни на децата могат да се съхраняват само за срока на сигнала и трябва да бъдат изтрити веднага след приключването или прекратяването на наказателното производство в съответствие с националните процедури, за които са били въведени в базата данни.

Докато периодът на съхранение на биометрични данни в базата данни може да бъде предвиден за относително дълъг период от време и определен съгласно националното законодателство, упражняването на правата на субектите на данни, и по-специално правото на коригиране и изтриване, предвижда допълнителна гаранция за ограничаване на намесата в правото на защита на личните данни на засегнатите субекти на данни.

Източник на информация:

- Видове субекти на данни:☒ Деца
- Източник на изображението ☒ друг: не е предварително определен, заподозряна жертва на отвличане на дете
- Връзка с престъплението ☒ Не е пряка във времето ☒ Не е пряка в географско отношение
- Начин на събиране на информацията:☒ в кабина или в контролирана среда
- Контекст: засягане на други основни права☒ Да, а именно:☒ различни

Референтна база данни (с която се сравнява заснетата информация):

- Специфичност ☒ специфична база данни

Алгоритъм:

- Вид на проверката:☒ идентифициране тип „1 към много“

Резултат:

- Въздействие ☒ Пряко
- Автоматизирано решение: ☒ НЕ, задължителен преглед от упълномощен служител

Правен анализ:

- Приложима правна уредба:☒ Специфичен национален закон за това обработване (лицево разпознаване)

2.2. Приложима правна уредба

Националното право предвижда специална правна уредба за създаване на базата данни, в която са определени целите на обработването, както и критериите за попълване, достъп и използване на базата данни. Законодателните мерки, необходими за неговото прилагане, предвиждат също така определянето на срок на съхранение, както и позоваване на приложимите принципи на неприкосновеност и поверителност. Законодателните мерки предвиждат също така условията за предоставяне на информация на субекта на данните и в този случай на носителя(ите) на

родителска отговорност, както и упражняването на правата на субекта на данните и евентуалното им ограничаване, ако е приложимо. По време на подготовката на предложението за съответната законодателна мярка трябваше да се проведе консултация с националния надзорен орган.

2.3. Необходимост и пропорционалност — цел/сериозност на престъплението/брой на лицата, които не са замесени, но са засегнати от обработването

Условия и гаранции за обработването

Сравняването на разпознаването на лица може да се извършва само от упълномощен служител като крайна мярка, освен ако няма други налични средства с по-малка степен на намеса и когато е строго необходимо, например в случай на съмнение относно автентичността на документа за самоличност на пътуващото малолетно или непълнолетно лице и/или след преглед на предишни доказателства и събрани материали, показващи възможна кореспонденция с описанието на изчезнало дете, за което се провежда наказателно разследване.

Допълнителна предпазна мярка е и задължителният преглед и проверка на сравнението на лицевото разпознаване от упълномощен служител, за да се потвърдят предишните доказателства с резултата от сравнението и да се изключат евентуални фалшиви положителни резултати.

Преследвана цел

Създаването на базата данни обслужва важни цели от общ обществен интерес, по-специално предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказателни санкции и защитата на правата и свободите на други лица. Установяването на базата данни и предвиденото обработване изглежда допринасят за идентифицирането на децата, които са жертви на отвличане, и поради това могат да се считат за мярка, подходяща за подкрепа на легитимната цел за разследване и наказателно преследване на такива престъпления.

Цел и попълване на базата данни

Целите на обработването са ясно определени от закона и базата данни се използва само за целите на идентифициране на изчезнали деца, за които е съобщено, че има съмнение за отвличане, и е започнало наказателно разследване под надзора на съдебен орган, и за които е подаден сигнал за отвличане на дете. Условията, определени от закона за попълването на базата данни, имат за цел строго ограничаване на броя на субектите на данни и личните данни, които ще бъдат включени в базата данни. Носещият родителска отговорност за детето трябва да бъде информиран за предприетото обработване и условията за упражняване на правата на детето във връзка с биометричното обработване, предвидено за целите на установяването на самоличността, или за личните данни на детето, съхранявани в базата данни.

2.4. Заключение

Като се има предвид необходимостта и пропорционалността на предвиденото обработване, както и висшият интерес на детето при извършването на такова обработване на лични данни и при условие че са налице достатъчни гаранции, за да се гарантира по-специално упражняването на правата на субекта на данните — особено като се вземе предвид фактът, че ще се обработват

данни на деца, може да се счита, че такова прилагане на обработване на данни за лицево разпознаване е вероятно съвместимо с правото на ЕС.

Освен това, като се имат предвид видът на обработването и използваната технология, която включва висок риск за правата и свободите на съответния субект на данни, ЕКЗД счита, че подготовката на предложение за законодателна мярка, която трябва да бъде приета от национален парламент, или на регулаторна мярка, основана на такава законодателна мярка, която се отнася до предвиденото обработване, трябва да включва предварителна консултация с надзорния орган, за да се гарантира съгласуваност и съответствие с приложимата правна уредба, вж. член 28, параграф 2 от ДПЗД.

3 СЦЕНАРИЙ 3

3.1. Описание

В хода на полицейските интервенции по време на размирици и последвалите разследвания редица лица са били идентифицирани като заподозрени, напр. от предишни разследвания, при които са използвани записи от камери за видеонаблюдение или свидетели. Снимките на тези заподозрени лица се сравняват със снимки на лица, които са били записани с камери за видеонаблюдение или мобилни устройства на мястото на престъплението или в околните райони.

За да получи по-подробни доказателства за лица, заподозрени в участие в размириците около дадена демонстрация, полицията създава база данни, състояща се от снимков материал, който има слаба местна и времева връзка с размириците. Базата данни включва лични записи, качени в полицията от граждани, материали от CCTV в обществения транспорт, материали за видеонаблюдение, притежавани от полицията, и материали, публикувани от медиите, без специално ограничение или защита. Проявата на сериозно престъпно поведение не е предпоставка за събиране на файловете в базата данни. Следователно лицата, които не са участвали в размириците — значителен процент от местното население, което е преминало в момента на демонстрацията или е участвало в демонстрацията, но не и в размириците — се съхраняват в базата данни. Това възлиза хиляди видеофайлове и файлове с изображения.

С помощта на софтуер за лицево разпознаване на всички лица, които се намират на тези файлове, се определят уникални лицеви идентификатори. След това лицата на отделните заподозрени се сравняват автоматично с тези лицеви идентификатори. Базата данни, състояща се от всички биометрични образци в хилядите видеофайлове и файлове със снимки, се съхранява до приключване на всички възможни разследвания. Положителните съвпадения се разглеждат от отговорните служители, които след това вземат решение за по-нататъшни действия. Това може да включва отнасяне на намереното в базата данни досие към наказателното досие на съответното лице, както и допълнителни мерки, като например разпит или задържане на това лице.

В национален закон е предвидена обща разпоредба, съгласно която обработването на биометрични данни с цел уникално идентифициране на физическо лице е допустимо, ако е строго необходимо и при спазване на подходящи гаранции за правата и свободите на засегнатото лице.

Източник на информация:
• Видове субекти на данни: ☒ всички лица

- Източник на изображението: ☒ публично достъпни пространства ☒ частноправен субект ☒ други лица ☒ други: медии
- Връзка с престъплението: ☒ Не непременно пряка географска или времева връзка
- Начин на събиране на информацията:☒ дистанционно
- Контекст — засягане на други основни права: ☒ Да, а именно: Свободата на събранията
- Налични допълнителни източници на информация за субекта на данните: ☒ други: не са изключени (например използване на банкомати или магазини), тъй като не може да се упражнява контрол върху мотивите на изображенията

Референтна база данни (с която се сравнява заснетата информация):

- Специфичност: ☒ специфични бази данни, свързани с областта на престъпността

Алгоритъм:

- Вид обработване:☒ идентифициране „1 към много“

Резултат:

- Въздействие:☒ Пряко (напр. субектът на данни може да бъде задържан, разпитван)
- Автоматизирано решение: ☒ НЕ
- Срок на съхранение: до прекратяване на всички възможни разследвания

Правен анализ:

- Вид предварителна информация за субекта на данните:☒ на уебсайта на ПО като цяло
- Приложима правна уредба:☒ ДПЗД най-често са копирани в националното право☒ Общо национално право за използването на биометрични данни от ПО

3.2. Приложима правна уредба

Както е пояснено по-горе, правните основания, които просто повтарят общата клауза на член 10 от ДПЗД, не са достатъчно ясни, за да дадат на физическите лица адекватна информация за условията и обстоятелствата, при които правоприлагащите органи са оправомощени да използват записи от видеонаблюдение от обществени места за създаване на биометричен образец на своето лице и да го сравняват с полицейски бази данни, други налични вътрешни системи за видеонаблюдение или частни записи и др. Следователно правната рамка, установена в този сценарий, не отговаря на минималните изисквания, за да служи като правно основание.

3.3. Необходимост и пропорционалност

В този пример обработването поражда различни опасения съгласно принципите на необходимост и пропорционалност по няколко причини:

Лица, които не са заподозрени в извършване на тежко престъпление. Проявата на сериозно престъпно поведение не е предпоставка за използване на файловете в базата данни, съдържаща снимков материал. Освен това пряката времева и географска връзка с престъплението не е задължително условие за използването на файловете в базата данни. В резултат на това значителен процент от местното население се съхранява в биометрична база данни за период от потенциално няколко години, докато всички разследвания бъдат прекратени.

Базата данни за местопрестъплението не е ограничена до изображения, отговарящи на изискванията за пропорционалност, което води до неограничен брой изображения за сравняване. Това противоречи на принципа на свеждане на данните до минимум. По-малкият

брой изображения би позволил да се разгледат и неалгоритмични и по-малко натрапчиви средства, например супер разпознаватели.[88]

Тъй като примерът е изведен от обстоятелствата около протест, вероятно е също изображенията да разкриват политическите възгледи на участниците в демонстрацията, тъй като това е втората специална категория данни, които е вероятно да бъдат засегнати в този сценарий. При този сценарий не е ясно как може да се предотврати събирането на тези данни и с какви предпазни мерки. Освен това, когато субектите на данни научат, че участието им в демонстрация е довело до вписването им в биометрична полицейска база данни, това може да има сериозни възпиращи последици за бъдещото им упражняване на правото им на събрания.

Биометричните образци в базата данни могат да се сравняват и помежду си. Това позволява на полицията не само да търси конкретно лице във всички свои материали, но и да пресъздаде поведенчески модел на дадено лице в продължение на няколко дни. Тя може също така да събира допълнителна информация за лицата, например социални контакти и политическо участие.

Намесата се засилва допълнително от факта, че данните се обработват без знанието на субектите на данни.

Като се има предвид, че фотографиите и видеоматериалите се записват от лица през цялото време и че дори повсеместното отразяване на CCTV може да се анализира биометрично, това може да доведе до сериозни възпиращи ефекти.

Широкото използване на частни снимки и видеоклипове, включително потенциалната злоупотреба с тях, като например подаване на донос, е друга причина за безпокойство. Тъй като злоупотребата с данни под формата на донос е риск, присъщ и на наказателните производства като цяло, рискът е значително по-висок, що се отнася до мащаба на обработваните данни и броя на засегнатите лица, тъй като хората могат да качват и материали, свързани с конкретно лице или група лица, които не харесват. Исканията на полицията за качване на снимки и видеоклипове може да доведат до много ниски прагове за предоставяне на материали, особено като се има предвид, че това може да е възможно да се направи анонимно или поне без да е необходимо човек да се яви и да идентифицира в полицейски участък.

3.4. Заключение

В примера не съществува конкретна разпоредба, която би могла да послужи като правно основание. Дори и да е налице достатъчно правно основание обаче изискванията за необходимост и пропорционалност не биха били изпълнени, което би довело до непропорционална намеса в правата на субекта на данните на зачитане на личния живот и защита на личните данни съгласно Хартата.

[88] Т.е. лица с изключителна способност за лицево разпознаване. Вж. също: Face Recognition by Metropolitan Police Super-Recognisers (Лицево разпознаване от супер разпознаватели към столичната полицейска служба), 26 февруари 2016 г., DOI: 10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/.

4 СЦЕНАРИЙ 4

4.1. Описание

Полицията прилага начин за идентифициране на заподозрените, извършили тежко престъпление, заснети от камери за видеонаблюдение (CCTV), чрез ретроспективна ТЛР. Служителят избира ръчно изображението (изображенията) на заподозрените лица във видеоматериалите, събрани от местопрестъплението или от друго място в рамките на предварително разследване, след което изпраща изображението (изображенията) на отдела по криминалистика. Отделът по криминалистика използва ТЛР, за да съпостави тези изображения със снимки на лица, които вече са събрани в база данни от полицията (т.нар. база данни с описания, която се състои от заподозрени лица и бивши осъдени лица). За тази процедура описателната база данни — временно и в изолирана среда — се анализира с ТЛР, за да може да се извърши процесът на съгласуване. За да се сведе до минимум намесата в правата и интересите на засегнатите лица, много ограничен брой служители в отдела по криминалистика имат разрешение да провеждат реалната процедура за намиране на съответствия, достъпът до данните е ограничен до служителите, на които е поверено конкретното досие, и се извършва ръчен контрол на резултатите преди предаването на резултатите на разследващия служител. Биометричните данни не се предават извън контролирана, изолирана среда. Единствено резултатът и снимката (а не биометричният образец) се използват по-нататък в разследването. Служителите преминават специално обучение относно правилата и процедурите за това обработване, а цялото обработване на лични и биометрични данни е достатъчно подробно описано в националното законодателство.

Източник на информация:

- Видове субекти на данни: ☒ заподозрени лица, идентифицирани от записите от видеонаблюдение
- Източник на изображението: ☒ обществено достъпни места ☒ интернет
- Връзка с престъплението: ☒ Пряка временна
  ☒ Пряка географска
- Начин на събиране на информацията:☒ дистанционно
- Контекст — засягане на други основни права: Да, а именно: ☒ Свобода на събранията ☒ Свобода на словото ☒ различни: __

Референтна база данни (с която се сравнява заснетата информация):

- Специфичност:☒ специфични бази данни, свързани с областта на престъпността

Алгоритъм:

- Вид обработване:☒ идентифициране „1 към много“

Резултат:

- Въздействие: ☒ Пряко (напр. субектът на данни е задържан, разпитан)
- Автоматизирано решение: ☒ НЕ

Правен анализ:

- Приложима правна уредба: ☒ Специално национално законодателство за това обработване (лицево разпознаване) за този компетентен орган

4.2. Приложима правна уредба

При този сценарий в националното законодателство е посочено, че биометричните данни могат да се използват при извършването на криминалистичен анализ, когато това е строго необходимо за постигане на целта за идентифициране на заподозрени лица, извършили тежко престъпление, чрез съпоставяне на снимките в описателната база данни. В националното законодателство се посочва кои данни могат да бъдат обработвани, както и процедурите за запазване на целостта и поверителността на личните данни и процедурите за тяхното унищожаване, като по този начин се предоставят достатъчно гаранции срещу риска от злоупотреба и произвол.

4.3. Необходимост и пропорционалност

Използването на лицево разпознаване очевидно е по-ефективно във времето, отколкото ръчното съпоставяне на криминалистично ниво. Ръчното избиране на изображения предварително ограничава намесата в сравнение с използването на всички видео материали в база данни и по този начин се прави разграничение и се преследват само лицата, които попадат в обхвата на целта, т.е. борбата с тежките престъпления. Все пак е важно да се прецени дали съпоставянето може да се извърши ръчно в рамките на разумен период от време, в зависимост от конкретния случай. Ограничаването на лицата с достъп до технологията и личните данни намалява въздействието върху правата на неприкосновеност на личния живот и защита на данните, както и биометричните образци, които не се съхраняват или използват на по-късен етап от разследването. Ръчното управление на резултата също така означава намаляване на риска от погрешни положителни резултати.

4.4. Заключение

Важно е националното законодателство да предоставя адекватно правно основание за обработването на биометрични данни, както и за националната база данни, с която се извършва съпоставянето. При този сценарий бяха въведени няколко мерки за ограничаване на намесата в правата на защита на данните, като например условията за използване на ТЛР, посочени в правното основание, броя на лицата с достъп до технологията и биометричните данни, ръчните проверки и др. ТЛР значително подобрява ефективността на разследващата дейност на отдела за криминалистични анализи на полицията, основава се на закон, който позволява на полицията да обработва биометрични данни, когато това е абсолютно необходимо, и следователно в рамките на тези периметри може да се счита за законна намеса в правата на лицето.

5 СЦЕНАРИЙ 5

5.1. Описание

Дистанционна биометрична идентификация е, когато самоличността на лицата се установява с помощта на биометрични идентификатори (изображение на лицето, походка, ирис и др.) от разстояние, на обществено място и по непрекъснат или текущ начин чрез сравняването им с (биометрични) данни, съхранявани в база данни[89]. Дистанционната биометрична идентификация се извършва в реално време, ако заснемането на снимковия материал, сравняването и идентификацията се извършват без значително забавяне.

Преди всяко внедряване на дистанционна биометрична идентификация в реално време полицията съставя списък за наблюдение на субектите, представляващи интерес, като част от разследването. Той се попълва с портретни снимки на лицата. Въз основа на разузнавателна

[89] https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

информация, която предполага, че лицата ще се намират в определена зона, например в търговски център или на обществен площад, полицията решава кога, къде и за колко време да внедри дистанционната биометрична идентификация.

В деня на акцията на място се позиционира полицейски микробус като контролен център с висш полицейски служител в него. В микробуса има монитори, на които се показват кадри от разположените наблизо камери за видеонаблюдение, инсталирани ad hoc или чрез свързване към видеопотоците на вече инсталирани камери. Когато пешеходците преминават покрай камерите, технологията изолира изображения на лицето, преобразува ги в биометричен образец и ги сравнява с биометричните образци на лицата от списъка за наблюдение.

Ако се открие потенциално съвпадение между списъка за наблюдение и лицата, преминаващи през камерите, се изпраща сигнал до полицаите във микробуса, които след това уведомяват служителите на място, ако сигналът е положителен, например чрез радиоустройство. След това полицаят на място ще реши дали да се намеси, да се доближи до лицето или в крайна сметка да го задържи. Мерките, предприети от полицая на място, се документират. В случай на дискретна проверка събраната информация (като например с кого е лицето, с какво е облечено и накъде отива) се съхранява.

Посоченият национален закон предвижда обща разпоредба, съгласно която обработването на биометрични данни с цел уникално идентифициране на физическо лице е допустимо, ако е строго необходимо и при спазване на подходящи гаранции за правата и свободите на съответното лице.

Източник на информация:

- Видове субекти на данни: ☒ всички лица
- Източник на изображението: ☒ обществено достъпни пространства
- Връзка с престъплението: ☒ Не непременно пряка географска или времева връзка
- Начин на събиране на информацията:☒ дистанционно
- Контекст — засягане на други основни права: Да, а именно: ☒ Свобода на събранията ☒ Свобода на словото ☒ различни
- Налични допълнителни източници на информация за субекта на данните: ☒ други: не са изключени (като например използване на банкомати или влизане в магазини)

Референтна база данни (с която се сравнява заснетата информация):

- Специфичност:☒ специфични бази данни, свързани с областта на престъпността

Алгоритъм:

- Вид обработване:☒ идентифициране „1 към много“

Резултат:

- Въздействие:☒ Пряко (напр. субектът на данни е задържан, разпитан)
- Автоматизирано решение: ☒ НЕ
- Срок на съхранение: до прекратяване на всички възможни разследвания

Правен анализ:

- Вид предварителна информация за субекта на данните:☒ на уебсайта на ПО като цяло
- Приложима правна уредба:☒ ДПЗД най-често се копира в националното право☒ Общо национално право за използването на биометрични данни от ПО

5.2. Приложима правна уредба

Правните основания, които само повтарят общата клауза на член 10 от ДПЗД, не са достатъчно ясни, за да дадат на лицата адекватна представа за условията и обстоятелствата, при които органите на реда са оправомощени да използват записи от видеонаблюдение на обществени места за създаване на биометричен образец на лицата им и сравняването им с полицейските бази данни. Следователно правната рамка, установена в този сценарий, не отговаря на минималните изисквания, за да служи като правно основание.[90]

5.3. Необходимост и пропорционалност

Колкото по-дълбока е намесата, толкова по-висока става летвата за необходимост и пропорционалност. Дистанционната биометрична идентификация на обществени места има няколко последици за основните права:

Сценариите включват наблюдение на всеки минувач в съответното обществено пространство. По този начин се засягат сериозно разумните очаквания на населението за анонимност на обществени места[91]. Това е предпоставка за много аспекти на демократичния процес, като например решението за присъединяване към гражданско сдружение, посещение на събирания и срещи с хора от всякакъв социален и културен произход, участие в политически протест и посещения на места от всякакъв вид. Понятието за анонимност в обществените пространства е от съществено значение за свободното събиране и обмен на информация и идеи. То запазва плурализма на мнения, свободата на мирни събрания и свободата на сдружаване, и защитата на малцинствата, и подкрепя принципите на разделение на властите, и принципите на взаимозависимост и взаимоограничаване. Подкопаването на понятието за анонимност в обществените пространства може да доведе до сериозен възпиращ ефект върху гражданите. Те могат да се въздържат от определени поведения, които попадат в обхвата на свободното и отворено общество. Това би засегнало обществения интерес, тъй като демократичното общество изисква самоопределение и участие на своите граждани в демократичния процес.

Ако такава технология бъде приложена, само ходенето по улицата, до метрото или до пекарната в засегнатия район ще доведе до събиране на лични, включително биометрични данни от правоприлагащите органи, а в първия случай — и до сравняване с полицейските бази данни. Ситуация, при която същото би било направено чрез снемане на пръстови отпечатъци, би била явно непропорционална.

Броят на засегнатите субекти на данни е изключително висок, тъй като всички, които вървят в съответната публична зона, са засегнати. Освен това сценариите биха предполагали автоматизирано масово обработване на биометрични данни, както и масово съпоставяне на биометрични данни с базите данни на полицията.

В европейската съдебна практика масовото наблюдение е забранено (напр. в решението по делото на Европейския съд по правата на човека S. и Marper с/у Обединеното кралство е счетено, че безразборното запазване на биометрични данни е „непропорционална намеса“ в правото на

[90] В случаите, в които за научен проект, който има за цел изследване на използването на ТЛР, ще трябва да се обработват лични данни, но това обработване не би попаднало в обхвата на член 4, параграф 3 от ДПЗД или би попаднало извън обхвата на правото на Съюза, ще се прилага ОРЗД. В случай на пилотни проекти, които ще бъдат последвани от операции по правоприлагане, ДПЗД все пак ще бъде приложима.
[91] Отговор на ЕКЗД до членовете на ЕП относно приложението за лицево разпознаване, разработено от Clearview AI, 10 юни 2020 г., референтен номер: OUT2020-0052.

неприкосновеност на личния живот, тъй като не може да се счита за „необходимо в едно демократично общество“).

Дистанционната биометрична идентификация е толкова податлива на масово наблюдение, че няма надеждни средства за ограничаване. Тя по същество се различава от видеонаблюдението като такова, тъй като евентуалното използване на видеозаписи без биометрична идентификация вече е силно вмешателство, но в същото време ограничено, докато ако се прилага ТЛР, вече широко разпространената система за видеонаблюдение като основен източник на данни ще претърпи промяна в качеството. Освен това, особено по отношение на предполагаемия възпиращ ефект, евентуалните ограничения в прилагането на вече съществуващите инсталации за видеонаблюдение няма да бъдат видими и следователно няма да се ползват с доверието на обществеността.

С дистанционната биометрична идентификация от страна на полицейските органи всеки се третира като потенциален заподозрян. В една правова държава обаче гражданите се считат за честни, докато не се докаже неправомерно поведение. Този принцип е отчасти отразен и в ДПЗД, в който се подчертава необходимостта от разграничаване, доколкото е възможно, на третирането на осъдените или заподозрените в извършване на престъпление лица, в които случаи за правоприлагащите органи трябва да има „*сериозни основания да се счита, че са извършили или ще извършат престъпление*“ (член 6, буква а) от ДПЗД), в сравнение с лицата, които не са осъдени или заподозрени в престъпна дейност.

Прилага се в транспортни възли или на обществени места, като правоприлагащите органи използват технология, способна да идентифицира едно лице по уникален начин и да проследява и анализира неговото местонахождение и движение, което ще разкрие до най-чувствителната информация за дадено лице (дори сексуални предпочитания, религия и здравословни проблеми). С това идва огромният риск от незаконен достъп и използване на данните.

Инсталирането на система, която дава възможност за разкриване на самата същност на поведението и характеристиките на индивида, води до силен възпиращ ефект. Това кара хората да се съмняват дали да се присъединят към дадена проява, като по този начин се накърнява демократичният процес. Също така да се срещат и да бъдат видени заедно с даден приятел, за когото се знае, че има проблеми с полицията или се държи по определен начин, може да бъдат считани за критични, тъй като всичко това би довело до привличане на алгоритъма на системата, а оттам и на правоприлагащите органи.

Не е възможно да се защитят уязвими субекти на данни като децата. Освен това са засегнати лица, които имат професионален интерес — и често съответно правно задължение — да поддържат контактите си поверителни, като например журналисти, адвокати и духовници. Това може да доведе например до разкриване на източника и журналиста или до факта, че дадено лице се консултира с адвокат по наказателни дела. Проблемът не се отнася само до случайни обществени места, на които се срещат например журналистите и техните източници, но естествено и до обществени пространства, необходими за достигане и достъп до институции или специалисти в това отношение.

Също така фактът, че хората изпитват дискомфорт от ТЛР, може да ги накара да променят поведението си, като избягват местата, където е внедрена ТЛР, и по този начин да се оттеглят от социалния живот и културните събития. В зависимост от степента на внедряване на ТЛР

въздействието върху хората може да бъде толкова значително, че да засегне тяхната способност да водят достоен живот[92].

Следователно има голяма вероятност да се засегне същността — недосегаемото ядро — на правото на защита на личните данни. Силните индикации (вж. раздел 3.1.3.2 от насоките) са по-специално следните: в голям мащаб уникалните биологични характеристики на хората се обработват автоматично от правоприлагащите органи с алгоритми, основани на вероятности, които предоставят само ограничена обосновка на резултатите. Ограниченията на правото на неприкосновеност на личния живот и на защита на данните се налагат независимо от индивидуалното поведение на лицето или от обстоятелствата, които го засягат. Статистически погледнато, почти всички субекти на данни, засегнати от тази намеса, са спазващи закона лица. Съществуват само ограничени възможности за предоставяне на информация на субекта на данни. В повечето случаи съдебното обжалване ще бъде възможно едва впоследствие.

Разчитането на система, основаваща се на правдоподобността и с ограничени възможности за обяснение, може да доведе до размиване на отговорността и липса на такава в областта на правните средства за защита и може да бъде стимул за небрежност.

След като такава система, която може да се прилага и за съществуващи камери за видеонаблюдение (CCTV), се прилага с много малко усилия и без да е видима за отделните лица, тя може да бъде използвана неправомерно и да е в състояние систематично и бързо да изготвя списъци на лица според етническия произход, пола, религията и т.н. Принципът на обработване на лични данни въз основа на предварително определени критерии, като например местонахождението на лицето и маршрута, по който лицето е пътувало, вече се прилага[93] и е податлив на дискриминация.

Поради чувствителността, изразителността и количеството на обработваните данни системите за дистанционно разпознаване на лица на обществено достъпни места са склонни да бъдат използвани неправомерно с вредни последици за засегнатите лица. Такива данни могат също така лесно да бъдат събрани и използвани за оказване на натиск върху ключови участници в принципа на контрол и баланс, като например политическата опозиция, полицейските служители и журналистите.

И накрая, системите за ТЛР обикновено включват силно предубедено въздействие по отношение на расата и пола: фалшивите положителни резултати засягат непропорционално хората с цвят на кожата и жените[94], което води до дискриминация. Полицейските мерки, предприети след получаването на фалшиви положителни резултати, като претърсвания и арести, допълнително заклеймяват тези групи.

---

92 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf, стр. 20.

93 Вж. член 6 от Директива (ЕС) 2016/681 на Европейския парламент и на Съвета от 27 април 2016 г. относно използването на резервационни данни на пътниците с цел предотвратяване, разкриване, разследване и наказателно преследване на терористични престъпления и тежки престъпления и член 33 от Регламент (ЕС) 2018/1240 на Европейския парламент и на Съвета от 12 септември 2018 г. за създаване на Европейска система за информация за пътуванията и разрешаването им (ETIAS) и за изменение на регламенти (ЕС) № 1077/2011, (ЕС) № 515/2014, (ЕС) 2016/399, (ЕС) 2016/1624 и (ЕС) 2017/2226.

94 https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

5.4. Заключение

Горепосочените сценарии относно дистанционното обработване на биометрични данни на обществени места с цел установяване на самоличността не успяват да постигнат справедлив баланс между конкуриращите се частни и обществени интереси, като по този начин представляват непропорционална намеса в правата на субекта на данни съгласно членове 7 и 8 от Хартата.

6 СЦЕНАРИЙ 6

6.1. Описание

Частноправен субект предоставя приложение, в което портретни снимки се взимат от интернет, за да се създаде база данни. След това потребителят, например полицията, може да качи снимка и посредством биометрична идентификация приложението ще се опита да я съпостави с портретните снимки или биометричните образци в своята база данни.

Местен полицейски отдел провежда разследване на престъпление, заснето на видеоклип, при което редица потенциални свидетели и заподозрени лица не могат да бъдат идентифицирани чрез съпоставяне на събраната информация с вътрешни бази данни или разузнавателни данни. Въз основа на събраната информация лицата не са регистрирани в нито една съществуваща полицейска база данни. Полицията решава да използва инструмент, както е описано по-горе, който се предоставя от частно дружество, за идентифициране на лицата чрез биометрична идентификация.

Източник на информация:

- Видове субекти на данни: ☒ всички граждани (свидетели) ☒ осъдени лица ☒ заподозрени лица
- Източник на изображението: ☒ Видеоматериал от обществено място или събран на друго място в рамките на предварителното разследване
- Връзка с престъплението: ☒ Не е необходима
- Начин на събиране на информацията:☒ дистанционно
- Контекст — засягане на други основни права: Да, а именно: ☒ Свобода на събранията ☒ Свобода на словото ☒ различни: __

Референтна база данни (с която се сравнява заснетата информация):

- Специфичност: ☒ бази данни с общо предназначение, попълнени от интернет

Алгоритъм:

- Вид обработване:☒ идентифициране „1 към много“

Резултат:

- Въздействие☒ Пряко (напр. субектът на данни е арестуван, разпитван, дискриминационно поведение)
- Автоматизирано решение: ☒ НЕ

Правен анализ:

- Вид предварителна информация за субекта на данните: ☒ Не

6.2. Приложима правна уредба

Когато частноправен субект предоставя услуга, която включва обработване на лични данни, за което определя целта и средствата (в този случай снемане на изображения от интернет за създаване на база данни), този частен субект трябва да има правно основание за това обработване. Освен това правоприлагащият орган, който реши да използва тази услуга за своите цели, трябва да има правно основание за обработването, за което определя целите и средствата. За да може правоприлагащият орган да обработва биометрични данни, трябва да има правна уредба, която да определя целта, личните данни, които ще се обработват, целите на обработването и процедурите за запазване на целостта и поверителността на личните данни, както и процедурите за тяхното унищожаване.

Този сценарий предполага масово събиране на лични данни от лица, които не знаят, че техните данни се събират. Такова обработване може да бъде законосъобразно само при много изключителни обстоятелства. В зависимост от това къде се намира базата данни, използването на такава услуга може да доведе до предаване на лични данни и/или специални категории лични данни извън Европейския съюз (от полицията, напр. чрез „изпращане“ на образа на лицето във видеозаписа от наблюдението или събирани по друг начин), което изисква специални условия за това предаване, вж. член 39 от ДПЗД.

В този сценарий няма специални правила, които да позволяват това обработване от страна на правоприлагащия орган.

6.3. Необходимост и пропорционалност

Използването на услугата от страна на правоприлагащия орган означава, че личните данни се споделят с частен субект, който използва база данни, в която личните данни се събират неограничено и масово. Няма връзка между събраните лични данни и преследваната от правоприлагащия орган цел. Споделянето на данни от правоприлагащия орган с частния субект означава също така липса на контрол от страна на органа по отношение на данните, обработвани от частния субект, и големи трудности за субектите на данни да упражняват правата си, тъй като те няма да знаят, че данните им се обработват по този начин. Това поставя много високи изисквания към ситуациите, при които дори би могло да се извърши такова обработване. Съмнително е дали някоя от целите би отговаряла на изискванията, посочени в директивата, тъй като всички дерогации и ограничения на правата на неприкосновеност на личния живот и защита на данните се прилагат само когато това е абсолютно необходимо. Общият интерес за ефективност в борбата с тежките престъпления сам по себе си не може да оправдае обработването на данни, когато се събират безразборно такива огромни количества данни. Следователно това обработване не би отговаряло на изискванията за необходимост и пропорционалност.

6.4. Заключение

Липсата на ясни, точни и предвидими правила, които да отговарят на изискванията на членове 4 и 10 от Директивата, както и липсата на доказателства, че това обработване е строго необходимо за постигане на предвидените цели, води до заключението, че използването на това приложение няма да отговаря на изискванията за необходимост и пропорционалност и би означавало непропорционална намеса в правата на субектите на данни на зачитане на личния живот и защита на личните данни съгласно Хартата.