Съвместно 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)

18 юни 2021 г.

Кратко изложение

На 21 април 2021 г. Европейската комисия представи своето предложение за Регламент на Европейския парламент и на Съвета за определяне на хармонизирани правила относно изкуствения интелект (наричано по-нататък „Предложението“). ЕКЗД и ЕНОЗД приветстват загрижеността на законодателя по отношение на употребата на изкуствен интелект (ИИ) в рамките на Европейския съюз (ЕС) и изтъкват, че предложението има открояващи се важни **последици за защитата на данните**.

ЕКЗД и ЕНОЗД отбелязват, че **правното основание** за предложението е на първо място член 114 от Договора за функционирането на Европейския съюз (ДФЕС). Освен това предложението се основава и на член 16 от ДФЕС, доколкото в него се съдържат специални правила относно защитата на физическите лица по отношение на обработването на лични данни, по-специално ограничения за използването на системи с ИИ за биометрична идентификация от разстояние в реално време на публично достъпни места за целите на правоприлагането. ЕКЗД и ЕНОЗД припомнят, че в съответствие с практиката на Съда на ЕС (СЕС), член 16 от ДФЕС представлява подходящо правно основание, когато защитата на личните данни е една от целите или основна съставна част от правилата, приемани от законодателя на Съюза. Прилагането на член 16 от ДФЕС предполага също така **необходимостта да се гарантира независим надзор за спазване** на изискванията относно обработването на лични данни, както се изисква и в член 8 от Хартата на основните права на ЕС.

По отношение на **приложното поле на предложението,** ЕКЗД и ЕНОЗД категорично приветстват факта, че то обхваща предоставянето и използването на системи с ИИ от институциите, органите или агенциите на ЕС. **Изключването на международното сътрудничество в областта на правоприлагането от приложното поле** на предложението обаче поражда сериозно безпокойство у ЕКЗД и ЕНОЗД, тъй като подобно изключване създава значителен риск от заобикаляне (например-трети държави или международни организации, управляващи високорискови приложения, на които разчитат публичните органи в ЕС).

ЕКЗД и ЕНОЗД **приветстват подхода, основан на риска**, който стои в основата на предложението. Този подход обаче следва да бъде пояснен и понятието „риск за основните права“ да бъде приведено в съответствие с ОРЗД и Регламент (ЕС) 2018/1725 (Регламента за защита на данните от институциите на ЕС), тъй като са включени аспекти, свързани със защитата на личните данни.

ЕКЗД и ЕНОЗД подкрепят изразената в предложението позиция, че класифицирането на дадена **система с ИИ като високорискова не означава непременно, че тя сама по себе си е законна** и може да бъде приложена от ползвателя като такава. **Може да е необходимо администраторът на данни да изпълни допълнителни изисквания вследствие на правото на ЕС в областта на защитата на данните**. Освен това съответствието със законовите задължения, произтичащи от законодателството на Съюза (включително относно защитата на личните данни), следва да бъде предварително условие за допускане до навлизане на европейския пазар като продукт с маркировка „CE“. За тази цел ЕКЗД и ЕНОЗД считат, че **изискването за гарантиране на съответствие с ОРЗД и Регламента за защита на данните от институциите на ЕС следва да се включи в дял III, глава 2**. Освен това ЕКЗД и ЕНОЗД считат, че е необходимо предвидената в предложението процедура за оценяване на съответствието да се адаптира, така че трети страни винаги да провеждат *предварителни* оценки на съответствието на високорискови системи с ИИ.

Предвид сериозния риск от дискриминация, в предложението се забранява „социалният рейтинг“, когато се извършва „в течение на определен срок“ или „от страна на публични органи или от тяхно име“. Частни дружества като социални медии и доставчици на облачни услуги обаче също може да обработват големи количества лични данни и да генерират социален рейтинг. Следователно **всякакъв вид социален рейтинг следва да бъде забранен в бъдещия регламент за ИИ**.

Дистанционната биометрична идентификация на физически лица на обществено достъпни места създава висок риск от намеса в личния живот на тези лица със сериозни последици за очакванията на населението за анонимност на обществени места. Поради тези причини ЕКЗД и ЕНОЗД **призовават за обща забрана на всякакво използване на ИИ за автоматизирано разпознаване на човешки черти на обществено достъпни места**, например разпознаване на лица, но също така на походка, пръстови отпечатъци, ДНК, глас, удари на клавиши и други биометрични или поведенчески сигнали, в какъвто и да е контекст. По същия начин се препоръчва и **забрана на системи с ИИ, които категоризират физическите лица въз основа на биометрични данни в групи** според техния етнически произход, пол, както и политическа или сексуална ориентация или друго основание за дискриминация съгласно член 21 от Хартата. Освен това ЕКЗД и ЕНОЗД считат, че използването на ИИ за **правене на заключения за емоциите на физически лица е в силна степен нежелателно и следва да бъде забранено.**

ЕКЗД и ЕНОЗД приветстват **определянето на ЕНОЗД като компетентен орган и орган за надзор на пазара за наблюдението на институциите, агенциите и органите на Съюза**. Ролята и задачите на ЕНОЗД обаче следва да бъдат допълнително изяснени, особено що се отнася до ролята му като орган за надзор на пазара. Освен това в бъдещия регламент за ИИ следва ясно да се установи **независимостта на надзорните органи** при осъществяването на техните надзорни и правоприлагащи задачи.

Определянето на органите за защита на данните (ОЗД) за национални надзорни органи би гарантирало по-хармонизиран регулаторен подход и би допринесло за последователно тълкуване на разпоредбите в областта на обработката на данни и за избягване на противоречия при прилагането им сред държавите членки. Следователно ЕКЗД и ЕНОЗД считат, че **органите за защита на данните следва да бъдат определени като национални надзорни органи в съответствие с член 59 от предложението.**

В предложението преобладаваща роля в Европейския комитет по изкуствен интелект (ЕКИИ) се определя на Комисията. Такава роля е в противоречие с необходимостта евентуален европейски орган за ИИ да бъде независим от всякакво политическо влияние. За да гарантира независимостта му, в бъдещия регламент за ИИ следва да се даде **повече независимост на ЕКИИ** и да се гарантира, че той може да действа по своя инициатива.

Предвид разпространението на системи с ИИ в рамките на единния пазар и вероятността от трансгранични случаи, съществува сериозна необходимост от хармонизирано правоприлагане и правилно разпределение на правомощията между националните надзорни органи. ЕКЗД и ЕНОЗД предлагат да се предвиди **механизъм, който гарантира за всяка система с ИИ единно звено за контакт за засегнатите от законодателството физически лица и дружества.**

По отношение на **използването на програми за анализ на определена информация** ЕКЗД и ЕНОЗД **препоръчват да бъдат изяснени техният обхват и цели**. В предложението следва също

така да се заяви ясно, че правното основание за такива програми следва да бъде в съответствие с изискванията, установени в съществуващата уредба в областта на защитата на данните.

Очертаната в предложението **система за сертификация** не е **обвързана ясно с правото на ЕС в областта на защитата на данните**, нито с друго право на ЕС или на държавите членки, приложимо спрямо всяка „област“ на високорискова система с ИИ, и не взема под внимание **принципите на свеждане на данните до минимум и защита на данните на етапа на проектирането** като един от аспектите, които следва да бъдат отчетени, **преди да бъде получена маркировката „CE“**. Следователно, ЕКЗД и ЕНОЗД препоръчват предложението да се измени така, че да се изясни връзката между издаваните по силата на предлагания регламент сертификати и сертифицирането, печатите и маркировките за защита на данните. На последно място, ОЗД следва да участват в изготвянето и установяването на хармонизирани стандарти и общи спецификации.

По отношение на **кодексите за поведение** ЕКЗД и ЕНОЗД считат, че е **необходимо да се изясни** дали защитата на личните данни следва да се разглежда като част от „допълнителните изисквания“, които може да се включат в тези кодекси за поведение, и да се гарантира, че „техническите спецификации и решения“ не са в противоречие с правилата и принципите на съществуващата уредба на ЕС в областта на защитата на данните.

СЪДЪРЖАНИЕ

Европейският комитет по защита на данните и Европейският надзорен орган по защита на данните

като взеха предвид член 42, параграф 2 от Регламент (ЕС) 2018/1725 от 23 октомври 2018 г. относно защитата на физическите лица по отношение на обработката на лични данни от институциите, органите, службите и агенциите на Съюза и свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО[1],

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

като взеха предвид искането за съвместно становище на Европейския надзорен орган по защита на данните и на Европейския комитет по защита на данните от 22 април 2021 г. относно предложението за Регламент за определяне на хармонизирани правила относно изкуствения интелект (Законодателен акт за изкуствения интелект),

ПРИЕХА СЛЕДНОТО СЪВМЕСТНО СТАНОВИЩЕ

1 ВЪВЕДЕНИЕ

1. Появата на системите с изкуствен интелект (ИИ) е много важна стъпка в еволюцията на технологиите и в начина, по който хората взаимодействат с тях. ИИ е набор от ключови технологии, които ще променят в дълбочина нашето ежедневие, било то от обществена или икономическа гледна точка. През следващите няколко години се очакват важни решения за ИИ, тъй като той ни помага да преодоляваме някои от най-големите предизвикателства, пред които сме изправени в множество области днес — от здравеопазването до мобилността или от публичната администрация до образованието.

2. Този обещан напредък обаче не е лишен от рискове. В действителност рисковете са много значими предвид факта, че последиците от системите с ИИ за отделния човек и за обществото са до голяма степен не са изпитани на практика. Генерирането на съдържание, правенето на прогнози или вземането на решение по автоматизиран начин, както го правят системите с ИИ, посредством техники за машинно самообучение или логически и основани на вероятностни изводи правила не е същото като извършване на тези дейности от човек посредством творческо или теоретично разсъждение, носейки пълна отговорност за последиците.

3. ИИ ще увеличи количеството на предвижданията, които могат да бъдат направени в много области, като се започне от измеримите корелации между данните, които са

[1] ОВ L 295, 21.11.2018 г., стр. 39—98.
[2] Позоваванията на „държави членки“ в настоящия документ следва да се разбират като позовавания на „държавите — членки на ЕИП“.

невидими за човешкото око, но се виждат от машините, което ще улесни живота ни и ще реши голям брой проблеми, но същевременно ще подкопае способността ни да даваме причинно-следствено тълкуване на резултатите, така че понятията за прозрачност, човешки контрол, отчетност и наказателна отговорност за резултатите ще бъдат поставени пред сериозно предизвикателство.

4. Данните (лични и нелични) в ИИ в много случаи са ключовата предпоставка за автономни решения, които неизбежно ще засегнат живота на физическите лица на различни равнища. Поради тази причина още на този етап ЕКЗД и ЕНОЗД изтъкват категорично, че предложението за Регламент за определяне на хармонизирани правила относно изкуствения интелект (Законодателен акт за изкуствения интелект) („Предложението“)[3] има **важни последици за защитата на данните**.

5. Прехвърлянето на машини на задачата за вземане на решения въз основа на данни ще създаде рискове за правата и свободите на физическите лица, ще засегне техния личен живот и може да нанесе вреда на групи или дори на цели общества. ЕКЗД и ЕНОЗД изтъкват, че правата на личен живот и на защита на личните данни, които са в противоречие с допускането за автономност на решенията на машините, което стои в основата на концепцията за ИИ, са стълб на ценностите на ЕС, признат във Всеобщата декларация за правата на човека (член 12), Европейската конвенция за правата на човека (член 8) и Хартата на основните права на ЕС (наричана по-нататък „Хартата“) (членове 7 и 8). Постигането на баланс между перспективата за растеж, предлагана от приложенията с ИИ, и централното, и първостепенно място на хората спрямо машините е много амбициозна, но при все това необходима цел.

6. ЕКЗД и ЕНОЗД приветстват участието в регламента на всички заинтересовани страни, имащи отношение към ИИ и въвеждането на конкретни изисквания за доставчиците на решения, тъй като те имат значително влияние върху продуктите, в които се използват техните системи. Въпреки това отговорностите на различните страни — ползвател, доставчик, вносител или дистрибутор на система с ИИ — трябва да бъдат ясно очертани и разпределени. По-специално, при обработването на лични данни следва да се обърне особено внимание на съгласуваността на тези роли и отговорности с понятията „администратор на лични данни“ и „обработващ лични данни“, предвидени в уредбата в областта на защитата на данни, тъй като двете норми не са сходни.

7. В предложението важно място се определя на понятието „човешки надзор“ (член 14), което ЕКЗД и ЕНОЗД приветстват. Както е посочено по-горе обаче, поради силното потенциално въздействие на определени системи с ИИ върху физически лица или групи физически лица, съсредоточаването върху важността на човека следва да мобилизира висококвалифициран човешки надзор и законосъобразно обработване, доколкото такива системи се основават на обработването на лични данни или обработват лични данни за изпълнението на задачите си, така че да се гарантира зачитането на правото човек да не е предмет на решение, което се основава единствено на автоматизирано обработване.

[3] COM(2021) 206 final.

8. Освен това поради интензивното използване на данни от множество приложения с ИИ, в предложението следва да се насърчава възприемането на подход на защита на данните на етапа на проектиране и по подразбиране на всяко равнище, като се насърчава ефективното прилагане на принципите за защита на данните (както са предвидени в член 25 от ОРЗД и член 27 от Регламента за защита на данните от институциите на ЕС) посредством най-съвременни технологии.

9. На последно място, ЕКЗД и ЕНОЗД изтъкват, че настоящото съвместно становище се предоставя единствено като предварителен анализ на предложението, без да се засягат евентуални по-нататъшни оценки и становища относно последиците на предложението и неговата съвместимост с правото на ЕС в областта на защитата на данните.

2 АНАЛИЗ НА КЛЮЧОВИТЕ ПРИНЦИПИ НА ПРЕДЛОЖЕНИЕТО

2.1 Приложно поле на предложението и връзка със съществуващата правна уредба

10. Съгласно обяснителния меморандум **правното основание** за предложението е на първо място член 114 от ДФЕС, който предвижда приемането на мерки за гарантиране на създаването и функционирането на вътрешния пазар[4]. Освен това предложението се основава на член 16 от ДФЕС, *доколкото той съдържа специални правила относно защитата на физическите лица по отношение на обработването на лични данни*, по-специално ограничения за използването на системи с ИИ за биометрична идентификация от разстояние в реално време на публично достъпни места за целите на правоприлагането[5].

11. ЕКЗД и ЕНОЗД припомнят, че в съответствие с практиката на СЕС член 16 от ДФЕС представлява подходящо правно основание, когато защитата на личните данни е една от целите или основна съставна част от правилата, приемани от законодателя на Съюза[6]. Прилагането на член 16 от ДФЕС предполага също така необходимостта да се гарантира независим надзор за спазване на изискванията относно обработването на лични данни, както се изисква и в член 8 от Хартата.

12. ЕКЗД и ЕНОЗД припомнят, че вече съществува всеобхватна уредба за защита на данните, приета на основание на член 16 от ДФЕС, която се състои от Общия регламент относно защитата на данните (ОРЗД)[7], Регламента за защита на данните от

[4] Обяснителен меморандум, стр. 5.
[5] Обяснителен меморандум, стр. 6. Вж. също съображение 2 от предложението.
[6] Становище от 26 юли 2017 г., *PNR Canada*, Процедура по Становище 1/15, ECLI:EU:C:2017:592, точка 96.
[7] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), ОВ L 119, 4.5.2016 г., стр. 1—88.

институциите, службите, органите и агенциите на Европейския съюз[8] и Директивата относно правоприлагането в областта на защитата на данните (ДП)[9]. Според предложението може да се счита, че на член 16 от ДФЕС се основават единствено съдържащите се в предложението допълнителни ограничения относно обработването на биометрични данни и следователно, че имат същото правно основание като ОРЗД, Регламента за защита на данните от институциите на ЕС или ДП. Това има важни последици за взаимоотношението на предложението с ОРЗД, Регламента за защита на данните от институциите на ЕС и ДП в по-общ план, както е описано по-долу.

13. По отношение на **приложното поле на предложението**, ЕКЗД и ЕНОЗД категорично приветстват факта, че предложението обхваща използването на системи с ИИ от институциите, органите или агенциите на ЕС. Предвид факта, че използването на системи с ИИ от тези образувания също може да има значително въздействие върху основните права на физическите лица, подобно на използването в рамките на държавите — членки на ЕС, е необходимо новата нормативна уредба за ИИ да се прилага както за държавите — членки на ЕС, така и за институциите, службите, органите и агенциите на ЕС, за да се гарантира съгласуван подход на цялата територия на Съюза. Тъй като институциите, службите, органите и агенциите на ЕС могат да действат и като доставчици, и като ползватели на системи с ИИ, ЕКЗД и ЕНОЗД считат, че е напълно подходящо тези образувания да бъдат включени в приложното поле на предложението на основание на член 114 от ДФЕС.

14. ЕКЗД и ЕНОЗД обаче изразяват сериозна загриженост във връзка с посоченото в член 2, параграф 4 изключване на международното сътрудничество в областта на правоприлагането от приложното поле на предложението. Изключването създава значителен риск от заобикаляне (например- трети държави или международни организации, управляващи високорискови приложения, на които разчитат публичните органи в ЕС).

15. Разработването и използването на системи с ИИ в много случаи ще включва обработване на лични данни. От първостепенно значение е да се гарантира яснота на връзката на настоящото предложение със съществуващото законодателство на ЕС в областта на защитата на данните. Предложението не засяга и допълва ОРЗД, Регламента за защита на данните от институциите на ЕС и ДП. Въпреки че в съображенията от предложението се изяснява, че използването на системи с ИИ следва да е в съответствие с правото в областта на защитата на данните, **ЕКЗД и ЕНОЗД препоръчват силно да се изясни в член 1 от предложението, че законодателството на Съюза за защита на личните**

[8] Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 година относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО, ОВ L 295, 21.11.2018 г., стр. 39—98.

[9] Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година 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, ОВ L 119, 4.5.2016 г., стр. 89—131.

данни, по-специално ОРЗД, Регламентът за защита на данните от институциите на ЕС, Директивата за правото на неприкосновеност на личния живот и електронни комуникации[10] и ДП, се прилагат спрямо всяко обработване на лични данни, което попада в приложното поле на предложението. В съответно съображение следва също така да се поясни, че предложението няма да засегне прилагането на действащото законодателство на ЕС, с което се урежда обработването на лични данни, включително задачите и правомощията на независимите надзорни органи, които са компетентни да следят спазването на тези инструменти.

2.2 Основан на риска подход

16. ЕКЗД и ЕНОЗД **приветстват подхода, основан на риска**, който стои в основата на предложението. Предложението би било приложимо спрямо всякакви системи с ИИ, включително тези, в които не се включва обработване на лични данни, но въпреки това могат да имат въздействие върху интереси или основни права и свободи.

17. ЕКЗД и ЕНОЗД отбелязват, че някои от разпоредбите в предложението не включват рисковете за групи физически лица или за обществото като цяло (например- общи последици с особено значение като групова дискриминация или изразяване на политически мнения на обществени места). ЕКЗД и ЕНОЗД препоръчват рисковете за обществото/групи лица, пораждани от системите с ИИ, също да бъдат оценени и смекчени.

18. ЕКЗД и ЕНОЗД считат, че основаният на риска подход на предложението следва да бъде пояснен и понятието „риск за основните права“ **да бъде приведено в съответствие с ОРЗД**, доколкото са включени аспекти, свързани със защитата на личните данни. Независимо дали става дума за крайни ползватели, просто за субекти на данни или за други лица, засегнати от системата с ИИ, пълното отсъствие на позоваване в текста на физическото лице, засегнато от системата с ИИ, изглежда като „сляпо петно“ в предложението. В действителност задълженията, наложени на участниците по отношение на засегнатите лица, следва да произтичат по-конкретно от защитата на физическото лице и на неговите права. Във връзка с това ЕКЗД и ЕНОЗД призовават настоятелно законодателите да разгледат изрично в предложението **правата и средствата за правна защита, които са на разположение на физическите лица,** станали предмет на системи с ИИ.

19. ЕКЗД и ЕНОЗД отбелязват избора да се предостави изчерпателен списък на **високорисковите системи с ИИ**. Този избор може да създаде „чернобял“ ефект, при който високорисковите ситуации да имат слаби привлекателни способности , като по този начин се подкопава цялостния подход, основан на риска, който стои в основата на предложението. Освен това в този списък с високорискови системи с ИИ, посочен в приложения II и III към предложението, липсват някои видове случаи на използване,

[10] Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации), изменена с Директива 2006/24/ЕО и Директива 2009/136/ЕО.

които включват значителни рискове, например използване на ИИ за определяне на застрахователна премия, за оценка на медицинско лечение или за целите на научни изследвания в здравеопазването. ЕКЗД и ЕНОЗД изтъкват също така, че тези приложения ще трябва да се актуализират редовно, за да се гарантира, че обхватът им е подходящ.

20. В предложението се изисква от **доставчиците** на системата с ИИ да извършат оценка на риска, но в повечето случаи администраторите на данни ще бъдат **ползвателите**, а не доставчиците на системите с ИИ (например ползвател на система за лицево разпознаване е „администратор на данни“ и следователно не е обвързан от изискванията към доставчиците на високорискови системи с ИИ съгласно предложението).

21. Освен това **за един доставчик невинаги ще е възможно да оцени всички употреби** на системата с ИИ. Така първоначалната оценка на риска ще бъде с по-общ характер в сравнение с тази, извършена от ползвателя на системата с ИИ. Дори ако първоначалната оценка на риска от доставчика не показва, че системата с ИИ е „високорискова“ съгласно предложението, това не следва да изключва **последваща (по-подробна) оценка** (оценка на въздействието върху защитата на данните съгласно член 35 от ОРЗД, член 39 от Регламента за защита на данните от институциите на ЕС или член 27 от ДП), **която следва да се извърши от ползвателя на системата**, като се вземат под внимание контекстът и конкретните случаи на използване. Тълкуването дали, съгласно ОРЗД, Регламента за защита на данните от институциите на ЕС и ДП, даден вид обработване е вероятно да доведе до висок риск следва да се извършва независимо от предложението. Категоризирането на система с ИИ като „високорискова“ поради нейното въздействие върху основните права обаче[11] **задейства презумпция за „висок риск“ съгласно ОРЗД, Регламента за защита на данните от институциите на ЕС и ДП, когато се обработват лични данни.**

22. **ЕКЗД и ЕНОЗД подкрепят посочената в предложението позиция, че класифицирането на дадена система с ИИ като високорискова не означава непременно, че тя *сама по себе си* е законна и може да бъде приложена от ползвателя като такава. Може да е необходимо администраторът на данни да изпълни допълнителни изисквания в резултат на правото на ЕС в областта на защитата на данните.** Освен това разсъждението, което стои в основата на член 5 от предложението, че за разлика от забранените системи, високорисковите системи може да бъдат допустими по принцип, следва да се разгледа и премахне от предложението, тъй като предложената маркировка „CE“ не предполага, че свързаното обработване на лични данни е законосъобразно.

[11] Агенцията на Европейския съюз за основните права (FRA) вече е разгледала необходимостта от провеждане на оценки на въздействието върху основните права, когато се използват ИИ или свързани технологии. В доклада си от 2020 г., озаглавен „Getting the future right — Artificial intelligence and fundamental rights“ (Правилен подход в бъдещето — изкуственият интелект и основните права), FRA определя „капани при използването на ИИ, например в превантивната полицейска дейност, медицинското диагностициране, социалните услуги и насоченото рекламиране“, и подчертава, че „частни и публични организации следва да извършват оценки за това как ИИ би могъл да навреди на основните права“, така че да се намалят отрицателните въздействия върху физическите лица.

23. Съответствието със законовите задължения, произтичащи от законодателството на Съюза (включително относно защитата на личните данни), обаче следва да бъде предварително условие за допускане до навлизане на европейския пазар като продукт с маркировка „CE“. За тази цел ЕКЗД и ЕНОЗД **препоръчват в дял III, глава 2 от предложението да се включи изискването за гарантиране на съответствие с ОРЗД и Регламента за защита на данните от институциите на ЕС**. Изпълнението на тези изисквания трябва да се одитира (чрез одит от трета страна), преди да се постави маркировка „CE“, в съответствие с принципа на отчетност. Първоначалната оценка на въздействието, която следва да се извърши от доставчика ще бъде от особена значимост по отношение на оценката, извършвана от трета страна.

24. Предвид сложността, която произтича от разработването на системи с ИИ, следва да се отбележи, че техническите характеристики на системите (например вида на подхода към ИИ) биха могли да доведат до по-големи рискове. Следователно във всяка оценка на риска на система с ИИ следва да се разгледат **техническите характеристики** заедно **със специфичните случаи на използването на системата и контекста**, в който работи тя.

25. С оглед на горепосоченото, ЕКЗД и ЕНОЗД препоръчват в предложението да се уточни, че **доставчикът** извършва първоначалната оценка на риска на въпросната система с ИИ, **като взема под внимание случаите на използване** (които следва да бъдат конкретизирани в предложението, например да се допълни приложение III, точка 1, буква а), където не са споменати случаите на използване на биометричните системи с ИИ), и че **ползвателят** на системата с ИИ, в качеството си на администратор на данни съгласно правото на ЕС в областта на защитата на данните (ако е относимо), извършва оценката на въздействието върху защитата на данните, както е разписана подробно в член 35 от ОРЗД, член 39 от Регламента за защита на данните от институциите на ЕС и член 27 от ДП, като взема под внимание не само техническите характеристики и **случаите на използване**, но **и конкретния контекст**, в който ще работи ИИ.

26. Освен това следва да се пояснят някои термини, споменати в приложение III към предложението, например терминът „основни частни услуги“ или малък доставчик, използващ за своя собствена употреба ИИ за оценка на кредитоспособността.

2.3 Забранени употреби на ИИ

27. ЕКЗД и ЕНОЗД считат, че **накърняващите форми на ИИ** — особено тези, които може да засегнат достойнството на човека — следва да се разглеждат като забранени системи с ИИ съгласно член 5 от предложението, вместо да бъдат категоризирани само като „високорискови“ в приложение III към предложението, например тези под номер 6. Това важи по-специално за сравняването на данни, което в голям мащаб засяга и лица, които са дали слабо основание или не са дали никакво основание да бъдат поставени под полицейско наблюдение, или за обработване, което накърнява принципа на ограничение на целите съгласно правото за защитата на данните. Използването на ИИ при полицейската дейност и правоприлагането изисква конкретни за дадената област, прецизни, предвидими и пропорционални правила, които трябва да отчитат интересите

на засегнатите лица и последиците за функционирането на едно демократично общество.

28. В член 5 от предложението формално се отдава дължимото на „ценностите“ и на забраната на системи с ИИ, които противоречат на тези ценности. В действителност обаче посочените в член 5 критерии за „квалифициране“ на системи с ИИ като забранени **ограничават обхвата на забраната** до такава степен, че тя би могла да се окаже безсмислена на практика (например „причинява или може да причини [...] физически или психологически вреди“ в член 5, параграф 1, букви а) и б); ограничаването до публични органи в член 5, параграф 1, буква в); неясна формулировка в буква в), подточки i) и ii); ограничаване само до дистанционна биометрична идентификация „в реално време“, без да се дава каквото и да е определение, и т.н.).

29. По-специално използването на ИИ за генериране на „социален рейтинг“, както се предвижда в член 5, параграф 1, буква в) от предложението, може да доведе до дискриминация и противоречи на основните ценности на ЕС. В предложението тези практики се забраняват само когато са извършени „в течение на определен срок“ или „от страна на публични органи или от тяхно име“. Частни дружества, по-специално социални медии и доставчици на облачни услуги, може да обработват големи количества лични данни и да генерират социален рейтинг. Следователно **в предложението следва да бъде забранен всякакъв вид социален рейтинг**. Следва да се отбележи, че във връзка с правоприлагането член 4 от ДП вече ограничава в значителна степен и дори на практика забранява такъв вид дейности.

30. **Дистанционната биометрична идентификация** на физически лица на обществено достъпни места създава висок риск от намеса в личния живот на физическите лица. Следователно, ЕКЗД и ЕНОЗД **считат, че е необходим по-строг подход**. Използването на системи с ИИ може да породи сериозни проблеми с пропорционалността, тъй като може да включва обработване на данните на произволен и непропорционален брой субекти на данни, за да бъдат открити малък брой физически лица (например пътници на летища и железопътни гари). **Безпрепятственото** естество на системите за дистанционна биометрична идентификация поражда също така проблеми с прозрачността и въпроси, свързани с правното основание за обработването съгласно правото на ЕС (ДП, ОРЗД, Регламента за защита на данните от институциите на ЕС и друго приложимо право). Все още остава неразрешен проблемът относно начина за надлежно уведомяване на физическите лица за това обработване, както и относно действителното и своевременно упражняване на техните права. Същото важи за **необратимия и сериозен ефект на тези системи върху** (основателното) **очакване на населението за анонимност на обществени места**, който води до пряка отрицателна последица за упражняването на свободата на изразяване на мнение, на събрания, на сдружаване, както и свободата на движение.

31. В член 5, параграф 1, буква г) от предложението се предоставя подробен **списък на изключенията**, при които дистанционна биометрична идентификация в реално време в обществено достъпни места се разрешава за целите на правоприлагането. ЕКЗД и ЕНОЗД считат, че **този подход е погрешен** в няколко отношения: На първо място, не е

ясно какво следва да се разбира под „значително забавяне“ и как то следва да се разглежда като смекчаващ фактор, като се вземе предвид фактът, че една система за масова идентификация е способна да определи самоличността на хиляди физически лица само за няколко часа. Освен това степента на намесата на обработването невинаги зависи от това дали идентификацията се извършва в реално време, или не. Последващата дистанционна биометрична идентификация при политически протест вероятно ще има значителен възпиращ ефект върху упражняването на основните права и свободи, например свободата на събранията и на сдружаването, а в по-общ план на основополагащите принципи на демокрацията. На второ място, степента на намесата на обработването не зависи непременно от неговата цел. Използването на тази система за други цели, например лична охрана, представлява същите заплахи за основните права на зачитане на личния и семейния живот, и защита на личните данни. На последно място, дори с предвидените ограничения, потенциалният брой на заподозрените лица или извършителите на престъпления ще бъде почти винаги „достатъчно висок“, за да оправдае непрекъснатото използване на системите с ИИ за откриване на заподозрени лица, въпреки допълнителните условия в член 5, параграфи 2—4 от предложението. В доводите за предложението изглежда е пропуснат фактът, че когато се наблюдават открити зони, задълженията съгласно правото на ЕС в областта на защитата на данните трябва да се изпълняват не само по отношение на заподозрените лица, но и по отношение на всички онези лица, които са наблюдавани на практика.

32. Поради всички тези причини ЕКЗД и ЕНОЗД **призовават за обща забрана на всякакво използване на ИИ за автоматизирано разпознаване на човешки черти на обществено достъпни места, например разпознаване на лица, но също така на походка, пръстови отпечатъци, ДНК, глас, удари на клавиши и други биометрични или поведенчески сигнали, в какъвто и да е контекст**. Настоящият подход на предложението е да бъдат определени и изброени всички системи с ИИ, които следва да бъдат забранени. Така от съображения за последователност **системите с ИИ за широкомащабна идентификация от разстояние в онлайн пространства** следва да бъдат забранени съгласно член 5 от предложението. Като се вземат предвид ДП, Регламентът за защита на данните от институциите на ЕС и ОРЗД, ЕНОЗД и ЕКЗД не могат да определят по какъв начин този вид практика би могла да изпълни изискванията за необходимост и пропорционалност и да се смята за такава, която в крайна сметка произтича от считаните от СЕС и ЕСПЧ за приемливи намеси в основните права.

33. Освен това ЕКЗД и ЕНОЗД **препоръчват въвеждането на забрана**, която да важи както за публичните органи, така и за частните образувания, върху **системи с ИИ, които категоризират физическите лица въз основа на биометрични данни (например от лицево разпознаване) в групи според етническия им произход, пола, както и политическата или сексуалната им ориентация, или друго основание за дискриминация, забранено по член 21 от Хартата, или** системи с ИИ, чиято научна валидност не е доказана или които са в пряко противоречие с основни ценности на ЕС (например полиграф, приложение III, точка 6, буква б) и точка 7, буква а)). Съответно „**биометричната категоризация**“ следва да бъде **забранена съгласно член 5**.

34. Освен това **достойнството на човека се засяга, когато той е определен или класифициран от компютър по отношение на бъдещо поведение, независимо от свободната му воля**. Системи с ИИ, предназначени да се използват от правоприлагащите органи за извършване на индивидуални оценки на риска за физически лица с цел преценка на риска дадено лице да извърши нарушение или повторно нарушение (вж. приложение III, точка 6, буква а)) или за предвиждане на извършването или на повторното извършване на действително или потенциално престъпление въз основа на профилиране на физически лица или за оценка на личностните черти и характеристики или на предишно престъпно поведение (вж. приложение III, точка 6, буква д)), когато са използвани по предназначение, ще доведат до кардинално подчиняване на вземането на решения от страна на полицейските и съдебните органи, при което засегнатото човешко същество е обективирано. Такива системи с ИИ, които засягат същността на правото на човешко достойнство, следва да бъдат забранени съгласно член 5.

35. Освен това ЕКЗД и ЕНОЗД считат, че използването на ИИ, за да се **правят заключения за емоциите на физически лица, е в силна степен нежелателно и следва да бъде забранено,** с изключение на определени ясно посочени случаи на използване, по-специално за здравни или научноизследователски цели (например при пациенти, при които разпознаването на емоциите е важно), като винаги се предоставят подходящи защитни мерки и, разбира се, при спазване на всички други условия и ограничения във връзка със защитата на данните, включително ограничение на целите.

2.4 Високорискови системи с ИИ

2.4.1 Необходимост от *предварителна* оценка на съответствието от външни трети страни

36. ЕКЗД и ЕНОЗД приветстват факта, че системите с ИИ, които представляват висок риск, трябва да бъдат подложени на предварителна оценка на съответствието, преди да могат да бъдат пуснати на пазара или използвани по друг начин в ЕС. По принцип този регулаторен модел се приветства, тъй като предлага добър баланс между благоприятстване на иновациите и висока степен на активна защита на основните права. За да може да се използва в специфични среди, например при процесите на вземане на решения на публичните институции или критичната инфраструктура, трябва да бъдат предвидени начини за проучване на целия първичен код.

37. Въпреки това ЕКЗД и ЕНОЗД се застъпват за адаптиране на процедурата за оценяване на съответствието съгласно член 43 от предложението, така че ***предварителна*** **оценка на съответствието от трета страна да трябва да се извършва по принцип за високорисковите системи с ИИ**. Въпреки че оценяването на съответствието от трета страна за високорисково обработване на лични данни не е изискване по ОРЗД или по Регламента за защита на данните от институциите на ЕС, пораженията от системите с ИИ рискове все още предстои да бъдат проучени напълно. Следователно, общото въвеждане на задължение за оценяване на съответствието от трета страна би засилило допълнително правната сигурност и доверието във всички високорискови системи с ИИ.

2.4.2 Приложното поле на регламента трябва да обхваща и вече използваните системи с ИИ

38. Съгласно член 43, параграф 4 от предложението, високорисковите системи с ИИ следва да се подлагат на нова процедура за оценяване на съответствието всеки път, когато бъде направена съществена промяна. Правилно е да се гарантира, че системите с ИИ съответстват на изискванията на регламента за ИИ през целия си жизнен цикъл. Системите с ИИ, които са пуснати на пазара или въведени в експлоатация преди прилагането на предложения регламент (или 12 месеца след това за широкомащабни информационни системи, изброени в приложение IX), са изключени от приложното поле, освен ако тези системи не са претърпели „значителни промени“ в проекта или предназначението си (член 83).

39. Въпреки това прагът за „значителни промени“ е неясен. В съображение 66 от предложението се посочва по-нисък праг за ново оценяване на съответствието, а именно „всеки път, когато настъпи промяна, която може да засегне съответствието“. Подобен праг би бил подходящ за член 83 най-малкото за високорискови системи с ИИ. В допълнение, за да бъдат запълнени евентуални пропуски в защитата, е необходимо системите с ИИ, които са вече установени и в експлоатация — след определена фаза на внедряване — също да бъдат в съответствие с всички изисквания на регламента за ИИ.

40. Множеството възможности за обработване на лични данни и външните рискове също засягат сигурността на системите с ИИ. Акцентът върху „значителни промени в проекта или предназначението“ в член 83 не включва позоваване на промени във външните рискове. Следователно в член 83 от предложението следва да се включи позоваване на промените в сценария за заплахите, произтичащи от външни рискове, например кибератаки, атаки на конкурентите и обосновани жалби от потребители.

41. Освен това тъй като датата на прилагане е предвидена да бъде 24 месеца след датата на влизане в сила на бъдещия регламент, ЕКЗД и ЕНОЗД не считат, че е подходящо системите с ИИ, които вече са пуснати на пазара, да бъдат освобождавани за още по-дълъг период от време. Въпреки че в предложението се предвижда също така, че изискванията на регламента се вземат под внимание при оценката на всяка широкомащабна информационна система, както е предвидено в правните актове, посочени в приложение IX, ЕКЗД и ЕНОЗД считат, че изискванията относно въвеждането в експлоатация на системи с ИИ следва да се прилагат от датата на прилагане на бъдещия регламент.

2.5 Управление и Европейски комитет по ИИ

2.5.1 Управление

42. ЕКЗД и ЕНОЗД приветстват определянето на ЕНОЗД като компетентен орган и орган за надзор на пазара за наблюдението на институциите, агенциите и органите на Съюза, когато попадат в приложното поле на настоящото предложение. ЕНОЗД е в готовност да изпълни новата си роля като регулатор на ИИ за публичната администрация на ЕС.

Освен това, ролята и задачите на ЕНОЗД не са разписани достатъчно подробно и следва да бъдат допълнително изяснени в предложението, особено що се отнася до ролята му като орган за надзор на пазара.

43. ЕКЗД и ЕНОЗД признават разпределянето на финансови ресурси, което е предвидено за Комитета и ЕНОЗД в качеството му на уведомяващ орган в предложението. Изпълнението на новите задължения на ЕНОЗД, дори когато действа като орган, който следва да бъде уведомяван по тези въпроси, би изисквало значително по-големи финансови и човешки ресурси.

44. На първо място, това се дължи на формулировката в член 63, параграф 6, която гласи, че ЕНОЗД „действа като [...] компетентен орган за надзор на пазара“ за институциите, агенциите и органите на Съюза, които попадат в обхвата на предложението — това не изяснява дали ЕНОЗД следва да се счита за пълноценен „орган за надзор на пазара“, както е предвидено в Регламент (ЕС) 2019/1020. Това повдига въпроси относно задълженията и правомощията на ЕНОЗД на практика. На второ място и при условие че отговорът на горепосочения въпрос е утвърдителен, не е ясно как ролята на ЕНОЗД така, както е предвидена в Регламента за защита на данните от институциите на ЕС, може да се съчетае със задачата, предвидена в член 11 от Регламент (ЕС) 2019/1020, която включва „ефективния надзор на пазара в рамките на тяхната територия на продукти, предоставяни онлайн“ или „физически и лабораторни проверки въз основа на подходящи проби“. Съществува риск, че поемането на новия набор от задачи без допълнителни пояснения в предложението може да застраши изпълнението на задълженията на ЕНОЗД като надзорен орган за защита на данните.

45. ЕКЗД и ЕНОЗД подчертават обаче, че някои разпоредби на предложението, в които се определят задачите и правомощията на различните компетентни органи в рамките на регламента за ИИ, взаимоотношенията между тях, тяхното естество и гаранцията за тяхната независимост, изглеждат неясни на този етап. Докато в Регламент 2019/1020 се заявява, че органът за надзор на пазара трябва да бъде независим, в проекта на регламент не се изисква надзорните органи да бъдат независими и дори се изисква от тях да докладват на Комисията относно определени задачи, извършвани от органите за надзор на пазара, които могат да бъдат различни институции. Тъй като в предложението се посочва също така, че ОЗД ще бъдат органите за надзор на пазара за системи с ИИ, използвани за целите на правоприлагането (член 63, параграф 5), това означава и че те ще бъдат предмет на задълженията за докладване на Комисията, евентуално чрез своя национален надзорен орган (член 63, параграф 2), което изглежда несъвместимо с тяхната независимост.

46. Следователно, ЕКЗД и ЕНОЗД считат, че тези разпоредби трябва да бъдат изяснени, така че да бъдат съгласувани с Регламент 2019/1020, Регламента за защита на данните от институциите на ЕС и ОРЗД, и в предложението следва да се установи ясно, че надзорните органи съгласно регламента за ИИ трябва да бъдат напълно независими при изпълнението на задачите си, тъй като това би била съществена гаранция за подобаващ надзор и правоприлагане на бъдещия регламент.

47. ЕКЗД и ЕНОЗД биха искали да припомнят също така, че органите за защита на данните (ОЗД) вече прилагат ОРЗД, Регламента за защита на данните от институциите на ЕС и ДП спрямо системи с ИИ, включващи лични данни, за да се гарантира закрилата на основните права, и по-специално правото на защита на личните данни. Следователно, както се изисква в предложението по отношение на националните надзорни органи, ОЗД вече имат до известна степен познания в областта на технологиите с ИИ, данните и изчисленията, основните права, както и експертен опит в оценяването на рисковете за основните права, пораждани от новите технологии. Освен това, когато системи с ИИ се основават на обработването на лични данни или обработват лични данни, разпоредбите на предложението са пряко преплетени с правната уредба в областта на защитата на данните, какъвто ще бъде случаят за повечето системи с ИИ в обхвата на регламента. Вследствие на това ще има взаимовръзки между правомощията на надзорните органи съгласно предложението и ОЗД.

48. Следователно, определянето на ОЗД за национални надзорни органи би гарантирало по-хармонизиран регулаторен подход и би допринесло за последователно тълкуване на разпоредбите, регламентиращи обработката на данни и за избягване на противоречия при прилагането им сред държавите членки. Освен това от полза за всички заинтересовани страни, имащи отношение към ИИ, би било създаването на единно звено за контакт за всички операции по обработване на лични данни, които попадат в приложното поле на предложението и взаимодействията да се ограничат до два различни регулаторни органа за обработването, които са засегнати от предложението и ОРЗД. ЕКЗД и ЕНОЗД считат, че **ОЗД следва да бъдат определени като национални надзорни органи в съответствие с член 59 от предложението**.

49. Във всеки случай, доколкото предложението съдържа специални правила относно защитата на физическите лица по отношение на обработването на лични данни, приети на основание на член 16 от ДФЕС, спазването на тези правила, по-специално на ограниченията за използването на системи с ИИ за биометрична идентификация от разстояние в реално време на публично достъпни места за целите на правоприлагането, **трябва да бъде предмет на контрол от страна на независими органи**.

50. В предложението обаче няма изрична разпоредба, която да дава правомощия за гарантиране на съответствие с тези правила под контрола на независими органи. Единственото позоваване на компетентните надзорни органи за защита на данните по ОРЗД или ДП се среща в член 63, параграф 5 от предложението, но само като органи за „надзор на пазара“, като за такива могат да бъдат определени и други институции. ЕКЗД и ЕНОЗД считат, че тази организация не гарантира съответствие с изискването за независим контрол, предвидено в член 16, параграф 2 от ДФЕС и член 8 от Хартата.

2.5.2 Европейски комитет по ИИ

51. С предложението се създава Европейски комитет по изкуствен интелект (ЕКИИ). ЕКЗД и ЕНОЗД признават необходимостта от съгласувано и хармонизирано прилагане на предлаганата уредба, както и от участието на независими експерти в разработването на политиката на ЕС в областта на ИИ. Същевременно в предложението се предвижда

преобладаваща роля на Комисията. В действителност тя не само ще бъде част от ЕКИИ, но и ще го председателства и ще има право на вето при приемането на правилника за дейността му. Това е в разрез с необходимостта от европейски орган за ИИ, който да бъде независим от всякакво политическо влияние. Следователно, ЕКЗД и ЕНОЗД считат, че бъдещият регламент за ИИ следва да дава **повече независимост на ЕКИИ**, за да му бъде осигурена възможност наистина да гарантира съгласувано прилагане на регламента в целия единен пазар.

52. ЕКЗД и ЕНОЗД отбелязват също така, че на ЕКИИ не се дават никакви правомощия по отношение на прилагането на предложения регламент. Освен това, предвид разпространението на системи с ИИ в рамките на единния пазар и вероятността от трансгранични случаи, съществува сериозна необходимост от хармонизирано правоприлагане и правилно разпределение на правомощията между националните надзорни органи. Във връзка с това ЕКЗД и ЕНОЗД препоръчват в бъдещия регламент за ИИ да бъдат конкретизирани механизмите за сътрудничество между националните надзорни органи. ЕКЗД и ЕНОЗД предлагат да се наложи механизъм, който да гарантира създаването на единно звено за контакт за всяка система с ИИ, за засегнатите от законодателството физически лица и дружества, както и за организации, чиято дейност обхваща повече от половината от държавите — членки на ЕС, като ЕКИИ да може да определя националния орган, който ще бъде отговорен за прилагането на регламента за ИИ за конкретната система.

53. Освен това предвид независимото естество на органите, от които ще бъде съставен Комитетът по ИИ, той трябва да има правото да действа по собствена инициатива, а не само да предоставя съвети и съдействие на Комисията. ЕКЗД и ЕНОЗД изтъкват необходимостта от разширяване на мисията, определена за Комитета, която не съответства на задачите, изброени в предложението.

54. За да може да изпълни тези цели, **ЕКИИ трябва да разполага с достатъчни и подходящи правомощия** и правният му статут да бъде изяснен. По-специално, за да може материалното приложно поле на бъдещия регламент да остане съотносимо, изглежда, че е необходимо в развитието му да бъдат включени органите, които отговарят за прилагането му. Във връзка с това ЕКЗД и ЕНОЗД препоръчват на ЕКИИ да бъдат дадени правомощия да предлага на Комисията изменения на приложение I, в което се определят техниките и подходите на ИИ, и на приложение III, в което се изброяват високорисковите системи с ИИ, на които се прави позоваване в член 6, параграф 2. Освен това Комисията следва да се консултира с ЕКИИ преди всяко изменение на тези приложения.

55. В член 57, параграф 4 от предложението се предвижда обмен между Комитета по ИИ и други органи, служби, агенции и консултативни групи на Съюза. ЕКЗД и ЕНОЗД препоръчват Агенцията на Европейския съюз за основните права да бъде разгледана като един от възможните наблюдатели в Комитета предвид предишната ѝ работа в областта на ИИ и експертния ѝ опит в областта на правата на човека.

3 ВЗАИМОДЕЙСТВИЕ С УРЕДБАТА В ОБЛАСТТА НА ЗАЩИТАТА НА ДАННИТЕ

3.1 Връзка на предложението с действащото право на ЕС в областта на защитата на данните

56. Ясно определената връзка между предложението и действащото право в областта на защитата на данните е съществена предпоставка за гарантиране и отстояване на зачитането и прилагането на достиженията на правото на ЕС в областта на защитата на личните данни. Това право на ЕС, по-специално ОРЗД, Регламентът за защита на данните от институциите на ЕС и ДП, следва да бъде взето под внимание като предпоставка, на основата на която може да се градят по-нататъшни законодателни предложения, без те да засягат или да се намесват в съществуващите разпоредби, включително по отношение на правомощията на надзорните органи и управлението.

57. Следователно, ЕКЗД и ЕНОЗД считат, че е важно в предложението да се избягват ясно каквито и да било несъответствия и евентуални противоречия с ОРЗД, Регламента за защита на данните от институциите на ЕС и ДП. Целта е не само да се постигне правна сигурност, но и да се избегне положение, при което предложението пряко или косвено застрашава основното право на защита на личните данни, както е предвидено в член 16 от ДФЕС и член 8 от Хартата.

58. По-специално самообучаващите се машини биха могли да защитават личните данни на физическите лица само ако това е вградено в тях на етапа на създаването им. От съществено значение е и незабавната възможност за упражняване на правата на физическите лица съгласно член 22 (Автоматизирано вземане на индивидуални решения, включително профилиране) от ОРЗД или член 23 от Регламента за защита на данните от институциите на ЕС, независимо от целите на обработването. В това отношение други права на субектите на данни, свързани с правото на заличаване, правото на коригиране съгласно законодателството в областта на защитата на данните, трябва да бъдат предвидени в системите с ИИ от самото начало, независимо от избрания подход или техническата архитектура.

59. Използването на лични данни за самообучение на системите с ИИ може да доведе до генериране на предубедени модели за вземане на решения в сърцевината на системата с ИИ. Поради тази причина в такива процеси следва да се изискват различни гаранции, и по-специално квалифициран човешки надзор, за да се осигури зачитането и гарантирането на правата на субектите на данни, както и за да се избегнат всякакви отрицателни последици за физическите лица. Компетентните органи също следва да са в състояние да предлагат насоки за оценяване на предубедеността в системите с ИИ и да подпомагат упражняването на човешки надзор.

60. Субектите на данни винаги следва да бъдат информирани, когато данните им се използват за самообучение на ИИ и/или за прогнозиране, да бъдат осведомени за правното основание за такова обработване, както и да получат общо обяснение на

логиката (процедурата) и обхвата на системата с ИИ. При тези случаи следва винаги да бъде гарантирано правото на физическите лица на ограничаване на обработването (член 18 от ОРЗД и член 20 от Регламента за защита на данните от институциите на ЕС), както и на заличаване/изтриване на данните (член 16 от ОРЗД и член 19 от Регламента за защита на данните от институциите на ЕС). Освен това администраторът на данните следва да има изричното задължение да уведомява субекта на данните за приложимите срокове за възражение, ограничаване, заличаване на данни и т.н. Системата с ИИ трябва да е в състояние да изпълни всички изисквания за защита на данните посредством подходящи технически и организационни мерки. Допълнителна прозрачност следва да се предостави чрез правото на получаване на обяснение.

3.2 Програми за анализ на определена информация и последващо обработване (членове 53 и 54 от предложението)

61. В рамките на съществуващите правни и морални граници е важно да се насърчават европейските иновации посредством инструменти като програмите за анализ на определена информация. Такава програма дава възможност за осигуряване на гаранции, необходими за изграждане на доверие към системите с ИИ и разчитане на тях. При възникване на сложни ситуации може да е трудно практиците в областта на ИИ да претеглят правилно всички интереси. Особено за малките и средните предприятия с ограничени ресурси използването на програми за анализ може да доведе до по-бързото стигане до заключения и оттам да насърчи иновациите.

62. В член 53, параграф 3 от предложението се посочва, че използването на програмите за анализ на определена информация не засяга надзорните и корективните правомощия. Макар това пояснение да е полезно, съществува необходимост и от разписване на указания или насоки за постигане на добър баланс между ролята на надзорен орган, от една страна, и даването на подробни насоки посредством анализа на определена информация, от друга.

63. В член 53, параграф 6 се посочва, че условията и редът за функциониране на програмите в областта на ИИ се определят в актове за изпълнение. Важно е да бъдат изготвени конкретни насоки, за да се гарантира съгласуваност и подкрепа при създаването и функционирането на тези програми. Обвързващите актове за изпълнение обаче биха могли да ограничат способността на всяка държава членка да персонализира анализа на определена информация според своите потребности и местни практики. Поради тази причина ЕКЗД и ЕНОЗД препоръчват вместо това ЕКИИ да предостави насоки за използването на програми за анализ на определена информация.

64. Целта на член 54 от предложението е да се предостави правно основание за последващо обработване на лични данни за разработване на някои системи с ИИ в обществен интерес чрез програми за анализ, които обхващат ИИ. Остава неясна връзката на член 54, параграф 1 от предложението с член 54, параграф 2 и съображение 41 от него, а оттам и с действащото право на ЕС в областта на защитата на данните. В ОРЗД и Регламента за защита на данните от институциите на ЕС обаче вече е налице установено основание за

„по-нататъшно обработване“. Особено по отношение на случаите, в които е от обществен интерес да се разреши по-нататъшното обработване, балансирането между интересите на администратора на данните и тези на субекта на данните не е нужно да възпрепятства иновациите. Понастоящем в член 54 от предложението не се разглеждат два важни въпроса: i) при какви обстоятелства и с използване на кои (допълнителни) критерии се претеглят интересите на субектите на данни и ii) дали тези системи с ИИ ще бъдат използвани единствено за целите на анализа на определена информация. ЕКЗД и ЕНОЗД приветстват изискването обработването в програмата на лични данни, събрани по силата на ДП, да се основава на правото на Съюза или на държава членка, но препоръчват да се конкретизира допълнително предвиденото тук, така че да се постигне съответствие с ОРЗД и Регламента за защита на данните от институциите на ЕС основно чрез поясняване, че правното основание за употребата на такива програми следва да е в съответствие с изискванията по член 23, параграф 2 от ОРЗД и член 25 от Регламента за защита на данните от институциите на ЕС, и чрез уточняване, че всяко използване трябва да бъде подложено на щателна оценка. Това важи и за пълния списък с условия в член 54, параграф 1, букви б)—й).

65. Някои допълнителни съображения относно повторното използване на данни в член 54 от предложението показват, че функционирането на програмите за анализ изисква много ресурси и поради тази причина е реалистично да се прогнозира, че възможност да участват ще получат малък брой предприятия. Участието в програмите би могло да представлява конкурентно предимство. Позволяването на повторно използване на данни би изисквало внимателно разглеждане на начина за избиране на участниците, за да се гарантира, че те са обхванати в приложното поле и да се избегне несправедливо третиране. ЕКЗД и ЕНОЗД изразяват загриженост, че позволяването на повторно използване на данни в рамките на програмата за анализ се отклонява от предвидения в ОРЗД подход на отчетност, при който отчетността е задължение на администратора на данни, а не на компетентния орган.

66. Освен това ЕКЗД и ЕНОЗД считат, че предвид целите на програмите, а именно разработване, изпитване и признаване на системи с ИИ, те не могат да попадат в приложното поле на ДП. Въпреки че в ДП се предвижда възможност за повторно използване на данни за научноизследователски цели, данните, обработвани за тази вторична цел, се превръщат в предмет на ОРЗД или на Регламента за защита на данните от институциите на ЕС и престават да бъдат предмет на ДП.

67. Не е ясно какво ще обхваща една програма за анализ на определена информация. Възниква въпросът дали предлаганата програма включва ИТ инфраструктура във всяка държава членка с някои допълнителни правни основания за по-нататъшно обработване, или тя просто организира достъп до експертни знания и насоки в регулаторната сфера. ЕКЗД и ЕНОЗД настоятелно призовават законодателя да изясни това понятие в предложението и да заяви ясно в него, че програмата не предполага задължение на компетентните органи да предоставят техническата си инфраструктура. При всички случаи, в съответствие с това пояснение, на компетентните органи трябва да бъдат предоставени съответните финансови и човешки ресурси.

68. Накрая, ЕКЗД и ЕНОЗД биха искали да изтъкнат разработването на трансгранични системи с ИИ, които ще бъдат на разположение на целия единен европейски цифров пазар. В случая на такива системи с ИИ, програмата за анализ като инструмент за иновации не следва да се превръща в препятствие пред трансграничното развитие. Следователно, ЕКЗД и ЕНОЗД препоръчват координиран трансграничен подход, който е достатъчно наличен на национално равнище за всички МСП и предлага обща рамка в цяла Европа, без да бъде твърде ограничителен. Трябва да се постигне баланс между европейската координация и националните процедури, за да се избегне противоречиво прилагане на бъдещия регламент за ИИ, което би възпрепятствало иновациите, които обхващат територията на целия ЕС.

3.3 Прозрачност

69. ЕКЗД и ЕНОЗД приветстват факта, че високорисковите системи с ИИ задължително ще се регистрират в публична база данни (посочена в членове 51 и 60 от предложението). Тази база данни следва да се разглежда като възможност за предоставяне на информация на широката общественост относно обхвата на приложение на системите с ИИ, известни дефекти и инциденти, които може да компрометират тяхното функциониране, и средствата за защита, възприети от доставчиците с цел тези дефекти и инциденти да бъдат разгледани и отстранени.

70. Основен принцип на демокрация е принципът на взаимозависимости и взаимоограничаване. Поради тази причина освобождаването на системите с ИИ, използвани за разкриване, предотвратяване, разследване и наказателно преследване на престъпления, от задължението за прозрачност е твърде широко. Трябва да се направи разграничение между системите с ИИ, използвани за разкриване и предотвратяване на престъпления, и тези, чиято цел е разследване или подпомагане на наказателното преследване на престъпления. Защитните мерки при предотвратяването и разкриването трябва да бъдат по-силни поради презумпцията за невинност. Освен това ЕКЗД и ЕНОЗД изразяват съжаление във връзка с отсъствието на предпазни предупреждения в предложението, което може да се тълкува като даване на „зелена светлина“ за използване дори на недоказани високорискови системи или приложения с ИИ.

71. В тези случаи, когато на обществеността не може да се осигури почти никаква прозрачност поради съображения за секретност, дори и в една добре функционираща демокрация, следва да бъдат въведени гаранции и тези системи с ИИ да бъдат регистрирани и да предоставят прозрачност пред компетентния надзорен орган.

72. Гарантирането на прозрачност в системите с ИИ е много трудна цел. Изцяло количественият подход при вземането на решения, който се използва в много системи с ИИ и който по своята същност се различава от човешкия подход, при който се разчита най-вече на причинно-следствени и теоретични разсъждения, може да влезе в противоречие с необходимостта от получаване на предварително разбираемо обяснение на резултатите от машината. В регламента следва да се насърчат нови, по-активни и своевременни начини за информиране на ползвателите на системи с ИИ относно моментното състояние на

системата (по отношение на вземането на решение) във всеки един момент, като се предоставят ранни предупреждения за потенциални вредни резултати, така че физическите лица, чиито права и свободи може да бъдат накърнени от автономното вземане на решения на машината, да могат да реагират или да използват средства за защита срещу решението.

3.4 Обработване на специални категории данни и данни, свързани с престъпления

73. Обработването на специални категории данни в областта на правоприлагането се урежда от разпоредбите на правната уредба на ЕС в областта на защитата на данните, включително от ДП, както и от нейното изпълнение на национално равнище. В предложението се твърди, че то не предоставя общо правно основание за обработването на лични данни, включително на специални категории лични данни (вж. съображение 41). В същото време член 10, параграф 5 гласи, че „доставчиците на такива системи могат да обработват специални категории лични данни“. Освен това в същата разпоредба се изискват допълнителни гаранции, като са дадени и примери. Поради тази причина предложението изглежда се намесва в прилагането на ОРЗД, ДП и Регламента за защита на данните от институциите на ЕС. Въпреки че ЕКЗД и ЕНОЗД приветстват опита да се предвидят подходящи гаранции, е необходим по-последователен регулаторен подход, тъй като настоящите разпоредби не изглеждат достатъчно ясни, за да създадат правно основание за обработването на специални категории данни, и трябва да бъдат допълнени с още защитни мерки, които също трябва да бъдат оценени. Освен това, когато личните данни са били събрани чрез обработване в рамките на приложното поле на ДП, ще трябва да бъдат взети под внимание и евентуалните допълнителни гаранции и ограничения, произтичащи от националното транспониране на директивата.

3.5 Механизми за съответствие

3.5.1 Сертифициране

74. Сертифицирането е един от основните стълбове на предложението. Очертаната в предложението система за сертифициране се основава на структура от образувания (уведомяващи/ органи/уведомявани органи/Комисията) и механизъм за оценяване на съответствието/сертифициране, който обхваща задължителните изисквания, приложими спрямо високорисковите системи с ИИ, и се основава на европейските хармонизирани стандарти, предвидени в Регламент (ЕС) № 1025/2012, и на общи спецификации, които предстои да бъдат изготвени от Комисията. Този механизъм е различен от системата за сертифициране, чиято цел е осигуряване на съответствие с правилата и принципите за защита на данните, посочена в членове 42 и 43 от ОРЗД. Не е ясно обаче как сертификатите, издавани от уведомяваните органи в съответствие с предложението, може да взаимодействат с предвидените в ОРЗД сертификати, печати и маркировки за защита на данните, за разлика от това, което е предвидено за други видове сертификати (вж. член 42, параграф 2 по отношение на сертификатите, издавани съгласно Регламент (ЕС) 2019/881).

75. Доколкото високорисковите системи с ИИ се основават на обработване на лични данни или обработват лични данни за целите на изпълнението на задачите си, тези несъответствия може да породят правна несигурност за всички засегнати органи, тъй като може да доведат до ситуации, в които системи с ИИ, сертифицирани съгласно предложението и носещи маркировка за съответствие „CE“, щом бъдат пуснати на пазара или въведени в експлоатация, може да се използват по начин, който не съответства на правилата и принципите за защита на данните.

76. В предложението липсва ясна връзка с правото в областта на защитата на данните, както и с други видове право на ЕС и на държавите членки, приложимо спрямо всяка от „областите“ на високорисковите системи с ИИ, изброени в приложение III. По-специално, в предложението следва да бъдат включени принципите на свеждане на данните до минимум и защита на данните на етапа на проектиране, като един от аспектите които следва да бъдат взети под внимание, преди да бъде получена маркировка „CE“, предвид евентуалната висока степен на намеса на високорисковите системи с ИИ в основните права на неприкосновеност на личния живот и на защита на личните данни и необходимостта да се гарантира високо равнище на доверие в системата с ИИ. Следователно, ЕКЗД и ЕНОЗД препоръчват предложението да се измени така, че да се изясни връзката между издаваните по силата на предлагания регламент сертификати и сертифицирането, печатите и маркировките за защита на данните. На последно място, органите за защита на данните следва да участват в изготвянето и установяването на хармонизирани стандарти и общи спецификации.

77. Във връзка с член 43 от предложението относно оценяването на съответствието, предвидената в член 47 дерогация от процедурата за оценяване на съответствието изглежда твърде широка и включваща твърде много изключения, например изключителни причини, свързани с обществената сигурност или защитата на живота и здравето на хората, опазването на околната среда и защитата на ключови промишлени и инфраструктурни активи. Предлагаме на законодателите да ги съкратят.

3.5.2 Кодекси за поведение

78. Съгласно член 69 от предложението, Комисията и държавите членки насърчават и улесняват изготвянето на кодекси за поведение, предназначени да насърчават доброволното прилагане, от страна на доставчиците на системи с ИИ, които не водят до високи рискове, на изискванията, приложими спрямо високорисковите системи с ИИ, както и допълнителни изисквания. В съответствие със съображение 78 от ОРЗД, ЕКЗД и ЕНОЗД препоръчват да се идентифицират и определят полезни взаимодействия между тези инструменти и кодексите за поведение, предвидени в ОРЗД, които подкрепят съответствието в областта на защитата на данните. В този смисъл е важно да се поясни дали защитата на личните данни следва да се разглежда като част от посочените в член 69, параграф 2 „допълнителни изисквания“, които може да бъдат разгледани в кодексите за поведение. Също така трябва да се гарантира, че посочените в член 69, параграф 1 „технически спецификации и решения“, разглеждани в кодексите за поведение, така както тези технически спецификации и решения са проектирани да насърчават съответствие с

изискванията на проекта за регламент за ИИ, не влизат в противоречие с правилата и принципите на ОРЗД и на Регламента за защита на данните от институциите на ЕС. По този начин придържането към тези инструменти от страна на доставчиците на системи с ИИ, които не водят до висок риск, доколкото тези системи се основават на обработването на лични данни или обработват лични данни за целите на изпълнението на своите задачи, би представлявало добавена стойност, тъй като ще се гарантира, изпълнението на задълженията на администратора на данни и обработващите лични данни да защитят данните при използването на тези системи.

79. Същевременно, правна уредба за надежден ИИ ще бъде допълнена с кодекси за поведение, като това ще насърчи доверието в използването на тази технология по безопасен и съответстващ на правото начин, включително при зачитане на основните права. Проектирането на тези инструменти обаче следва да се укрепи, като бъдат предвидени механизми, насочени към потвърждаване, че тези кодекси предоставят ефективни „технически спецификации и решения“ и задават „ясни цели и ключови показатели за ефективност за измерване на постигането на тези цели“ като неразделна част от тяхното съдържание. Освен това отсъствието на каквото и да е позоваване на (задължителни) механизми за наблюдение за кодексите за поведение, които да потвърждават, че доставчиците на системи с ИИ, които не водят до висок риск спазват техните разпоредби, както и възможността отделните доставчици сами да създават (и прилагат) посочените кодекси (вж. точка 5.2.7 от обяснителния меморандум) може да отслабят допълнително ефективността и способността за прилагане на тези инструменти.

80. На последно място, ЕКЗД и ЕНОЗД искат разяснения по отношение на видовете инициативи, които Комисията може да разработва съгласно съображение 81 от предложението, „за да улесни намаляването на техническите пречки, които възпрепятстват трансграничния обмен на данни за разработването на ИИ“.

4 ЗАКЛЮЧЕНИЕ

81. Въпреки че ЕКЗД и ЕНОЗД приветстват предложението на Комисията и считат, че такъв регламент е необходим за гарантиране на основните права на гражданите на ЕС и на лицата, пребиваващи в него, те считат, че то трябва да бъде адаптирано по няколко въпроса, за да се гарантира неговата приложимост и ефективност.

82. Предвид сложността на предложението, както и въпросите, които то си е поставило за цел да урежда, остава да бъде свършена много работа, докато то бъде в състояние да предостави добре функционираща правна уредба, която допълва ефективно ОРЗД по отношение на защитата на основните права на човека, като същевременно насърчава иновациите. ЕКЗД и ЕНОЗД ще продължат да бъдат на разположение и да предлагат подкрепата си по този въпрос.

Брюксел, 18 юни 2021 г.

За Европейския комитет по защита на данните

Председател

Andrea JELINEK

За Европейския надзорен орган по защита на данните

Надзорник

Wojciech Rafał WIEWIÓROWSKI