АКТЪТ ЗА ИИ –
ПРОПУСКИ И ВЪЗМОЖНОСТИ
ОТ ПРАВОЗАЩИТНА ГЛЕДНА ТОЧКА

СЪДЪРЖАНИЕ НА НАСТОЯЩАТА СТАТИЯ:

Автор: Радина Банова-Стоева, правен консултант в БЦНП

Редактор: Надя Шабани, Директор на БЦНП

Септември, 2024 г.

КАКВА ЦЕЛ СИ ПОСТАВЯ АИИ?

От началото на август 2024 г. в сила влезе Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 г. за определяне на хармонизирани правила за изкуствения интелект (т.нар. „Акт за изкуствения интелект“ / „АИИ“ / „Регламентът/а“). Макар и приложението на части от АИИ да започва по различно време (глави I и II от 02.02.2025 г., а други текстове – в конкретен момент в периода 02.08.2025 – 02.08.2027 г.), Регламентът е факт.

Предметното поле на Акта отразява опита на европейските институции да балансират в сложните отношения между бизнес, национални интереси и интересите на конкретния човек (основни права). Както в чл. 1, така и още в първи параграф от преамбюла на АИИ, е заложена целта *„да се подобри функционирането на вътрешния пазар чрез установяване на единна правна рамка“*, *„в съответствие с ценностите на Съюза“*, *„да се насърчи навлизането на ориентиран към човека и надежден изкуствен интелект (ИИ), като същевременно се гарантира високо равнище на защита на здравето, безопасността и основните права, залегнали в Хартата на основните права на Европейския съюз, включително демокрацията, принципите на правовата държава и опазването на околната среда, да се осигури защита срещу вредните последици от системите с ИИ в Съюза и да се подкрепят иновациите“*.
Съществен позитив и утвърждаване на правата на човека като базова ценност в регулацията на ИИ в ЕС е това, че те фигурират още в предмета на АИИ. Регламентът, като част от вторичното право на ЕС, е с пряко действие във всяка държава членка. На колкото по-принципна и обща основа е поставен даден обект на защита, толкова по-всеобхватно може да е търсенето на тази защита. А оттук следва и солидната база за застъпничество за основните човешки права на всеки етап от процеса по създаване, изпитване и ползване на системите с ИИ.

РЕГУЛАЦИЯ НА ДВЕ НИВА: НИВО ЕС VS. НИВО ДЪРЖАВИ ЧЛЕНКИ

В общия положителен план светва и една голяма червена лампа: до колко на държавите членки се дава възможност за приемане на национално законодателство във връзка с Регламента. Погледът към преамбюла не дава твърде оптимистична прогноза по въпроса. Посочва се, че *„не се допуска държавите членки да налагат ограничения върху разработването, предлагането на пазара и използването на системи с ИИ, освен ако това не е изрично разрешено с настоящия регламент“*. В нормите на АИИ почти не се открива възможност държавите-членки да задълбочат или дообогатят правната рамка, свързана с ИИ[1], а това което има на ниво Регламент е условно и е твърде ограничени хипотези.

Подобен подход на централизация на ИИ уредбата може да създаде казуси, предвид различните национални контексти, в които нормативният акт ще бъде прилаган. Все пак е важно да се отчете, че в цялост АИИ разчита на немалък брой вторична спрямо самия себе си уредба (делегирани актове, насоки, актове за изпълнение, образци, технически стандарти и кодекси за прилагане).

Друг пример за балансиране на централизираната регулация (независимо на ниво ЕС или на ниво държави членки) е възможността за ангажиране на различни заинтересовани страни в процесите по изграждане на грамотност в областта на ИИ[2] и за разработване на Кодексите за поведение (чл. 95). Това са доброволни кодекси, отнасящи се до системи с ИИ, различни от високорискови, и могат да включват някои или всички изисквания, установени за високорисковите ИИ системи, *„като вземат предвид наличните технически решения и най-добрите практики в сектора, които позволяват прилагането на такива изисквания“*. Именно тук, в процеса по изготвяне на кодексите за поведени, се признава и капацитетът на гражданските организации да са участник в застъпничеството за човешките права, наравно с всички заинтересовани страни[3].

---

[1] Чл. 2, пара. 11: *„Настоящият регламент не е пречка Съюзът или държавите членки да запазят или въведат законови, подзаконови или административни разпоредби, които са по-благоприятни за работниците по отношение на защитата на правата им във връзка с използването от работодателите на системи с ИИ, нито да насърчават или разрешават прилагането на колективни трудови договори, които са по-благоприятни за работниците.“*
Чл. 26, пара. 10, ал. 7: „Държавите членки могат да въведат, в съответствие с правото на Съюза, по-ограничителни законови разпоредби относно използването на системи за последваща дистанционна биометрична идентификация.“

[2] Пара. 20 от преамбюла и чл. 4.

[3] Чл. 95, пара. 3: *„Кодексите за поведение могат да бъдат изготвяни от отделни доставчици или внедрители на системи с ИИ или от организации, които ги представляват, или съвместно,*

РИСК-БАЗИРАНИЯТ ПОДХОД: КАКЪВ Е ПРОБЛЕМЪТ?

Пътят към създаване на АИИ беше дълъг и трънлив. Редица международни, европейски и национални организации, защитаващи правата на човека и мониториращи процесите по създаване на регулация, която засяга основните права, отправяха редица апели[4] за създаване на такъв АИИ, който напълно да съответства на стандартите за върховенство на правото и да ползва като основа подход стандартите на основните права. Самата Европейска комисия призна в своя „Доклад за Изкуствеиият интелект: европейски подход за високи постижения и доверие“, че *„Основните рискове, свързани с използването на ИИ, са свързани с прилагането на правилата, предназначени за защита на основните права (включително защитата на личните данни и неприкосновеността на личния живот и недискриминацията), както и въпросите, свързани с безопасността и отговорността“*[5]. Все пак, въпреки призивите[6] от страна на гражданския сектор в основната на Регламента да залегнат стандартите за защита на основните права като подход за оценка на безопасността на ИИ системите поприицип, тези стандарти се запазват само в оценката на въздействието върху основните права, която се извършва от внедрителите по отношение на високорисковите ИИ системи. Европейските институции се спряха на подхода, базиран на риска.

От АИИ могат да се изведат 4 нива на риск, посочени в схемата по-долу:

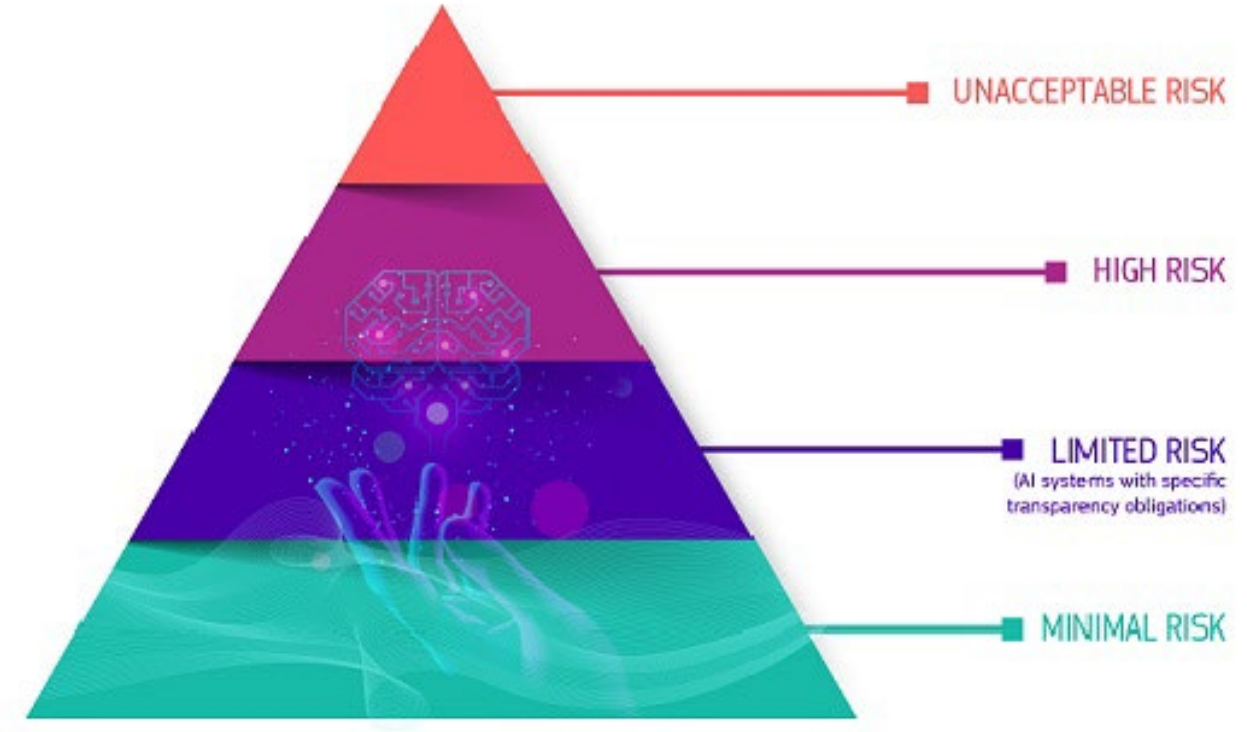
---

*включително с участието на всички заинтересовани страни и техните представителни организации, включително **организации на гражданското общество** и академичните среди. Кодексите за поведение могат да обхващат една или повече системи с ИИ, като се отчита сходството в предназначението на съответните системи.“*

[4] https://ecnl.org/sites/default/files/2023-09/AI_and_RoL_Open_Letter_final_27092023.pdf; https://bcnl.org/news/zakonodatelniyat-akt-za-izkustveniya-intelekt-na-es-tryabva-da-garantira-osnovnite-prava-bez-kompromisi.html

[5] https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_en?filename=commission-white-paper-artificial-intelligence-feb2020_en.pdf

[6] Становище, подписано от над 120 международни граждански организации, с препоръки за уредбата на правата на човека в АИИ и призив за възприемане на подход, базиран върху тези права, а не риск-базиран подход: https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf; вж. също Насоките на високоекспертната група по въпросите за ИИ – AI HLEG, съставена от 52-ма експерти по ИИ от областта на академията, неправителствения сектор и бизнеса, и действала като консултативен орган към Комисията в процеса на изготвяне на АИИ.



Източник: Европейска комисия, https://digital-strategy.ec.europa.eu/bg/policies/regulatory-framework-ai

1. Неприемливият риск е регулиран като забранени практики;
2. Високорисковите ИИ системи (определяеми с правила за класификация по чл. 6, който препраща и към списък с такива системи – приложение III) – трябва да отговарят на изискванията за сигурност, прозрачност и качество, както и да се подлагат на оценка на съответствието;
3. ИИ системи, създаващи ограничен риск – задължения само за прозрачност;
4. Създаващите минимален риск ИИ системи не са регулирани

ИИ с общо предназначение следва да отговарят на изисквания за прозрачност и допълнителни оценки за моделите с високи възможности.

Основе проблем на риск-базирания подход е фактът, че **нивото на риска не може да бъде напълно определено предварително и зависи и от контекста**, в който се внедрява дадена система. В допълнение се създава необходимост от извършване на преценки и оценка на различни нива при усложнени механизми. Подходът за прилагане на стандартите за основните права на човека е най-

ясният, създаван до момента механизъм за защита на индивидуалните права. Основните права са универсални и дефинирани в редица международни актове, сред които Хартата за основните права на ЕС, Европейската конвенция за правата на човека и основните свободи на Съвета на Европа, и не на последно място, основополагащата Всеобща декларация за правата на човека на ООН. Те са част от демократичните правни системи, които са адаптирани за тяхното разпознаване и прилагане. В този смисъл и нарушаването на основните права е много по-лесно установимо, независимо от контекста на извършването му, в сравнение процедурите по установяване на нарушение в новосъздаден риск-базиран подход на регулация.

ДО КОЛКО ЗАБРАНЕНИ СА ЗАБРАНЕНИТЕ ПРАКТИКИ В ОБЛАСТТА НА ИИ?

Всъщност, нито една от забранените практики в областта на ИИ не е **абсолютно забранена**. При някои от тях има завишени или много конкретни критерии за противоправен резултат, а при други са предвидени изключения, които в действителност правят практиката възможна.

В обзора на забранени практики по-долу представяме и възможни посоки към оптимизиране на текстовете, които намираме за полезни с оглед споделяните и от нас препоръки на международни правозащитни[7] организации:

1. При практиките, свързани най-общо с измама и манипулиране, се иска да е налице *„съществено изменение на поведението на дадено лице или група лица“* или *„значително нарушаване на способността за вземане на информирано решение“*. Правим допускане, че количественото изменение на поведението или на степента на нарушаване на способността за вземане на решение са основанието за забрана, но само ако са в нещо като висока степен или горна граница на количествен спектър. Измерител обаче липсва, поради което това допускане остава само хипотеза.
   Посока към подобрение: Всяка система, която *„си служи със техники, действащи на подсъзнанието и отвъд рамките на съзнаваното от човека, или с умишлено манипулативни или измамни техники“* следва да бъде забранена независимо от целта. В допълнение, всеки ефект върху поведението на човек и всяко нарушаване на способността му да вземе решение в следствие ползването на манипулативни и измамни ИИ системи представлява нарушаване на човешките права и следва да бъде допустим противоправен резултат.
2. Забраната на *„система с ИИ, която използва някое от уязвимите места на дадено физическо лице или на конкретна група лица, дължащи се на възраст, увреждане или конкретно социално или икономическо положение“* също е свързана с *„последици, изразяващи се в съществено изменение на поведението на това лице или на лице“* и *„значителни вреди“* като резултат. Липсата на „съществено“ изменение и/или на „значителни“ вреди ще значи ли липса на основание за забрана на конкретната ИИ система?

[7] Отново, в Становище, подписано от над 120 международни граждански организации, с препоръки за уредбата на правата на човека в АИИ и призив за възприемане на подход, базиран върху тези права, а не риск-базиран подход: https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf

Посока към подобрение: събирането на данни за уязвимостта на хората, независимо по какъв критерий, следва да е недопустима практика, защото създава предпоставки за злоупотреба с подобна информация, което е пряка злоупотреба с основни човешки права.

3. ИИ системи, целящи *„оценка или класифициране на физически лица или групи от лица ... въз основа на тяхното социално поведение или известни, изведени или предполагаеми лични или личностни характеристики“* са също забранени, но само ако водят до: 1) *„увреждащо или неблагоприятно третиране ... в социален контекст, който няма връзка с контекста, в който първоначално са били генерирани или събрани данните“* или 2) *„увреждащо или неблагоприятно третиране ... което е неоправдано или непропорционално с оглед на тяхното социално поведение или на тежестта, която му се отдава“*. Ако контекстът има връзка или ако третирането е оправдано или пропорционално, то тази класифицираща ИИ система става ли позволена?

   Посока към подобрение: Не съществува оправдано или пропорционално третиране, което да е увреждащо и неблагоприятно. Който и какъвто и да е контекстът на събиране на данните, няма контекст, който да позволява събиране на данни с оглед ползването им за увреждащо и неблагоприятно третиране. И двете хипотези представляват нарушаване на основните права и следва категорично подобен тип оценяващи или класифициращи ИИ системи да бъдат забранени без уточнения и изключения.

4. Налице е забрана ИИ да се ползва за оценки на риска или вероятността физическо лице да извърши престъпление, въз основа единствено на профилирането му или на оценката на личностните му черти и характеристики. Последвалото изключение относно такива ИИ системи, базирани върху обективни и проверими факти, пряко свързани с престъпна дейност, обаче прави подобно профилиране позволено. Въпрос на конкретика е как се установява тази обективност.

   Посока към подобрение: Към момента не е известна ИИ система, която да не допуска грешки. Допустимостта на прилагането на ИИ технология в процеса по оценка на риска даден човек да извърши престъпление демонстрира непознаване на значителните проблеми, които ИИ системите създават в този контекст, поради предразсъдъчните данни, с които се захранват те. Предвид съществуващата вече порочна практика да се ползват ИИ системи за предвиждане на риска или вероятността за

извършване на престъпления[8], подобни системи следва да попадат под абсолютна забрана.

5. Системите с ИИ, *„които създават или разширяват бази данни за разпознаване на лица чрез нецеленасочено извличане на лицеви изображения от интернет или записи от видеонаблюдение“* са забранени, но ако това извличане е целенасочено, допускаме ли, че забраната следва да отпадне?
   Посока към подобрение: ако всички от изброените практики са действително и ефективно забранени, отпада необходимостта да има ИИ системи, които да създават или разширяват база данни за разпознаване на лица. В този смисъл подобен текст е ненужен или следва да съдържа генерална забрана, а не само такава за нецеленасочено извличане на лицеви изображения.
6. Медицинските съображения или тези за безопасност (понятията не са дефинирани, като не са изведени и критерии или препратка с указание за прилагането им) водят до допустимост на ИИ системи, създадени с цел да се направят заключения за емоциите на дадено физическо лице на работното място или в образователните институции (иначе забранена практика по Регламента).
   Посока към подобрение: подобна формулировка прави възможно нарушаването на правата на човека от работодател или образователна институция на база основание безопасност или медицински съображения. Все още се справяме с последиците от пандемията с Ковид-19 и ефектите върху обществото. Безопасността е основание в редица държави в света в момента да се приема анти-демократично законодателство. Възможността частни субекти да преценяват ad hoc допустимостта на ползване на ИИ системи за класификация на база емоционално състояние е непропорционално нарушаване на правото на личен живот и неприкосновеност на физическите лица, работещи и учещи в съответните организации и институции. С оглед изложеното подобни ИИ системи следва да са забранени в абсолютна стойност и да не фигурират изключения за позволяване на прилагането им.
7. Системи за биометрично категоризиране въз основа на биометрични данни на физически лица *„с цел да се направят заключения или логически изводи за тяхната раса, политически възгледи, членство в синдикални организации, религиозни или философски убеждения, сексуален живот или сексуална ориентация“* са забранена практика. Забраната обаче *„не обхваща обозначаването или филтрирането на законно придобити набори*

[8] https://www.propublica.org/article/what-algorithmic-injustice-looks-like-in-real-life

от биометрични данни, например основани на биометрични данни изображения, или категоризиране на биометрични данни в правоохранителната област“. Изброените характеристики са част от Хартата на основните права на ЕС, чл. 21 „Недискриминация“ и възникват въпроси на какво основание и поради каква причина някой би събирал такива данни за едно физическо лице, какво би било законовото основание за това, за да се предвижда въобще подобно изключение?

Посока към подобрение: действително не можем да намерим причина, поради която е приемливо да се цели направата на заключение за нечии *„раса, политически възгледи, членство в синдикални организации, религиозни или философски убеждения, сексуален живот или сексуална ориентация“*. Какво би било основанието да се цели подобно заключение, за да се търси неговата юридическа обосновка. Подобен текст отваря вратата пред индивидуализиране на отговорността и разправа с конкретни хора, а не справяне с големите процеси по разделение и противопоставяне, на които сме свидетели в Европа и света в момента.

8. Принципно забраненото използване на *„системи за дистанционна биометрична идентификация в реално време*[9] *на обществено достъпни места за правоохранителни цели“* е преодоляно при следните хипотези:
   8.1. *„целево издирване на конкретни жертви на отвличане, трафик на хора и сексуална експлоатация на хора, както и издирване на изчезнали лица“*;
   8.2. *„предотвратяване на конкретна, значителна и непосредствена заплаха за живота или физическата безопасност на физически лица или на действителна и настояща или действителна и предвидима заплаха от терористично нападение“* – как може да се установи тази заплаха, ако не се извършва постоянно наблюдение в реално време?
   8.3. *„установяване на местонахождението или самоличността на лице, заподозряно в извършването на престъпление, за целите на провеждането на разследване или наказателно преследване или на изпълнението на наказание за престъпления...“*

Забранените практики са всъщност единствено ограничени. А основните права, тяхното нарушаване или заобикаляне не са отчетени като критерий за забрана.

[9] Въпросът за дистанционната биометрична идентификация, извършвана на запис, въобще не е засегнат в сферата на забранените практики, което следва да покаже, че подобна идентификация е позволена.

ВИСОКОРИСКОВИТЕ ИИ СИСТЕМИ И КАК СА УРЕДЕНИ ТЕ?

Със силна и многостранна регулация са снабдени високорисковите системи с ИИ. Оценка на съответствието, система за управление на риска *(„непрекъснат цикличен процес, планиран и протичащ през целия жизнен цикъл на високорисковата система с ИИ и изискващ редовен и систематичен преглед и актуализиране“*[10]), изисквания към наборите данни за захранване на тези системи и към съдържанието на техническата документация към системите, установено е задължение за поддържане на регистри от „записи“ (*„автоматичното записване на събития“ „с цел да се гарантира равнище на проследимост на функционирането на високорисковата система с ИИ, което е подходящо с оглед на нейното предназначение“* [11]) и изискване за проектиране в условия на прозрачност, което *„да позволи на внедрителите да тълкуват резултатите, получени от системата, и да ги използват по подходящ начин“*[12]. Задължението за подсигуряване на „точност, надеждност и киберсигурност“ е предшествано от задължението високорисковите системи с ИИ да *„се проектират и разработват … по такъв начин, че върху тях да може да бъде упражняван ефективен контрол от физически лица в периода, през който се използват“*[13]. Макар и значителна стъпка в правилната посока, човешкият контрол като изискване поставя и въпроса за отговорността: ако в сравнение с останалите гаранции, единствено при човешкият контрол има *„цел предотвратяването или свеждането до минимум на рисковете за здравето, безопасността или основните права“*, това значи ли, че отговорността при потенциално нарушаване на основните права в процеса на ползване на високорискова система ще падне единствено върху конкретните хора, осъществяващи въпросния човешки контрол върху ИИ системата? Разпоредбата на чл. 14 въвежда ограничения в тази отговорност в посока целесъобразност и пропорционалност. Все пак обръщаме внимание и на факта, че отново се намесват големите изключения на Регламента: *„Изискването за отделна проверка от най-малко две физически лица не се прилага за високорискови системи с ИИ, използвани за правоохранителни цели или за целите на миграцията, граничния контрол или убежището, когато правото на Съюза или националното право счита прилагането на това изискване за непропорционално“*[14].

[10] Чл. 9, пара. 2
[11] Чл. 12, пара 1 и 2
[12] Чл. 13, пара. 1
[13] Чл. 14, пара. 1
[14] Чл. 14, пара. 5, ал. 2

ГОЛЕМИЯТ ПРОБИВ – ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ОСНОВНИТЕ ПРАВА

Изключителен шанс пред гражданските организации, защитаващи основните права, се открива в задължението пред внедрителите, които са публични органи или са частни субекти с публични функции, да извършват Оценка на въздействието (ОВ) върху основните права преди внедряване на високорискови системи с ИИ. Съгласно изискванията на чл. 27 от Регламента ОВ следва да съдържа:

- описание на процесите на внедрителя;
- срока, в рамките на който е предназначена за използване високорисковата система с ИИ, и честотата, с която е предназначена да се използва;
- категориите физически лица и групи, които е вероятно да бъдат засегнати;
- конкретните рискове от настъпване на вреди;
- описание на изпълнението на мерките за упражняване на човешки контрол съгласно инструкциите за употреба;
- мерките, които трябва да се предприемат, ако тези рискове се проявят, включително мерките за вътрешно управление и механизмите за подаване на жалби.

В този процес НПО, разполагащи с експертиза на тема права на човека могат да бъдат ефективни партньори на администрацията в стремежа към създаване на добри стандарти за извършване на оценка на въздействието по ефективен и ефикасен начин. Службата по ИИ (AI Office) е натоварена с отговорността да изработи такъв образец на въпросник *„за да улесни внедрителите при изпълнението на задълженията“*, а задача пред гражданските организации е да проведат устойчиви и съдържателни застъпнически кампании за съдържанието на този въпросник.

Към момента в България е в ход инициатива, по която Български център за нестопанско право е партньор на МЕУ по реализиране на Мярка № 4 „Реализиране на различни форми на ефективен обществен диалог за разработване на общи стандарти при използването на изкуствения интелект в процеса на дигитализация с цел осигуряване на гаранции за равен достъп и зачитане на правата на човека“ към ТЕМАТИЧНА ОБЛАСТ „ПОЧТЕНО УПРАВЛЕНИЕ И БОРБА С КОРУПЦИЯТА“ от Четвъртия национален план на Република България в инициативата „Партньорство за открито управление“.

ИИ С ОБЩО ПРЕДНАЗНАЧЕНИЕ – ПРЕДСТОЯЩАТА ЗАДАЧА ЗА РЕШАВАНЕ

Понятието „модел на ИИ с общо предназначение“ е дефинирано в Регламента по следния начин: *„модел на ИИ, включително когато такъв модел е обучен с голямо количество данни, като се използва самонадзор в голям мащаб, който има до голяма степен общ характер и е в състояние компетентно да изпълнява широк набор от отделни задачи, независимо от начина на пускане на модела на пазара, и който може да бъде интегриран в различни системи или приложения надолу по веригата, с изключение на моделите на ИИ, използвани за научноизследователски и развойни дейности и като прототипи преди пускането им на пазара“*[15]. Доставчиците (разработилите такива модели) на ИИ модели с общо предназначение са задължени[16] да:

1. Поддържат техническа документация, която да предоставят на Службата за ИИ и националните компетентните органи при поискване;
2. Да предоставят тази документация и информация на внедрителите на такива модели и системи;
3. Да въведат политики за спазване на законодателството на ЕС за авторското право и сродните права;
4. Да оповестяват публично резюме относно съдържанието, ползвано за захранване на ИИ модела с общо предназначение.

Ако ИИ моделът с общо предназначение създава системен риск[17], то доставчиците трябва да:

1. Подсигурят неговото идентифициране и смекчаване;
2. Документират и докладват на Службата за ИИ и националните компетентните органи за сериозни инциденти и възможни коригиращи мерки за справяне с тях;
3. Осигурят адекватно ниво на киберсигурност и защита.

[15] Чл. 3, т. 63

[16] Чл. 53, пара 1

[17] Чл. 3, т. 65: *„системен риск“ означава риск, присъщ за способностите с висока степен на въздействие на моделите на ИИ с общо предназначение, които оказват значително въздействие върху пазара на Съюза поради своя обхват или поради реалните си или разумно предвидими отрицателни последици върху общественото здраве, безопасността, обществената сигурност, основните права или обществото като цяло, който може да се разпространи в голям мащаб по цялата верига за създаване на стойност“*

Силно впечатление правят две неща: 1) основните права не са застъпени в нормите, регулиращи ИИ моделите с общо предназначение, и 2) в самостоятелен раздел е предвидена възможността за създаване на Кодекси за добри практики, с изрично посочване, че „Организациите на гражданското общество“ и други заинтересовани страни „могат да подкрепят процеса“, организиран от Службата за ИИ. Подобна инициатива е в ход и Български център за нестопанско право е сред заявилите интерес от участие в работната група към Службата за ИИ.

ВЪЗМОЖНОСТИТЕ ПРЕД НПО – ЕКСПЕРТНАТА ГРУПА И КОНСУЛТАТИВНИЯ ФОРУМ

Малко предварителни разяснения по органната структура, която Регламентът предвижда:

1. Европейски съвет за ИИ (European AI Board) - Съветът за ИИ включва представители на всяка държава членка на ЕС, и се подпомага от Службата за ИИ (секретариат на Съвета) в рамките на Европейската комисия. Съветът се председателства от една от държавите членки на ЕС. Съветът играе ключова роля в рамката за управление по АИИ, като осигурява ефективното прилагане на Регламента в целия Европейски съюз. Европейският надзорен орган по защита на данните и държавите от Европейското икономическо пространство – Европейска Асоциация за свободна търговия (Исландия, Лихтенщайн, Норвегия и Швейцария) участват в заседанията на Комитета като наблюдатели.
2. Служба за ИИ (AI Office) – Службата беше създадена в началото на 2024 в рамките на Европейската комисия с идеята да играе роля на център за експертни познания в областта на ИИ и да бъде в основата на единна европейска система за управление на ИИ. Самата ЕК носи цялостна отговорност за ефективното прилагане АИИ. Тя ще издава делегирани актове и насоки, ще създава съответните органи и ще назначава техните членове, както и ще извършва оценки на Регламента. Службата за ИИ ще развива капацитета на ЕС в областта на ИИ и ще подпомага изпълнението и прилагането на Акта. Тя е снабдена и с конкретни правомощия за прилагане на разпоредбите на АИИ, свързани с ИИ с общо предназначение. Съставена е от 5 звена и двама съветници.
3. Европейски надзорен орган по защита на данните – ЕНОЗД ще бъде надзорен орган на пазара по отношение на европейските институции и агенции.
4. Национални органи – Регламентът предвижда на национално ниво да има орган за надзор на пазара и нотифициращ орган. Относно надзорните органи се очаква те да бъдат компилация между съществуващите органи по защита на лчините данни (каквато е КЗЛД в България), секторни институции (например, сфера финанси – НАП), и новосъздадени органи. Нотифициращите органи следва да отговарят за мониторинг на оценката за съответствие при високорисковите системи.
5. Национална институция по защита на правата на човека – за тях е уредено право на достъп до документация от доставчик или внедрител с оглед изпълнение на правомощието им за защита на основните права. Ще се

изисква взаимодействието им с органите по надзор на пазара, което също открива възможност за застъпнически инициативи пред гражданския сектор.

6. Експертна група (Scientific Panel) – основна цел на групата е да съветва Службата за ИИ относно моделите на ИИ с общо предназначение и да подпомага органите за надзор на пазара на национално равнище или в трансгранични дейности, по тяхно искане. Пример в конкретика е възможността Експертната група да дава „квалифицирано предупреждение“ на Службата за ИИ, ако има съмнения, че даден модел с общо предназначение следва да бъде да бъде класифициран като пораждащ системни рискове. Тя ще бъде съставена от независими експерти, избрани от Комисията въз основа на актуален научен или технически опит в областта на ИИ, като предстои ЕК да издаде акт за изпълнение, с който да определи правила за подбор на членовете на групата.
7. Консултативен съвет (Advisory Forum) – основната цел на този орган е да предоставя технически опит и да съветва Европейския Съвет за ИИ и ЕК въпросите на ИИ. По Регламент Консултативният съвет включва редица заинтересовани страни, включително гражданското общество, както и индустрията, стартиращи предприятия, МСП и академичните среди. КС трябва да се осигури баланс между търговските и нетърговските интереси, като членовете му се назначават от Европейската комисия. Постоянни членове са Агенцията за основните права и техническите и стандартизиращи органи на ЕС.

Предстои да разберем какви ще бъдат изискванията за членовете, които да съставят Експертната група и Консултативния съвет. И при двата вида органи с функции, които подпомагат дейността на основните институции по прилагане на АИИ, има реална възможност за застъпническа кампания от страна на правозащитните НПО в тях да се осигури възможност да членуват и експерти от гражданския сектор.

КАКВО ПРЕДСТОИ?

3 години на имплементация. В доклад от август 2024 г., подготвен за Европейския фонд за ИИ и обществото, Европейският център за нестопанско право (ЕЦНП)[18] отправя следните препоръки към гражданските организации и финансиращите организации във връзка с изпълнението на АИИ:

1. **Координираност в НПО сектора.**
   От съществена важност е не само провеждане на съвместни действия и колективен подход от страна на гражданските организации, но и настояване от страна на сектора да се подсигури ясен и структуриран механизъм за взаимодействие между гражданските организации и компетентните институции на европейско (Службата за ИИ, Европейския надзорен орган по защита на данните) и национално (местният надзорен орган на пазара) ниво. Следва да се предприемат координирани застъпнически инициативи с оглед номиниране на представители на гражданския сектор в Консултативния форум (Advisory forum)[19] и Експертната група (Scientific Panel)[20].
   В тази нелека задача се предоставя възможност пред донорите да предоставят финансиране за създаване на такива мрежи и координация между организациите на гражданското общество и да създадат възможности за обмен между НПО на национално и европейско ниво.

2. **Изследвания**
   Застъпнически стратегии, изградени върху данни от проведени изследвания и правни анализи, базирани върху основните права ще трасират пътя пред гражданските организации към ефективно включване в процеса по прилагане на АИИ. За тази цел ще са необходими както изграждане на капацитет за подобен вид дейности у НПО, така и наблюдение над публичните бази данни в ЕС с оглед своевременно констатиране на пропуски при вече идентифицираните високорискови ИИ системи или нарушения на забранените практики в областта на ИИ.
   Освен с административно финансиране за изграждане на този капацитет и за провеждане на подобни изследвания, пред донорите се открива възможност за съдействие в посока изграждане на връзки между НПО

[18] Европейският център за нестопанско право (ECNL) е неправителствена организация в обществена полза, базирана в Хага, Нидерландия, която работи за овластяване на гражданското общество чрез създаване на благоприятни правни и политически рамки.
[19] Пара. 150 от преамбюла; чл. 67.
[20] Пара. 151 и 163 от преамбюла; чл. 68.

сектора и академията и идентифициране на граждански активни ИИ експерти професионалисти.

3. **Застъпничество**

Всяко добро застъпничество се гради на предварително предприетите мерки по препоръки едно и две – координация и изследвания. На европейско и национално ниво приоритетите са различни, като бихме обърнали внимание върху следните:

- Ниво ЕС: Изработване на такива насоки (guidelines) относно забранените практики и високорисковите системи, които са съобразени с и вземат предвид основните права;
- Ниво ЕС: изработване на Кодекс за поведение относно ИИ с общо предназначение и стимулиране изработването на бланка за Оценката на въздействието върху основните права;
- Национално ниво: въвеждане на строго ограничаване върху дистанционната биометрична идентификация; застъпничество за приемане на национално законодателство за гарантиране на основните права във връзка с национална сигурност, ИИ в правоохранителната дейност и изпълнение и миграцията; контрол над работата на надзорните органи на местно ниво и над Европейския надзорен орган по защита на данните да предоставят отговори на ползвалите механизма за подаване на жалба засегнати лица.

Отвъд финансовата подкрепа за ангажираните със застъпничество НПО, донорите биха могли да съдействат по тази препоръка с подкрепа към гражданските организации за мониториране на сформирането на националните органи и чрез възлагане на изследване на всички правоприлагащи структури на местно ниво, свързани с АИИ.

4. **Стратегически съдебни дела**

Предвид ограничените възможности за противопоставяне на изключението „национална сигурност“ и за това забраната на дистанционна биометрична идентификация да бъде действително абсолютна, ЕЦНП допуска, че стратегически съдебни дела ще се концентрират около забранените практики в областта на ИИ. А за провеждане на успешни стратегически съдебни дела от съществено значение ще са и предварителните проучвания.

По тази препоръка донорите биха могли да подкрепят правозащитните граждански организации чрез поддържане на условия за координация между

ангажираните НПО, идентифициране на правни експерти, които да оказват съдействие и чрез финансиране за провеждане на такива дела.

5. **Кампании и създаване на движения**
   Освен вече съществуващите кампании във връзка с ИИ (Reclaim Your Face Campaign), съществена роля биха изиграли и новосъздавани кампании и движения, особено в държави, в които има предприети ходове за приемане на законодателство за дистанционна биометрична идентификация.
   И по тази препоръка донорите биха могли да осигуряват финансиране, съдействие за осъществяване на връзки и координация между граждански организации от различни държави членки.

Бихме допълнили този списък с интересна възможност, която се открива пред правозащитните организации от гражданския сектор, а именно грамотността в областта на ИИ[21]. Гражданските организации работят с целия спектър групи в обществото и познават техните нужди и казуси. Могат да допуснат какви възможности е нужно да открие пред тях ползването на ИИ системи, съответно и да предвидят потенциалните рискове пред потенциално засегнатите лица. В този смисъл ние, организациите на гражданското общество и гражданските активисти, можем да бъдем стабилен партньор в процеса по създаване на грамотността в областта на ИИ, за да може риск-базираният наратив да се смекчи и да изградим общи стратегии на основа защита на човешките права в дигитална ИИ среда.

[21] Пара. 20 от преамбюла, чл. 2, т. 56 и чл. 4.

ОБОБЩЕНИЕ

Сроковете за изпълнение на задълженията по Регламента вече текат: до 2 ноември 2024 *г. „всяка държава членка определя публичните органи или структури, посочени в параграф 1“*, а именно органите за защита на основните права по чл. 77 от Регламента. Предвид предстоящата времева линия за влизане в сила на различни части от АИИ, сега е моментът подготовката на гражданското общество. Под гражданско общество следва да се разбира възможно най-широкият спектър лица: активисти, граждански организации, неформални групи, особено представляващите обществения интерес и работещите в обществена полза. В резултат от общи, координирани и проактивни усилия можем да изградим капацитет и способности, които са съществени за провеждане на правилните застъпнически кампании така, че АИИ да бъде правилно прилаган в условия на вече установената парадигма на основните права на човека.