DOI 10.69085/si20251075

ВИСОКОРИСКОВИ AI СИСТЕМИ – СЪЩНОСТ И ИЗИСКВАНИЯ

Гл. ас. д-р Катя Владимирова
Юридически факултет
Университет за национално и световно стопанство

Резюме: *През месец юни 2024 година Съветът на Европа прие Регламент (ЕС) 2024/1689 за установяване на хармонизирани правила относно изкуствения интелект. Той поставя началото на първата правна регламентация относно ИИ и има за цел да преодолее притесненията и заплахите във взаимоотношенията между хората и ИИ. В него за първи път са регламентирани четири системи за ИИ, като в зависимост от техния вид са въведени различни изисквания за тях. Самото обособяване на различните видове системи за ИИ е извършено на базата на риска, който носи съответната система за обществото. Така системите на ИИ се разделят на системи с ИИ, представляващи явна заплаха за хората; системи с ИИ, представляващи висок риск; системи с ИИ с ограничен риск и системи с ИИ с минимален риск.*

Настоящото изложение има за цел да разгледа високорисковите AI системи и тяхната правна регламентация. Те представляват потенциално висок риск за правата и свободите на хората, поради което са подчинени на строга регламентация.

Ключови думи*: Регламент за ИИ, високорискови системи с ИИ, изкуствен интелект*

HIGH-RISK AI SYSTEMS – ESSECE AND REQUIREMENTS

Assis. Prof. Katia Vladimirova, PhD
Faculty of Law
University of National and World Economy

Abstract: *In June 2024, the Council of Europe adopted Regulation (EU) 2024/1689 on establishing harmonized rules on artificial intelligence, or the so-called "The AI Act." It marks the beginning of the first legal regulation on AI and aims to overcome concerns and threats in the relationship between humans and AI. In it for the first time, four AI systems are regulated, and depending on their type, different requirements have been introduced for them. The very differentiation of different types of AI systems is done on the basis of the risk that the respective system brings to society. Thus, AI systems are divided into AI systems that pose a clear threat to humans, AI systems that pose a high risk, AI systems with limited risk, and AI systems with minimal risk.*

This presentation aims to examine high-risk AI systems and their legal regulation. They pose a potentially high risk to people's rights and freedoms, which is why they are subject to strict regulation.

Keywords: *AI Act, high-risk AI systems, Artificial Intelligence*

През месец юни 2024 г. Съветът на Европа прие Регламент (ЕС) 2024/1689 за установяване на хармонизирани правила относно изкуствения интелект. Той пос-

тавя началото на първата правна регламентация относно ИИ и има за цел да преодолее притесненията и заплахите във взаимоотношенията между хората и ИИ[1, 2].

Регламентът за ИИ ще влезе поетапно в сила, като това ще стане в период от три години, но през този период от време е необходимо разработките, засягащи системите за ИИ, да бъдат съобразени с новите правила, така че при настъпване на съответните срокове бизнесът да бъде изцяло подготвен в прилагането на Регламента. Само така биха могли да се създадат устойчиви стандарти в разработването и използването на системите за ИИ.

В Регламента за първи път е дадено определение на понятието „система на изкуствен интелект", като тя е определена като „машинно базирана система, която е проектирана да работи с различни нива на автономност, която може да прояви адаптивност след внедряването си и която с явна или подразбираща се цел, въз основа на въведените в нея входящи данни, извежда начина на генериране на резултати като прогнози, съдържание, препоръки или решения, които могат да окажат влияние върху физическа или виртуална среда"[3].

Разграничени са четири системи за ИИ, като в зависимост от техния вид са въведени различни правила за доставчиците и внедрителите. Самото обособяване на различните видове системи за ИИ е извършено на базата на риска, който носи съответната система за обществото.

Така системите за ИИ се разделят на системи на ИИ, представляващи явна заплаха за хората; системи с ИИ, представляващи висок риск; системи с ИИ с ограничен риск и системи с ИИ с минимален риск.

Първият вид системи, представляващи явна заплаха за хората, са изцяло забранени, останалите три с висок риск, с ограничен риск и с минимален риск, могат

---

[1] Навлизането на ИИ в живота на хората доведе до множество проблеми и опасности. Така например грешка в алгоритъма за търговия на Knight Capital доведе до загуби на $440 милиона USD за 30 минути /https://www.henricodolfing.com/2019/06/project-failure-case-study-knight-capital.html/

Жители на щата Мичиган бяха неправомерно обвинени в измама от система за ИИ, използвана от държавата, което доведе до изплащането от щата на обезщетение в размер на 20 млн. щатски долара /https://www.michigan.gov/ag/news/press-releases/2022/10/20/som-settlement-of-civil-rights-class-action-alleging-false-accusations-of-unemployment-fraud/

В Нидерландия в резултат на използването на алгоритъм за откриване на предполагаеми измами с обезщетения бяха засегнати над 10 000 души /https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms// и др.

[2] Повече за въздействието на ИИ виж Bughin, J.; J. Seong; J. Manyika; M. Chui; R. Joshi; „Notes From the AI Frontier: Modelling the Impact of AI on the World Economy," McKinsey Global Institute, 4 September 2018, https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy; Brundage, M. et al.; „The Malicious Use of Artificial Intelligence," Future of Humanity Institute, February 2018, https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf; Chatterjee, S.; „Impact of AI Regulation on Intention to Use Robots: From Citizens and Government Perspective," *International Journal of Intelligent Unmanned Systems*, December 2019, p.109–11

[3] чл. 2, ал. 1 от Регламент (ЕС) 2024/1689
https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32024R1689

да бъдат разработвани и прилагани при спазване на определени правила, които създават безопасност и сигурност за хората и по този начин минимизират рисковете от тяхната употреба.

Настоящото изложение има за цел да разгледа високорисковите системи с ИИ и тяхната правна регламентация.

Регламента за ИИ възприема концепцията, че високорисковите системи с ИИ представляват потенциално висок риск за правата и свободите на хората, поради което тези системи са подчинени на строга регламентация. По отношение на тях са въведени строги изисквания.

Регламента за ИИ разграничава две групи системи за ИИ като високорискови, а именно:

А. Системи с ИИ, които се считат за високорискови съгласно законодателството на ЕС за хармонизация[4]. За да попадне в тази категория дадена система за ИИ, следва да отговаря на следните две условия: 1. Системата с ИИ е предназначена да се използва като защитен елемент на продукт или самата система с ИИ е продукт, попадащ в обхвата на законодателството на Съюза за хармонизация, посочено в приложение I и II. Продуктът или системата трябва да преминат през оценка на съответствието от трета страна съгласно приложимото законодателство на ЕС за хармонизация.

В тази група се включват на първо място системите на ИИ, които представляват продукт. Като тук следва да се посочи, че една система на ИИ може да представлява едновременно както продукт на ИИ, така и друга форма на продукт. Тези продукти следва да са обхванати от законодателството на Съюза за хармонизация, посочено в приложение към Регламента за ИИ на ЕС. Също така, те следва да бъдат подложени на оценка на съответствието от трета страна, преди да бъдат пуснати на пазара или в действие. Пример за такива продукти са: медицински устройства, индустриални машини, самолети, автомобили и др.

В групата на високорисковите системи с ИИ, които се считат за такива съгласно законодателството на ЕС за хармонизация, попадат и т. нар. „предпазни компоненти на регулирани продукти“. Те представляват предпазни компоненти на даден продукт, които са включени в дадена система на ИИ. При наличието на такива компоненти самата система се класифицира като високорискова само, ако тя би могла да представлява опасност за здравето, безопасността и живота на хората. По подобие на предходната група и тук е необходимо даденият продукт, от който е част компонентът, да е обхванат от законодателството на Съюза за хармонизация и да бъде подложен на оценка на съответствието от трета страна, преди да бъде пуснат на

[4] Виж член 6, параграф 1, и Приложение I от Закона за ИИ
https://eur-lex.europa.eu/legal-content/bg/TXT/?uri=CELEX%3A32024R1689

пазара или в експлоатация в ЕС, съгласно това законодателство. Като примери за такива компоненти бихме могли да посочим различните предпазни компоненти за лична помощ на инвалиди; предпазни компоненти в медицински изделия; предпазни компоненти при роботи за лична помощ; предпазни компоненти за железопътна инфраструктура, асансьори или уреди и др. подобни.

Ако дадена система на ИИ не е компонент за безопасност на продукт, то тя няма да попадне сред високорисковите системи. Например, система с ИИ в автомобил, избираща музиката в него. Тази система не е високорискова, тъй като евентуално проблеми с нея няма да доведат до риск за здравето и безопасността на хората.

Б. Втората група високорискови системи са тези, които отговарят на описанието на някоя от системите с изкуствен интелект, изброени в приложение III към Закона за изкуствен интелект на ЕС.

Списъкът обхваща системи с ИИ, използвани в осем различни специфични отрасли, а именно: биометрия, критична инфраструктура, образование, заетост, достъп до основни услуги, правоохранителни органи, миграция, правораздаване и демократични процеси.

1. Първата група обхваща системите за ИИ, които извършват обработката на биометрични данни. Това са системи за идентифициране на физически лица без тяхно участие. Обикновено идентифицирането се осъществява на база съществуващи биометрични данни – например за лице, височина и т. н.

Следва да се има предвид, че по-голяма част от системите за ИИ, обработващи биометрични данни, са изцяло забранени от Регламента за ИИ. Така например, абсолютно забранени са системите с ИИ, използващи биометрични данни, които имат за цел да съберат или да анализират данни относно раса, политически възгледи, членство в профсъюзи, религиозни или философски вярвания, сексуален живот или сексуална ориентация. Също така, забранени са и системи за ИИ, които създават или обработват бази данни за разпознаване на лица чрез нецеленасочено изтриване на изображения на лица от интернет или записи.

Като високорискови са определени системите за ИИ за дистанционна биометрична идентификация, системите за ИИ, предназначени да се използват за биометрично категоризиране въз основа на чувствителни или защитени признаци и системи с ИИ, предназначени за разпознаване на емоции.

Не са високорискови системи с ИИ, които включват обработка на биометрични данни, ако те са предназначени единствено за удостоверяване и потвърждаване на самоличност, като част от приложение за лице на мобилен телефон.

Също така, от високорисковите системи са изключени биометричните системи с ИИ, които са предназначени да бъдат използвани единствено и само в киберсигурността и защитата на личните данни.

2. Следващата група високорискови системи, съгласно приложение III, е т. нар. „критична инфраструктура“. Тук се включват системи с ИИ, предназначени да се използват като компоненти за безопасност при управлението и експлоатацията на критична цифрова инфраструктура, а именно: в движението по пътищата, водоснабдяването, газоснабдяването, отоплението, електроснабдяването и др. Тук биха могли да попаднат и системи за контрол на налягането на водата, противопожарни аларми и др. подобни. В мотивите на Регламента за изкуствения интелект включването на тази група се обосновава с възможността при повреди и аварии на тези системи да се изложат на риск животът и здравето на големи групи хора и да настъпят смущения в нормалния им живот.

3. Третата сфера, определена като рискова, е образованието. Тази група е включена в Приложение III на високорисковите системи, тъй като отклонения в нея могат да засегнат правото на достъп и избор на образование на всеки един от нас. Също така, могат да доведат до дискриминация, обоснована на пол, възраст, етническа и социална ориентация. Тази група най-общо обхваща четири случая, а именно:

- системи с ИИ, чрез които се определя достъпът до прием или насочване на физическо лице към образованието;
- предназначени да бъдат използвани за оценяване на учебните резултати, включително когато тези резултати се използват за направляване на учебния процес на физически лица;
- системи с ИИ, предназначени да се използват за оценка на подходящото ниво на образование;
- системи с ИИ, предназначени да бъдат използвани за определяне на достъпа до приема в или насочването на физически лица към институции на всички нива на образованието и професионалното обучение;
- системи с ИИ, предназначени да се използват за наблюдение и откриване на забранено поведение на учащите по време на изпити.

4. Четвъртата високорискова сфера е заетостта.

Тези системи са включени в Приложението поради обстоятелството, че могат да доведат до нарушаване на основни права на гражданите, а така също и да повлияят на взимането на решения и на бъдещата кариера на физическите лица. Тук се включват системите с ИИ, предназначени да бъдат използвани за набиране и подбор на персонал и системите с ИИ, използвани за вземане на решения във връзка с полагането на труд, разпределяне на задачите и др.

5. Следващата група високорискови системи за достъп до основни услуги – както частни, така и публични, са системи, които могат да окажат неблагоприятно влияние върху благосъстоянието на хората и да нарушат техни основни права, като

право на човешко достойнство, социална защита и др. Те се разделят на няколко подгрупи:

- системи с ИИ, предназначени да бъдат използвани от публични органи или от името на публични органи за оценка на допустимостта на физически лица за получаване на основно обществено подпомагане и услуги;
- системи с ИИ, включително услуги в областта на здравеопазването, както и за отпускане, намаляване, прекратяване или възстановяване на такова подпомагане и услуги;
- системи с ИИ, предназначени да се използват за оценка на риска и ценообразуване по отношение на физически лица в случай на животозастраховане и здравно застраховане;
- системи с ИИ, предназначени за оценка и класифициране на спешни повиквания от физически лица, включително полицията, пожарната и медицинската помощ, както и на системите за разпределяне на пациенти за спешна здравна помощ.

6. На шесто място са системите с ИИ в правоохранителната дейност.

По подобие на биометричните системи с ИИ и при тези са налице такива, които са квалифицирани като абсолютно забранени, като например системи, използвани за дистанционно управление в реално време на биометрична идентификация на публично достъпни места с цел принудително изпълнение[5].

Извън забранените системи с ИИ в правоохранителната дейност – всички останали се квалифицират като високорискови. Това е така, тъй като тези системи могат да засегнат правото на защита на човека, правото на справедлив процес, да нарушат принципа за невинност в наказателното преследване и др. Тук се включват: системи за оценка на риска дадено лице да стане жертва на престъпление; системи в подкрепа на полиграфи и др. подобни инструменти; системи за оценка на надеждността на доказателства в хода на наказателното преследване; системи за оценка на риска на дадено физическо лице да извърши престъпление и др.

7. Седмата група случаи е свързана с миграцията и граничния контрол.

Тази група е създадена поради обстоятелството, че обикновено тези системи засягат силно уязвими групи от обществото. Това са хора, които обикновено са в неравностойно, тежко положение и те нямат възможност да защитават сами своите права. В повечето случаи тези хора разчитат на съответните държавни органи. Именно поради това се налага те да бъдат защитени от евентуални злоупотреби.

Тук се включват: системи за оценка на риск, включително риск за сигурността, риск от незаконна миграция или риск за здравето, породен от физическо лице, което възнамерява да влезе или е влязло на територията на държава-членка; системи

[5] От посочената забрана има изключение – виж чл. 5, параграф 2 от Закона за ИИ.

за подпомагане разглеждането на молби за убежище, визи, разрешения за пребиваване; системи за откриване, разпознаване или установяване на самоличността на физически лица, с изключение на проверката на документи за пътуване и др.

Не попадат в графата високорискови системи с ИИ системите, използвани само за проверка на документи за пътуване на дадено лице през граничните пунктове.

8. Последната група, посочена в Приложение III от Регламента, обхваща т. нар. „правораздаване и демократични процеси“. Тук се включват системи с ИИ, предназначени да бъдат използвани от съдебните органи за разрешаване на спорове, да им помогнат в тълкуването на факти и обстоятелства. Също така, тук се включват и системи с ИИ, предназначени да повлияят на резултат от изборите, на поведението на хората при гласуване и др.

Независимо от обстоятелството, че някои системи попадат в така изброените, те няма да бъдат считани за високорискови и по отношение на тях няма да се прилага Законът за ИИ. Например, не представляват високорискови системи с ИИ тези, които са предназначени за използване изключително за военни цели, отбрана, национална сигурност. Не представляват високорискови системи с ИИ и тези, които са разработени единствено с научно изследване, изследователска, тестова или развойна дейност.

Не само това – не представлява високорискова система с ИИ тази, която „не представлява значителен риск от увреждане на здравето, безопасността или основните права на физическите лица, включително не влияе съществено на резултата от вземането на решения“[6].

За да се определи една система като значително рискова е необходимо да е налице поне едно от следните обстоятелства:

- системата с AI е предназначена да изпълнява тясна процедурна задача;
- системата AI е предназначена да подобри резултата от предварително завършена човешка дейност;
- системата AI е предназначена да подобри резултата от предварително завършена човешка дейност;
- системата с ИИ е предназначена да изпълнява подготвителна задача с оглед на извършването на оценка, която е от значение за целите на случаите на използване, посочени в приложение III.

Така например, ако имаме една система с ИИ за избор на музика в автомобил. Тя представлява компонент от продукт, но този компонент не е свързан с безопасност за

[6] Виж чл. 6, параграф 3 от Закона за ИИ, https://eur-lex.europa.eu/legal-content/bg/TXT/?uri=CELEX%3A32024R1689

живота и здравето на хората. Тази система не е високорискова, тъй като евентуално проблеми с нея няма да доведат до риск за здравето и безопасността на хората.

В същото време в чл. 6, параграф 3 е посочено, че независимо дали отговаря на посочените по-горе критерии, всяка една система с ИИ автоматично ще се счита за система с изкуствен интелект с висок риск, ако системата извършва профилиране на лица.

Със Регламента за ИИ се въвеждат определени изисквания, на които следва да отговарят високорискови системи с ИИ. Тези изисквания са свързани с управлението на риска, качеството на данните, прозрачността, човешкия контрол и др. подобни. Тяхната регламентация се съдържа в разпоредбите на чл. 8 до чл. 15 вкл. от Регламента за ИИ. Като тези изисквания следва да бъдат съобразени с предназначението на системата с ИИ, както и с общоприетите съвременни технически постижения в областта на ИИ.

Когато даден продукт съдържа система с ИИ и тя попада под регламентацията на Закона за ИИ, към продукта се прилагат както изискванията на Закона за ИИ, така и всички останали изисквания съгласно законодателството.

Въвеждат се следните изисквания, на които трябва да отговарят високорисковите системите с ИИ:

1. Система за управление на риска

За всяка една високорискова система с ИИ следва да бъда изградена и приложена система за управление на риска. Системата за управление на риска представлява непрекъснат цикличен процес, планиран и протичащ през целия жизнен цикъл на високорисковата система с ИИ и изискващ редовен и систематичен преглед и актуализиране. Тя включва следните елементи: установяване и анализ на известните и разумно предвидимите рискове, които високорисковата система с ИИ може да породи по отношение на здравето, безопасността и основните права, когато високорисковата система с ИИ се използва в съответствие с предназначението си; прогноза и оценка на рисковете при използване на системата по предназначение и при предвидима неправилна експлоатация; анализ на данните от мониторинг след пускане в употреба на системата; приемане на подходящи и целенасочени мерки за управление на риска.

Системата за управление на риска следва да дава възможност за отчитане на техническите познания, опит, образование и др. подобни, които се очакват от доставчиците и внедрителите на системата с ИИ.

Мерките за управление на риска трябва да са такива, че съответният остатъчен риск, свързан с всяка опасност, да бъде приемлив.

Начинът на оценка на риска повдига множество въпроси и проблеми. На първо място, възниква въпросът какво представлява понятието „остатъчен риск“.

Би могло да се каже, че остатъчният риск е рискът, който остава след прилагането на мерки за намаляване на риска. За да определят, обаче, размера на остатъчния риск, доставчиците на високорискови системи с ИИ ще трябва да претеглят рисковете и ползите. Начинът на претегляне е неясен. Липсват каквито и да е критерии. В правната норма не е посочено нищо, а липсва и практика по въпроса.[7,8]

2. Управление на данните

Следващото изискване на закона е свързано с управление на т. нар. „висококачествени данни“. То означава, че при разработване на системата с ИИ следва да се гарантира, че наборът от данни за обучение, тестване и валидиране на системата е подходящ, представителен и без грешка. Могат да бъдат използвани всякакви методи, като от значение за Регламента е да бъдат документирани практиките за управление на данни, както и процесите по подготовка, валидиране и наблюдение.

3. Техническа документация

Тя играе важна роля за гарантиране на съответствието с нормативните изисквания на високорисковите системите с ИИ. В същото време чрез документацията се постига прозрачност в процесите. Съгласно чл. 11, параграф 1 от Регламента за ИИ техническата документация на високорисковата система с ИИ следва да бъде изготвена, преди тя да бъде пусната в действие. През целия период на работа на системата нейната документация следва да бъде поддържана актуална. Тя да съдържа най-малко данни, посочени в приложение IV от Регламента за ИИ, като например: общо описание на системата, което включва име, предназначение и др., подробно описание на елементите на системата, подробна информация за мониторинга и т. н.

Предприятията сами ще избират начина на представяне на посочената техническа документация. Съгласно NLF[9,10], европейското законодателство не определя директно техническите спецификации, а по-скоро определя „съществените изиск-

[7] Повече виж Shuett, J. Risk Management in the Artificial Intelligence Act, Cambridge University Press: 08 February 2023 – https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/risk-management-in-the-artificial-intelligence-act/2E4D5707E65EFB3251A76E288BA74068#fn120

[8] Fraser, H., & Bello y Villarino, J.-M. (2021). *Where residual risks reside: A comparative approach to Art 9(4) of the European Union's proposed AI Regulation.*
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3960461
Fraser, H., & Bello y Villarino, J.-M. (2023). Acceptable risks in Europe's proposed AI Act: Reasonableness and other principles for deciding how much risk management is enough. *European Journal of Risk Regulation*, 1–16.
https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/acceptable-risks-in-europes-proposed-ai-act-reasonableness-and-other-principles-for-deciding-how-much-risk-management-is-enough/97720BC04BF5F43721392FC23BFF4B2E

[9] NLF или Нова законодателна рамка, представлява рамка от общи принципи и правила, която има за цел да направи законодателството на стоки на единния европейски пазар по-ефективно, по-ясно и по- последователно чрез установяване на обща правна рамка на продуктите. NLF обхваща 23 директиви и регламента.

[10] https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/sec/2011/1375/COM_SEC(2011)1375_EN.pdf

вания“, на които трябва да отговарят продуктите, оставяйки на доставчиците и производителите сами да решат как да постигнат техническите изисквания.

Предприятията ще имат възможност да се възползват и от т. нар. „опростен формуляр“ за техническа документация, който ще бъде съобразен с нуждите на малките и средните предприятия. Предстои той да бъде изготвен от Комисията[11].

4. Поддържане на регистри

Въвежда се изискване високорисковата система за ИИ да има възможност да записва автоматично събитията в системата. По този начин се гарантира проследимостта на всички събития. Създават се предпоставки да бъдат видени евентуални проблеми и рискове в системата, след като тя бъде пусната в производство. Предвидено е, че за високорисковите системи в Приложение III записите следва да осигуряват най-малко записване на времето на всяко ползване; входящите данни, за които търсенето е довело до съвпадение и др.[12]

5. Човешки контрол

Той представлява създаването на възможност за упражняване на ефективен контрол от човек, когато дадената високорискова система се използва. Този контрол има за цел да предотврати или сведе до минимум рисковете за живота, здравето и безопасността на човек или да предотврати засягането на основни човешки права. Контролът означава, че е необходимо винаги да е налице отговорно лице, което да следи работата на системата и при необходимост да предприеме мерки за преодоляване на възникнали проблеми.

6. Прозрачност

Прозрачността означава достъп до всяка информация, свързана с системата с ИИ, като тази информация следва да бъде предоставена на лесен и разбираем език. Чрез нея се цели да се създаде прозрачен режим на технологиите за изкуствен интелект, който да позволи на юридическите лица да разработват и внедряват отговорно ИИ, а на физическите лица да разбират дизайна и да използват безопасно системата.

Високорисковите системи с ИИ следва да се проектират и разработват, така че да се гарантира, че функционирането им ще бъде достатъчно прозрачно. Също така, прозрачността предполага да се създадат условия внедрителите да тълкуват резултатите, получени от системата, и да ги използват по подходящ начин. За тази цел високорисковите системи с ИИ задължително следва да бъдат съпътствани с

[11] Повече за техническата документация вж. Gornet, M., Maxwell W. The European approach to regulating AI through technical standards 16 Jul 2024
https://policyreview.info/articles/analysis/regulating-ai-through-technical-standards

[12] Виж чл. 12, параграф 3 от Закона за ИИ
https://eur-lex.europa.eu/legal-content/bg/TXT/?uri=CELEX%3A32024R1689

инструкции за употреба, като последните могат да бъдат предоставени в цифров или в друг формат.

7. Последното изискване за високорисковите системи е свързано със създаване на условия за точност, надеждност и киберсигурност

Те играят важна роля във връзка с производителността и сигурността на системите с ИИ. Чрез тях се постига сигурност относно функционирането на системите през целия им живот. За тази цел следва да се обявяват нивата на точност и техните показатели в придружаващата инструкция на системата с ИИ. Създават се и се предприемат мерки за предотвратяване на грешки, недостатъци и несъответствия в системите.

Въпреки положителния аспект на тази разпоредба, следва да отбележим, че тя не е достатъчно пълна по отношение на мерките за киберсигурност. Разпоредбата се фокусира върху изграждане на сигурност при обучение на модела. Не е обърнато внимание на проблемите относно сигурността по време на внедряване на модела. На практика, системите с ИИ, които продължават да се обучават, след като са пуснати на пазара, не са обхванати от защитни механизми[13].

Предвидените по-горе изисквания към високорисковите системи за ИИ обхващат като цяло всички проблемни области при разработването и внедряването на високорискови системи с ИИ. Неясно остава към този момент доколко тези изисквания ще могат да бъдат приложени в практиката. Прилагането им се затруднява и от използваните до голяма степен общи формулировки от законодателя, като например: „доколкото е технически осъществимо“; „където е подходящо“; „общоприети съвременни технически постижения“; „разумно предвидимите рискове“ и др. За всички тези понятия се очаква да бъде необходимо допълнително тълкуване било от Комисията или в процеса на самото правоприлагане.

Прави впечатление и въведената сред изискванията обширна документация, която поставя въпроса доколко бизнесът ще се справи с нейното въвеждане и няма ли да възпрепятства развитието на тези технологии. Обширната документация и нейната проверка ще наложат и създаването на обширен административен апарат от служители, които би следвало да притежават съответната квалификация в сферата на ИИ, което поне за нашата страна трудно ще бъде постигнато на този етап.

Въпреки посочените недостатъци, считам че приетите изисквания за високорисковите системи с ИИ са добра стъпка напред в гарантиране на правата и свободите на хората и създаването на условия за устойчиво регламентиране на взаимоотношенията между хората и ИИ.

[13] Виж Casarosa, F. The risk of unreliable standards: Cybersecurity and the Artificial Intelligence *Actq Scuola Superiore Sant'Anna, Pisa, Italyq 29 Feb 2024*
https://policyreview.info/articles/news/cybersecurity-and-artificial-intelligence-act/1742