КОМИСИЯ ЗА ЗАЩИТА
НА ЛИЧНИТЕ ДАННИ

СЪВРЕМЕННИ ЗАПЛАХИ И ПРЕДИЗВИКАТЕЛСТВА ПРЕД ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ В КОНТЕКСТА НА ТЕНДЕНЦИИТЕ В РАЗВИТИЕТО НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ И НОВИТЕ ТЕХНОЛОГИИ ЗА ЛИЦЕВО РАЗПОЗНАВАНЕ

Настоящият информационен материал има за цел да подпомогне практическото прилагане на изискванията за защита на личните данни в контекста на тенденциите в развитието на изкуствения интелект и новите технологии за лицево разпознаване. Същият няма задължителен характер и не претендира за изчерпателност.

1. Същност, определение и съдържание

Изкуствен интелект

Изкуственият интелект (ИИ) е набор от технологии, които съчетават данни, алгоритми и изчислителна мощ, и има потенциал да трансформира основни сектори на индустрията, услугите и обществото като цяло. Според възприетата дефиниция системите с изкуствен интелект са софтуерни (и евентуално хардуерни) системи, проектирани от хората, които, при зададена сложна цел, действат във физическото или цифровото измерение, възприемайки средата си чрез събиране на данни, интерпретиране на събраните структурирани или неструктурирани данни, разсъждавайки върху знанието или обработвайки информацията, извлечена от тези данни, в резултат на което вземат решения за най-добрите действия, които водят до постигане на поставената цел.

Теорията на изкуствения интелект се основава на хипотезата, че основно човешко качество като интелигентността, може да бъде описано с достоверна точност, така че да бъде симулирано от машина. Затова изкуственият интелект може да бъде дефиниран като способността на една машина да демонстрира способности, присъщи за хората – да разсъждава, да се учи, да планира или да твори. Говорим за ИИ, когато технически системи наблюдават околната си среда, получават данни (които са подготвени от другиго или които набират сами), преработват ги и извършват действия, свързани с постигането на конкретна цел.

Изкуственият интелект е наука за концепциите, методите и средствата за създаване на интелигентни компютърни програми, както и измерване, и изследване на естествения интелект чрез компютърни системи с цел техното подобряване.

Лицево разпознаване

В духа на динамичното развитие на технологиите, важна роля оказват системите за разпознаване на лица или т.н. „лицево разпознаване“. Тъй като системите за лицево разпознаване включват измерване на физиологичните характеристики на човека, те се категоризират като „биометрични“.

Лицевото разпознаване представлява технология, способна да съпостави човешко лице от цифрово изображение или видеокадър с база данни от лица. Технологията обикновено се използва за удостоверяване автентичността на потребителите при използване на услуги чрез точно определяне и измерване на черти на лицето от дадено изображение или видеокадър. Задачата на системите за лицево разпознаване е да идентифицират човешко лице, което е триизмерно и променя външния си вид, въз основа на неговото двуизмерно изображение.

За да изпълнят тази изчислителна задача, системите за лицево разпознаване изпълняват четири стъпки. В първата стъпка се сегментира лицето от фона на изображението. Във втората стъпка сегментираното изображение на лицето се подравнява, за да отчете позата на лицето, размера на изображението и фотографските свойства. Целта на процеса на подравняване е да даде възможност за точната локализация на чертите на лицето в третата стъпка, в която се извличат характеристиките на лицето. Така установеният вектор на характеристиките на лицето след това, в четвъртата стъпка, се съпоставя с база данни от лица и се идентифицира.

2. Ползи от развитието на изкуствения интелект и новите технологии за лицево разпознаване

За съвременните програми изкуственият интелект е важен елемент на информационните технологии, използван за разрешаване на някои от най-трудните задачи в областта на информатиката. Изследванията в областта на изкуствения интелект са силно специализирани и обособени в няколко подобласти, които според някои критици в много случаи не успяват да взаимодействат ефективно. Общи за повечето подобласти на изследванията на ИИ са задачи като възможността за разсъждение, обучение и подобряване на ИИ чрез обучение, възприемане, планиране, общуване, а също и способността за движение, и управление на движението на обекти с ИИ като коли и други. Системите с изкуствен интелект са способни да адаптират поведението си до известна степен, като анализират резултатите от предишни действия и работят автономно. Изкуственият интелект е интелектът, демонстриран от компютри, това е и науката за концепциите в компютърната наука, които правят възможно компютрите да извършват задачи, които могат да бъдат разглеждани като интелигентни.

Изкуственият интелект при поставяне на задача има способност да анализира обкръжаващата го среда и да предприема действия, които увеличават възможността за постигане на определени цели. Изучаването на възможностите за създаване на такива програми или устройства, наричани „интелигенти агенти“, е предмет на обособен дял от информатиката. Изкуственият интелект е един от основните двигатели на цифровата трансформация в Европа и значим фактор за осигуряване на конкурентоспособността на европейската икономика и високо качество на живот.

В основата на съвременните системи за видеонаблюдение се използват алгоритми и процеси на изкуствения интелект, които създават условия за автоматизирано вземане на решения с важни последици за субектите на данни. Такова е лицевото разпознаване. От създаването си системите за лицево разпознаване намират широко приложение в технологиите, една от които са системите за видеонаблюдение, които масово навлизат във всички сфери на живота и непрекъснато се използват поради тяхната достъпност и приложимост. Доскоро системите за видеонаблюдение са били приоритет за специални обекти, банкови офиси и големи предприятия, но днес те се използват за охрана на училища, жилищни комплекси, болници, хотели, офиси, магазини и др.

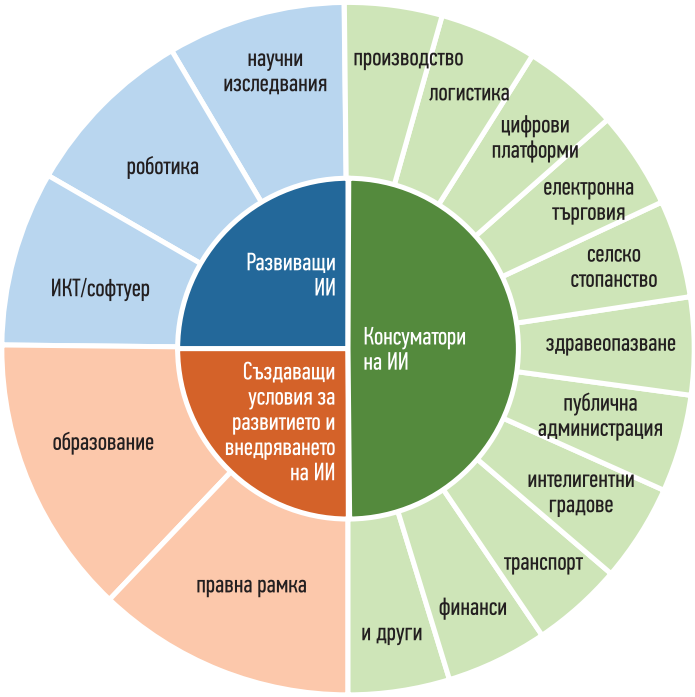
По отношение на създаването и използването на ИИ в различни отрасли основно се открояват три групи сектори, а именно:

- Развиващи изкуствен интелект *(такива са съвременните информационно-комуникационни технологии/софтуер, роботиката и научните изследвания)*;

- Консуматори на изкуствен интелект *(това са всички проявления на съвременния начин на живот, като напр. производство, логистика, цифрови платформи, електронна*

търговия, селско стопанство, публична администрация, здравеопазване, интелигентни градове, транспорт, финанси и др.);

• Създаващи условия за развитието и внедряването на изкуствен интелект *(правна рамка и образование).*



3. Рискове от използването на изкуствения интелект и новите технологии за лицево разпознаване

Развитието на изкуствения интелект и на новите технологии за лицево разпознаване ще доведат до цялостна промяна на парадигмата,

до революционен обрат, който ще постави на преразглеждане основни обществени отношения, лични избори и човешки ценности.

Динамичното развитие на технологиите и все по-широкото използване на различни алгоритми за изкуствен интелект, лицево разпознаване и др., създават възможности за безпрецедентно по обем и дълбочина навлизане в личното пространство и личната неприкосновеност на физическите лица.

Използването на технологиите на изкуствен интелект крие редица потенциални рискове, като непрозрачност на процеса на вземане на решения, нарушаване на личното пространство и употреба на тези технологии за извършване на незаконосъобразни действия. ИИ може да доведе до предубеждения и по този начин до различни форми на дискриминация, основана на пол, раса, цвят на кожата, етнически или социален произход, генетични характеристики, език, религия или убеждения, политически или други мнения, принадлежност към национално малцинство, имотно състояние, рождение, увреждане, възраст или сексуална ориентация.

4. Изисквания, на които трябва да отговорят приложенията с изкуствен интелект

Общоприети са седем ключови изисквания, които приложенията с ИИ трябва да спазват, за да се смятат за надеждни:

Човешки фактор и надзор

Системите с ИИ да не накърняват автономността на човека и да не причиняват други неблагоприятни последствия.

Техническа стабилност и безопасност

Физическата и психическа безопасност на системите с ИИ да бъде проверима на всеки етап от всички засегнати страни.

Управление на данните и неприкосновеност на личния живот

Данните да са изчистени от неточности или грешки и да не отразяват социални предубеждения.

Обяснимост и прозрачност

Да се регистрират и документират както решенията, взети от системите с ИИ, така и целият процес, който е довел до тези решения.

Многообразие, недискриминация и справедливост

Да се гарантира универсален дизайн за равноправен достъп на лицата с увреждания.

Обществено и екологично благополучие

Да се следи социалното въздействие на ИИ, както и устойчивостта и екологичната отговорност на системите с ИИ;

Отчетност

Да се гарантират отговорност и отчетност за системите с ИИ и техните резултати, да се свеждат до минимум потенциалните отрицателни въздействия.

5. Препоръки по отношение използването на изкуствения интелект и новите технологии за лицево разпознаване

Основните изводи и препоръки по отношение на съвременните заплахи и предизвикателства пред защитата на личните данни в контекста на тенденциите в развитието на изкуствения интелект и новите технологии за лицево разпознаване, биха могли да се обобщят в следното:

• В системите с ИИ трябва да се избягват предубеждения, водещи до дискриминация и не трябва да се възпроизвеждат дискриминационни процеси. Тези рискове следва да бъдат взети предвид при разработването на технологии с ИИ, както и при работата с доставчиците на технологии с ИИ, за да се предприемат

мерки за преодоляване на все още съществуващите пропуски, които улесняват дискриминацията.

• Мрежите от взаимосвързани ИИ следва да бъдат защитени и да се предприемат сериозни мерки за предотвратяване на нарушения на сигурността, изтичане на данни, заразяване на данни, кибератаки и злоупотреба с лични данни. Това ще изисква съответните институции както на равнище Европейския съюз, така и на национално равнище да работят заедно и в сътрудничество с крайните потребители на тези технологии. Държавите членки следва да гарантират зачитането на ценностите на ЕС и зачитането на основните права по всяко време, когато разработват и внедряват технологии с ИИ, за да гарантират сигурността и устойчивостта на цифровите си инфраструктури.

• Възможността, осигурявана от тези технологии, за използването на лични данни с цел категоризиране и насочване към определени лица, откриване на уязвимите страни на отделни лица или извличане на полза от точни предвидими знания, трябва да бъде неутрализирана чрез ефективно прилагане на принципите за защита на данните и неприкосновеността на личния живот, като например свеждане на данните до минимум, правото на възражение във връзка с профилирането и контрола върху ползването на данните, правото на получаване на обяснение за решение, основаващо се на автоматизирана обработка, и защита на неприкосновеността на личния живот още на етапа на проектиране на дадена технология, както и чрез прилагане на принципите на пропорционалност, необходимост и ограничение въз основа на строго определени цели, в съответствие с Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните).

• Всяко обработване на лични данни, извършвано в контекста

на разработването, внедряването и използването на ИИ и свързаните с него технологии, включително лични данни, извлечени от нелични данни, и биометрични данни, да се извършва в съответствие с Регламент (ЕС) 2016/679.

• Да се насърчават научноизследователските проекти, насочени към намиране на решения, основаващи се на ИИ и свързаните с него технологии, които имат за цел насърчаване на социалното приобщаване, демокрацията, плурализма, солидарността, справедливостта, равенството и сътрудничеството.

• Всяка нова регулаторна рамка за ИИ, състояща се от правни задължения и етични принципи за разработването, внедряването и използването на изкуствения интелект и свързаните с него технологии, следва да зачита човешкото достойнство, самостоятелността и самоопределянето на личността, да предотвратява вреди, да насърчава справедливостта, приобщаването и прозрачността, да премахва предубедеността и дискриминацията, включително по отношение на малцинствените групи, и да зачита и спазва принципите за ограничаване на отрицателните външни ефекти на използваната технология, за обяснимост на технологиите и гарантиране, че технологиите съществуват, за да служат на хората, а не да ги заменят или да вземат решения вместо тях, като крайната цел е увеличаване на благоденствието на всеки отделен човек.

• ИИ и свързаните с него технологии в областта на правоприлагането и граничния контрол биха могли да подобрят обществената безопасност и сигурност, но също така се нуждаят от всеобхватен и строг обществен контрол и от възможно най-високо равнище на прозрачност по отношение на оценката на риска за отделните приложения, както и от общ преглед за използването на

изкуствения интелект, роботиката и свързаните с тях технологии в областта на правоприлагането и граничния контрол. Тези технологии крият значителни рискове, които трябва да бъдат обмислени подобаващо, като се отчитат възможните неблагоприятни последици за физическите лица, по-специално във връзка с техните права за неприкосновеност на личния живот, защита на личните данни и недискриминация.

• В контекста на широкоразпространената дезинформационна война, подклаждана по-специално от неевропейски участници, технологиите с ИИ могат да окажат неблагоприятно въздействие в етичен план чрез експлоатиране на предубеденост в данните и алгоритмите или чрез преднамерено променяне на данните на ИИ от страна на трета държава, и те биха могли да бъдат изложени също така на други форми на опасна и зловредна манипулация, извършвана по непредвидими начини и водеща до неизмерими последици. Затова е налице все по-належаща необходимост да се продължи с инвестициите в областта на научните изследвания, анализа, иновациите и трансграничния и междусекторен трансфер на знания с цел разработване на технологии с изкуствен интелект, които да са независими от всякакъв вид профилиране, предубеденост и дискриминация, и които да могат да допринасят ефективно за борбата с фалшивите новини и дезинформацията, като същевременно се зачитат неприкосновеността на личните данни и правната рамка на Съюза.

• ИИ не следва никога да замества хората, като решенията, които се основават единствено на автоматизирана обработка и произвеждат правно действие по отношение на физически лица или засягат тези лица в значителна степен, трябва винаги да включват съдържателно оценяване и преценка, извършена от човек.

• Всички технологии с ИИ и свързаните с него технологии, включително софтуерът, алгоритмите и данните, използвани или генерирани от такива технологии, които са разработвани, внедрявани и използвани в ЕС, следва изцяло да зачитат правата на гражданите на неприкосновеност на личния живот и защита на личните данни.

• Използването и събирането на биометрични данни с цел дистанционна идентификация на обществени места, като биометрично разпознаване или разпознаване на лица, носи специфични рискове за основните права и се внедрява или използва единствено от публичните органи на държавите членки за цели от съществен обществен интерес. Тези органи следва да гарантират, че това внедряване или използване е оповестено публично, е пропорционално и целенасочено, ограничено до конкретни цели и места, а също така и по времетраене, в съответствие с правото на Съюза и националното право, по-специално Регламент (ЕС) 2016/679.

6. Ключови аспекти за бъдещи действия

Повишаването на обществената осведоменост относно заплахите и възможностите, които виртуалното пространство създава пред субектите на данни и относно защитата на информационните им права в цифровата ера са от първостепенно значение за надзорните органи по защита на данните. За да се реализира тази амбиция в контекст, в който потоците от данни преминават безпроблемно през границите и дигиталният бизнес достига до клиентите в световен мащаб, следва разработващите системи с изкуствен интелект да станат все по-ефективни в предвиждането, тълкуването и влиянието на подобен напредък в начина на използване на данните, с което да

се изгради доверие, подкрепено от високите стандарти за защита на данните.

Въпреки че Регламент (ЕС) 2016/679 съдържа ефективни решения за правното регулиране на изкуствения интелект и в частност в случаите на обработка на лични данни чрез автоматизирано вземане на решения (член 22), Комисията за защита на личните данни силно препоръчва да се следят тенденциите в европейски план относно границите, в рамките на които е допустимо обработване на лични данни в този контекст. Във връзка с това е необходимо да се отчитат препоръките, становищата и предложенията на Европейската комисия, Европейският парламент, Европейския комитет по защита на данните и Европейския надзорен орган по защита на данните:

- за налагане на мораториум върху масовото наблюдение чрез системи за изкуствен интелект;
- за недопускане на автоматизираното лицево разпознаване на обществени места или за целите на граничния контрол;
- за строги гаранции за физическите лица, когато инструментите на изкуствения интелект се използват в правоприлагането, особено в случаите с прогнозиране на извършители на престъпления;
- за определяне на хармонизирани правила относно изкуствения интелект и за насърчаване разглеждането на проблемите с използването на системи с ИИ, включително използването им от институциите, органите и агенциите на ЕС;
- за изграждане на регулаторна рамка, основаваща се на „етика по подразбиране“ и „етика при проектирането“, която да гарантира, че всеки пуснат в действие ИИ изцяло зачита и спазва законодателството в областта на защитата на личните данни;

• за прилагане на подход, основан на риска, уеднаквен с правната рамка на ЕС в областта на защитата на личните данни, съобразно който се търси пресечната точка и баланса между развитието на технологиите и правата на човека (необходимост и пропорционалност);

• за оценка и намаляване на обществения риск за групите от физически лица;

• за обща забрана върху използването на ИИ за автоматично разпознаване на човешки черти на обществено достъпни места и на някои други употреби на ИИ, които могат да доведат до несправедлива дискриминация, например разпознаване на лица, походка, пръстови отпечатъци, ДНК, глас, натискане на клавиши и други биометрични или поведенчески данни, в какъвто и да било контекст поради изключително високия риск, свързан с дистанционната биометрична идентификация на лица на обществено достъпни места;

• за забрана върху използването на биометрични данни в рамките на системи с ИИ за категоризиране на отделни лица в групи въз основа на етническа принадлежност, пол, политическа или сексуална ориентация или на други основания, при които има забрана на дискриминация;

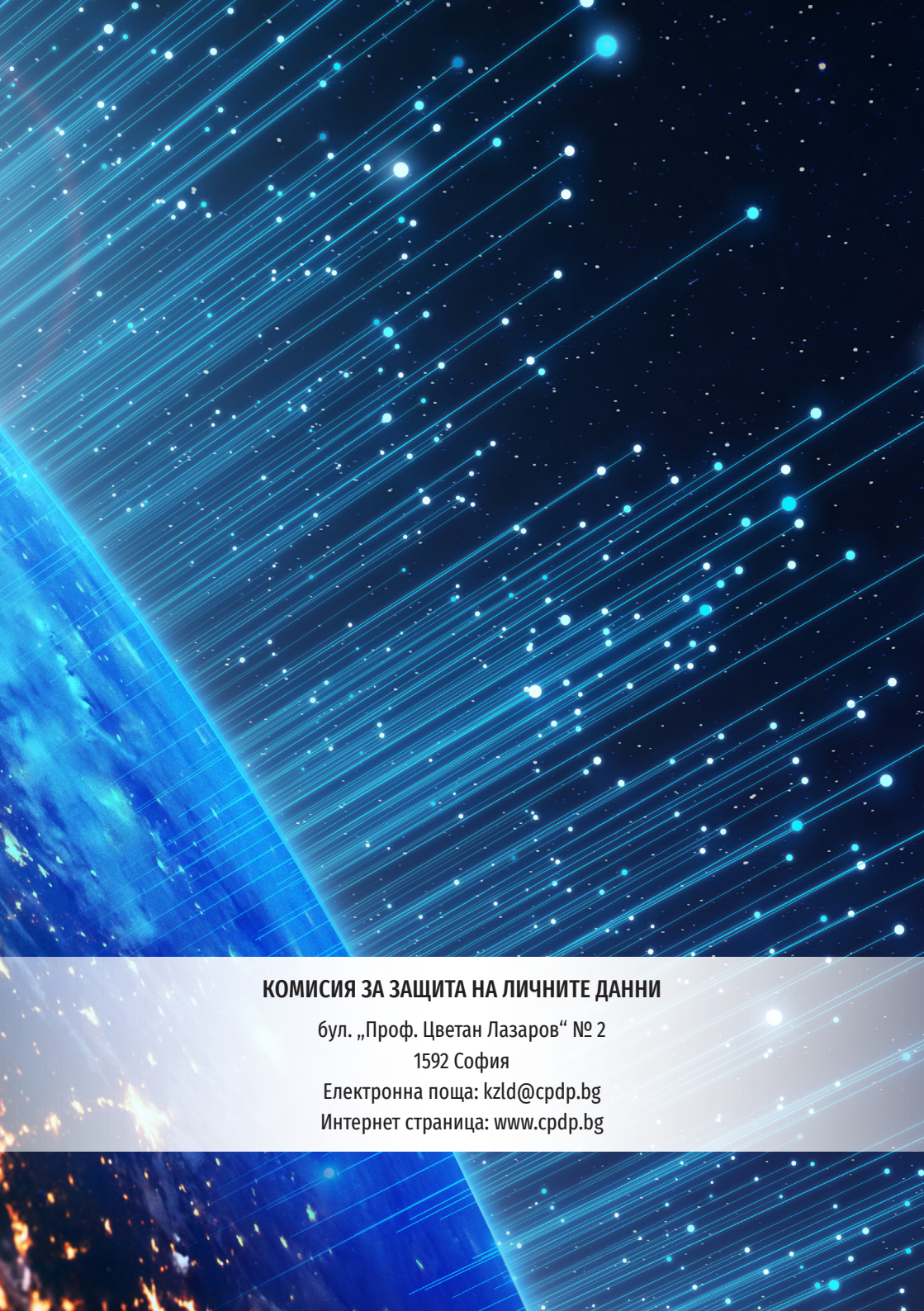
• за забрана върху използването на ИИ за всякакъв вид социална оценка и за съставяне на изводи за емоциите на физически лица (освен в много специфични случаи, например по здравословни причини, когато разпознаването на емоциите е важно).

• разпознаване на човешки черти на обществено достъпни места и на някои други употреби на ИИ, които могат да доведат до несправедлива дискриминация, например разпознаване на лица, походка, пръстови отпечатъци, ДНК, глас, натискане на

клавиши и други биометрични или поведенчески данни, в какъвто и да било контекст поради изключително високия риск, свързан с дистанционната биометрична идентификация на лица на обществено достъпни места;

• за забрана върху използването на биометрични данни в рамките на системи с ИИ за категоризиране на отделни лица в групи въз основа на етническа принадлежност, пол, политическа или сексуална ориентация или на други основания, при които има забрана на дискриминация;

• за забрана върху използването на ИИ за всякакъв вид социална оценка и за съставяне на изводи за емоциите на физически лица (освен в много специфични случаи, например по здравословни причини, когато разпознаването на емоциите е важно).



КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

бул. „Проф. Цветан Лазаров“ № 2
1592 София
Електронна поща: kzld@cpdp.bg
Интернет страница: www.cpdp.bg