ПРАВОТО В ЕПОХАТА НА ЦИФРОВАТА ТРАНСФОРМАЦИЯ: ПРЕДИЗВИКАТЕЛСТВА И ВЪЗМОЖНОСТИ

Сборник доклади

от научна конференция,
19 май 2023 г., НБУ

НОВ БЪЛГАРСКИ УНИВЕРСИТЕТ

ПРАВОТО В ЕПОХАТА НА ЦИФРОВАТА ТРАНСФОРМАЦИЯ: ПРЕДИЗВИКАТЕЛСТВА И ВЪЗМОЖНОСТИ

Поредица
ФОРУМ „ЮРИДИЧЕСКИ ИЗСЛЕДВАНИЯ“
Книга първа

Series
LEGAL RESEARCH FORUM
Book One

ПРАВОТО В ЕПОХАТА НА ЦИФРОВАТА ТРАНСФОРМАЦИЯ: ПРЕДИЗВИКАТЕЛСТВА И ВЪЗМОЖНОСТИ

Сборник доклади
от научна конференция,
19 май 2023 г.,
Нов български университет

Под съставителството и научната редакция на
Деница Топчийска

НОВ
БЪЛГАРСКИ
УНИВЕРСИТЕТ

Форум „Юридически изследвания“, Книга първа

Legal Research Forum, Book One

ISSN 3033-1129 (Print), 3033-1137 (Online)

Правото в епохата на цифровата трансформация: предизвикателства и възможности.
Сборник доклади от научна конференция, 19 май 2023 г., Нов български университет

Съставителство и научна редакция: доц. д-р Деница Топчийска

Рецензент: проф. д-р Веселин Вучков

Коректор: Лора Султанова

ул. „Монтевидео“ 21, 1618 София
www.nbu.bg
www.bookshop.nbu.bg

Печат: „Симолини-94“ ООД

ISBN 978-619-233-336-2 (печатно издание)
978-619-233-337-9 (електронно издание)

Поредица

ФОРУМ „ЮРИДИЧЕСКИ ИЗСЛЕДВАНИЯ“

Книга първа

Поредицата представя резултатите от ежегодните международни и национални научни конференции, организирани от департамент „Право“ на Нов български университет. Всяко издание събира задълбочени изследвания и анализи от водещи учени, практици и млади изследователи, обединени около актуални теми, които отразяват динамиката и предизвикателствата на съвременното правно пространство.

Целта на поредицата е да разшири научния дебат и да стимулира развитието в областта на правото, като насърчи обмена на идеи и знания по широк кръг от теоретични и практически въпроси. Изданията се характеризират с висока степен на методологична прецизност и научна обоснованост, което ги прави ценен ресурс както за академичната общност, така и за практикуващите юристи, студенти и всички заинтересовани от развитието на правната мисъл.

Series

LEGAL RESEARCH FORUM

Book One

This series presents the results of the annual international and national scientific conferences organized by the Department of Law at New Bulgarian University. Each edition gathers in-depth research and analyses from leading scholars, practitioners, and young researchers, focused on relevant topics that reflect the dynamics and challenges of the contemporary legal landscape.

The purpose of this series is to expand the scholarly debate and foster progress in the field of law by encouraging the exchange of ideas and knowledge on a broad array of theoretical and practical issues. The volumes are distinguished by a high degree of methodological precision and scientific rigor, making them a valuable resource for the academic community, practicing lawyers, students, and all those interested in the advancement of legal thought.

СЪДЪРЖАНИЕ

Новите законодателни и технологични инициативи – предизвикателства и възможности пред защитата на личните данни

Венцислав Караджов*

Настоящият текст разглежда предизвикателствата и възможностите пред защитата на личните данни, обект на предложената през 2020 г. Европейска стратегия за данните. Текущият труд се фокусира върху значението и основните елементи на предложените законодателни и технологични инициативи и вече действащото законодателство на ЕС, които се стремят да гарантират справедливост при достъпа и използването на данни в съответствие с европейските правила и ценности. Същевременно същите целят да улеснят споделянето на данни между отделни сектори и държави от ЕС, за да се използва потенциалът на данните в полза на гражданите и бизнеса, като се въведат общоприложими правила за пускането на пазара, въвеждането в експлоатация и използването на системи с изкуствен интелект в ЕС, както и правила за прозрачност (яснота и разбираемост), когато тези системи взаимодействат с физически лица.

Разглеждат се както една от най-нашумелите и използвани технологии и нейното взаимодействие с европейското законодателство, така и усилията на ЕС да отговори на развитието на базираните на информационни технологии услуги чрез установяване на ясни правила за защитата на физическите и юридическите лица при обработката на данни в цифровата среда, като се обръща специално внимание на правата на зачитане на личния живот и тайната на съобщенията. Обръща се специално внимание на конкретни цели на Европейската стратегия за данните, а именно насърчаването на иновациите, растежът и конкурентоспособността и улесняването на разрастването на по-малките платформи, МСП и стартиращите предприятия, справянето с трудностите при предотвратяване на незаконни и вредни дейности онлайн, както и разпространение на дезинформация.

Ключови думи: *защита на личните данни, изкуствен интелект, иновации, цифрови предизвикателства*

* Венцислав Караджов, председател на Комисията за защита на личните данни и заместник-председател на Европейския комитет по защита на данните до 25.05.2023 г.

The New Legislative and Technological Initiatives – Challenges and Opportunities for the Protection of Personal Data

Ventsislav Karadjov*

The current text examines challenges and opportunities for the protection of personal data which are the subject of the proposed in 2020 European Strategy for Data. It focuses on the meaning and main elements of the active European legislation and the proposed legislative and technological initiatives of the EU, which seek to ensure fairness in data access and use while respecting European rules and values. At the same time, they aim to facilitate the sharing of data between EU sectors and countries in order to use the potential of data for the benefit of citizens and businesses, to introduce harmonized rules for the marketing, commissioning and use of artificial intelligence systems in the EU, as well as transparency rules when these systems interact with natural persons.

It examines both one of the most popular and used technologies and its interaction with European legislation, as well as the EU efforts to respond to the development of information technology-based services by establishing clear rules to guarantee the protection of natural and legal persons when processing their data in the digital environment, paying particular attention to the rights to respect private life and the confidentiality of communications. As well as other objectives covered in the European Strategy for Data which include fostering innovation, growth and competitiveness and facilitating the growth of smaller platforms, SMEs and start-ups, tackling also the challenges of preventing illegal and harmful activities online and the spread of disinformation.

Keywords: *personal data protection, artificial intelligence, innovation, digital challenges.*

* Ventsislav Karadjov, Chairman of the Commission for Personal Data Protection and Deputy-Chair of the European Data Protection Board until 25th May 2023.

През 2020 г. със своята Европейска стратегия за данните ЕК достига до извода, че цифровите технологии преобразуват икономиката и обществото, като засягат всички действащи сектори на икономиката, така и всекидневния живот на всички европейци. Отчете се, че данните са в центъра на тази трансформация, както и че в бъдеще предстоят дори още по-големи промени. На всеки е ясно, че основаните на данни иновации ще донесат допълнителни ползи на гражданите, например посредством подобрена персонализирана медицина, нова мобилност и също така ще допринесат за постигане и на целите на Европейския зелен пакт – модерна, ресурсно ефективна икономика, където икономическият растеж не зависи само от наличието и използването на природни ресурси. В общество, в което отделните членове създават и използват все по-големи количества данни, **начинът, по който данните се събират и използватот частния и публичния сектор**, трябва да поставя на първо място интересите на отделната личност в съответствие с европейските ценности, основни права и правила. **Гражданите ще имат доверие и ще възприемат основаните на данни иновации само ако са уверени, че при всяко споделяне на данни в ЕС напълно ще бъдат спазвани строгите правила на ЕС за защита на данните и гарантираните им с това права.**

В същото време, трябва да съзнаваме, че технологичните промени в начина на съхранение и обработка на данните нарастващите обеми на неличните промишлени данни и публичните данни в Европа ще представляват потенциален източник на растеж и иновации, който следва да бъде използван.

Обемът на произведените в света данни нараства бързо, от 33 зетабайта[1] през 2018 г. на прогнозните 175 зетабайта през 2025 г. Понастоящем 80% от обработката и анализа на данни се извършва в центрове за данни и централизирани изчислителни системи, а 20% – в интелигентни свързани обекти (*smart devices*), като автомобили, домакински уреди или промишлени роботи, и в изчислителни системи в близост до потребителя („периферни изчисления“). До 2025 г. тези стойности вероятно ще си разменят местата.

Европейското пространство на данни, което е целта на обсъжданата стратегия, ще даде на предприятията в ЕС възможността да надграждат в условията на мащабността на единния пазар. Общите европейски правила и ефикасните механизми за правоприлагане следва да гарантират, че:

- данните могат да се движат свободно в ЕС и между отделните сектори на икономиката в общия пазар;

[1] Един петабайт (PB) е равен на 1024 TB (терабайта), а един ексабайт (EB) – на 1 млн. терабайта. Зетабайтовете са значително по-големи – 1 EB представлява само една хилядна част от зетабайта.

- за тази цел е необходимо изцяло да се спазват европейските правила и ценности, по-специално защитата на личните данни, законодателството за защита на потребителите и правото в областта на конкуренцията;
- въведените правила за достъп и използване на данните са справедливи, практични и ясни и съществуват ясни и заслужаващи доверие механизми за управление на данните. Налице е открит и работещ механизъм, при който международните потоци от данни се обработват при спазване на европейските ценности и завишените гаранции, които европейското право предоставя.

1. С **Общия регламент относно защита на данните (ОРЗД)** се определят правилата по отношение на защитата на физическите лица във връзка с обработването на лични данни, както и правилата по отношение на свободното движение на лични данни. Чрез него се постига защита на основни права и свободи на физическите лица и по-специално се гарантира възможността за упражняване правото на защита на лични данни. Не на последно място, свободното движение на лични данни в рамките на Съюза не се ограничава, нито се забранява по причини, свързани със защитата на физическите лица във връзка с обработването на техни лични данни.

2. За разлика от ОРЗД, **Законодателният акт за данните (Data Act)**, предложен от ЕК през месец февруари 2022 г. има за цел да гарантира справедливост при достъпа и използването на данни и най-вече, че европейските правила и ценности са спазени. Този законодателен акт допълва предложения през ноември 2020 г. Регламент за управление на данните (Data Governance Act – DGA) и цели да регламентира кой и при какви условия може да ползва данни, генерирани от така наречените „интелигентни“/ „умни“ устройствата (*smart devices*) в глобалната мрежа (*Internet of thinks devices*). Поначало ползвателите на тези *smart devices* в мрежата остават с разбирането, че те са единствените собственици на информацията, която генерират от използването на собствените си устройства. Това обаче невинаги е така. Производителите на тези устройства невинаги ги разработват така, че да дадат пълен достъп на собствениците на устройствата до цялата информация, която те генерират в мрежата, най малкото поради необходимостта от данни с оглед подобряване на функционалността на използвания софтуер или хардуер. Това води до неясни правила за ползването и достъпа до тази информация и затруднява като цяло цифровото развитие в икономика, базирана на дигитализацията.

По тази причина Законодателният акт за данните въвежда общи изисквания за тяхното ползване с цел да предостави по-голям достъп до тези данни на фирмите, гражданите и публичната администрация. Примерно органите и институциите в публичния сектор ще могат да разполагат с информация, която представлява данни, генерирани в частния сектор с оглед възможността да предоставят определени публични услуги като обществено здравеопазване, реакция при бедствия и аварии, борба с изменението на климата, изготвяне и разпространение на официални статистики и др.

В по-общ смисъл регламентът създава задължение за осигуряване на достъп до данните, генерирани от използването на продукти или свързани с тях услуги, регламентира правото на ползвателите на достъп и използване на данните, генерирани от използването на продукти или свързани с тях услуги, налага правото на споделяне на данни с трети страни само по искане на ползвателя на тези данни, както и условията, при които държателите на данни предоставят данни на получателите на данни. Както в повечето европейски актове, така и в този са определени забрани и редки изключения при неравноправни договорни условия, наложени едностранно от държателя на данните спрямо физическо лице или спрямо микро, малко или средно предприятие.

Регламентът по дефиниция е пряко обвързан с желанието на европейските институции за пълна оперативна съвместимост, като в случая се регламентират изискванията към операторите на данни и оперативната съвместимост на услугите за обработка на данни. Налице е и изискване за определяне на национален орган, компетентен по прилагането на акта.

3. Акт за управление на данни (Data Governance Act – DGA)

Обхват:

- Създаване на условията за *повторното използване* в рамките на Съюза на някои категории данни, притежавани от организациите от обществения сектор;
- Създаване на рамка за уведомяване и надзор при предоставяне на посреднически услуги за данни;
- Създаване на рамка за доброволна регистрация на субекти, които събират и обработват данни, предоставени за *алтруистични цели*;
- Създаване на рамка за *учредяването на Европейски комитет за иновации* в областта на данните.

Както в Data Act, и тук понятието за данни е въведено в широк смисъл (цифрово представяне на документи, факти или информация, както и всяка

съвкупност от такива документи, факти или информация, включително под формата на звукозапис, видеозапис или аудио-визуален запис). Личните данни са зададени като отделна категория, дефинирана съгласно чл. 4, т. 1 от Регламент (ЕС) 2016/679. Дефинициите за „субект на данни“ и на „съгласие“, използвани в този регламент, са същите, разписани в Регламент (ЕС) 2016/679. Особеното в този регламент е, че:

> ***DGA се фокусира върху повторното използване на данни от физически или юридически лица***. Тези данни следва да са притежавани от организации от обществения сектор и целта е да се използват повторно за търговски или нетърговски цели, различни от първоначалната цел в рамките на обществената задача, за която данните са били създадени/събрани. От тази цел е изключен обменът на данни между организации от обществения сектор, свързан с изпълнение на техните обществени функции, т.нар. „междуинституционален обмен“ на информация с оглед възможността и задължението на публичните органи да изпълняват възложените им със закон функции, т.нар. „оперативни данни“.

И тук съществен елемент е разграничението между **ползвател на данни** (физическо или юридическо лице, което има право да използва дадени лични или нелични данни за търговски цели) и **притежател на данни** (юридическо лице, което не е субектът, създал конкретните данни, но има право да предоставя достъп до тях или да ги споделя), като *целта на регламента е да се насърчи споделянето на тези данни*. **Новост в тази правна рамка е въведената фигура на** *посредническа услуга за данни*, **което означава услуга, която има за цел установяването на *търговски отношения за целите на споделянето на данни* между неопределен брой субекти ползватели на данни и притежателите на тези данни (обикновено юридически лица, регистрирани за тази цел)** чрез технически, правни или други средства.

Друга непозната до момента фигура е **„алтруизъм по отношение на данните“**, който представлява доброволното споделяне на данни въз основа на съгласие на субектите на данни за обработване на отнасящи се до тях лични данни или въз основа на разрешения на притежатели на данни за използване на техни нелични данни, ***без да се иска или получава възнаграждение*, което надхвърля възстановяването на разходите, направени от субектите на данни или притежателите на данни при предоставянето на техните данни за цели от обществен интерес**. Идеята е, че доброволно

могат да се предоставят лични данни за цели от обществен интерес, когато касаят например: ***здравеопазване, борба с изменението на климата, подобряване на мобилността, улесняване на разработването, изготвянето и разпространението на официални статистики, подобряване на предоставянето на обществени услуги, формулиране на публични политики или научноизследователски цели от обществен интерес.***

В този контекст DGA забранява изключителните договорки между притежателите на данни от обществения сектор, които формално или реално възпрепятстват повторното използване на притежаваните от тях публични данни от други субекти (в този случай „субект“ не съответства с дефиницията по Регламент (ЕС) 2016/679).

Същевременно с DGA се създават единни европейски правила за повторното използване на данни с особен фокус върху организациите от обществения сектор с цел да се създаде единна информационна точка, която да определя реда и условията, както и да предоставя възможност за такова повторно недискриминационно използване.

По дефиниция изискванията за повторно използване на данни са:

а) достъп до данни за повторно използване се предоставя само когато органът от обществения сектор или компетентният орган е гарантирал, че данните са:
   i) анонимизирани, в случай че съдържат лични данни;
   ii) променени, обобщени или обработени чрез друг метод за контрол на разкриването в случай на поверителна търговска информация, включително търговски тайни или съдържание, защитено с права върху интелектуална собственост;

б) дистанционният достъп и дистанционното повторно използване на данните се осъществява в защитена среда за обработване, предоставена или контролирана от организацията от обществения сектор;

в) достъпът и повторното използване на данните се осъществява в рамките на физическите помещения, в които се намира защитената среда за обработване, в съответствие със строги стандарти за сигурност, при условие че дистанционният достъп не може да бъде осъществен, без да се застрашат правата и интересите на трети страни.

С въвеждането на алтруизма при споделянето на данни DGA въвежда изисквания за създаването на публични регистри на признатите

организации за алтруистично споделяне на данни и определя условията за регистрация на организациите. Основен фокус при осъществяване на дейността на тези организации е прозрачността и особено въвеждането на конкретни изисквания за защитата на правата и интересите на субектите на данни.

На този етап е в ход организация по въвеждането на регламента и предстои да бъдат определени органите за регистрация на организациите за алтруистично споделяне. ***Международният достъп и предаването на данни до трети държави е само по отношение на неличните данни, като по отношение на личните данни се запазва общият режим по Регламент (ЕС) 2016/679, а компетенциите на КЗЛД по надзор остават непроменени.***

Регламентът е обнародван на 03.06.2022 г. и влиза в сила на 24.09.2023 г.

4. Акт за изкуствения интелект (Artificial Intelligence Act) – регламент, предложен от ЕК на 21.04.2021 г.

Въвежда хармонизирани правила за пускането на пазара, въвеждането в експлоатация и използването на системи с изкуствен интелект („системи с ИИ“) в ЕС, както и правила за прозрачност (яснота относно тяхното функциониране), когато тези системи взаимодействат с физически лица, с цел разпознаване на емоции, биометрично категоризиране или генерират или обработват образ, аудио или видео съдържание. Въвеждат се специфични изисквания за високорисковите системи с ИИ и задължения за операторите на такива системи. Въвеждат се правила за наблюдение и надзор на пазара, включително чрез забрани на някои практики в областта на изкуствения интелект.

Данните (лични и нелични) в ИИ в голяма част от случаите са ключовата предпоставка за автономни решения, които неизбежно ще засегнат живота на физическите лица на различни равнища – обществен, професионален и личен живот. Поради тази причина предложението за Регламент за определяне на хармонизирани правила относно изкуствения интелект има важни последици за защитата на данните. Освен това **поради интензивното използване на данни от множество приложения с ИИ, в предложението тепърва следва да се насърчава възприемането на подход за 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.

Подход, базиран на риска: в предложението се изисква от доставчиците на системата с ИИ да извършат оценка на риска при обработване на информация, която съдържа лични данни. Разбира се, *в повечето случаи администраторите на данни ще бъдат ползвателите, а не доставчиците на системите с ИИ*, поради което за един доставчик невинаги ще е възможно да оцени всички употреби на системата с ИИ от лицето, което я е закупило. Така първоначалната оценка на риска ще бъде с по-общ характер в сравнение с тази, извършена от ползвателя на системата, който се явява и администратор на данните, събрани или генерирани в резултат на нейното използване. 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 Регламент (ЕС) 2018/1725 или член 27 от ДП), **която следва да се извърши от ползвателя/администратора на системата**, като се вземат под внимание контекстът и конкретните случаи на използване.

Забранени употреби на ИИ: все още е отворен въпросът за накърняващите форми на ИИ – особено тези, които може да засегнат достойнството на човека, – дали следва да се разглеждат като забранени системи с ИИ. **Остава отворен въпросът и за безпрепятственото използване на системите за дистанционна биометрична идентификация, която освен проблем с пропорционалността поражда също така проблеми с „прозрачността“, повдига и въпроси, свързани с правното основание за обработване на биометрията съгласно правото на ЕС** (ОРЗД , Регламент за защита на данните в институциите на ЕС и друго приложимо право). Остава неразрешен и 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 обществото за анонимност на публични места, който води до пряка отрицателна последица за упражняването на свободата на изразяване на мнение, на събрания, на сдружаване, както и свободата на движение.

Една от целите, които ЕК си поставя с предложението е да се улесни развитието на единен пазар за законни, безопасни и надеждни приложения с ИИ и да предотврати разпокъсаност на пазара чрез предприемане

на действия от страна на всяка държава членка на съюза. Затова ЕС чрез този законодателен акт определя минимални изисквания за системите с ИИ, които могат да бъдат пускани на пазара и използвани в съюза в съответствие с действащото законодателство в областта на основните права и безопасността. По този повод ЕК предвижда въвеждането с регламента на 9 приложения, които задават правни и технически спецификации към разработването, въвеждането, разпространението и референтната правна уредба на ИИ.

5. OpenAI Limited Liability Company (LLC) и услугата им Chat GPT

На 30 март 2023 г. надзорният орган по защита на личните данни на Италия (Garante per la protezione dei dati personali) издаде решение за прекратяване на достъпа до услугата ChatGPT в границите на Италия. В своето решение относно ChatGPT, който от пускането си за свободна употреба през ноември 2022 г. се превърна в една от най-нашумелите и използвани технологии, базирани на изкуствен интелект, италианският надзорен орган посочва, че след извършена проверка е установено, че:

- не се предоставя информация на потребителите, нито на заинтересованите страни, чиито данни са събрани от компанията, отговорна за управлението на услугата (OpenAI, LLC), нито за тези, обработени чрез услугата ChatGPT;
- липсва проверка на възрастта на потребителите във връзка с услугата ChatGPT, която съгласно условията, публикувани от OpenAI LLC, е запазена за лица, които са навършили поне 13 години.

В решението на Garante се посочва също, че:

• са установени многобройни намеси на медиите във функционирането на услугата ChatGPT;

- липсва подходящо правно основание във връзка със събирането на лични данни и тяхното третиране с цел обучение на алгоритмите, залегнали в работата на ChatGPT;
- обработването на личните данни на заинтересованите страни е неточно, тъй като информацията, предоставена от ChatGPT, невинаги съответства на реалните данни.

Вследствие на установените нарушения надзорният орган на Италия на 30 март 2023 г.[2] налага на дружеството, създало и въвело услугата –

[2] Решение на надзорния орган по защита на личните данни на Италия (30 март 2023), Provvedimento del 30 marzo 2023 [9870832] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832

OpenAI LLC, собственик на ChatGPT, мярката за временно ограничаване на обработката на лични данни на субекти на данни, установени на територията на Италия. На 11 април 2023 г.[3] Garante публикува решение, с което се задължава OpenAI LLC да въведе допълнителни мерки, чрез които да гарантира правата на субектите на данни. Дружеството, представляващо ChatGPT, в рамките на същия месец, а именно на 28 април 2023 г., изпраща писмо до италианския надзорен орган, в което посочва, че вече са въведени част от предложените на 11 април мерки с цел ChatGPT да бъде приведен в съответствие с ОРЗД. След анализ на направените промени Надзорният орган на Италия разреши услугата да бъде възобновена в границите на Италия, считано от 28 април 2023 г.[4]

6. ePrivacy Regulation – цели определянето на правила по отношение защитата на основните права и свободи на физическите и юридическите лица при предоставянето и използването на електронни съобщителни услуги и по-специално правата на зачитане на личния живот и тайната на съобщенията и защитата на физическите и юридическите лица при обработката на данни. Предложението за регламент има за цел да гарантира свободното движение на данни от електронни съобщения и електронни съобщителни услуги в рамките на Съюза, **което не се ограничава, нито забранява по причини, свързани със зачитането на неприкосновеността на личния живот и тайната на съобщенията на физическите и юридическите лица и защитата на физическите лица при обработката на личните им данни.**

Така например достъпът до електронните съобщителни мрежи изисква редовното изпращане на определени пакети данни, за да се открие или поддържа връзка с мрежата или други устройства в нея. Освен това устройствата трябва да разполагат с уникален адрес, определен именно с цел да могат да бъдат идентифицирани в тази мрежа. Безжичните и мобилните телефонни стандарти също така включват изпращането на активни сигнали, съдържащи уникални идентификатори като MAC адрес, IMEI (международен идентификатор на мобилно устройство), IMSI и т.н. Всяка безжична базова станция (т.е. предавател и приемник), като например точка за безжичен достъп, има конкретен обхват, в който тази информация може да бъде улавяна. Появиха се доставчици на услуги, които предлагат

[3] Решение на надзорния орган по защита на личните данни на Италия (11 април 2023), Provvedimento dell'11 aprile 2023 [9874702] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702

[4] Press release: ChatGPT: OpenAI riapre la piattaforma in Italia garantendo più trasparenza e più diritti a utenti e non utenti europei: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9881490

услуги за проследяване на основата на сканиране на тази информация за устройствата. Тези услуги имат различни функционални възможности, включително за преброяване на хора, предоставяне на данни за броя на чакащите на опашка, установяване на броя на хората в даден район и т.н. Като винаги тази информация може да се използва и за по-агресивни цели, като изпращане на търговски съобщения до крайни ползватели, например при влизане в магазин, и персонализирани предложения.

Макар някои от тези функции да не водят до високи рискове за неприкосновеността, други ги пораждат, например тези, които включват следенето на лица за определени периоди от време, включително повтарящи се посещения на конкретни места. Доставчиците, упражняващи такива практики, следва да поставят лесно забележими надписи по периметъра на района на покритие, за да информират крайните ползватели преди да влязат в него, че технологията е в действие в определен периметър, за целта на проследяването, за отговорното лице и за наличието на мерки, които крайният ползвател може да вземе, за да ограничи или спре събирането на данни. *Когато се събират лични данни, съгласно член 13 от Регламент (ЕС) 2016/679 следва да бъде предоставяна допълнителна информация.*

По отношение на обществено достъпни указатели доставчиците следва да получат съгласието на крайните ползватели, които са физически лица, да включат техните данни в указателя и съответно съгласието на тези крайни ползватели за всяка различна категория лични данни, която ще се включи в публичния указател от доставчика. Доставчиците предоставят на крайните ползватели, които са физически лица, възможност да проверят, поправят или заличат свързаните с тях лични данни, които подлежат на публикуване в указателя.

Целта е да се надгради Директива 2002/58 (т.нар. Цифров кодекс) и да се хармонизират изцяло правилата в рамките на ЕС. Основни проблематични моменти са формите на съгласие на крайните потребители и оттеглянето му, както и задържането и последващото обработване на данни от крайните устройства. Изрично е упоменато, че разпоредбите на предложения регламент конкретизират и допълват Регламент (ЕС) 2016/679 чрез определяне на конкретни правила за целите. Като съществен дебат по текста е и тежестта на съгласието на крайния ползвател на услугата[5], както и ролята му върху настройките по подразбиране на крайните устройства. Приема се, че съгла-

[5] 2a. Consent directly expressed by an end-user in accordance with Paragraph (2) shall prevail over software settings. Any consent requested and given by an end-user to a service shall be directly implemented, without any further delay, by the applications of the end user's

сието на лицето има предимство пред настройките на производителя. Ще е налице и нужда от допълнителни усилия от държавите членки по определяне и ясно разпределяне на надзорните функции на различните надзорни органи по отношение спазване на този регламент и на ОРЗД, в частност КЗЛД ще продължи да упражнява надзор над защитата на личните данни на крайните потребители, както и на трафичните данни, какъвто е правният режим и към настоящия момент. Документът е сред приоритетните теми на Шведското председателство на Съвета на ЕС.

7. Законодателните актове за цифровите услуги и цифровите пазари имат за цел да създадат по-безопасно цифрово пространство, в което основните права на ползвателите са защитени, и да създадат еднакви условия на конкуренция на предприятията. Регламентите относно единния пазар на цифрови услуги (Digital Service Act) и относно цифровите пазари (Digital Markets Act) целят установяването на общи правила за:

– ефективно противодействие на нелоялните практики от страна на дружествата, които действат като контролиращи достъпа предприятия в икономиката на онлайн платформите (DMA);
– предоставянето на посреднически услуги на вътрешния пазар (DSA).

Digital Markets Act – законодателен акт за цифровите пазари

Със Законодателния акт за цифровите пазари се въвеждат тясно определени ***обективни критерии за големите онлайн платформи***, които отговарят на критериите за т.нар. „пазачи на информационния вход“ (съгласно дефиницията това е така наречената „основна платформена услуга“ – посреднически онлайн услуги, онлайн търсачки, услуги за онлайн социални мрежи, операционни системи, уеб браузъри, виртуални асистенти, компютърни услуги „в облак“, онлайн рекламни услуги).

Целта е справянето с проблема, предизвикан от големите, системни онлайн платформи в случаите, когато по определени критерии бъдат квалифицирани като „контролиращи предприятия“. Критериите за това са следните:

• дадено дружество има силна икономическа позиция, значително въздейства върху вътрешния пазар на общността и развива дейност в множество държави от ЕС;

terminal, including where the storage of information or the access of information already stored in the end-user's terminal equipment is permitted.

- дадено дружество има силна посредническа позиция, което означава, че свързва голяма потребителска база с голям брой предприятия, ползватели на услугата;
- дадено дружество има (или е на път да има) трайно установена и постоянна позиция на пазара, което означава, че тя е стабилна във времето, ако дружеството е отговаряло на посочените по-горе два критерия през всяка от последните три финансови години.

Контролиращото достъпа предприятие няма да може да извършва никоя от следните дейности:

а) да обработва лични данни на крайните ползватели на услуги, използващи основните платформени услуги на контролиращото достъпа предприятие с цел предоставяне на рекламни услуги на трети лица;

б) да съчетава лични данни от съответната основна платформена услуга с лични данни от други основни платформени услуги или от всякакви други услуги, предоставяни от контролиращото достъпа предприятие с лични данни от услуги, които предлага на трети лица;

в) да ползва лични данни от съответната основна платформена услуга съвместно с други услуги, предоставени отделно от контролиращото достъпа предприятие, включително други основни платформени услуги и обратно;

г) да включва крайни ползватели в други услуги на контролиращото достъпа предприятие с цел съчетаване на лични данни.

Контролиращите достъпа предприятия често събират пряко лични данни на крайните ползватели с цел предоставяне на онлайн рекламни услуги, когато крайните ползватели използват уебсайтове и софтуерни приложения на трети лица. Трети лица също така предоставят на контролиращите достъпа предприятия лични данни на своите крайни ползватели, за да използват определени услуги, предоставяни от контролиращите достъпа предприятия в контекста на техните основни платформени услуги, като например персонализирана аудитория. Обработването за целите на предоставянето на онлайн рекламни услуги на лични данни от трети лица, използващи основни платформени услуги, дава на контролиращите достъпа предприятия **потенциални предимства по отношение на натрупването на данни, като по този начин създава пречки за навлизане на пазара на други бизнеси, т.е. монополизира пазара на услуги и създава нелоялна конкуренция**. Това е така, защото контролиращите достъпа предприятия

обработват лични данни от значително по-голям брой трети лица, отколкото други предприятия могат да обработват самостоятелно. С цел да се гарантира, че контролиращите достъпа предприятия не ограничават несправедливо достъпността на основните платформени услуги, контролиращите достъпа предприятия следва да дават възможност на крайните ползватели свободно да изберат да участват в практики на обработване на данни и влизане, като предлагат по-малко персонализирана, но равностойна алтернатива, и без да обвързват използването на основната платформена услуга или някои нейни функции със съгласието на крайния ползвател, т.е. да не го лишават от качествена услуга, ако не получат съгласие за обработване.

Когато контролиращото достъпа предприятие поиска съгласие, то следва по собствена инициатива да представи лесно за ползване решение на крайния ползвател, за да даде, измени или оттегли съгласие по изричен, ясен и опростен/лесен от техническа гледна точка начин. По-специално съгласието следва да бъде дадено чрез ясно потвърждаващо действие или изявление, с което се установява свободно изразено, конкретно, информирано и недвусмислено указание за съгласие от страна на крайния ползвател по смисъла на определението в Регламент (ЕС) 2016/679. В момента на даването на съгласие и само когато е приложимо, крайният ползвател следва да бъде информиран, че отказът на съгласие може да доведе до по-малко персонализирано предлагане, като същевременно основната платформена услуга ще остане непроменена и няма да бъдат премахнати никакви функции.

Оттеглянето на съгласието следва да бъде също толкова лесно, колкото и даването му. Контролиращите достъпа предприятия не следва да проектират, организират или експлоатират своите онлайн интерфейси по начин, който подвежда, манипулира или по друг начин съществено изопачава или накърнява способността на крайните ползватели свободно да дават съгласие. ***По-специално на контролиращите достъпа предприятия не следва да се позволява да подтикват крайните ползватели повече от веднъж годишно да дават съгласие за същата цел на обработване, по отношение на която първоначално не са дали съгласие или са оттеглили съгласието си.***

Настоящият регламент не засяга Регламент (ЕС) 2016/679, включително предвидената в него рамка за изпълнение, който остава изцяло приложим по отношение на всякакви искове на субекти на данни, свързани с нарушение на техните права съгласно посочения регламент.[6]

[6] Регламент (ЕС) 2022/1925 на Европейския парламент и на Съвета от 14 септември 2022 година за достъпни и справедливи пазари в цифровия сектор и за изменение на

По отношение на онлайн търсачките от контролиращите достъпа предприятия следва да се изисква да предоставят достъп при справедливи, разумни и недискриминационни условия до данните относно класирането, търсенето, избирането и прегледа във връзка с безплатно и платено търсене, извършено от страна на потребители на онлайн търсачки, за други предприятия, предоставящи такива услуги, така че тези предприятия – трети лица, да могат да оптимизират своите услуги и да конкурират съответните основни платформени услуги.

Такъв достъп следва да се предостави на трети лица, които са сключили договор с доставчик на онлайн търсачка и които действат като лица, обработващи тези данни за тази онлайн търсачка. При предоставяне на достъп до своите данни за търсене контролиращото достъпа предприятие трябва да осигури защитата на личните данни на крайните ползватели, включително срещу възможни рискове от повторно идентифициране, чрез подходящи средства, като анонимизирането на такива лични данни, без съществено да се влошава качеството, нито полезността на данните.

Съответните данни са анонимизирани, ако личните данни са необратимо изменени по такъв начин, че информацията не е свързана с идентифицирано или подлежащо на идентифициране физическо лице, или когато личните данни са анонимизирани по такъв начин, че субектът на данните не може да бъде или повече не може да бъде идентифициран.

Регламентът е обнародван на 12.10.2022 г. и се прилага от 02.05.2023 г.

Digital Service Act – Законодателен акт за цифровите услуги

Законодателният акт за цифровите услуги включва правила за посредническите онлайн услуги за предлагане услуги на информационното общество, т.е. на мрежова инфраструктура: ***интернет доставчици, регистратори на имена на домейни, включително: хостинг услуги; онлайн платформи като онлайн пазари, магазини за приложения; много големите онлайн платформи (предвидени са специални правила за платформите, достигащи до над 10% от 450-те милиона потребители в Европа),*** т.е. задълженията на различните онлайн участници са съобразени с тяхната роля, размер и въздействие в онлайн средата.

директиви (ЕС) 2019/1937 и (ЕС) 2020/1828 (Акт за цифровите пазари) (текст от значение за ЕИП) (12.10.2022 г.): https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32022R1925

Новите правила насърчават иновациите, растежа и конкурентоспособността и улесняват разрастването на по-малките платформи, МСП и стартиращите предприятия. Отговорностите на потребителите, платформите и публичните органи са разпределени в съответствие с европейските ценности, като гражданите заемат централно място.

С правилата се:

- осигурява по-добра онлайн защита на потребителите и техните основни права;
- създава надеждна рамка за прозрачност и отчетност за онлайн платформите;
- насърчават иновациите, растежът и конкурентоспособността в рамките на единния пазар.

Всички онлайн посредници, които предлагат услугите си на единния пазар, независимо дали са установени в ЕС или извън него, ще трябва да спазват новите правила. Микропредприятията и малките предприятия ще имат задължения, пропорционални на техните възможности и размер, като същевременно ще продължат да носят отговорност[7].

От гледна точка на посредниците, които предлагат услуги, DSA представлява рамка за условно освобождаване от отговорност при добросъвестно осъществяване на обикновен пренос и предоставяне на достъп в далекосъобщителна мрежа, когато не започва преносът, не избира получателя на информацията и не избира или променя самата информация в преноса. Подобно освобождаване от отговорност е налице и при осъществяване на „кеширане“, в случай че не се променя информацията, спазват се условията за достъп до и за актуализиране на информацията.

Това освобождаване е скрепено обаче с изисквания за по-голям надзор и контрол над системните платформи и възможност за намеса при идентифициране на действия по манипулиране или дезинформация.

По отношение на защитата на личните данни и по-специално при използването им за целите на персонализираната реклама регламентът предвижда от доставчиците на онлайн платформи да се изисква да гарантират, че получателите на услугата разполагат с определена индивидуализирана информация, която им е необходима, за да разберат кога

[7] Европейска комисия: Законодателен акт за цифровите услуги – осигуряване на безопасна и отговорна онлайн среда: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_bg

и от чие име е представена дадена реклама. Те следва да гарантират, че информацията е пределно ясна, включително чрез стандартизирани визуални или аудио бележки, ясно разпознаваеми и недвусмислени за средностатистическия получател на услугата, като тя следва да бъде адаптирана към естеството на индивидуалния онлайн интерфейс на услугата.

Освен това получателите на услугата следва да разполагат с информация, пряко достъпна от онлайн интерфейса, на който е представена рекламата, относно основните параметри, въз основа на които конкретна реклама им бива представяна, което ще им даде съдържателно обяснение на използваната за целта логика, включително когато тя се основава на профилиране.

Тези обяснения следва да включват информация относно метода, използван за представянето на рекламата – например дали е контекстуална или друг вид реклама, и когато е приложимо – основните използвани критерии за профилиране; тя следва също така да информира получателя за всички налични средства за промяна на тези критерии. Изискванията относно предоставянето на информация, свързана с рекламата, не засягат прилагането на съответните разпоредби на Регламент (ЕС) 2016/679 и по-специално разпоредбите относно правото на възражение, автоматизираното вземане на индивидуални решения, включително профилирането, и в частност необходимостта от получаване на съгласие от субекта на данните преди обработването на лични данни за целево рекламиране. (Съображение 68 на Регламент (ЕС) 2022/2065)

Регламентът е обнародван на 27.10.2022 г. и влиза в сила на 17.02.2024 г.

С други думи, **DSA и DMA** имат две основни цели:

- да се създаде по-безопасно цифрово пространство, в което са защитени основните права на всички ползватели на цифрови услуги;
- създаване на еднакви условия на конкуренция за насърчаване на иновациите, растежа и конкурентоспособността както на единния европейски пазар, така и в световен мащаб.

През декември 2020 г. Комисията предложи Акта за цифровите пазари, за да се справи с отрицателните последици от някои видове поведение на онлайн платформите, действащи като контролиращи достъпа предприятия в цифровата сфера на единния пазар на ЕС.

В Акта за цифровите пазари се посочва кога големи онлайн платформи следва да бъдат определени за „контролиращи достъпа предприятия“. Това са цифрови платформи, които осигуряват важен портал, свързващ бизнес с

ползвателите и потребителите, и чиято силна позиция може да им позволи да определят правилата като частен играч и съответно да се превърнат в пречка в цифровата икономика. За да реши тези проблеми, Актът за цифровите пазари определя редица задължения, включително забрана на определено поведение на контролиращите достъпа предприятия.

С Акта за цифровите пазари се установява списък на това какво трябва и какво не трябва да се прави, който контролиращите достъпа предприятия ще трябва да прилагат в ежедневните си операции, за да гарантират справедливи и отворени цифрови пазари. Тези задължения спомагат за разкриването на възможности за дружествата да се конкурират на пазарите и да оспорват позицията на контролиращите достъпа предприятия на базата на качествата на своите продукти и услуги, като на дружествата се предоставя по-голямо пространство за иновации.

Когато контролиращо достъпа предприятие осъществява практики, като например облагодетелстване на собствените си услуги или възпрепятстване на други бизнес услуги да достигнат до потребителите, това може да попречи на конкуренцията, водейки до по-малко иновации, по-ниско качество и по-високи цени. Освен това, когато контролиращо достъпа предприятие има нелоялни практики, като например налагане на несправедливи условия за достъп до своя магазин за приложения или предотвратяване на инсталирането на приложения от други източници, има вероятност потребителите да плащат по-високи цени или дори да бъдат лишени от предимствата, които биха им донесли алтернативните услуги.

С влизането в сила на Акта за цифровите пазари ще се премине към решаващата фаза на прилагането му, като той ще започне да се прилага след шест месеца, считано от 2 май 2023 г.

Актът за цифровите пазари ще се прилага чрез стабилна надзорна уредба, съгласно която Европейската комисия ще бъде единственият правоприлагащ орган, в тясно сътрудничество с органите в държавите от ЕС. Комисията ще може да налага санкции и глоби в размер до 10% от световния оборот на дадено дружество и до 20% в случай на повторни нарушения. В случай на системни нарушения Комисията ще може също така да налага поведенчески или структурни коригиращи мерки, необходими за гарантиране на ефективното изпълнение на задълженията, включително забрана на по-нататъшни придобивания.[8]

[8] Европейска комисия: Законодателен акт за цифровите пазари: https://ec.europa.eu/commission/presscorner/detail/bg/ip_22_6423

Считано от 12 октомври 2022 г., DMA беше публикуван в Официален вестник. DMA ще влезе в сила и ще започне да се прилага шест месеца по-късно. Определените пазачи на информационния вход ще разполагат с максимум шест месеца след решението на Комисията за определяне, за да гарантират спазването на задълженията, предвидени в Акта за цифровите пазари.

Библиография:

1. Регламент (ЕС) 2022/868 на Европейския парламент и на Съвета от 30 май 2022 година относно европейска рамка за управление на данните и за изменение на Регламент (ЕС) 2018/1724 (Акт за управление на данните, Data Governance Act, DGA).
2. Регламент (ЕС) 2022/1925 на Европейския парламент и на Съвета от 14 септември 2022 година за достъпни и справедливи пазари в цифровия сектор и за изменение на директиви (ЕС) 2019/1937 и (ЕС) 2020/1828 (Акт за цифровите пазари) (текст от значение за ЕИП) – Digital Markets Act, DMA.
3. Регламент (ЕС) 2022/2065 на Европейския парламент и на Съвета от 19 октомври 2022 година относно единния пазар на цифрови услуги и за изменение на Директива 2000/31/ЕО (Акт за цифровите услуги, Digital Services Act, DSA).
4. Директива (ЕС) 2016/681 на Европейския парламент и на Съвета от 27 април 2016 година относно използването на резервационни данни на пътниците с цел предотвратяване, разкриване, разследване и наказателно преследване на терористични престъпления и тежки престъпления.
5. Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните, ОРЗД).
6. Предложение за Регламент на Европейския парламент и на Съвета относно хармонизирани правила за справедлив достъп до данни и тяхното използване (Законодателен акт за данните, Data Act).
7. Предложение за Регламент на Европейския парламент и на Съвета за определяне на хармонизирани правила относно изкуствения интелект (Законодателен акт за изкуствения интелект) и за изменение на някои законодателни актове на съюза (Artificial Intelligence Act).
8. Предложение за Регламент на Европейския парламент и на Съвета относно зачитането на личния живот и защитата на личните данни в електронните

съобщения и за отмяна на Директива 2002/58/ЕО (Регламент за неприкосновеността на личния живот и електронните съобщения, ePrivacy Regulation).

9. 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. [онлайн]. [прегледано на 08 май 2023]. Достъпно на: https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_bg.pdf.

10. Доклад относно предложението за регламент на Европейския парламент и на Съвета относно зачитането на личния живот и защитата на личните данни в електронните съобщения и за отмяна на Директива 2002/58/ЕО (Регламент за неприкосновеността на личния живот и електронните съобщения) [онлайн]. [прегледан на 8 май 2023]. Достъпен на: https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_BG.html.

11. Interreg Greece – Bulgaria qualfarm, Европейски фонд за регионално развитие (ЕФРР) – Европейска политика и европейска стратегия за данните [онлайн]. [прегледан на 8 май 2023]. Достъпен на: https://rdu.bg/wp-content/uploads/2022/12/2022-10_5.pdf.

12. Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите относно Европейска стратегия за данните [онлайн]. [прегледано на 8 май 2023]. Достъпно на: https://commission.europa.eu/document/download/b456e96e-5810-4bb3-94ca-16c4d8d911b2_bg.

13. Бенифеи, Бр., Тудораке Др. (2022). Хармонизирани правила относно изкуствения интелект (Законодателен акт за изкуствения интелект) и за изменение на някои законодателни актове на Съюза. Европейски парламент.

14. Годишен отчет на Комисията за защита на личните данни за 2022 г. достъпен на: https://www.cpdp.bg/userfiles/file/Annual%20Reports/Annual%20report_2022_CPDP.pdf.

15. Европейска комисия: Законодателен акт за цифровите услуги — осигуряване на безопасна и отговорна онлайн среда [онлайн]. [прегледан на 08 май 2023]. Достъпен на: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online environment_bg.

16. Европейска комисия: Законодателен акт за цифровите пазари [онлайн]. [прегледан на 8 май 2023]. Достъпен на: https://ec.europa.eu/commission/presscorner/detail/bg/ip_22_6423.

17. Информационни фишове за Европейския съюз, Европейски парламент: Малки и средни предприятия [онлайн]. [прегледани на 8 май 2023]. Достъпни на: https://www.europarl.europa.eu/factsheets/bg/sheet/63/малки-и-средни-предприятия

18. Официална интернет страница на Европейската комисия: https://commission.europa.eu/index_bg.

19. Решение на надзорния орган по защита на личните данни на Италия (30 март 2023), Provvedimento del 30 marzo 2023 [9870832] [онлайн]. [прегледано на 8 май 2023]. Достъпно на: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832.

20. Решение на надзорния орган по защита на личните данни на Италия (11 април 2023), Provvedimento dell'11 aprile 2023 [9874702] [онлайн]. [прегледано на 8 май 2023]. Достъпно на: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702.

21. Press release: ChatGPT: OpenAI riapre la piattaforma in Italia garantendo più trasparenza e più diritti a utenti e non utenti europei [онлайн]. [прегледано на 08 май 2023]. Достъпно на: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9881490.

Предизвикателствата пред дигиталното развитие на европейското законодателство в областта на трансграничното съдебно сътрудничество

Емил Радев*

Подкрепата на ЕС за развитието на електронното правосъдие е приоритет в редица стратегически документи и планове за действие. В този контекст настоящият доклад разглежда необходимостта от общоевропейски подход при интегрирането на новите информационни технологии в правосъдието на ЕС, като залага на законодателните лостове за преодоляване на фрагментацията и несъвместимостта в системите, на слабостите в трансграничния обмен.

Сред постиженията на дигитализацията, ускорена от COVID-19, са Европейският портал за електронно правосъдие и системата e-CODEX, която е в сърцевината на новите правила. С тях електронната комуникация при сътрудничеството по граждански и наказателни дела става стандарт за работа. Предложеният на 2 декември 2020 г. регламент осигурява правна рамка за развитие на e-CODEX като инструмент за бърз и сигурен обмен на информация в трансграничните производства.

За повече ефективност при решаването на наказателноправни въпроси в ЕС се предвижда платформа за съдебно сътрудничество на съвместните екипи за разследване. Управлявана от eu-LISA, тя ще обедини съществуващи IT инструменти за сигурен обмен на данни. За това допринася и новият регламент, който ЕК предложи относно цифровия обмен на информация за тероризъм. Досегашните практики ще се модернизират и с въвеждането на цифрова система за управление на дела и кръстосана проверка на информацията между държавите членки и институции като Евроюст, Европол и Европейската прокуратура.

За да преодолее различията в дигиталното правосъдие на отделните държави членки, ЕС разчита на хармонизация и развитие на цифровите компетентности в съдебния сектор. Осигурявайки улеснен достъп до правосъдие, по-добро управление на делата, прозрачност на процедурите и по-ефективно сътрудничество, цифровизацията създава предпоставки за повече доверие в съдебната система, а чрез него и за интегритета на вътрешния пазар и икономическия растеж в ЕС.

Ключови думи: *ЕС, дигитализация, трансграничен, съдебно сътрудничество, Е-кодекс*

* Емил Радев, доктор по право, член на Европейския парламент,
ел. поща: emil.radev@europarl.europa.eu

The challenges facing the digitalization of European legislation in the field of cross-border judicial cooperation

Emil Radev*

EU support for the development of e-justice is a priority in a number of strategic documents and action plans. In this context, this report examines the need for a pan-European approach to the integration of new information technologies in EU justice, relying on legislative levers to overcome fragmentation and incompatibility in systems and on weaknesses in cross-border exchanges.

Among the achievements of digitization, accelerated by COVID-19, are the European e-Justice Portal and the e-CODEX system, which is at the heart of the new rules. With them, electronic communication in cooperation in civil and criminal cases becomes a working standard. The regulation proposed on 2.12..2020 provides a legal framework for the development of e-CODEX as a tool for fast and secure exchange of information in cross-border proceedings.

For more efficiency in solving criminal law issues in the EU, a platform for judicial cooperation of joint investigation teams is envisaged. Managed by eu-LISA, it will bring together existing IT tools for secure data exchange. The new regulation proposed by EC on the digital exchange of terrorism information also contributes to this. Current practices will also be modernized with the introduction of a digital system for case management and cross-checking of information between member states and institutions such as Eurojust, Europol and the EPPO.

To overcome the differences in digitalization within Member States, the EU relies on the harmonization and development of digital competences in the judicial sector. By providing easier access to justice, better case management, transparency of procedures and more effective cooperation, digitalization creates the conditions for more trust in the judicial system and, through it, for the integrity of the internal market and economic growth in the EU.

Keywords: *EU, digitalization, cross-border, judicial cooperation, E-codex*

* Emil Radev, PhD, Member of the European Parliament,
e-mail: emil.radev@europarl.europa.eu

Въведение

Ефективността на правосъдните системи в Европейския съюз (ЕС) е от съществено значение за функционирането на вътрешния пазар и важна предпоставка за икономически растеж. В общото пространство на свобода, сигурност и правосъдие достъпът до правосъдие и съдебното сътрудничество между държавите членки са едни от основните цели, залегнали в чл. 67 от Договора за функционирането на ЕС.

Темата за цифровизацията на правосъдието и по-специално в областта на трансграничното съдебно сътрудничество през последните години се утвърди сред приоритетите на ниво ЕС. Ускоряването на процесите в сферата на дигиталното правосъдие се дължи основно на COVID пандемията, която наложи нови форми на комуникация в съдебните производства. В отговор на нуждата от приспособяване към развиващия се цифров свят, ЕС предприе значителни стъпки по отношение на правната рамка за цифрово правосъдие. Разглеждайки тенденциите в развитието на цифровизацията на трансграничното съдебно сътрудничество през призмата на европейското законодателство, ще обърна внимание на мерките за постигане на по-бързи и по-достъпни за гражданите съдебни производства.

Трябва да отбележим, че съдебните процедури могат да бъдат ефективно средство за решаване на споровете, възникващи в обществото само ако са достъпни за гражданите и бизнеса. Така се гарантира, че всеки, който се нуждае от справедливост, може адекватно да защитава своите интереси по съдебен път. Наред с фактори като бързината, ефикасността и легитимността на процедурите, достъпността допринася за повишаване на доверието в правосъдната система като цяло.

Цифровизацията в правосъдието е част от този процес. Тя генерира съществени ползи както по отношение на качеството, така и на легитимността, която предполага висока степен на прозрачност и отчетност в целия процес – от взимането на решение до съответните резултати. Цифровизацията осигурява по-ефективно управление на делата, ускорява времето за обработка и подобрява качеството на информацията, улеснява достъпа до правосъдие чрез използването на онлайн инструменти като цифрови производства и виртуални изслушвания на свидетели, допринася за прозрачността на процедурите, за използването на правни електронни документи и т.н.

Разликите в развитието на дигиталното правосъдие между държавите членки обаче остават големи. В някои страни производствата все още се осъществяват на хартиен носител и използването на дистанционна форма на комуникация като видеоконферентна връзка не е развито, докато в други

имаме сериозен напредък в дигитализирането на съдебните производства. Ето защо през последните години ЕК приоритизира европейския подход в дигитализирането на съдебното сътрудничество между държавите членки както по граждански, така и по наказателни въпроси.

1. Необходимост от общоевропейски подход в дигитализацията на правосъдните системи в ЕС

Засягайки всички сфери на живота ни, цифровата трансформация изисква непрекъснато да се адаптираме. Това важи в пълна степен и за промените в областта на правосъдието. ЕС не може да избяга от тенденциите, които предопределя напредъкът на новите технологии. Усилията на институциите, насочени към развитието на европейското електронно правосъдие, имат за цел именно да се подобри достъпът до правосъдие в ЕС, да се разработят и интегрират информационни и комуникационни технологии в работата на съдебните системи. Цифровизираните процедури и електронната комуникация между участниците в съдебни производства вече са важен елемент за ефикасното функциониране на съдебната система в държавите членки на ЕС.

Трите основни европейски институции – Европейската комисия, Европейският парламент и Съветът, ясно демонстрираха своята ангажираност към развитието на електронното правосъдие. Основните документи, определящи до момента действията на ЕС в тази област, са Многогодишният план за действие за периода 2009–2013 г. в областта на европейското електронно правосъдие и Стратегията за европейското електронно правосъдие за периода 2014–2018 г., заменени на свой ред от Стратегия и план за действие 2019–2023 г.

Първият от най-важните резултати вследствие на цифровизацията на правосъдието досега, е Европейският портал за електронно правосъдие, който представлява обслужване на едно гише за различни аспекти и онлайн инструменти, свързани с правосъдието в дадена държава членка. Заключенията на Съвета на ЕС от 25 ноември 2020 г. – „Достъпът до правосъдие – оползотворяване на възможностите, предоставяни от цифровизацията“[1], зададоха посоки, приканващи ЕК да оцени възможните действия в областта на съдебното сътрудничество по гражданските и търговските въпроси, надграждайки вече постигнатия напредък при модернизацията на трансграничния обмен между компетентните органи на държавите членки. Като ключови фактори за изпълнението на тази цел се отчитат цифровизацията

[1] https://data.consilium.europa.eu/doc/document/ST-11599-2020-INIT/bg/pdf

и използването на информационни технологии в съответствие с правилата за връчване на документи и събиране на доказателства и преминаване към принципа „цифров по подразбиране“.

На 2 декември 2020 г. Европейската комисия излезе с изцяло нов пакет от мерки в областта на цифровизацията на европейските правосъдни системи, който включва Съобщение относно Цифровизация на правосъдието в ЕС – Инструментариум от възможности, Предложение за регламент относно компютърна система за комуникация в трансгранични граждански и наказателни производства (система e-CODEX), както и Съобщение „Гарантиране на справедливост в ЕС – европейска стратегия за съдебно обучение за периода 2021–2024 г.“.

На практика съществуващото дотогава законодателство на ЕС не изисква цифрови трансфери на данни в трансграничното сътрудничество и в резултат на това „по-голямата част от комуникацията остава на хартиен носител, като по този начин генерира неефективност в трансграничния обмен (главно по отношение на скоростта, надеждността, проследимостта и цената), усложнявайки достъпа на лицата и бизнеса до информация и забавяйки обмен между органите на държавите-членки“[2].

За да се решат тези проблеми, в Съобщението се обявяват редица законодателни инициативи, предвидени за 2021 г., като превръщане на цифровото съдебно сътрудничество в опция по подразбиране, създаване на съвместна платформа за сътрудничество на екипи за разследване по наказателни дела, актуализиране на правната рамка на системата за управление на дела на Евроюст.

Ясно се посочва поетата посока: „Въпреки че вече е направено много, предстои да бъде извършена значителна работа както на национално, така и на европейско равнище за по-нататъшното засилване на устойчивостта на правосъдните системи и повишаване на капацитета им за работа онлайн“[3].

Да оставиш изцяло в ръцете на държавите членки обаче разработването на собствени национални ИТ решения, крие риск от фрагментация и несъвместимост на системите, затова Европейската комисия очерта две направления, по които трябва да се насочат бъдещите действия. На първо място, на национално равнище е важно да се подкрепи дигиталното развитие

[2] Съобщение относно цифровизацията на правосъдието в ЕС, COM(2020) 710, Европейска комисия, декември 2020 г., с. 1.

[3] Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите „Цифровизация на правосъдието в ЕС Инструментариум от възможности“ (SWD(2020) 540 fina).

на правосъдните системи на държавите членки, да се засили „цифровото“ сътрудничество между различните национални съдебни органи, за да се извлече максимална полза за гражданите и предприятията.

На второ място, се поставя акцент върху нуждата от европейски подход в подобряването на трансграничното съдебно сътрудничество. Усилията трябва да се насочат върху по-нататъшната цифровизация на обществените услуги в областта на правосъдието, използването на сигурна и висококачествена технология за комуникация от разстояние (видеоконферентна връзка), улесняването на взаимното свързване на националните бази данни и регистри и насърчаването на използването на сигурни електронни канали за предаване на информация между компетентните органи. Именно върху втория аспект от посочените приоритети ще поставя акцент в настоящия текст.

2. Бърз напредък в приемането на европейско законодателство в областта на дигитализацията на трансграничното съдебно сътрудничество

Като израз на приоритизирането на електронното правосъдие на ниво ЕС през последните няколко години Европейската комисия предложи множество регламенти относно съдебното трансгранично сътрудничество, както и други законодателни инструменти в областта на гражданското, а също и на наказателното право.

А. Актуални законодателни текстове в областта на съдебното сътрудничество по гражданскоправни въпроси

Прилагането на комуникации от разстояние досега бе ограничено в ЕС. Например регламентът относно процедурата за европейска заповед за плащане и европейската процедура за искове с малък материален интерес (ЕПИММИ) позволяват само използването на комуникация от разстояние за подаване на заявление или отговор на иск[4]. Държавата членка, където се подава заявлението или трябва да се подаде искът, е тази, която определя дали това може да стане по електронен път. В Регламента относно европейската процедура за искове с малък материален интерес използването на технология и за изслушвания от разстояние чрез видеоконферентна връзка е

[4] Регламент (ЕС) 2015/2421 на Европейския парламент и на Съвета от 16 декември 2015 година за изменение на Регламент (ЕО) № 861/2007 за създаване на европейска процедура за искове с малък материален интерес и Регламент (ЕО) № 1896/2006 за създаване на процедура за европейска заповед за плащане, https://eur-lex.europa.eu/eli/reg/2015/2421/oj

включено като възможност. Процедурата за европейска заповед за плащане може да се управлява изцяло по електронен път, но само няколко държави членки са включили това.

Напредък бе постигнат и с приемането на регламента относно онлайн разрешаването на потребителски спорове[5], с който се създаде Платформата за онлайн решаване на спорове. Тя представлява единен портал за достъп, който позволява на потребителите и търговците в ЕС да уреждат споровете си, свързани както с национални, така и с трансгранични онлайн покупки. Това става чрез насочване на споровете към националните органи за алтернативно решаване на спорове, които са свързани към платформата.

През юни 2019 г. ЕС прие Директивата относно преструктурирането и втория шанс[6]. Една от целите на документа е процедурите по несъстоятелност постепенно да бъдат цифровизирани, което със сигурност ще помогне за намаляване на разходите и скъсяване на сроковете. Това са предпоставки, които стимулират бизнеса да се възползва по-пълноценно от възможността за правна защита на интересите си.

Европейските институции предложиха нов подход към цифровизацията на трансграничното съдебно сътрудничество с регламентите, одобрени на 25 ноември 2020 г.[7] и публикувани в Официалния вестник на ЕС на 2 декември 2020 г., които се отнасят до събирането на доказателства и връчването на документи по граждански или търговски дела. Чрез текстовете се установява така необходимата електронна комуникация между националните органи в контекста на трансграничното сътрудничество. В свят, в който цифровите технологии навлизат все повече, тези регламенти предвиждат електронното предаване като канал по подразбиране, що се отнася до комуникация и обмен на документи. Също така изрично се посочва принципът, че правната сила и

[5] Регламент (ЕС) № 524/2013 на Европейския парламент и на Съвета от 21 май 2013 година относно онлайн разрешаването на потребителски спорове и за изменение на Регламент (ЕО) № 2006/2004 и Директива 2009/22/ЕО, ОВ L 165/1.

[6] Директива (ЕС) 2019/1023 на Европейския парламент и на Съвета от 20 юни 2019 година за рамките за превантивно преструктуриране, за опрощаването на задължения и забраната за осъществяване на дейност, за мерките за повишаване на ефективността на производствата по преструктуриране, несъстоятелност и опрощаване на задължения и за изменение на Директива (ЕС) 2017/1132, ОВ L 172, 26.6.2019г., с. 18–55.

[7] Регламент (ЕС) 2020/1784 на Европейския парламент и на Съвета от 25 ноември 2020 г. относно връчване в държавите членки на съдебни и извънсъдебни документи по граждански или търговски дела („връчване на документи“) *(преработен текст)* Регламент (ЕС) 2020/1783 на Европейския парламент и на Съвета от 25 ноември 2020 г. относно сътрудничеството между съдилища на държавите членки при събирането на доказателства по граждански или търговски дела (събиране на доказателства) *(преработен текст)*

допустимостта на един електронен документ като доказателство в съдебни производства не могат да бъдат оспорени единствено на основанието, че той е в електронна форма.

Преразгледаният регламент относно връчването в държавите членки на съдебни и извънсъдебни документи по граждански или търговски дела предвижда още:

- всички комуникации и обмен на документи следва да се извършват чрез сигурна и надеждна децентрализирана ИТ система, включваща национални ИТ системи, които са взаимосвързани и технически оперативно съвместими, например базирани на e-CODEX. Предвижда се също така тази комуникация и обмен да се извършват при надлежно зачитане на основните права и свободи;
- използването на традиционни средства за комуникация трябва да се извършва само в случаи на прекъсване на ИТ системата или други извънредни обстоятелства;
- механизмите за директно трансгранично връчване следва да бъдат укрепени, като се позволи електронно връчване между държавите членки и същевременно се осигурят процесуални гаранции за страните.

Подобни разпоредби намираме и в преработения текст на регламента относно сътрудничеството между съдилища на държавите членки при събирането на доказателства по граждански или търговски дела. Като допълнение той предвижда, че с цел опростяване и ускоряване на събирането на доказателства видеоконферентната връзка или други комуникационни технологии от разстояние следва да се използват по-широко за директно събиране на доказателства от съдилищата.

Специално внимание заслужава един конкретен инструмент, който бих определил като най-важния и който в пакета от мерки на Европейската комисия е представен със законодателно предложение за нов регламент за компютризирана система за комуникация в трансгранични граждански и наказателни производства или т.нар. система e-CODEX.

Системата e-CODEX е „цифровият гръбнак“ на съдебното сътрудничество в ЕС по граждански и наказателни дела. Защо този елемент от пакета е толкова важен? Всъщност e-CODEX е основният инструмент за създаване на оперативно съвместима, сигурна и децентрализирана комуникационна мрежа между националните ИТ системи при трансгранични граждански, търговски и наказателни производства. Между 2010 и 2016 г. системата беше разработена и поддържана с финансиране от ЕС от консорциум от 21

държави членки. Доскоро обаче ѝ липсваше ясна и единна правна основа за целия ЕС.

За да коригира тази ситуация, на 2 декември 2020 г. Комисията представи предложение за регламент за e-CODEX като правен инструмент за официално създаване на системата на ниво ЕС. Предложеният регламент възлага на Агенцията на ЕС за оперативно управление на широкомащабни ИТ системи в областта на свободата, сигурността и правосъдието (eu-LISA) да поеме от 2023 г.[8] по-нататъшното разработване и поддържане на системата e-CODEX. Предаването на e-CODEX на eu-LISA ще стане не по-рано от 1 юли 2023 г. До този момент eu-LISA ще придобие необходимия капацитет (финансов и кадрови), за да управлява централния инструмент за цифрово съдебно сътрудничество в Европа.

Системата e-CODEX позволява на потребителите, независимо дали са съдебни органи, юристи или граждани, да изпращат и получават документи, правни форми, доказателства или друга информация по бърз и сигурен начин. Държавите членки вече са прилагали системата доброволно в процедури като Европейската заповед за плащане или европейската процедура за искове с малък материален интерес. Комисията разработва и системата за електронен обмен на електронни доказателства (eEDES), използвайки e-CODEX като комуникационен канал. Осен това e-CODEX е и софтуерното решение за създаването на децентрализирана ИТ система в контекста на трансграничното връчване на документи и исканията за събиране на доказателства.

Обхватът на регламента е ограничен до граждански и наказателни дела от компетентността на ЕС. Точките за достъп до e-CODEX могат да бъдат разрешени съгласно националното законодателство или законодателството на ЕС. Добавя се и ново правило, с което основните права и свободи на всички лица, участващи в електронния обмен на информация чрез системата e-CODEX, и по-специално правото на ефективен достъп до правосъдие, правото на справедлив процес, принципът на недискриминация, правото на защита на личните данни и правото на неприкосновеност на личния живот трябва да бъдат спазвани и зачитани в съответствие с правото на ЕС. Ново правило се добавя и относно правното действие на електронните доку-

[8] Регламент (ЕС) 2022/850 на Европейския парламент и на Съвета от 30 май 2022 година относно компютризирана система за трансграничен електронен обмен на данни в областта на съдебното сътрудничество по гражданскоправни и наказателноправни въпроси (система e-CODEX) и за изменение на Регламент (ЕС) 2018/1726, https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32022R0850

менти, според което документ не може да бъде отказан само на основание, че не е на хартиен носител. Комисията получава правомощията да издава актове за изпълнение, определящи подробни аспекти на функционирането на e-CODEX.

Като следваща стъпка в развитието на дигиталното трансгранично сътрудничество в своето Съобщение от декември 2020 г. ЕК посочва, че ще работи по законодателно предложение, чиято цел е цифровизацията на съдебното сътрудничество и на достъпа до правосъдие по трансгранични гражданскоправни, търговскоправни и наказателноправни въпроси и за изменение на определени актове в областта на съдебното сътрудничество. На 1 декември 2021 г. Комисията внесе предложение за хоризонтален регламент относно цифровизацията на съдебното сътрудничество и достъпа до правосъдие, предназначен да се прилага както за граждански и търговски, така и за наказателни производства от трансграничен характер в рамките на ЕС[9]. Като хоризонтален законодателен акт този регламент не заменя съществуващите правила за цифрово предаване на документи, цифрови изслушвания и други употреби на информационните технологии за трансгранично съдебно сътрудничество.

В законодателното предложение вече е включено „изискването“ съдилищата и другите компетентни органи на държавите членки да използват по подразбиране цифрови канали за трансгранична комуникация и обмен на данни, както и да приемат електронна комуникация. Това ще става чрез сигурна и надеждна децентрализирана информационна система, състояща се от информационни системи и оперативно съвместими точки за достъп, необходими за целите на трансграничния обмен между съответните органи на държавите членки. Използването на тези системи е задължително за компетентните съдебни или други органи на страните в ЕС, докато за физическите лица ще бъде по избор.

Чл. 3, пар.1 от предложението ясно посочва, че: „писмената комуникация между компетентните органи в случаите, които попадат в обхвата на правните актове, изброени в приложения I и II, включително обменът на формуляри, установени в тези актове, се осъществява чрез сигурна и надеждна децентрализирана информационна система“.

[9] https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A52021PC0759 Регламент на Европейския парламент и на Съвета относно цифровизацията на съдебното сътрудничество и на достъпа до правосъдие по трансгранични гражданскоправни, търговскоправни и наказателноправни въпроси и за изменение на определени актове в областта на съдебното сътрудничество.

Създава се също така Европейска точка за електронен достъп, която се намира на европейския портал за електронно правосъдие. Европейската точка за електронен достъп ще бъде част от децентрализираната информационна система и може да се използва от физическите и юридическите лица за електронна комуникация със съдилищата и компетентните органи по гражданскоправни и търговскоправни въпроси с трансгранично значение.

Предложението за Регламент въвежда и хоризонтални правила за провеждане на видеоконферентни връзки по граждански и търговски, а и по наказателни дела.

Вследствие на предприетите стъпки развитието на дигитализацията в областта на трансграничното съдебно сътрудничество обхваща не само гражданското, но и наказателното право.

Б. Актуални законодателни актове в областта на трансграничното съдебно сътрудничество по наказателноправни въпроси

Цифровизацията в областта на трансграничното съдебно сътрудничество по наказателноправни въпроси също се откроява като съществен аспект в Съобщението от декември 2020 г.

Предложението за регламент за създаване на платформа за сътрудничество и подпомагане на функционирането на Съвместните екипи за разследване (СЕР) от 1 декември 2021 г. е част от широката стратегия за цифровизация на правосъдието, предложена от ЕК. В Съобщението си относно цифровизацията на правосъдието в ЕС – инструментариум от възможности, Комисията обясни, че ефективността на съвместните разследващи екипи може да бъде допълнително подобрена чрез специфична ИТ среда, съобразена с техните нужди. Това би направило сътрудничеството по-лесно и по-интензивно, позволявайки създаването на съвместните екипи и допринасяйки за по-ефективната им работа чрез инструменти за комуникация и обмен и съхранение на документи/доказателства.

Създадени с Рамково решение на Съвета от 13 юни 2002 г., съвместните екипи за разследване обединяват следователи и прокурори от държавите членки, а също и от страни извън ЕС, когато е необходимо, подпомагани от Европол и Евроюст. Те са широко признати като една от най-ефективните стъпки при извършване на трансгранично разследване.

Комисията направи законодателно предложение за регламент за създаване на специална ИТ платформа, която да се използва на доброволна основа в подкрепа на функционирането на съвместните екипи за разследване. Предложението установява правила за работа на платформата и разпределе-

ние на отговорностите, определя условия за достъп и въвежда специфични разпоредби, така че да осигури адекватно ниво на защита и сигурност на данните. Основната цел е да се повиши ефикасността и ефективността на разследванията и съдебните преследвания, извършвани от съвместни екипи в трансгранични случаи чрез улесняване на комуникацията и сътрудничеството. За да се изпълни този ангажимент, се предлага създаването на специална ИТ платформа, достъпна за всички участници в съвместните екипи. Тя се състои от централизирана информационна система за временно съхранение на данни и комуникационен софтуер, който позволява сигурното локално съхранение на комуникационни данни в устройствата на ползвателите на платформата за сътрудничество (чл. 4). Въпреки че за да осигури гъвкав достъп платформата ще работи по интернет, още при дизайна ѝ ще се акцентира върху осигуряването на конфиденциалност чрез алгоритми за криптиране на данни в транзит или в покой.

Регламент (ЕС) 2023/969 на Европейския парламент и на Съвета от 10 май 2023 година за създаване на платформата за сътрудничество за подпомагане на функционирането на съвместните екипи за разследване беше публикуван в Официалния вестник на ЕС на 17.05.2023 г.[10]. Той ще влезе в сила на 20-ия ден след публикуването, а самата платформа трябва да стане активна не по-късно от 7 декември 2025 г.

Регламентът признава успеха на съвместните екипи за подобряване на съдебното сътрудничество за разследване и наказателно преследване на трансгранични престъпления. Той предоставя две правни рамки за създаване на съвместни екипи за разследване – предвижда екипите да включват поне две държави членки на ЕС и позволява на трети държави да участват, когато има правно основание за това.

Регламентът подчертава значението на международното сътрудничество при справяне с трансгранични престъпления и улеснява обмена на информация и доказателства между националните компетентни органи и международните съдебни органи, какъвто например е Международният наказателен съд.

За да бъдат по-резултатни трансграничните разследвания, регламентът създава платформа за сътрудничество на съвместните екипи за разследване. Тя ще гарантира сигурни комуникационни канали, ще даде възможност за обмен на информация и доказателства, ще подкрепи проследимостта на доказателствата и ще улесни оценката на дейността на екипите (чл. 5).

[10] https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32023R0969

Платформата ще се управлява от Агенцията на ЕС за оперативно управление на широкомащабни ИТ системи (eu-LISA) и ще бъде свързана със съществуващи ИТ инструменти като например Мрежовото приложение за защитен обмен на информация (SIENA), управлявано от Европол. Евроюст ще осигури подкрепа чрез секретариата на мрежата на съвместните екипи за разследване, който ще подпомага потребителите на платформата за сътрудничество, ще предоставя насоки и обучение, а също и връзка с вече съществуващите ИТ инструменти.

Като част от своя пакет от мерки за цифровизиране на европейските съдебни системи, ЕК предложи на 1 декември 2021 г. регламент по отношение на цифровия обмен на информация по дела за тероризъм.[11]

Предложението изменя както регламента за Евроюст, така и Решение 2005/671/ПВР на Съвета, за да модернизира настоящите практики за обмен на информация по съдебни дела, свързани с тероризма, между държавите членки и Евроюст. Амбицията е да се засили ролята на агенцията, предвидена в Регламента за Евроюст по отношение на координацията и сътрудничеството между националните разследващи и наказателни органи при тежки престъпления и особено при тероризъм. Очаква се новите правила да повишат ефективността и сигурността на обмена на данни между държавите членки, Евроюст и трети държави и да позволят идентифицирането на връзките между паралелни трансгранични разследвания и съдебни преследвания по отношение на терористични престъпления.

По силата на новите правила държавите членки ще трябва да споделят с Евроюст информация за всяко наказателно разследване, свързано с тероризъм, още на ранен етап, след като данните бъдат отнесени до националните съдебни органи. Регламентът също така ще създаде модерна (цифрова) система за управление на дела за съхраняване и кръстосана проверка на получената информация. Това ще подобри координацията в борбата на ЕС срещу тежката трансгранична престъпност и тероризма. Така и трите органа – Евроюст, Европол и Европейската прокуратура, ще бъдат запознати с текущите разследвания и наказателни преследвания.

Европейските съзаконодатели засилват разпоредбата относно защитата на данните, ограничавайки предаването на лични данни до нуждите за идентификация.

Договореният текст беше потвърден от Съвета (Корепер) на 22 декември 2022 г. Комисията по граждански свободи, правосъдие и вътрешни

[11] https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52021PC0757

работи на Европейския парламент даде зелена светлина на споразумението на 11 януари 2023 г. В момента тече преглед от юристите лингвисти на двете институции. Окончателното приемане се очаква в най-кратки срокове.

Заключение

Всеки от предлаганите инструменти е важна стъпка напред, но съвкупността от тях ни дава усещането за реален напредък по пътя към необходимата модернизация на трансграничното съдебно сътрудничество в дигиталната ера. Процесът на модернизация и хармонизация на законодателството в ЕС със сигурност ще продължи да се развива и през следващите години, защото има потенциал допълнително да подобри достъпа до правосъдие и ефективността на съдебната система като цяло, да ускори работата и структурирането на производствата, да сведе до минимум разходите за гражданите и бизнеса.

Важно е да не оставяме тези инструменти на добрата воля на държавите членки, а да ги превърнем в императивни норми, които надграждат добрите практики в съдебните производства и в трансграничното сътрудничество във всички държави членки. Разбира се, европейският подход трябва да гарантира и процесуалните права при използването на цифрови инструменти в правосъдните системи за тези, които нямат достъп до необходимите технологии или умения да работят с тях.

Ефективната трансформация не би била възможна без насърчаване на цифровата компетентност в сектора на правосъдието, така че съдиите, прокурорите, съдебните служители и другите практикуващи юристи да прилагат пълноценно новите инструменти при надлежно зачитане на правата и свободите на лицата, търсещи правосъдие.

Библиография:

1. Съобщение на Европейската комисия до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите „Цифровизация на правосъдието в ЕС Инструментариум от възможности“ (SWD(2020) 540 final).
2. Commission staff working document Accompanying the Communication Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions „Digitalisation of justice in the European Union a toolbox of opportunities“ (SWD(2020) 540 final).

3. Предложение за регламент на Европейския парламент и на Съвета относно компютърна система за комуникация в трансгранични граждански и наказателни дела производство (система e-CODEX) и за изменение на Регламент (ЕС) 2018/1726.
4. Commission staff working document: Impact Assessment report Accompanying the document Proposal for a regulation of the European parliament and the Council on a computerised system for communication in cross-border civil and criminal proceedings (e-CODEX system), and amending Regulation (EU) 2018/1726
5. Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите „Гарантиране на справедливост в ЕС – европейска стратегия за съдебно обучение за периода 2021–2024 г.“, COM(2020) 713 final.
6. Заключения на Съвета ПВР от 12–13 юни 2007 г., с. 43 от документ 10267/07.
7. Заключения на Съвета „Достъп до правосъдие – оползотворяване на възможностите, предоставяни от цифровизацията“, 13 октомври 2020 г., 11599/20.
8. Съобщение на Европейската комисия: „Към европейска стратегия в областта на електронното правосъдие“ от 5 юни 2008 г. (COM(2008) 329 окончателен.
9. Резолюция на Европейския парламент относно електронното правосъдие от 18 декември 2008 г., 2008/2125 (INI).
10. Многогодишен план за действие за периода 2009–2013 г. в областта на европейското електронно правосъдие (ОВ С 75, 31.3.2009 г.).
11. Многогодишен план за действие за периода 2014–2018 г. в областта на европейското електронно правосъдие (ОВ С 182, 14.6.2014 г.).
12. Проект за Стратегия за европейското електронно правосъдие за периода 2014–2018 г. (ОВ С 376, 21.12.2013 г.).
13. Directorate-General for Justice and Consumers (European Commission), Trasys International Study on the use of innovative technologies in the justice field, Final Report, September 2020.
14. Eric Hilgendorf Introduction: Digitization and the Law – a European Perspective page 9–20.
15. Antonio Cordella, Francesco Contini, Digital Technologies for Better Justice A Toolkit for Action, April 2020.

16. Eisele K., Digitalisation of cross-border judicial cooperation, EPRS, European Parliament, April 2022.
17. European Commission, Directorate-General for Justice and Consumers, Study on the digitalisation of cross-border judicial cooperation in the EU: final report, 2022, https://data.europa.eu/doi/10.2838/174474
18. European Commission, Directorate-General for Justice and Consumers, Cross-border digital criminal justice: final report, Publications Office, 2020, https://data.europa.eu/doi/10.2838/118529
19. Deloitte , Directorate-General for Justice and Consumers (European Commission): Cross-border Digital Criminal Justice Final Report, June 2020.
20. Xandra Kramer*, Digitising access to justice: the next steps in the digitalisation of judicial cooperation in Europe, Published in Revista General de Derecho Europeo 56 (2022), p. 1–9 (editorial article).
21. Vasile Nemeş, Gabriela Fierbinţeanu. „DIGITAL TOOLS FOR JUDICIAL COOPERATION ACROSS THE EU – THE BENEFITS OF DIGITAL TECHNOLOGIES IN JUDICIAL PROCEEDINGS“. LESIJ – Lex ET Scientia International Journal 1:7–15.
22. Marek Swierczyniski, Critical evaluation of new Council of Europe guidelines concerning digital courts Review of European and Comparative Law 2022, Vol. 48, No. 1, 133-155, Published: 10 March 2022.

Интелектуалната собственост и изкуственият интелект – основни положения и очаквания

Лилия Симеонова*,
докторант, Югозападен университет „Неофит Рилски“

Статията има за цел да отбележи технологичния напредък в различни сектори на обществения живот, в частност появата на ИИ в сферата на творчеството и иновациите. Отделено е внимание на необходимостта от съобразяване и адаптиране на правната уредба, регулираща правото на интелектуалната собственост, на ефективността на неговия режим спрямо развитието на технологиите и културните промени, с които се намира в неразривна връзка. Поставя се акцент върху основни въпроси, касаещи риска от нарушения върху изобретенията и авторството им.

***Ключови думи**: изкуствен интелект (ИИ), интелектуална собственост, авторско право, Европейски съюз*

* Лилия Симеонова е адвокат, завършила е право в Софийски университет „Св. Климент Охридски“. Специализира в областта на наказателното право и процес. Участва в разработване на законопроекти за изменение и допълнение на НПК, ЗЗДН, ЗМ и др. Към момента е заместник-председател на Националното бюро за правна помощ, ел. поща: adv.lilia.simeonova@gmail.com

Intellectual Property and Artificial Intelligence – basic notions and expectations

Liliya Simeonova*,
PhD student, Southwest University „Neofit Rilski“

The article aims to explain the technological advances in various sectors of public life, in particular the emergence of AI in the field of creativity and innovation. Attention is paid to the need to take into account and adapt the legal framework regulating Intellectual.Property law, the effectiveness of its regime in relation to the development of technology and the cultural changes with which it is inextricably linked. The article focuses on key issues concerning the risk of infringement of inventions and authorship.

Keywords*: Artificial Intelligence/AI/, Intellectual Property, Copyright, European union*

* Liliya Simeonova is a lawyer, Master of Law from Sofia University “St. Kliment Ohridski”. Specializing in criminal law and criminal process. Has participated in the development of projects for amendments and additions to the Criminal Procedure Code (CPC), Domestic Violence Protection Act (DVPA), Mediation Law (ML), etc. She is currently the Deputy Chairman of the National Legal Assistant Bureau, e-mail: adv.lilia.simeonova@gmail.com

Технологичният напредък ярко бележи нашето време, а редица сектори на живота ни го приветстват, като все по-широко отварят вратите си за посрещане на новите постижения на цифровите технологии. Те от своя страна неумолимо и необратимо променят живота на хората. Но тази трансформация трябва да бъде в полза на обществото и да не вреди на природата ни. С тази цел органите на ниво Европейски съюз предприемат редица актове, с които укрепват своя цифров суверенитет и определят стандарти, които да осигурят тази защита.[1]

От култови моменти от научнофантастични филми и романи, през силно развито въображение, развити фантазии до съвременна реалност – до това доведе настъпването на цифровата ера, в която живеем. Правната уредба следва бурното развитие на човечеството и дължи своевременно адаптиране, с цел охрана на неговите интереси.

В последните месеци все повече се говори за генеративен изкуствен интелект и приложенията като ChatGPT, Midjourney, Bing и др., задвижвани от изкуствен интелект, които биват използвани ежедневно, и то от представители на все по-ниски възрастови групи.

Изкуственият интелект (ИИ) се появява в сферата на творчеството и иновациите и вече е неизменна част от нашата реалност. Новите технологии на ИИ предоставят впечатляващи възможности за развитие на творческите изкуства, развлекателната индустрия, както и за изобретения, подобряващи живота, напр. в медицината и други сериозни сфери. Това налага социални, икономически и етични последици, както и необходимост от адаптиране на политиката за тях. Така през септември 2019 г. Световната организация за интелектуална собственост (СОИС) провежда дебат за интелектуалната собственост и ИИ, в който участват държавите членки и други заинтересовани страни, за да се обсъди въздействието на ИИ върху политиката в областта

[1] Вж. Съобщение на Комисията до Европейския парламент, Съвета, Икономическия и социален комитет и Комитета на регионите – Изкуствен интелект за Европа, достъпен на: https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52018DC0237&from=EN

Регламент (ЕС) 2022/2065 На Европейския парламент и на Съвета от 19 октомври 2022 година относно единния пазар на цифрови услуги и за изменение на Директива 2000/31/ЕО (Акт за цифровите услуги), достъпен на: https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32022R2065

Communication from the Commission to the European Parliament, the Council, the European Economic And Social Committee and the Committee of the Regions 2030 Digital Compass: the European way for the Digital Decade, достъпен на: https://commission.europa.eu/system/files/2023-01/cellar_12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02_DOC_1.pdf

на интелектуалната собственост, за да се обобщят основните въпроси, които следва да бъдат поставени. През декември 2019 г. СОИС публикува своя доклад с апел за коментари от възможно най-широка световна аудитория.[2]

Интелектуалната собственост (ИС) е в неразривна връзка с развитието на новите технологии, от тяхната поява и на свой ред правната уредба следва да бъде съобразявана и адаптирана спрямо развитието на технологиите и културните промени. Основни въпроси, касаещи собствеността и нарушенията върху изобретенията и авторството, поставят с пълна сила необходимостта от засилване на ефективността на режима на интелектуалната собственост.

Общоприетата дефиниция на термина „интелектуална собственост“ Световната организация за интелектуална собственост отнася до „творения на ума, като изобретения; литературни и художествени произведения; дизайни; и символи, имена и изображения, използвани в търговията“. С оглед същината на днешното изложение, няма да акцентираме върху същината на понятието и приложимата нормативна рамка. Последната, към актуалния момент, можем да обобщим като трайно установила се, хармонизирана на ниво Европейски съюз или в процес на хармонизация, и пред която като основно предизвикателство стои именно интеракцията на интелектуалната собственост с изкуствения интелект.[3] Изкуственият интелект влияе върху сегашната система на правата върху интелектуална собственост. Инструментите на ИИ се използват за улеснение на търсенето, проучването, администрирането и прилагането на правата върху ИС. Инструментите на ИИ и произведенията създадени от тях може да бъдат защитени с инструментите на авторското право и патентната закрила. Такава защита може да стимулира по-нататъшното им разработване, но и да ограничи ползването и разпространението им.

Може би е достатъчно да отбележим, че интелектуалната собственост включва две категории права – индустриалната собственост, обхващаща патенти, търговски марки, промишлени дизайни и модели и наименования

[2] Draft Issues Paper on Intellectual Property Policy and Artificial Intelligence, WIPO/IP/AI/2/GE/20/1, December 13, 2019, достъпен на: https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_ai_2_ge_20/wipo_ip_ai_2_ge_20_1.pdf

[3] В този смисъл са: Регламент (ЕС) 2017/1001 на Европейския парламент и на Съвета от 14 юни 2017 година относно марката на Европейския съюз; Директива 2001/29/ЕО на Европейския парламент и на Съвета от 22 май 2001 година относно хармонизирането на някои аспекти на авторското право и сродните му права в информационното общество; Директива (ЕС) 2019/790 на Европейския парламент и на Съвета от 17 април 2019 година относно авторското право и сродните му права в цифровия единен пазар и за изменение на директиви 96/9/ЕО и 2001/29/ЕО и др.

за произход, и авторското право и сродните му права, обхващащи художествените и литературните произведения.

По-комплексни са въпросите, отнасящи се до второто понятие – „изкуствен интелект“. Прието е, че терминът изкуствен интелект води началото си от 1956 г. на научна конференция в Дартмут, която се възприема като основополагащ момент в създаването на ИИ като отрасъл. Докато за авторско право се говори още през 1700 г., та и преди това, за ИИ – от 1956.

Преди да разгледаме актуалното положение, следва да направим кратко уточнение, свързано с неимоверните усилия на европейските институции с оглед създаването на първия акт, регулиращ изкуствения интелект. Към 7 май 2023 г., след месеци на продължителни и натоварени преговори, различията между членовете на Европейския парламент са преодолени и е постигнат консенсус относно текста на първия законодателен акт за изкуствения интелект на ниво Европейски съюз.

На 11 май Комитетът по вътрешния пазар и Комитетът по граждански свободи приеха проект на мандат за преговори относно първите в историята правила за изкуствен интелект с 84 гласа „за“, 7 „против“ и 12 „въздържал се“.[4] Чрез поправките си към предложението на Комисията членовете на Европейския парламент се стремят да се осигурят гаранции, че системите за изкуствен интелект се наблюдават от хора, че са безопасни, прозрачни, проследими, недискриминационни и щадящи околната среда. Цели се приемане на единно определение за Изкуствения интелект, което да се използва за в бъдеще. Правилата следват подход, основан на риска. С тях се предвиждат задължения за доставчиците и потребителите, които са поставени в зависимост от нивото на риска, който Изкуственият интелект може да генерира. Задълженията за доставчиците на модели в областта на ИИ трябва да гарантират стабилна защита на основните права, здравето и безопасността и околната среда, демокрацията и върховенството на закона.

Моделите на генеративната основа, като ChatGPT, ще спазват допълнителни изисквания за прозрачност, например да оповестяват, че съдържанието е генерирано от ИИ, да проектират модела така, че да предотвратят генерирането на незаконно съдържание и да публикуват резюмета на защитените с авторски права данни, използвани за обучение. Заявена е подкрепа за иновациите и защита на правата на гражданите, а с предвидените изключения от тези правила за научноизследователски дейности и компоненти на

[4] Прессъобщение на Европейския парламент*:* AI Act: a step closer to the first rules on Artificial Intelligence, достъпно на: https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence

ИИ се цели да бъдат стимулирани иновациите в областта на ИИ. Отделено е внимание към широк кръг възможности за гражданите да подават жалби относно системите за ИИ и да получават обяснения за решения, основани на високорискови системи за ИИ, които оказват значително въздействие върху техните права.

На 14 юни Европейският парламент прие своята преговорна позиция по Акта за изкуствения интелект преди започването на преговорите със Съвета на ЕС по окончателния вид на закона[5]. С 499 гласа „за“, 28 „против“ и 93 „въздържал се“ се решава новите правила да гарантират, че разработеният и използван в Европа ИИ е в пълно съответствие с правата и ценностите на ЕС, включително човешкия надзор, безопасността, неприкосновеността на личния живот, прозрачността, недискриминацията и социалното и екологичното благосъстояние.

В момента освен с проекта за регламент, можем да боравим и с множество официални документи на институциите на ЕС като становища, препоръки, доклади и предложения, доказателство за неимоверните усилия на ниво ЕС за постигане на споразумение върху бъдещата регламентация.[6]

Да се върнем на понятието за ИИ в проекта за регламент на ИИ[7]. В преамбюла на този документ се посочва, че понятието „система за изкуствен интелект“ следва да бъде ясно дефинирано, за да се осигури правна сигурност, като същевременно се гарантира гъвкавост за приспособяване към бъдещото технологично развитие. Дефиницията трябва да се основава на ключовите функционални характеристики на софтуера, по-специално способността, за даден набор от дефинирани от човека цели, да генерира резултати като съдържание, прогнози, препоръки или решения, които влияят на средата, с която системата взаимодейства, било то във физическо или цифрово измерение. А система на ИИ е дефинирана като „софтуер, който е разработен с една или повече от техниките и подходите, изброени в приложение I, и може за даден набор от цели, дефинирани от човека, да генерира резултати като съдържание, прогнози, препоръки или решения, влияещи върху средата, с която взаимодействат“.

---

[5] Прессъобщение на Европейския парламент: https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai

[6] Подробен списък на приложими документи на: https://artificialintelligenceact.eu/documents/

[7] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial IntelligenceAact) and amending certain Union legislative acts, достъпен на: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

Многобройни са примерите, доказващи, че технологиите на ИИ се проявяват в множество сектори на икономиката, а изследователските и творческите дейности са в пряка зависимост от тези технологии. Градиращата сложност на тези технологии на ИИ пораждат множество предизвикателства към цялото общество за преосмисляне на основните, ориентирани към човека концепции за правото на интелектуална собственост.[8] Така например, наблюдавайки динамичния подем на технологиите, които използват ИИ, ставаме свидетели на един вид реализация на гениалните идеи на сценаристи и режисьори на множество "sci-fi" филми от нашето детство – чатботове пишат домашни, курсови работи, а дори и клаузи на договори и присъди, автомобили се управляват сами, умни асистенти постоянно ни подпомагат в работата и ежедневието ни, прахосмукачките се управляват сами, приложения създават картини по модел и стил на най-великите художници в историята на изкуството и множество други примери.

С оглед това интензивно навлизане на ИИ във всички сфери на живота, все по-значим става въпросът за приемане на такава регулаторна рамка, която да осигури гаранции за безопасност и минимизиране на рисковете, свързани с използването на ИИ, за управление и ефективно прилагане на съществуващото законодателство и за създаване и развитие на единен пазар за законни, безопасни и надеждни приложения.

След щрихираната картина на приложимостта на изкуствения интелект във всяка сфера от живота ни, следва да обърнем внимание на въпроса какви са възможните интеракции между изкуствения интелект и интелектуалната собственост. В тази връзка интерес буди връзката изкуствения интелект и авторското право. Последното е символ на себеизразяване, на творчески дух и талант от висше естество, което мнозина биха могли да интерпретират всъщност като антипод на феномена изкуствен интелект. От някогашната борба на великите френски автори като Виктор Юго и Балзак за защитата на неимуществените права[9] и интереси на авторите днес се изправяме пред нова изява на необходимост от защита на авторски и сродни права в съвсем различен съвременен и модерен контекст.

Както стана ясно, приложенията с изкуствения интелект могат да създават самостоятелно литературни, музикални и художествени произведения. Това е прекрасно, но възникват въпроси за системата на авторското

[8] Както изрично подчертава Anke Moerland в „AI and Intellectual Property Law" в: Lim, E., and Morgan P., "The Cambridge Handbook of Private Law and Artificial Intelligence".

[9] Atkinson, B., Fitzgerald, B. 2011. A short history of copyright – The Genie of Information, с. 50.

право и тясно свързаните с него подвъпроси за признанието на автора, за възнаграждението му, за неговите неимуществени/морални права и др. Всъщност системата на авторското право датира от началото на XVIII в. И от времето на печатарската преса е съвкупност от закони, които предоставят изключителни права върху авторски произведения: изключителното право да се копира или възпроизвежда дадено произведение, да се публикува и да се изпълнява или предава публично.

Същевременно е невъзможно разрешаването на проблемите да стане с простото изключване на произведенията, рожба на изкуствения интелект, от правото на закрила. Несъмнено такъв подход не би бил приемлив, защото към настоящия момент, онагледено предадено, тези конкретни алгоритми функционират на базата на въведени данни, които служат за основа за генериране на друго ново произведение/изображение. Европейският законодател допуска като възможно в бъдеще да се достигне до автономност на изкуствения интелект или поне до ниво, при което човешкият принос би бил незначителен. Следователно може в бъдеще да достигнем ера, в която машините не само ще подпомагат хората в творческия процес, но и напълно сами ще изобретяват творби. Към днешна дата обаче този процес не е изцяло автономен, а по-скоро се касае до взаимност в действията на творци или изобретатели и изкуствения интелект. Затова понастоящем правото на интелектуална собственост се прилага към 1) изобретения, реализирани с изкуствения интелект, и стимулира тяхното разработване и към 2) продукти, създадени с помощта на изкуствения интелект и генерирани от изкуствения интелект. Такава е класификацията на изследователска група към института „Макс Планк“ за иновации и конкуренция, която прави разграничения между а) изобретения, създадени от изкуствения интелект (когато изкуственият интелект действа без човешка намеса – автономно), б) изобретения, подпомагани от изкуствения интелект (когато хората използват изкуствения интелект като инструмент за изобретяване) и в) изобретения, реализирани от ИИ (когато ИИ е реализиран като част от изобретението). И тук възникват много въпроси, които предстои в бъдеще да получат своя отговор: Кой следва да бъде признат за автор на произведение, създадено с помощта на технология на ИИ? Каква следва да бъде дефиницията на изискването за оригиналност на произведенията в контекста на такива, генерирани от изкуствения интелект? Системата на авторското право е свързана с човешкия творчески дух за насърчаване на себеизразяването на човешкото същество.

В основополагащото решение по делото *Painer* на Съда на ЕС от 2011 г[10]. Съдът постановява, че едно интелектуално творение е собствено на автора, ако отразява неговата личност. Това е така, ако авторът е бил в състояние да изрази творческите си способности при създаването на произведение, като е направил свободен и творчески избор… като прави тези различни избори, авторът на портретна снимка може да запечата създаденото произведение със своя „личен почерк“. Това подчертава необходимостта от принос на човешката личност към създаването на произведения, защитени с авторско право. Така съгласно дългогодишната практика на СЕС става ясно, че е необходим принос на човешката личност към създаването на произведения, защитени с авторско право. Или въведеният от съдебната практика стандарт за оригиналност в друго свое решение (*Infopaq*)[11] съдържа два елемента – произведението да не е било копирано и да представлява интелектуално творение. Първото изискване може да е изпълнено от система с изкуствения интелект, но второто – не. Разширяването на защитата на авторските права чрез включването и на произведения, генерирани от изкуствения интелект, би могло, съгласно някои автори, да подкопае основите на философските възгледи и възприятия за същността на авторското право и базата, върху която се изгражда защитата.

Далеч не съм изчерпателна с оглед и краткото време, с което разполагам, за експозе по тази изключително обширна тема, тъй като обективно в настоящия форум няма време да засегнем въпроса за връзката патенти – изкуствен интелект, марки и изкуствен интелект и другите подгрупи на интелектуалната собственост, да засегнем проблемите, свързани със защитата на интелектуалната собственост за технологиите с изкуствения интелект, за компютърните програми, прилагащи технология за изкуствения интелект, патентната защита на компютърно реализираните изобретения и др., както и да развием в дълбочина връзката авторско право – изкуствен интелект.

И все пак можем да обобщим, че есенцията на проблематиката във взаимовръзката между изкуствения интелект и авторското право в частност се състои именно в анализа дотук – защитата, авторството и собствеността върху творческите продукти, създадени с помощта на изкуствен интелект и генерирани такива от ИИ, защото това е фундаментално предизвикателство

[10] Judgment of the Court (Third Chamber) of 1 December 2011, *Eva-Maria Painer v Standard VerlagsGmbH and Others*, C-145/10.

[11] Judgment of the Court (Fourth Chamber) of 16 July 2009, *Infopaq International A/S v Danske Dagblades Forening*, C-5/08.

за антропоцентричния режим на авторското право, в който главна роля има човешкото същество. Твърде консервативно би било оставянето на такива произведения, създадени с участието на ИИ, без закрила. Но все пак предстои да бъде даден отговор на много въпроси, както и да се задълбочат изследванията относно потенциално вредните последици както от оставянето на такива произведения без закрила, така и от евентуално предоставянето на еднаква по обем такава с предоставяната на произведения, плод на чисто човешка дейност. Предизвикателствата и въпросите са много, затова е необходимо политици, законодатели, интелектуалци от цял свят да обединят усилия и да дадат адекватен законодателен отговор.

В заключение, внимание заслужава фактът, че на 28 април 1838 г. Оноре дьо Балзак и петдесет писатели, сред които Виктор Юго, Жорж Санд и Александър Дюма, се срещат при Луи Деноайе, директор на известен в онзи момент вестник, за да изготвят устава на Обществото на хората на литературата. Причината за тази безпрецедентна инициатива е формулирана от самите тях чрез призива „Защитавайте моралните и имуществените права на авторите“. Тази инициатива е важна стъпка в историята за очертаване на законодателната рамка за защита на авторските произведения. Опитът на тази смела група следва да бъде използван и сега, когато се поставят основите за разширяване на законодателната рамка за защита на авторските права чрез включване в обхвата ѝ и на произведения, родени с намесата на изкуствения интелект.

Начинът на защита на творенията на системите с изкуствен интелект чрез авторското право е един от най-значимите и сложни правни въпроси на нашето време. Обсъждан от заинтересованите страни по целия свят, въпросът досега е избегнал консенсус. Въпреки това към актуалния момент мнозина приветстват появата на генеративния и изкуствен интелект, виждайки в него още една мощна технология, като софтуерните текстоборотващи програми и видеоредакторите, която ще даде възможност на творците да се изразяват по-добре.

Други се опасяват, че изкуственият интелект ще обезцени художествените произведения и самите творци, като замени живото човешко творчество със студен, безчувствен алгоритъм. Може би обективният извод е някъде по средата. Предстои да разберем.

Библиография:

1. Директива 2001/29/ЕО на Европейския Парламент и на Съвета от 22 май 2001 година относно хармонизирането на някои аспекти на авторското право и сродните му права в информационното общество.
2. Директива (ЕС) 2019/790 на Европейския парламент и на Съвета от 17 април 2019 година относно авторското право и сродните му права в цифровия единен пазар и за изменение на директиви 96/9/ЕО и 2001/29/ЕО.
3. Прессъобщение на Европейския парламент: AI Act: a step closer to the first rules on Artificial Intelligence, достъпно на: https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence
4. Прессъобщение на Европейския парламент: https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai
5. Приложими документи по темата, достъпни на: https://artificialintelligenceact.eu/documents/
6. Съобщение на Комисията до Европейския парламент, Съвета, Икономическия и социален комитет и Комитета на регионите – *Изкуствен интелект за Европа*, достъпен на: https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52018DC0237&from=EN
7. Регламент (ЕС) 2022/2065 на Европейския парламент и на Съвета от 19 октомври 2022 година относно единния пазар на цифрови услуги и за изменение на Директива 2000/31/ЕО (Акт за цифровите услуги), достъпен на: https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32022R2065
8. Регламент (ЕС) 2017/1001 на Европейския парламент и на Съвета от 14 юни 2017 година относно марката на Европейския съюз
9. Anke Moerland в „AI and Intellectual Property Law”в: Lim, E., and Morgan P., “The Cambridge Handbook of Private Law and Artificial Intelligence”.
10. Atkison, B., Fitzgerald, B, 2011, A short history of copyright – The Genie of Information.
11. Communication from the Commission to the European Parliament, the Council, the European Economic And Social Committee and the Committee of the Regions 2030 Digital Compass: the European way for the Digital Decade, достъпен на: https://commission.europa.eu/system/files/2023-01/cellar_12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02_DOC_1.pdf

12. Draft Issues Paper on Intellectual Property Policy and Artificial Intelligence, WIPO/IP/AI/2/GE/20/1, December 13, 2019, достъпен на: https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_ai_2_ge_20/wipo_ip_ai_2_ge_20_1.pdf
13. Judgment of the Court (Third Chamber) of 1 December 2011, Eva-Maria Painer v Standard VerlagsGmbH and Others, C-145/10.
14. Judgment of the Court (Fourth Chamber) of 16 July 2009, Infopaq International A/S v Danske Dagblades Forening, C-5/08.
15. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial IntelligenceAact) and amending certain Union legislative acts, достъпен на: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

Електронното управление и обработването на лични данни за целите на архивирането в обществен интерес, за научни или исторически изследвания

Райна Николова*

Докладът се фокусира върху европейското и националното законодателство, които гарантират възможността да се разкриват конкретни лични данни за целите на архивирането, при научни и исторически изследвания. Преследваните цели са легитимни от гледна точка на защитата на обществения интерес – тогава те са колективни: да се съхрани националното архивно наследство, да се запази културната памет и защити националната идентичност. Легитимни могат да са и преследваните от индивида лични, субективни цели: да се упражни свободата на художественото и научното творчество или защита на семейния живот чрез проучване на родословието и по този начин запазване на фамилната свързаност и кръвна идентичност.

Ключови думи: *архивиране, лични данни, научни и исторически изследвания*

* Райна Николова, доктор на науките, професор в департамент „Право“ на Нов български университет, ел. поща: rnikolova@ nbu.bg.

The electronic management and processing of personal data for archiving purposes in the public interest, scientific or historical research

Raina Nikolova*

The report focuses on the European and national legislation that guarantees the possibility to disclose specific personal data for archiving purposes, scientific and historical research. The objectives pursued are legitimate from the point of view of protecting the public interest – they are then collective: to preserve the national archival heritage, to preserve cultural memory and to protect national identity. The personal, subjective aims pursued by the individual may also be legitimate: to exercise freedom of artistic and scientific creativity or to protect family life through genealogical research and thus preserve family coherence and blood identity.

Keywords: *Archiving, Digital Services, Personal Data, Scientific And Historical Research Purposes*

* Raina Nikolova, Dr. Habil., Professor, Law Department, New Bulgarian University, e-mail: rnikolova@nbu.bg.

Увод

Научните изследвания в юридически смисъл се разглеждат почти задължително през темата за нормативната уредба на дейността по опазването на националната културна памет, отразена в архивното наследство. Това институционално усилие се осъществява чрез съхраняването на архивните фондове и предоставянето на административни услуги на представителите на изследователската общност и електронното споделяне на данни със съответните служби на общинската администрация. Самото запазване на националното нематериално богатство се извършва от редица публичноправни организации в Република България. При използването на архивни документи за научни или исторически изследвания неминуемо се засягат лични данни на гражданите, за които се провеждат съответните проучвания. Тези данни е от обществен интерес да станат достъпни за широк кръг лица. Това е и смисълът на всяко научно издирване. Често пъти интересът към историческото познание се конфронтира с личната информация за гражданите, която е от частен интерес и по принцип не е значима за обществото[1]. С особена сила този проблем възниква при провеждането на родови проучвания и отказа на общинската администрация да предоставя сведения. Трудностите при електронното управление и споделянето на информация при обработването на лични данни за целите на архивирането по повод осъществяването на тези изследвания от обществен интерес са предмет на разглеждане от настоящата статия.

1. Архивната дейност в Република България

Нормативната уредба в областта на административното право, която се отнася до запазването и ползването на архивни документи, се съдържа в един общ нормативен акт – Закон за Националния архивен фонд (ЗНАФ)[2]. Самият общ закон препраща пряко или индиректно към няколко специални административни закона. Държавна агенция „Архиви“ поддържа фонд, в който се съхраняват документи от определен вид, период или начин на създаване. Съхраняването и осигуряването на онлайн достъп до архиви представлява особено важна част от електронното управление в сферата на културата и научноизследователската дейност. Както администрации, така

[1] Николова, Р. Административноправна същност на информацията. София: Дружество „Европейско право“, 2016, 83.

[2] Обн. ДВ, бр. 57 от 13.07.2007 г.

и публичноправни организации отговарят за тази дейност по уточнените устройствени административни специализирани закони.

Архивите, които съхраняват документи на Националния архивен фонд, са:

1. държавни архиви;
2. архиви и архивни сбирки на културни и други публични институции;
3. архивни сбирки на държавни и общински музеи и библиотеки;
4. архивни сбирки на читалища и религиозни институции;
5. частни архиви.

Държавна агенция „Архиви“ създава дигитални колекции, като: „Войните на България (1878–1945)“, „Еврейската общност в България“, „Полицейски досиета на известни личности от периода преди 1944 г.“, „Народният съд (1944-1945 г.)“, „Протоколи на Политбюро и на ЦК на БКП (1944–1989)“, „Промяната 1989. Преди и след“, „Старопечатни еврейски книги“, Фотоархив, АртАрхив, „Гоце Делчев (1872–1903)“, „Константин Стоилов (1853–1901)“[3]. В държавните и общинските музеи и библиотеки, в читалищата, в културните, религиозните и други публични институции се пазят исторически формирали се архивни сбирки и постъпват документи, притежание на юридически и физически лица при писмено изразено желание от страна на собствениците им. Към изброените видове архиви се причисляват и печатните и други произведения, създадени при ползването на архивни документи от Националния архивен фонд, се депозират в Държавна агенция „Архиви“:

1. произведения, тиражирани върху хартиен или друг носител по печатарски или подобен на него способ – печатни произведения, издадени от български физически или юридически лица;
2. произведения, тиражирани върху звуконосител, чиито продуценти са български физически или юридически лица;
3. произведения, тиражирани върху филмов носител, чийто продуцент, поне един от копродуцентите или производителите са български физически или юридически лица;
4. произведения, тиражирани върху електронен носител от български физически или юридически лица;

[3] Виж в рубриката „Архивите говорят“, достъпна на адрес: https://archives.bg/, посетен на 1.06.2023 г.

5. произведения в дигитална форма, публикувани в електронни комуникационни мрежи, предназначени за четене или възприемане по други начини, разпространявани за обществено ползване от български физически или юридически лица;
6. дисертационни и хабилитационни трудове, защитени в страната или в чужбина, ако авторът е български гражданин (чл. 9, т. 6 във връзка с чл. 3, ал. 1, т. 1–6 от ЗЗДПДПОРДМУ).

Законът за обществените библиотеки (ЗОБ)[4] предвижда запазването на архиви, доколкото обществените библиотеки са образователни, информационни и културни институти с национално и местно значение, които събират, обработват, организират, съхраняват и предоставят за обществено ползване печатни и други произведения и информация, включително за книжовното и литературното културно наследство.

Направление „Ръкописно-документално и книжовно наследство“ на Националната библиотека „Св. св. Кирил и Методий“ (НБКМ) съставя фонд за документи от времето на възникването на българската държава и за документи на видни общественици, писатели, културни и научни дейци до 1878 г.

Националната библиотека поддържа следните основни библиотечни колекции, някои от които са част от проекта „Дигитална библиотека“[5]:

1. уникални колекции от български, славянски, ориенталски и други чуждоезични ръкописи, архивни документи, редки и ценни старопечатни книги;
2. колекции от специални издания (официални издания; картографски и графични издания, музикални издания и други);
3. колекция от печатни и други произведения на българската книжнина по реда на Закона за задължителното депозиране на печатни и други произведения и за обявяване на разпространителите и доставчиците на медийни услуги (Архив на българската книга);
4. представителна колекция от чуждестранна литература във всички области на знанието;

[4] Обн. ДВ, бр. 42 от 5.06.2009 г.

[5] Дигиталната библиотека на НБКМ се съдържа на адрес: https://www.nationallibrary.bg/www/%D0%B4%D0%B8%D0%B3%D0%B8%D1%82%D0%B0%D0%BB%D0%BD%D0%B0%D0%B1%D0%B8%D0%B1%D0%BB%D0%B8%D0%BE%D1%82%D0%B5%D0%BA%D0%B0, посетен на 1.06.2023 г.

5. колекция от публикации в чужбина на български език или свързани по съдържанието си с България, както и преводни издания на български автори, издадени в чужбина (Булгарика).

Важна роля за формирането на колекцията Архив на българската книга изпълнява Законът за задължителното депозиране на печатни и други произведения и за обявяване на разпространителите и доставчиците на медийни услуги (ЗЗДПДПОРДМУ)[6]. Регионалните библиотеки поддържат архив на краеведския печат и литература и координират събирането, съхраняването, организирането и разпространението на краеведска информация и библиографията по краезнание (чл. 27, ал. 1, т. 3 от ЗОБ).

Някак извън законодателната уредба, но с основоформираща функция за архивното дело в България се разглежда Научният архив на Българската академия на науките (БАН), който започва своята дейност още с учредяването на Българското книжовно дружество (БКД) в Браила през септември 1869 г. и може да се счита за най-старата архивна институция в страната (чл. 6 от Устава на БКД). Специализиран е като архив на документите на Академията (независимо от времето на тяхното създаване), а също и за личните фондове на български учени, членове на БАН. В исторически аспект се е формирал значително по-рано от държавните архиви и има собствен принос за опазването на документалното културно-историческо наследство. Понастоящем нормативното основание за дейността на този архив се съдържа в чл. 3, ал. 1 и чл. 4 от Закона за Българската академия на науките[7] и чл. 81 от Устава на БАН[8], който посочва, че Научният архив на БАН е самостоятелно звено с предмет на дейност: комплектуване, научно-техническа обработка, научна експертиза, запазване и реставрация на архивни документи, както и тяхното използване. Той ръководи методически звената на академията по тяхната работа с деловодства и архиви.

Законът за културното наследство (ЗКН)[9] определя като архивни движими културни ценности документите с културно и научно значение, независимо от времето, мястото, носителя и техниката на създаването им. Като книжовни движими ценности нормативният акт посочва ръкописните културни ценности до края на XVIII в., старопечатни редки и ценни издания, които притежават научна, културна, полиграфическа или библиографска стойност. Министерството на културата създава Инспекторат за опазване

[6] Обн. ДВ, бр. 108 от 29.12.2000 г.
[7] Обн. ДВ, бр. 85 от 15.10.1991 г.
[8] Обн. ДВ, бр. 34 от 22.04.1994 г.
[9] Обн. ДВ, бр. 19 от 13.03.2009 г.

на културното наследство, който осъществява контрол по опазване на книжовни и литературни културни ценности, съхранявани в библиотечните и архивните колекции – ръкописи, архивни документи и старопечатни издания. Значителна част от архива се съхранява от музеите. Архивът на Националния институт за недвижимото културно наследство обединява Националния регистър на недвижимите културни ценности, документации за недвижими културни ценности и за обектите, свързани с българската история и култура извън страната. Националният институт за недвижимо културно наследство поддържа национален документален архивен фонд, включително в електронен вид.

Законът за радиото и телевизията (ЗРТ)[10] предвижда в чл. 62, т. 2, че Управителният съвет на БНР, съответно на БНТ приема за съхраняването и ползването на фондовете. Архивът на Българското национално радио се състои от „Златен фонд“ за фонодокументи. Архивът на Българската национална телевизия се състои от кино– и телевизионни филми, видеофилми и звукозаписи.

Законът за филмовата индустрия (ЗФИ)[11] дефинира, че филмова индустрия по смисъла на закона е производството, разпространението, промоцията, показът и съхранението на филми. Дейността по съхраняването на филми се осъществява от Българската национална филмотека като държавен културен институт с национално значение. Българската национална филмотека съхранява българските игрални, документални, хроникални, научнопопулярни и анимационни филми и документацията по тяхното произвеждане, за популяризиране на киноизкуството и кинематографичната култура у нас.

Агенцията по геодезия, картография и кадастър поддържа държавния геодезически, картографски и кадастрален фонд (Геокартфонд), който приема, съхранява и предоставя за ползване по установения от Закона за Националния архивен фонд ред геодезически, картографски, кадастрални и други материали и данни (чл. 12, т. 3 от Закона за кадастъра и имотния регистър[12] и чл. 20, ал. 1 от Закона за геодезията и картографията[13]). Унищожаване на геодезически и картографски материали и данни, съхранявани в Геокартфонда, се извършва по реда на Закона за Националния архивен фонд

[10] Обн. ДВ, бр. 138 от 24.11.1998 г.
[11] Обн. ДВ, бр. 105 от 2.12.2003 г.
[12] Обн. ДВ, бр. 34 от 25.04.2000 г.
[13] Обн. ДВ, бр. 29 от 7.04.2006 г.

(чл. 21, ал. 5 от Закона за геодезията и картографията). В срок до 30 юни 2026 г. Агенцията по вписванията дигитализира наличния хартиен архив в службите по вписванията (§8 от Преходните и заключителни разпоредби на Закона за изменение и допълнение на Закона за кадастъра и имотния регистър[14]). Направление „Архитектура и градоустройство“ на Столична община чрез отдел „Архивно обслужване и дигитален архив“ на основание чл. 2, т. 5 от Наредбата за определяне и администриране на местни данъци и цени на услуги, предоставяни от Столична община, осигурява достъп до архив-инвестиционни проекти и архив-застроителни и регулационни планове.

Архивът на Министерството на вътрешните работи (МВР) съхранява документи, създадени в резултат на дейността на структурите в министерството, които се съхраняват постоянно от Министерството на вътрешните работи (чл. 33, ал. 1, т. 8 от ЗНАФ). Органите на МВР събират такси за копиране, микрофилмиране, фотокопиране или сканиране на архивен документ, както и за предоставяне на архивен документ за заснемане на филм (§2, т. 8 от Допълнителните разпоредби на Закона за МВР[15]).

С по-особен режим се характеризира съхраняването на архивни документи на основание Закона за достъп и разкриване на документите и за обявяване на принадлежност на български граждани към Държавна сигурност и разузнавателните служби на Българската народна армия[16], съгласно който се въвеждат оперативен архив, служебен и партиен архив. Достъпът до този архив е ограничен, доколкото в чл. 31, ал. 1, т. 3 във връзка с ал. 6 от специалния закон е предвидено, че подлежат на достъп по реда на Закона за достъп до обществена информация за научноизследователска, публицистична и проучвателна дейност съхраняваните от комисията документи, ако съдържанието на документите не може съществено да наруши права и законни интереси на трети лица, чиито имена са споменати в документите, и има изрично писмено съгласие от тях или от техните законни наследници, като се предоставят копия, които не включват данните, отнасящи се до третите лица.

[14] Обн. ДВ, бр. 8 от 25.01.2023 г.
[15] Обн. ДВ, бр. 53 от 27.06.2014 г.
[16] Обн. ДВ, бр. 102 от 19.12.2006 г.

2. Обработването на лични данни при използването на архивни документи и за целите на научни и исторически изследвания

Електронното управление в областта на културата и научноизследователската дейност в България се развива с твърде бавни темпове. Въпреки това Държавна агенция „Архиви“ използва онлайн комуникация за предоставяне на достъп до архивни документи. При осигуряването на тези данни важно значение има обработването на личните данни на посочените в документите лица, които попадат в обхвата на правото на личен и семеен живот, заложено в чл. 8 от Европейската конвенция за защита правата на човека (ЕКПЧ) на Съвета на Европа. Европейският подход за определяне на рамката, в която се съдържа личната неприкосновеност на гражданите, разглежда комплексно въпроса, като акцентира върху физическия, психическия и моралния интегритет на лицата. Спецификите за дефиниране на защитата на личната неприкосновеност се свързват със задълженията на държавата да се въздържа от намеса в личния живот. Това са обсъжданите от правната теория лични права, т.нар. „отрицателни права“ (*status negativus*) от първо поколение, свързани с индивидуална отговорност според класификацията на Карел Вашак. Лични административни права са онези субективни изрично признати на гражданите в специален административен закон юридически релевантни блага и ценности, достъпът и използването на които позволява задоволяването на конкретни духовни потребности, свързани с определени аспекти на тяхната физическа и/или психическа (персонална) същност и интегритет[17]. Към тази категория обществени отношения можем да поставим и правото на семеен живот, доколкото се отнася до идентифицирането на роднински връзки на определено физическо лице.

Правото на лична неприкосновеност и на зачитане на семейния живот не е абсолютно и то търпи ограничения, предвидени в закона, необходими в едно демократично общество за защита на сигурността и благосъстоянието в обществото, както и здравето, морала и правата на другите (чл. 8, параграф 2 от ЕКПЧ)[18]. Именно в тази последна категория ограничения се въвежда критерият „правата на другите“, когато се обработват лични данни за целите на научни и исторически изследвания. В случая при изследване на

[17] Николова, Р. (2022). Административни права и задължения на гражданите – същност и видове. Административно правосъдие, № 6, 25.

[18] Топчийска, Д. (2022). Съвременната концепция за лична неприкосновеност в дигиталната среда в правните системи на ЕС и САЩ. Веселин Вучков, състав. Тридесет години България в Съвета на Европа – върховенство на правото, демокрация, права на човека. София: Нов български университет, 145–146.

родословното дърво става въпрос за фундаментално индивидуално право, предвидено в чл. 42 от Хартата на основните права на ЕС (ХОПЕС): правото на достъп до документи, както и на защита на семейството в юридически аспект (чл. 33, т. 1 от ХОПЕС). При извършването на научни проучвания, които засягат трети лица и нямат отношение към личния живот на дирещото информация лице, е налице обществен интерес да се разкрият подробности относно живота на изследваната личност, но и упражняване на културното индивидуално административно право на научни изследвания, уредено в чл. 13 от ХОПЕС. Културните административни права според доктрината са онези субективни изрично признати на гражданите в специален административен закон юридически релевантни блага и ценности, достъпът и използването на които позволява задоволяването на конкретни духовни и материални потребности; насочени към утвърждаване и съхраняване на личностната културна идентичност, насърчаване на стремежа към образование и научен прогрес, гарантиране участието в културния живот на общността, постигането на свобода на художественото, научното и техническото творчество, гарантирано създаване, проучване, разпространение и опазване на културни ценности, както и резултатите от тази дейност[19].

Ограниченията на правото на лична неприкосновеност представляват лични административни задължения, които правната теория разглежда като публичноправно изрично институционализирани в специален административен закон изисквания на субективно дължимо поведение на гражданите, изразяващи се в потребност да изтърпят конкретни неизбежно необходими, временни по своята продължителност, обхват (обем) и интензитет неблагоприятни мерки по ограничаване на определена област от дейността на човека, за изпълнението на които са предвидени правни гаранции в личната правна сфера по ограничаване на своята физическа и/или психическа същност, цялост или идентичност, за изпълнението на които са предвидени правни гаранции[20].

Съгласно чл. 25н от Закона за защита на личните данни (ЗЗЛД)[21] онези лични данни, първоначално събрани за друга цел, могат да се обработват за целите на Националния архивен фонд, за целите на научни или исторически изследвания или за статистически цели. В тези случаи администраторът прилага подходящи технически и организационни мерки, които гарантират

[19] Николова, Р. (2022). Административни права и задължения на гражданите – същност и видове. Административно правосъдие, № 6, 28.

[20] Николова, Р. (2022). Административни права и задължения на гражданите – същност и видове. *Административно правосъдие*, № 6, 25.

[21] Обн. ДВ, бр. 1 от 4.01.2002 г.

правата и свободите на субекта на данни в съответствие с чл. 89, параграф 1 от 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)[22]. Основен принцип в този случай е създаването на гаранции с оглед на спазването на принципа на свеждане на данните до минимум. Същото положение предвижда в чл. 13 от 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[23].

Законът за гражданската регистрация (ЗГР) в чл. 28 предвижда, че електронният личен регистрационен картон се пази в продължение на 130 години, считано от датата на създаване, след което се предава на Държавния архив. Разпоредбата на чл. 85, ал. 3 от ЗГР посочва, че приключените регистри от формуляри на актове се подвързват и се предават за ползване и съхраняване в административния център на общината до 130 години от съставянето им, след което се предават в Държавния архив. В §74 от ПЗР на ЗИДЗГР (обн. ДВ, бр. 39 от 2011 г., в сила от 20.05.2011 г.) е указано, че личните регистрационни картони, съставени на хартиен носител, се използват за справки и се съхраняват в общината, кметството или района в продължение на 130 години, считано от датата на създаването им, след което се предават в Държавния архив. В случаите на провеждане на научни изследвания или на исторически проучвания, сред които са изследванията на родословието, публичната общинска администрация често пъти се позовава на Закона за защита на личните данни и отказва да предостави личните данни – дата на раждане и смърт, трите имена, брак, имена, рождени дати и такива на смърт на наследници, всякакви други роднински връзки, адресна регистрация. Аргументът е, че доколкото не са изминали 130 години от съставянето на съответния акт и той не е предаден на Държавна агенция „Архиви“, държавните служители нямат право да нарушават тайната на подобна информация, тъй като разпоредбата на чл. 106, ал. 1 от ЗГР предвижда, че данните от ЕСГРАОН се предоставят при строго определени условия на:

[22] ОВ L 119, 4.5.2016 г., с. 1–88.
[23] ОВ L 295, 21.11.2018 г., с. 39–98.

1. българските и чуждестранните граждани, както и на лицата без гражданство, за които се отнасят, а също така и на трети лица, когато тези данни са от значение за възникване, съществуване, изменение или прекратяване на техни законни права и интереси;
2. държавни органи и институции съобразно законоустановените им правомощия;
3. български и чуждестранни юридически лица – въз основа на закон, акт на съдебната власт или разрешение на Комисията за защита на личните данни.

Европейското законодателство действа в пълен синхрон с българския закон и посочва изрично, че когато личните данни се обработват за целите на *архивирането в обществен интерес*, правото на Съюза или правото на държава от ЕС може да предвижда отмяна на правата по членове 15 (право на достъп до данните и информация във връзка с обработването), 16 (право на коригиране), 18 (право на ограничаване на обработването), 19 (право да получи уведомление във връзка с обработването на данните), 20 (право на преносимост на данните) и 21 (право на възражение), доколкото има вероятност тези права да направят невъзможно или сериозно да затруднят постигането на конкретните цели (ползването на архивни документи, включително от значение за научни или исторически проучвания), и посочените дерогации са необходими за постигането на тези цели (чл. 89, параграф 3 от Общия регламент относно защитата на данните).

Когато личните данни се обработват за *научни или исторически изследвания* или за статистически цели, правото на Съюза или правото на държава членка може да предвижда дерогации от правата по членове 15 (право на достъп до данните и информация във връзка с обработването), 16 (право на коригиране), 18 (право на ограничаване на обработването) и 21 (право на възражение), доколкото има вероятност тези права да направят невъзможно или сериозно да затруднят постигането на конкретните цели, и посочените дерогации са необходими за постигането на тези цели (чл. 89, параграф 2 от Общия регламент относно защитата на данните).

Когато лични данни се обработват за целите на *научни или исторически изследвания* или за статистически цели, субектът на данните има право, въз основа на конкретното си положение, да възрази срещу обработването на лични данни, отнасящи се до него, освен ако обработването е необходимо за изпълнението на задача, осъществявана по причини от обществен интерес (чл. 23, параграф 4 от Регламент (ЕС) 2018/1725). За да се балансират личният и обществеият интерес, се възприема правилото на чл. 25, параграф

3 от същия акт, който предвижда, че когато личните данни се обработват за целите на *научни или исторически изследвания* или за статистически цели, в правото на Съюза, което може да включва вътрешни правила, приети от институции и органи на Съюза по въпроси, свързани с тяхната дейност, могат да бъдат предвидени дерогации от правата, посочени в членове 17 (право на достъп до данните), 18 (право на коригиране), 20 (право на ограничаване на обработването) и 23 (право на възражение), доколкото има вероятност тези права да направят невъзможно или сериозно да затруднят постигането на конкретните цели и посочените дерогации са необходими за постигането на тези цели.

Тук се налага прилагането на тест относно баланса на конкуриращи се права, които си противостоят: правото да не се разкриват лични данни на лицето – обект на документно описание в архива, на научно или историческо изследване и правото на обществото да се направят необходимите проучвания от значение за запазване на културната национална памет и идентичност или удовлетворяване на индивидуалния интерес на издирващия своите родственици и произход:

- същност и източник на законния интерес и дали обработването е необходимо за упражняването на основно право, ако не е, дали е в обществен интерес;
- ефект върху субекта на данните и неговите разумни очаквания какво ще стане с данните, както и характера на данните и начина, по който са обработвани;
- допълнителни защитни мерки, които биха ограничили нежелания ефект върху субекта на данните, като минимизиране на данните[24].

Законният интерес е предвиден както в актовете на ЕС, така и в българския Закон за защита на личните данни. При проучване на родословното дърво очевидно е налице основно индивидуално право на защита на личния и семеен живот на търсещия роднински връзки и сведения за лицето, като в този смисъл държавата има съответните позитивни задължения – да му окаже съдействие за установяването на тези семейни отношения. При провеждане на научни проучвания е налице обществен интерес да се представи конкретен исторически контекст на живота и дейността на лицето, чиито данни се разкриват. Ефектът върху отбелязването на трите имена, датите на раждане и/или смърт, адресна регистрация в миналото не следва

[24] Топчийска, Д. (2018). Балансът на права и легитимни интереси като основание за обработване на лични данни съгласно Общия регламент на ЕС за защита на личните данни. Годишник на департамент „Право“ 2017. София: Нов български университет, 207.

и не могат да окажат негативно въздействие върху неговия живот или този на наследниците. Допълнителните защитни мерки в посока запазване на идентификацията в някакви определени граници е свързана с конкретната тема на правените изследвания (минимизиране на данните).

Заключение

Европейското и националното законодателство гарантират възможността да се разкриват конкретни лични данни за целите на архивирането, при научни и исторически изследвания. Преследваните цели са легитимни от гледна точка на защитата на обществения интерес – тогава те са колективни: да се съхрани националното архивно наследство, да се запази културната памет и защити националната идентичност. Легитимни могат да са и преследваните от индивида лични, субективни цели: да се упражни свободата на художественото и научното творчество или защита на семейния живот чрез проучване на родословието и по този начин запазване на фамилната свързаност и кръвна идентичност.

Библиография:

1. Николова, Р. Административноправна същност на информацията. София: Дружество „Европейско право“, 2016.
2. Николова, Р. (2022). Административни права и задължения на гражданите – същност и видове. Административно правосъдие, 2022 (6).
3. Топчийска, Д. Балансът на права и легитимни интереси като основание за обработване на лични данни съгласно Общия регламент на ЕС за защита на личните данни. Годишник на департамент „Право“ 2017. София: Нов български университет, 2018.
4. Топчийска, Д. Съвременната концепция за лична неприкосновеност в дигиталната среда в правните системи на ЕС и САЩ. Веселин Вучков, състав. Тридесет години България в Съвета на Европа – върховенство на правото, демокрация, права на човека. София: Нов български университет, 2022.

За информиращото право

Доц. д-р Орлин Радев*

Развиват се идеи за някои основни насоки и възможности за качественото и ефективно въздействие на правото в съвременния информационен свят.

Ключови думи: *закон, информация, организация, право, регулация, рефлексия, съзнание*

* Доцент, д-р Орлин Радев, Юридически факултет на Варненския свободен университет „Черноризец Храбър“, ел. поща: justor@abv.bg

About the Informative Law

Assoc. Prof. Orlin Radev, PhD*

Ideas are developed for some basic directions and possibilities for the qualitative and effective impact of law in the modern information world

Keywords*: law, information, organization, law, regulation, reflection, consciousness*

* Associate Professor Orlin Radev, PhD, Faculty of Law of the Varna Free University „Chernorizets Hrabar“, e-mail: justor@abv.bg

Още от средата на миналия век видният полски учен, философ и писател Станислав Лем предупреждаваше, че развиващият се във все по-големи мащаби тогава информационен „бум“ скоро може да се превърне в информационен „шум“. В правото той може да се разкрие като „свръхзаконодателстване“, израз на надмогващия все още (все повече?!) правен фетишизъм – че със законодателни средства могат да се решат всички общочовешки проблеми. Правото е натоварено с очаквания да преодолее и замести човешките несъвършенства, но вместо това като че ли създава нови – вместо простичкото, почтено, близко до здравия разум договаряне (да си спомним „Контрактъ“ на Чудомир), сега многостранични договори имат претенции (но за съжаление – и силата) да „уреждат“ отношенията между хората. Появи ли се проблем – ще направим закон за неговото „обхващане“. А още отпреди хилядолетия древният китайски мъдрец констатира – колкото повече правила, толкова повече нарушения. Информационното общество по-скоро допринася за засилването, не толкова за решаването на все по-сложните обществени отношения, включително различия, противопоставяния, конфликти. Информационната (пре)наситеност от закони в полето на правото[1] като че дава повече „пара за свирката“ на общественото развитие, нежели за неговия двигател.

В България това особено остро проличава след присъединяването ни към Европейския съюз, когато, наред с и без това „мащабното“ ни „правописане“ след промените от 1989 г., се насложиха и изискванията за хармонизация на законодателството ни с актовете на Съюза, както и прякото действие на редица норми на международното и европейското право. За съжаление, освен обективните причина на все по-усложняващите се обществени отношения много често се забелязват повече или по-малко явни прояви от субективно естество (нарушения в законодателния процес, прикрит или откровен лобизъм, непочтеност, дори „обикновена“ некомпетентност на призваните да определят правилата на нашето поведение и добруване).

Стъпвайки на територията на информационноправните изследвания, бихме могли да формулираме някои насоки на техните „свръхзадачи“, реализиращи се всъщност в непосредственото общуване на учени, преподаватели и студенти, и рефлексиите му в правното и общественото пространство:

1. Сред основните ТЕОРЕТИЧНИ приоритети трябва да бъде поставено осмислянето, разработването и развиването на проблематиката на

[1] Подробно различни аспекти на проблематиката са разработени в: Радев О. (2022). Етюди за правото и информацията, или Законовите двери в полето на Правото, София: Сиби.

нормативния акт като специфичен юридико-социален инструмент, съдържащ в себе си цялото многообразие на информационната интерпретация на правните категории и институти, и съпътстващите, но с голямо значение и често със самостоятелна тежест въпроси, свързани с правотворчеството, строежа и езика на правните актове, юридическата техника, реквизитите на акта и пр. Още авторитети като Живко Сталев, Борис Спасов, Димитрина Милкова, Вихър Кискинов, Бойка Чернева и мн. др. са поставяли и работили през годините по тази тематика, всеки със самостоятелен принос, но с една насока, тъга и порив – за създаване на едно действително ефективно, полезно и познато право в полза на обществото. За съжаление, българската правна регламентация е отдавнашен длъжник на юристите и на всички граждани в това отношение. Многобройни са печалните примери за некачествено законодателство, все по-често произтичащи от непознаване, неразбиране, неприлагане и дори открито пренебрегване на принципите и юридическите закономерности на правото, на неговите информационни характеристики и значение. Дори основният акт, който би трябвало безпротиворечиво и компетентно да създава условия за изработване на качествено законодателство – Законът за нормативните актове, отдавна не е в състояние да изпълни заложените в предмета му функции – въпреки многобройните му промени (понякога само „козметични“), въпреки постоянно изготвяни (и „замразявани“) проекти за нови промени и дори за изцяло нов акт, дори и съдържащите се в него положителни идеи и правила редовно се пренебрегват от законо„творците“. Така е и при другия значим акт в тази материя – Правилника за организацията и дейността на Народното събрание, често пъти продукт на конюнктурни компромиси в удобство на същите тези законо„творци“, и въпреки това отново пренебрегвани, заобикаляни или открито нарушавани в практиката на приемането на законите. И разбира се, не бива да се отминава, макар това да е част от цяла група мащабни въпроси, задачата с поставяне на качествени основи на нормотворчеството със самата Конституция – достатъчно е да отбележим например само проблемите с номенклатурата на нормативните актове, която непрекъснато се мени „в движение“ по волята на химикалката на законо„твореца“, без никаква опора в основния закон.

2. В ПРИЛОЖЕН аспект стои организирането на правната информация в правно-информационни системи, които в съвременния свят вече са немислими без използването на информационните и комуникационни технологии. Вече не хартията, не книжното тяло става най-важният, най-гъвкав

и подходящ носител на правната информация. Отдавна отмина времето на изданието „Нормативни актове“, което беше своеобразен връх в тогавашните възможности за предоставяне и актуализиране на правната информация на хартиен носител. Съвременната информационноправна среда съдържа все по-разширяващо се многообразие на компютърно и интернет базирани бази данни, продукти и системи. Тук стоят въпросите за най-подходящото, най-възприемаемо, най-организирано и свързано представяне на правната информация – разработват се идеи например за нейното 3D организиране в облак, търсят се най-ефикасни решения за смислови търсения в правната материя – не само по ключови думи, но и чрез привличане на възможностите на изкуствения интелект, както и на създаване на експертни продукти (анализи, коментари, стратифициране на правната информация според интересите на потребителите и др. под.). Почти всички съвременни правно-информационни системи притежават висока степен на експертност и организираност на правната информация (поради и въпреки непрекъснато нарастващите ѝ обеми), с включени препратки и хипервръзки към други актове, практика, анализи, представяне на предходни състояния на акта („машина на времето“), различни типове „срезове“, конструкции и много други изключително богати и полезни инструменти за (за)познаване на правната материя. Особено полезна е функцията по създаване на консолидиран текст на акта (с постоянно актуализиране с последващите му изменения и допълнения). И докато в България изготвянето на този текст е плод на експертната работа и тълкуване на специалистите към съответните правно-информационни системи (които в голямата си част са частни и за търговско разпространение, т.е. те нямат официална задължителна сила; своеобразен „аналогов“ вариант на такава консолидация са периодично обновяваните сборници с нормативни актове на издателство „Сиби“ – изключително полезен продукт, винаги „подръка“ на участниците в съдебните производства, и не само в тях), за актовете на Европейския съюз консолидираният текст се изготвя от Правната служба на Европейската комисия, въпреки че и тук все още, както изрично е отбелязано, консолидираната версия е само средство за документиране и не обвързва европейските институции; пълната библиографска справка се посочва в първоначалния текст на акта. Но от 1 юли 2013 г. само електронното издание на Официален вестник на Европейския съюз (ОВ) е автентично и има правно действие (Регламент (ЕС) № 216/2013 на Съвета). Хартиените издания вече нямат правна стойност освен в случаите, в които поради непредвидена и извънредна повреда на компютърните системи на Службата за публикации електронното издание на ОВ не може да бъде

публикувано. Обратното важи за българския „Държавен вестник“, въпреки че и при нас настъпи, макар и ограничена, реформа в електронното представяне на официалната правна информация, като българският електронен „Държавен вестник“ е само за обнародване на обществените поръчки, с оглед облекчаване на обема на хартиеното тяло, което и без това е на границите на възможното (а и на допустимото за възприемане – вж. напр. бр. 102 от 2022 г. с обнародвани 12 закона, с които се променят още 87 (!) други закона, 38 постановления на Министерския съвет, и „само“ 5 наредби и 1 инструкция, с които също се внасят промени в редица подзаконови актове, и 1 акт с неконституционното, но „законово“ наименование „Условия и ред“). Необходимостта от създаване на официална електронна държавна система за правна информация с всички възможности за достъп и използване е въпиюща.

3. Свързани с горните са задачите по обнародването и публичността на правните текстове – ПРАВНАТА ИНФОРМИРАНОСТ на обществото. Значими са достиженията на информационноправните изследвания в разработването на проблемите на правните структури, на правното моделиране и прогнозиране, на източниците, каналите и потребителите на правна информация, на информационните потоци, на организирането на правото в теоретико-практическия конструкт на конкретната функционална правна система като информационно единство на правна норма, правно отношение и правно съзнание. Включването именно на правното съзнание като същностен, генетично заложен елемент на правното въздействие изразява един от аспектите на новата, активна парадигма в правното информиране – за ролята на субекта на правото, носител не само на задължения, но и на не по-малко важни и същностни информационни права. И това информиране трябва да става не само по единствения, макар и отдавна изостанал от обществените изисквания начин – с обнародването в „Държавен вестник“ да се счита, че правните субекти (по-скоро – „обекти“ на правото) са информирани за своите права и задължения. Теоремите на Клод Шенън за допълнителните канали за връзка дават насоки за разрешение на подобряване на протичането на информационните потоци. Ролята на такива канали могат да играят много структури – медиите, науката, гражданското общество, всички те особено стимулирани от възможностите и постиженията на интернет. Важното за правото обаче е предаваната по такива канали информация да има винаги възможност за тестване на нейната достоверност с официална, общодос-

тъпна правна информация (скорошен пример, многократно мултиплициран от различни медии, за „влизане в сила“ на промени в точковата система за санкции при шофиране на определена дата в действителност касаеше само „обнародването“ на тези промени в „Държавен вестник“, като влизането им в сила беше от по-късна дата; а както да кажем за масовото, с редки изключения, използване във всички избори досега на израза „Купуването и продаването на гласове Е престъпленИЕ“, докато правилното е „...СА престъпленИЯ“). Нелицеприятната реалност обаче е, че дори хартиеният „Държавен вестник“ (доколкото може да бъде открит в общественото пространство) е загубил огромна част от своя престиж и изискване за достоверност – „допуснати“ волни или неволни грешки, претовареност с излишни текстове страници, актове със странни наименования, „плод“ на многобройни органи с официализирана нормотворческа компетентност и др. под., правят ползването му непосилна задача не само за обикновения гражданин, но и за квалифицираните юристи. Затова от пасивната парадигма – да се обнародва, пък който иска – да чете; незнанието на закона не оправдава неговото нарушаване (популярна, но никъде непрогласена (без)принципна постановка), трябва да се премине към новата, активна парадигма – задължение за активни и отговорни действия именно на държавата, нейните органи и институции, по информиране, разясняване, достигане и формиране на правното съзнание на всеки правен субект относно нейните правни актове, политики и практики. За целта Законът за нормативните актове, а и цялото ни право трябва рефлексивно да се огледа, съизмери, развие в съответствие с новите обществени нагласи и реалности, за да могат да се приложат всички съвременни достижения в правотворчеството – редукция, консолидация, кодификация, вътрешно пречистване от излишни и затормозяващи текстове, програми за изследване на законодателството, семантични и лингвистични методи, включително с изкуствен интелект, изграждане на смислови структури, изследване на процесите на нормативно усилване и нормативно заглъхване, поставяне на по-високи изисквания към всички етапи на нормотворческия процес и по-важното – тяхното изпълняване за постигане на крайната цел – достигане на правото до правното съзнание и превръщането му в същностен, неотменен елемент от характеристиката на човешкото поведение. Проучвания за качеството на нормативния текст, направени през 80-те години от американска изследователска организация сред общини в България за нуждите на подобряване на местното самоуправление, показват, че текст с повече от 45 думи вече е трудно възприемаем за „потребителя“ на право-

то. Но това е установил векове по-рано и Джонатан Суифт (самият той и юрист) в своите „Пътешествия на Гъливер“, задължавайки законодателите в измислената от него страна под страх от смъртно наказание (!) да не правят закони с повече от 30 думи. Близостта на бройката е впечатляваща. И това изразява респект не толкова и не само към нормативния текст, колкото и най-вече към правото като ценност (затова законотворецът в древния гръцки полис прави предложение за промяна на закон с примка на шията – ако то се отхвърли, примката се затяга, защото се е осмелил да тръгне срещу свещения, божествен ред, олицетворяван от правото). В съвременния свят, разбира се, не може да се апелира към придържане към такова правило, но днес все повече осъзнаваме, че ценността, „светостта“ на правото идва от начина на възприемането му от хората, от възпитаването във взаимно уважение, съпричастност, толерантност, зачитане на волята на индивида и общността. Един от инструментите за това например е засилване на самоуправлението, намаляване на централизираната регулация, всячески наместваща се и заместваща индивидуалната воля, и дори дерегулация – диспозитивното начало е само началото на такъв процес. Но зловещата символика с примката може би би била отрезвителна за някои законо„творци“, изживяващи се като юридически божества, само че не с гръмотевици, а с химикалки, дращейки бледи и нетрайни знаци върху вековечната еманация на свободния човешки дух – правото. За такова посегателство трябва да се търси не толкова (и най вече – не само) политическа отговорност (изпразнена от реално съдържание), но морална (по Сенека – дори законът да позволява, срамът забранява), и най-вече значима юридическа отговорност – трудна, но не невъзможна задача спрямо самодоволната недосегаемост на тези, които определят правилата, но не и правото.

4. Накрая, но не и по значение, трябва да се акцентира и върху ВЪЗПИТАТЕЛНАТА роля, функция и задача на правото. Чувството за прецизност, за отговорност към думите, към изказа, съобразяването с информационното въздействие върху адресатите, дори изяществото и хармонията в нормативните текстове, които са всъщност превърната форма на мярата в правото, ще доближат и сближат законовите изисквания с ежедневните нужди на правните адресати, за които те ще станат част от нормалното, естествено поведение в съобщността с другите свободни индивиди. Значими юристи през вековете (Йеринг, Савини, Якоб Грим, Плешнер и мн. др.) са оставили своите разсъждения за естетиката, красотата и поезията

в правото, да не говорим, че поетическата форма от дълбока древност е най-честото проявление на материализацията на свещените закони. В България също има достойни следовници на тези схващания (М. Костова, В. Брайков, О. Герджиков) – всъщност вероятно всеки юрист в един или друг момент се е чувствал запленен от въздействащата сила на изящен правен изказ. Изконното разбиране за правото като изкуство на доброто и справедливостта се развива и в информационноправните изследвания и изведените от тях идеи за юридически закономерности – израз на ролята му не да ограничава, а да подпомага, разгръща и изпреварва, стимулирайки ги, обществените необходимости. Същностна задача става култивирането на положително критическо мислене (не само у юристите – особено за обучаващите се в право, но и във всички отговорни членове на гражданското общество), към текста, смисъла, съдържанието и изявата, въздействието на акта, на чувство за отговорност и съпричастност за състоянието и ефективното действие на правото. Информираният субект вече не може просто да е „запознат“ с правните разпоредби; битуващата мантра, че „незнанието на закона не извинява“, отдавна не е оправдана за съвременното демократично информационно общество, изискващо от създаващия нормите да ги доведе по адекватен начин до знанието, и по-важно – до съзнанието на „потребителите“ на правото. Просветеното мислене и действие, развиването на възможностите както на юристите, така и на цялото общество за „мониторинг“ спрямо правото в нормативното му проявление, ще доведе до промяна на неговото качество и ефективност на въздействие (една система, поставена под наблюдение, променя своето поведение – това е желаният резултат, който ни извежда извън ограниченията, постулирани от теоремата на Гьодел). И не количествените критерии – да си броим законите, а качеството на техният положителен ефект върху битието на хората трябва да е измерител на напредъка на едно общество. Уважението към правото означава заедно с това и преди всичко уважение и респект към всеки отделен човек и към цялата общност.

По станалите класически думи на Чърчил – демокрацията е много лошо нещо, но по-добро от нея не е измислено. Ние се задоволяваме с втората част на тази сентенция, но често забравяме и пренебрегваме значението на първата, а тя все по-често напомня за себе си. Наред с „утвърждаване на демократичните ценности“ („лоши“ според Чърчил), трябва да се полагат усилия и за тяхното развиване и преосмисляне (към „по-добро“ – пак според Чърчил). Светът, Европа и България преживяват тревожен и може

би преломен момент. От едната страна е безпокойството от промяна на статуквото, сигурността, спокойствието, задоволството; от другата страна е все по-силното осъзнаване на необходимостта, наложителността, неизбежността на такава промяна. Правото, въплътило и изразило човешките възделения, става провиждащият бъдещето инструмент за въздействие, създаващ информираната среда за обществения напредък, която, проникнала и формирала общественото съзнание, по естествен начин ще проведе правните предписания в реалността.

Библиография:

1. Радев О. (2022). Етюди за правото и информацията, или Законовите двери в полето на Правото, София: Сиби.

Обработване на лични данни на членове на домакинството на работника или служителя от работодателя

Андрей Александров*

Всеки работодател по необходимост се явява и администратор на лични данни на работниците и служителите. Такова обработване е не само задължителен, но и постоянен и особено интензивен елемент от всекидневната работодателска дейност. Събирането на лични данни започва още в преддоговорните отношения на страните, за да позволи възникването на трудово правоотношение между тях. Лични данни се обработват по повод сключването на трудовия договор, изпълнението на правата и задълженията по него, прекратяването му. Този процес обикновено и „надживява“ трудовото правоотношение, най-малкото защото данни за бивши служители се съхраняват с пенсионноосигурителни цели. Интерес за настоящото изследване представлява обработването на лични данни на трети лица, което се извършва в контекста на трудовото правоотношение, без титулярите на данните да са страна по него. Ще бъде потърсен отговор на въпросите в кои случаи това е допустимо, как се събира тази информация и изисква ли се съгласието на засегнатите лица за обработването на данните им.

Ключови думи: *Лични данни, обработване, работодател, трети лица, трудово правоотношение*

* Доцент, доктор. Институт за държавата и правото при Българската академия на науките; Югозападен университет „Неофит Рилски“;
ел. поща: a.alexandrov@kambourov.biz

Processing of personal data of members of the employee‘s household by the employer

Andrey Aleksandrov*

Each employer is – by necessity – also personal data controller of employees’ personal data. Such processing is not only mandatory, but also a permanent and particularly intensive element of everyday employer activity. The collection of personal data begins already in the pre-contractual relations of the parties to allow the establishment of an employment relationship between them. Personal data is processed for the purposes of conclusion of the labor contract, the fulfillment of the rights and obligations under it, its termination. This process usually “outlives” the employment relationship, not least because data on former employees is kept for pension purposes. Of interest to the present research is the processing of personal data of third parties, which is carried out in the context of the employment relationship, without the data subjects being a party to it. An answer will be sought to the questions in which cases this is permissible, how can such information be collected, and whether the consent of the affected persons is required for the processing of their data.

Keywords*: Personal data, processing, employer, third parties, employment relationship*

* Associate Professor, PhD. Institute for the State and the Law – Bulgarian Academy of Sciences; South-West University “Neofit Rilski”, e-mail: a.alexandrov@kambourov.biz

Общият регламент относно защитата на данните[1], който започна да се прилага от 25 май 2018 г., не промени съществено основните понятия и принципи на законодателството в областта на защитата на данните, въведени още през 1995 г.[2] Що се отнася до обработването на лични данни в контекста на трудовото правоотношение, без съмнение може да се обоснове изводът, че принципните положения са утвърдени от десетилетия. За да е възможно изпълнението на правата и задълженията по един трудов договор, работодателят обработва голям обем от лични данни на работника или служителя: имена, ЕГН, постоянен адрес, данни за образованието и стажа на лицето, за банкови сметки и т.н. В рамките на трудовото правоотношение често се обработва и чувствителна информация, свързана например със здравния статус – при ползване на отпуски поради временна неработоспособност, трудоустрояване и т.н. В този смисъл работодателите са една от най-големите групи администратори на лични данни и това обстоятелство никога не може да се промени, защото – за да функционира трудовото правоотношение – е необходимо да се събират и да се обработват съответните данни на работника или служителя като страна по него. Накратко може да се обобщи, че отношенията във връзка с обработването на лични данни в рамките на трудовото правоотношение, са „отношения, непосредствено свързани с трудовите“[3], както ги обозначава разпоредбата на чл. 1, ал. 1 КТ, и това обяснява и обосновава изучаването им от трудовоправната доктрина.

Ако казаното дотук не поражда някакви особени тълкувателни затруднения, не така стои въпросът с обработването на лични данни на трети лица, което отново се извършва във връзка с трудовото правоотношение, без титулярът на данните да е страна по него. Въпреки че на пръв поглед подобна ситуация изглежда по-скоро като изключение, внимателният анализ показва, че случаите далеч не са изолирани. Без претенция за изчерпателност, хипотезите, в които работодателят обработва данни на трети лица по

[1] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО.

[2] Съобщение на Комисията до Европейския парламент и Съвета: По-силна защита, нови възможности – насоки на Комисията относно прякото прилагане, считано от 25 май 2018 г., на Общия регламент относно защитата на данните. Document 52018DC0043 [онлайн]; [прегледан на 16 май 2023]. Достъпен на: https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A52018DC0043.

[3] За отношенията, непосредствено свързани с трудовите като предмет на трудовото право вж. по-подробно Мръчков, В. – В: Мръчков, В., Кр. Средкова, А. Василев, Е. Мингов. Коментар на Кодекса на труда, 13 изд. С.: Сиби, 2021, 27–28; Средкова, Кр. Трудово право. Обща част. С.: УИ „Св. Климент Охридски“, 2010, 18–19.

повод на трудови правоотношения, в които е встъпил, могат да се обособят в следните групи:

- Данни на лица от домакинството на работника или служителя, чието обработване е и непосредственият предмет на настоящото изследване. Най-често това са лица, с които работникът или служителят се намира в брак или родствена връзка, но умишлено тук е избрано по-общото понятие „домакинство“, а не „семейство“. Възможно е работникът или служителят да споделя общо домакинство с лице или лица, с които няма семейна/родствена връзка. Тези случаи не се ограничават до фактическото съжителство (в смисъла на фактическо съпружеско съжителство без сключен граждански брак), а обхващат и други често срещани ситуации, например на наето от две или повече лица жилище, което ги прави съквартиранти. Макар и отново не съвсем прецизно, понятието „домакинство“ отразява в по-голяма степен тази идея, отколкото употребата на „семейство“ или „съжителство“.
- Редица задължения на работодателите по новия Закон за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения /ЗЗЛПСПОИН/ (обн. ДВ, бр. 11 от 2.02.2023 г., в сила от 4.05.2023 г.) също предполагат обработване на лични данни на трети лица от работодател, получил тези данни от свой работник или служител. Сигнализиращо лице по смисъла на закона е физическо лице, което подава сигнал или публично оповестява информация за нарушение, станало му известно в качеството му на работник или служител (чл. 5, ал. 1, т. 1 ЗЗЛПСПОИН). В разпоредбата на чл. 32, ал. 1 ЗЗЛПСПОИН изрично е предвидено, че всяко обработване на лични данни, извършено по силата на този закон, включително обмен или предаване на лични данни от компетентните органи, се извършва в съответствие с Регламент (ЕС) 2016/679 и Директива (ЕС) 2016/680, а когато в предаването участват институции, органи, служби или агенции на Европейския съюз – в съответствие с Регламент (ЕС) 2018/1725, както и със Закона за защита на личните данни. Всъщност, дори да липсваше такава препращаща норма, едва ли би възникнало съмнение, че за обработването на лични данни се прилагат правилата на законодателството по защита на личните данни и в този смисъл разпоредбата се явява излишна. Тук този закон се споменава само за пълнота. Без съмнение, той повдигат

редица интересни от трудовоправна гледна точка въпроси, които заслужават внимание в самостоятелен анализ.

- Отново за пълнота следва да се посочи, че като „трети“ лица могат да се обозначат и бившите работници и служители на работодателя. Между тях и администратора на лични данни е съществувало, но вече не съществува трудово правоотношение. Все пак в определени случаи се налага съхраняване и обработване на техни данни (напр. при ползване на фондовете за социално-битово и културно обслужване от пенсионери, работили при същия работодател съгласно чл. 300 КТ).

Разбира се, работодателят може да е администратор или обработващ лични данни и на други категории трети лица като клиенти, контрагенти и пр., но обработването на техните данни няма връзка с работодателското му качество, затова и не е предмет на настоящия анализ.

Обработването на лични данни на членове на домакинството на работниците и служителите от работодателя повдига въпроса кое би било условието за допустимост на обработването във всеки конкретен случай и докъде се простират границите на работодателските правомощия за намеса в личната сфера на тези лица.

Както беше посочено, наред с личните данни на работниците и служителите, работодателите често съхраняват и обработват информация и за други лица, с които те имат семейни, родствени или други взаимоотношения. Тези хипотези на обработване могат условно да се разделят в следните подгрупи:

1. Случаи, при които е налице изрична правна норма, на основание на която работодателят изисква и обработва лични данни за трети лица, свързани с работника или служителя

Трудовото законодателство съдържа множество хипотези, налагащи обработване на лични данни на трети лица – членове на домакинството на работника или служителя. Ползването на различни видове отпуски например налага събиране на информация за други лица от семейството на служителя. Отпускът за отглеждане на дете до 2-годишна възраст може да се разреши на бащата (осиновителя) или на баба или дядо на детето, ако те работят по трудово правоотношение. За целта майката (осиновителката) дава декларация по образец, приложен към Наредбата за работното време, почивките и

отпуските. В този случай работодателят на лицето, което ползва отпуска, ще получи документ, съдържащ личните данни и на двамата родители, както и данните на детето.[4] Съгласно чл. 162, ал. 1 КТ работникът или служителят има право на отпуск за гледане на болен или на карантиниран член от семейството, належащо придружаване на болен член от семейството за медицински преглед, изследване или лечение, както и за гледане на здраво дете, върнато от детско заведение поради карантина в заведението или на детето. В болничния лист за гледането на болен член от семейството се вписват имената на болния, ЕГН, родствената връзка и диагнозата.[5] Наличието на основание за ползване на отпуска по чл. 157, ал. 1, т. 1 КТ се удостоверява със свидетелство за граждански брак, съдържащо личните данни и на другия съпруг.[6] Обезщетенията при преместване в друго населено място (чл. 216 КТ)[7] обикновено покриват разноските на служителя и на членове на неговото семейство, които трябва да бъдат индивидуализирани и пр.

Дадените по-горе примери могат да се увеличат, но и изложените са напълно достатъчни, за да обосноват извода, че законоустановените случаи на обработване на лични данни на членове на семейството на служители от техните работодатели далеч не са изолирани. Това от своя страна налага и изследването на въпроса за допустимостта на такова обработване.

Данните за членовете на домакинството представляват едновременно лични данни на тези лица и лични данни на самия работник или служител, тъй като разкриват семейната му идентичност.[8] Средствата и целите на обработването са същите като за данните на самите работници и служители. Физически информацията се съхранява в трудовите досиета на служителите (напр. актът за граждански брак, в който фигурира информация и за двамата съпрузи, ще се класира в досието на съответния служител, встъпил в брак).

Условията за допустимост на обработването обаче не могат да са идентични. Разпоредбата на чл. 6 ОРЗД въвежда като изискване за законосъобразност на обработването да е налице поне едно от изчерпателно

[4] Вж. Симеонова, Ст. Наръчник по трудово право (Предотвратяване на некоректни действия на страните по трудовото правоотношение – практически съвети), С.: Интер Интелект, 2007, 336–337.

[5] Вж. Недкова, Ат. Правна закрила на лицата, които полагат трайни грижи за възрастен или инвалидизиран член на семейството. – В: Актуални проблеми на трудовото и осигурителното право. Т. 6, С.: УИ „Св. Климент Охридски“, 2013, 168–170.

[6] Вж. Средкова, Кр. Трудово право. Специална част. Дял I Индивидуално трудово право. С.: УИ „Св. Климент Охридски“, 2011, с. 217.

[7] Вж. Василев, А., Е. Мингов. Коментар на Кодекса на труда, 728–730.

[8] Вж. по-подробно Александров, А. Защита на личните данни на работниците и служителите. С.: ИК Труд и право, 2016, 43.

изброени условия: субектът на данните да е дал съгласие за обработване на личните му данни за една или повече конкретни цели; обработването да е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор; обработването да е необходимо за спазването на законово задължение, което се прилага спрямо администратора и т.н. Ако за самите работници и служители несъмнено е налице условието за допустимост на обработването „за изпълнението на договор, по който субектът на данните е страна“ (т.е. трудовия договор), това условие не е налице по отношение на разглежданата тук група лица.

Донякъде може да се приеме, че е налице хипотезата „обработването е необходимо за целите на легитимните интереси на администратора“, в смисъл че работодателят обработва посочените данни, за да е в състояние да изпълни задълженията си по трудовото правоотношение с работника или служителя. Все пак този извод не е съвсем безспорен и не е изключено титулярите на личните данни да оспорват обработването им като незаконосъобразно. Като че ли по-адекватното условие за допустимост на такова обработване трябва да се търси в хипотезата „обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора.“

Необходимо е тук да се отчете още един нюанс. Съгласно чл. 3 ЗЛС лицата, които не са навършили 14-годишна възраст, са малолетни. Вместо тях и от тяхно име правни действия извършват техните законни представители – родители или настойници. Следователно за ползването на различни права по трудовото правоотношение от родител (предварителна закрила на майки с деца до 3-годишна възраст по чл. 333, ал. 1, т. 1 КТ, отпуск за отглеждане на дете до 8-годишна възраст и др.), които предполагат представяне на акт за раждане на детето, става въз основа на действията на родителя. Правновалидна воля вместо малолетното лице формира родителят или настойникът му.[9] Що се отнася до дееспособните членове на семейството на работник или служител, чиито лични данни се обработват от работодателите, при тях често е налице и съгласието като условие за допустимост на обработването. Декларациите – приложения към НРВПО се подписват от съответните лица именно заради желанието им да постигнат предвидените в трудовото законодателство правни последици от подаването им. В този случай не може

[9] Влахов, Кр. Извършване на разпоредителни действия с имуществото на малолетни и непълнолетни и новият Закон за закрила на детето. Собственост и право, 2000, № 10, 51–57.

да има никакво съмнение дали титулярът на данните е съгласен с обработването им. Така например Декларация – приложение № 2 към чл. 46, ал. 3 НРВПО (Декларация за ползване на отпуск по чл. 164, ал. 1 и 3 от Кодекса на труда от бащата (осиновителя) или от един от родителите на майката (осиновителката) или бащата (осиновителя)) се подписва както от титуляря на правото на отпуск, така и от лицето, на което прехвърля ползването му.

Следва да се отбележи обаче, че не е препоръчително да се разчита на съгласието на титуляра на данните като условие за законосъобразност на обработването. Основният практически проблем е, то лесно може да бъде оттеглено, а тогава ще възникне въпросът с настъпилите вече правни последици от извършените до момента действия.[10] Разбира се, майката на детето може по всяко време да оттегли даденото от нея съгласие за прехвърляне на отпуск по майчинство и това ще прекрати ползването на отпуска от съответното трето лице – бащата или баба или дядо на детето. Но ако тя поиска преустановяване на обработването на личните ѝ данни от работодателя на лицето, ползвало отпуска, той няма как да удостовери използвания отпуск и всъщност не може да заличи данните. Затова и изобщо не следва да се разсъждава в посока на съгласието като условие за допустимост на обработването, ако е мислимо да се намери друго такова условие.

Въпреки че понякога в практиката двете теми се смесват, съвсем отделен въпрос от съгласието на титуляря на данните за обработването им е този за правото му на информация относно обработването. Общият регламент за защита на данните разграничава две хипотези – когато личните данни се събира пряко от субекта на данните (чл. 13 ОРЗД) и личните данни не са получени от субекта на данните (чл. 14 ОРЗД).[11] Обемът на дължимата информация в двете хипотези показва някои различия, но и в двата случая е задължително тя да бъде предоставена. Спецификата на обработването на лични данни в контекста на трудовите отношения е, че данните на третите лица обикновено не се предоставят на работодателя пряко от тях – напр. служителят удостоверява пред работодателя си правото да ползва отпуск за гледане на болен член от семейството чрез представяне на болничен лист с реквизитите по чл. 38, ал. 3 – 4 НМЕ, а не самият болен, за чието гледане е издаден документът. Редки ще са случаите, при които третите лица – титуляри на данните, ги предоставят пряко на работодателя. Такъв директен

[10] Александров, А. – В: Кръстева, Д., А. Александров. Защита на личните данни – мисия възможна. 2-ро изд., С.: РЕЗОН България, 2018, 93–104.

[11] Кръстева, Д. – В: Кръстева, Д., А. Александров. Защита на личните данни – мисия възможна, 56–58.

контакт е мислим, когато трудовото правоотношение е прекратено поради смъртта на работника или служителя, а наследниците му претендират изплащане на дължими трудови възнаграждения и обезщетения, като за целта следва да представят удостоверение за наследници.

Работодателите следва да са подготвени и за двете възможни хипотези, в които могат да получат лични данни на трети лица, за да могат да изпълнят задълженията си да ги информират за определени обстоятелства като идентифициране на администратора и координатите за връзка с него; координатите за връзка с длъжностното лице по защита на данните, когато е приложимо; целите на обработването, за което личните данни са предназначени, както и правното основание за обработването; получателите или категориите получатели на личните данни, ако има такива и т.н.

2. Случаи, при които липсва пряко нормативно основание за обработване на личните данни на трети лица, свързани с работника или служителя

Някои разпоредби в трудовото ни законодателство имплицитно предпоставят обработването на лични данни на трети за трудовото правоотношение лица, без обаче да го предвиждат изрично. Например разпоредбата на чл. 299 КТ предвижда възможността средства от фондовете за социално-битово и културно обслужване да се ползват от семействата на работниците и служителите по решение на общото събрание и в съответствие с колективния трудов договор.[12] Логично е, че това ползване не може да става безотчетно и работодателят ще изисква и съхранява информация кои лица са ползвали съответния фонд и в каква връзка се намират те с определен работник или служител.

Мислими са и случаи, при които работникът или служителят предоставя на работодателя си лични данни на членове на своето домакинство, без те дори да не са информирани за това. Например в колективния трудов договор може да е предвидена възможност за допълнително доброволно здравно осигуряване на служителите и членове на техните семейства (при преференциални условия, договорени за служителите).[13] Обикновено в такива случаи работниците и служителите заявяват писмено кои свои близки искат да осигуряват. Аналогична ситуация може да възникне с предоставяне

[12] Вж. по-подробно Средкова Кр. – В: Коментар на Кодекса на труда, 894–895.

[13] Относно предмета на колективния трудов договор вж. по-подробно Йосифов, Н. Колективният трудов договор в България. С.: Албатрос, 2005, 106–134.

на „Мултиспорт“ карти на работници и служители, които могат да посочат като „придружител“ (т.е. лице, което може също да се възползва от намаленията, които дава картата) член от домакинството си.

В тази група случаи следва да се въведе и изискване за декларация от страна на титуляря на данните, че е съгласен с обработването им за посочената цел. Тук липсва друго условие за допустимост на обработването, което да се приложи. Впрочем, същото становище застъпва и Комисията за защита на личните данни: „Допустимо е ползватели на услугата [Мултиспорт карти – б.м, А.А.] да бъдат и трети лица, напр. съпрузи и деца на служителя, като по отношение на техните лични данни също следва да се прилага съгласието като основание за законосъобразност на обработването“ (Становище на КЗЛД рег. № НДМСПО-17-949/28.11.2018 г. относно въпроси, свързани с карти „Multisport“).[14]

3. Случаи, при които обработването на лични данни на трети лица, свързани с работника или служителя, влиза в противоречие с принципите на Общия регламент за защита на данните и националното законодателство

Често се среща погрешното схващане, че съгласието на физическото лице – титуляр на данните може да преодолее всякакви ограничения пред обработването им. Разбира се, подобно твърдение е несъстоятелно. Даденото съгласие за обработване на личните данни от субекта само по себе си не може да валидира всяко обработване, ако то е в противоречие с принципите на законодателството по защита на личните данни. По-конкретно, дори да е налице писмена декларация от субекта, че е съгласен администраторът да обработва неговите данни, това обработване отново няма да е законосъобразно, ако не е подчинено на конкретни, изрично указани и легитимни цели, или пък събраните и обработвани данни нарушават принципа за свеждане на данните до минимум (арг. от чл. 5, пар. 1, б. „б“ и „в“ ОРЗД).

Конкретният повод да се подчертае това правило в рамките на настоящото изложение са нагласите на някои работодатели да обработват

[14] Становището е достъпно на сайта на Комисията за защита на личните данни [онлайн]; [прегледан на 2 май 2023 г.], https://www.cpdp.bg/?p=element_view&aid=2148.
Вж. също: Захариев, М. Картите „Мултиспорт“ и защитата на личните данни. ТИТА, 2019, № 122, [онлайн]; [прегледан на 16 май 2023 г.] достъпен на: https://www.tita.bg/danatsi_tita/edition/135/article/3311; Захариев, М. Основни задължения на работодателите относно защитата на личните данни. ТИТА, 2022, № 3. [онлайн]; [прегледан на 16 май 2023 г.] достъпен на: https://www.tita.bg/trud_osigurovki/edition/3/ article/33.

неотносима информация, в т.ч. за трети лица – членове на домакинствата на работниците и служителите, за чието събиране нито има пряко законово основание, нито такова може да се изведе по тълкувателен път. Вероятно причината може да се търси не толкова в опит за злоупотреба с работодателските правомощия (в крайна сметка работодателят няма интерес да инвестира време и ресурси в обработването на информация, която не му е необходима), колкото в търсенето на своеобразно „презастраховане“ и/или недостатъчно познаване на действащата регулация. Своя принос за тази тенденция безспорно има и изключително некачественото законодателство от последните години, създаващо твърде много неясноти и объркващо адресатите си.[15]

Казаното може да се онагледи с добилата особена популярност по време на извънредното положение и последвалата го извънредна епидемична обстановка в страната „дистанционна работа“. Терминът не е легален, но служи за обобщение на две форми на организация на работа, изнесена извън служебните помещения на предприятието – надомната работа и работата от разстояние. Те отдавна имат своята уредба в трудовото ни законодателство. Още през 2011 г. в гл. V КТ бяха въведени допълнителни условия за извършване на надомна работа (нов раздел VIIIа, чл. 107б–107ж КТ) и допълнителни условия за извършване на работа от разстояние (нов раздел VIIIб, чл. 107з–107п КТ). За съжаление от самото си приемане уредбата страдаше от редица правнотехнически несъвършенства, а и проблеми по същество, които така и не бяха отстранени. Те също са ставали обект на обоснована критика в правната литература.[16] Може би единствено поради по-ограниченото приложно поле на тези форми на работа до 2020 г. практическото значение на посочените проблеми не беше толкова голямо, колкото

[15] Вж. Александров, А. Практически проблеми на трудовото право, произтичащи от системата на неговите източници. – Труд и право, 2016, № 12, 13–18; Александров, А. Извънредното положение не може да е оправдание за извънредно некачественото трудово законодателство. – Съвременно право, 2020, № 1, 61–73.

[16] Вж. Средкова, Кр. За „специфичното“ в правната уредба на специфичните трудови правоотношения. – В: Актуални проблеми на трудовото и осигурителното право. Т. 6, С.: УИ „Св. Климент Охридски“, 2013, 26–39; Великова – Стоянова, А. Същност и условия за работа от разстояние. – В: Юбилеен сборник, посветен на 80-годишнината на проф. д.ю.н. Васил Мръчков. С.: ИК Труд и право, 2014, 263–276; Мръчков, В. Работата от разстояние – законова уредба, обща характеристика и особености. – Труд и право, 2016, № 3, Приложение.; Мръчков, В. Надомната работа – законова уредба, обща характеристика и особености. – Труд и право, 2016, № 4, Приложение.; Александров, А. Проблеми на трудовите отношения в условията на обявено извънредно положение или обявена извънредна епидемична обстановка. С.: Спотинов принт, 2022, 41–76.

стана по време на пандемията и свързано с нея „антикризисно трудово законодателство“.

Дистанционните форми на работа поставят множество правни проблеми, включително в контекста на допустимостта на обработването на лични данни на трети за трудовото правоотношение лица. На първо място, осъществяването на работодателски контрол по отношение на качеството на изпълнение на служебните задължения на работника или служителя, уплътняването на работното време и пр., при условията на надомна работа или работа от разстояние, се сблъсква с навлизането в личната сфера на широк кръг трети лица – членове на домакинството на работника или служителя. Възможните механизми за осъществяване на дистанционен контрол са свързани или с използването на технически средства, напр. видеонаблюдение, или с проверки на място, като и двете форми поставят и въпроса за личната неприкосновеност на третите лица. Очевидно използването на технически средства, които интензивно навлизат в личната сфера на лицата, ще се окаже непропорционално на целите на обработка на данните. Работодателят не може да монтира нито камери за видеонаблюдение в дома на работника или служителя, нито да използва други технически средства за контрол, които ще запишат информация и за лицата, с които работникът или служителят живее. Що се отнася до проверките на място, изглежда, че правилото на чл. 107д, т. 2 КТ (в материята на надомната работа), че работникът или служителят е длъжен да осигурява достъп на работодателя до помещението, където е работното място, има по-скоро пожелателен характер. Аналогичното правило в материята на работата от разстояние е с далеч по-„плахата“ формулировка: „Работниците и служителите, които извършват работа от разстояние, нямат право да откажат достъп до работното място без основание за това, в рамките на установеното работно време и/или на уговореното в индивидуалния и/или в колективния трудов договор“ (вж. чл. 107к, ал. 6 КТ). Основателен ли би бил отказът на работника или служителя да предостави достъп до помещението с аргумента, че съжителстващото с него лице/лица не позволява/т това? Струва ми се, че отговорът на този въпрос следва да е утвърдителен.

Следваща група правни проблеми при надомната работа и работата от разстояние, с аналогично значение за личната сфера и неприкосновеност на третите лица – членове на домакинството, са свързани с осигуряването на здравословни и безопасни условия на труд. От една страна, работодателят е носител на общо задължение за осигуряване на такива условия на труд, включително когато работното място е домът на работника или служителя. От друга, поради изложените и по-горе съображения е твърде съмнително доколко представители на работодателя имат правото да навлязат в личното

пространство на работника или служителя и членовете на неговото домакинство, било то и с цел проверка на факторите на работната среда.

В търсене на механизъм за преодоляване на посочените затруднения, някои работодатели се насочиха към изискването на декларации от членовете на домакинствата на дистанционно работещите работници и служители, че са съгласни с полагането на тази форма на труд, че не възразяват срещу възможни проверки и пр. Подобна практика е категорично незаконосъобразна. Липсва легитимна цел за обработване на данни за членове на домакинствата на работниците и служителите за установяването на обстоятелство, което е правно ирелевантно. Казано с други думи, трудовото законодателство не забранява работник или служител да полага надомен труд или работа от разстояние, дори член/членове на домакинството му да се противопоставят на това. При това положение нищо не оправдава изискването на подобна декларация от работодателя. На следващо място, следва да се има предвид още, че в разглежданата хипотеза става дума за едно твърде интензивно навлизане в личната сфера както на работниците и служителите, така и на членовете на техните домакинства. Напълно е възможно някои лица да не желаят да разкриват с кого съжителстват. Не е изключено също предоставянето на такава информация да засегне и лични данни от категориите на т.нар. „чувствителни“ данни (напр. относно сексуална ориентация).

Поради изложените по-горе следва да се приеме, че работодателят няма нито задължение, нито право да изисква от членовете на домакинствата на работниците и служителите предоставяне на съгласие последните да работят от домовете си. Известно е, че в правомощията на КЗЛД като надзорен орган по спазване на законодателството за защита на личните данни е включено налагането на изключително високи като размер санкции, затова е препоръчително такива рискове да се избягват. Достатъчно е да се припомни, че според ОРЗД и националното ни законодателство по защита на личните данни наказанията глоба или имуществена санкция са диференцирани за различни видове нарушения и могат да достигнат до 20 млн. евро или до 4% от общия годишен световен оборот на предприятието за предходната финансова година (която от двете суми е по-висока) за нарушаване на основните принципи за обработване на лични данни, включително условията, свързани с даването на съгласие.[17]

Заключение

[17] Вж. по-подробно Александров, А. Отново за размерите на глобите и имуществените санкции за нарушения в правния режим на защита на личните данни. – Труд и право, 2018, № 6, 59–64.

В резултат на предложения анализ може да се достигне до извода, че мислимите хипотези на обработване на лични данни на членове на домакинствата на работниците и служителите от работодателите са три:

Първо, когато обработването е в изпълнение на изрично предвидено в закона задължение на администратора на лични данни. В тези случаи става дума предимно за съпрузи и роднини по пряка или съребрена линия, доколкото законодателството ни все още придава неоправдано малко правно значение на фактическото съжителство и правни норми, по силата на които работодателят е задължен да обработва данни за трети лица, които не са съпрузи или родственици на работниците или служителите, са все още по-скоро изключение.[18]

Второ, когато необходимостта от обработване на лични данни на трети лица може да се извлече по тълкувателен път, без да е изрично предвидена в закона. Когато например в чл. 270, ал. 3, изр. първо КТ законодателят предвижда, че трудовото възнаграждение се изплаща лично на работника или служителя по ведомост или срещу разписка или по писмено искане на работника или служителя – на негови близки, той не дефинира понятието „близки“ и не го ограничава само до съпрузи и роднини. Разбира се, работодателят е длъжен да провери самоличността на лицето, на което ще изплати възнаграждението съгласно полученото писмено искане за това от работника или служителя, но няма нито правото да изследва какви са отношенията на близост между лицата, нито да откаже изплащането на сумата с аргумента, че те на са „близки“. В тази група хипотези може да се използва съгласието на титуляря на данните като условие за законосъобразност на обработването им.

Трето, обработване, което влиза в разрез с принципите на законодателството по защита на личните данни и е незаконно, дори за него да е поискано и получено изрично съгласие от титулярите на данните. Това са

[18] Все пак се наблюдават първите плахи стъпки на придаване на правно значение и на фактическото съжителство в трудовото право – напр. чл. 107а, ал. 1, т. 1 КТ забранява сключването на трудов договор за работа в държавната администрация с лице, което би се оказало в йерархическа връзка на ръководство и контрол със съпруг или съпруга, **с лице, с което е във фактическо съжителство**, с роднина по права линия без ограничения, по съребрена линия до четвърта степен включително или по сватовство до четвърта степен включително. Като всяка друга забранителна норма в законодателството, и тази не може да се тълкува разширително, което поставя под съмнение ефективността ѝ. По-конкретно, ако лицата са в интимна връзка, но нямат брак и не живеят заедно, формално те не нарушават забраната. Работодателят на практика няма правен механизъм да установи фактическото съжителство, ако то не е декларирано пред него и адресната регистрация на лицата е различна.

хипотези, при които обработването на данните засяга по недопустим начин личната сфера и неприкосновеност както на работниците и служителите, така и на свързаните с тях лица. Тук може да се причисли всяка форма на събиране на информация, която по директен или индиректен начин разкрива обстоятелства от техния интимен живот или личностни убеждения, която е ирелевантна за трудовото правоотношение.

Препоръчително е, при всички случаи, при които работодателят обработва данни за трети лица в контекста на трудовите правоотношения, в които е встъпил, да се извършва внимателен предварителен анализ на законосъобразността на такова обработване. Ако в организацията има определено длъжностно лице по защита на данните, следва да се поиска и неговото становище. Отговорното отношение на работодателите към действията по обработване на лични данни, които извършват, е гаранция както за интересите на засегнатите лица, така и за самите работодатели, ако не искат да рискуват ангажиране на отговорността им.

Библиография:

1. Александров, А. Защита на личните данни на работниците и служителите. С.: ИК Труд и право, 2016.
2. Александров, А. Практически проблеми на трудовото право, произтичащи от системата на неговите източници. – Труд и право, 2016, № 12, 13–18.
3. Александров, А. Отново за размерите на глобите и имуществените санкции за нарушения в правния режим на защита на личните данни. – Труд и право, 2018, № 6, 59–64.
4. Александров, А. Извънредното положение не може да е оправдание за извънредно некачественото трудово законодателство. – Съвременно право, 2020, № 1, 61–73.
5. Александров, А. Проблеми на трудовите отношения в условията на обявено извънредно положение или обявена извънредна епидемична обстановка. С.: Спотинов принт, 2022, 41–76.
6. Великова – Стоянова, А. Същност и условия за работа от разстояние. В: Юбилеен сборник, посветен на 80-годишнината на проф. д.ю.н. Васил Мръчков. С.: ИК Труд и право, 2014, 263–276.
7. Влахов, Кр. Извършване на разпоредителни действия с имуществото на малолетни и непълнолетни и новият Закон за закрила на детето. Собственост и право, 2000, № 10, 51–57.

8. Захариев, М. Картите „Мултиспорт“ и защитата на личните данни. ТИТА, 2019, № 122, [онлайн]; [прегледан на 16 май 2023 г.] достъпен на: https://www.tita.bg/danatsi_tita/edition/135/article/3311.

9. Захариев, М. Основни задължения на работодателите относно защитата на личните данни. ТИТА, 2022, № 3. [онлайн]; [прегледан на 16 май 2023 г.] достъпен на: https://www.tita.bg/trud_osigurovki/edition/3/article/33.

10. Йосифов, Н. Колективният трудов договор в България. С.: Албатрос, 2005.

11. Кръстева, Д., А. Александров Защита на личните данни – мисия възможна. 2-ро изд. С.: РЕЗОН България, 2018.

12. Мръчков, В. Работата от разстояние – законова уредба, обща характеристика и особености. – Труд и право, 2016, № 3, Приложение.

13. Мръчков, В. Надомната работа – законова уредба, обща характеристика и особености. – Труд и право, 2016, № 4, Приложение.

14. Мръчков, В., Кр. Средкова, А. Василев, Е. Мингов Коментар на Кодекса на труда, 13 изд. С.: Сиби, 2021.

15. Недкова, Ат. Правна закрила на лицата, които полагат трайни грижи за възрастен или инвалидизиран член на семейството. – В: Актуални проблеми на трудовото и осигурителното право. Т. 6, С.: УИ „Св. Климент Охридски“, 2013, 168–170.

16. Симеонова, Ст. Наръчник по трудово право (Предотвратяване на некоректни действия на страните по трудовото правоотношение – практически съвети), С.: Интер Интелект, 2007.

17. Средкова, Кр. Трудово право. Обща част. С.: УИ „Св. Климент Охридски“, 2010.

18. Средкова, Кр. Трудово право. Специална част. Дял I Индивидуално трудово право. С.: УИ „Св. Климент Охридски“, 2011.

19. Средкова, Кр. За „специфичното“ в правната уредба на специфичните трудови правоотношения. – В: Актуални проблеми на трудовото и осигурителното право. Т. 6, С.: УИ „Св. Климент Охридски“, 2013, 26–39.

Изкуственият интелект и предизвикателствата пред зачитането на правото на справедлив процес по наказателни дела

Аделина Хаджийска*

Докладът разглежда понятието за изкуствен интелект (ИИ) и очертава възможни предизвикателства пред защитата правата на човека, по-конкретно правото на справедлив процес. В контекста на нарастващото приложение на ИИ, правото по чл. 6 ЕКПЧ е идентифицирано като застрашено право, което може да бъде засегнато по различен начин при прилагането на различни компютърни информационни системи с възможност за автономно взимане на решения. В тази връзка е обсъдено прилагането на ИИ по наказателни дела и съотношението с някои основни елементи от правото на справедлив процес. В заключение са обобщени препоръките към държавите членки, вкл. към Република България, които следва да се спазят при създаване на правна рамка на ИИ на национално ниво.

Ключови думи: *вътрешно убеждение, изкуствен интелект, наказателно производство, справедлив процес, презумпция за невиновност*

* Гл. асистент д-р по наказателнопроцесуално право в ЮФ на Университета за национално и световно стопанство, ел. поща: adelina.hadjiiska@gmail.com

Artificial intelligence and the challenges to respecting the right to a fair trial in criminal cases

Adelina Hadzhiyska[1]

The report examines the concept of artificial intelligence (AI) and outlines possible challenges to the protection of human rights, specifically the right to a fair trial. In the context of the growing application of AI, the right under Art. 6 ECHR has been identified as a threatened right that may be affected differently in the application of different computerized information systems with the possibility of autonomous decision-making. In this regard, the application of AI in criminal cases and the relationship with some basic elements of the right to a fair trial are discussed. In conclusion, the recommendations to the member states are summarized, incl. to the Republic of Bulgaria, which should be observed when creating a legal framework for AI at the national level.

Keywords: *artificial intelligence, fair trial, inner conviction, presumption of innocence, criminal proceedings*

* PhD, Chief Assistant in Criminal Procedure Law, Faculty of Lawof the University of National and World Economy (UNWE), e-mail: adelina.hadjiiska@gmail.com

„Смятаме, че бъдещето са роботите и колите на въздушна възглавница, но може би то наистина е тук!“

Чък Уендиг[1]

В епохата на изкуствения интелект (ИИ) се очертават редица предизвикателства пред защитата на основните човешки права. Едно от тях е правото на справедлив процес по чл. 6 от Европейската конвенция за защитата правата на човека (ЕКПЧ), което беше идентифицирано като рисково от Съвета на Европа и Агенцията на Европейския съюз за основните права през 2018 г.[2] Правото по чл. 6 § 1 ЕКПЧ е фундаментално право за всяко демократично общество и неговото зачитане е основен ангажимент на националните законодателства, включително когато дигитализацията обхваща редица държавни дейности като разглеждането и решаването на наказателни дела. Тази трансформация на формата и внедряването на нови технологии при разглеждането и решаването на дела поставя редица въпроси, свързани със съвместимостта на ИИ и процесуалните гаранции, свързани със справедливата процедура.

1. Понятие за изкуствен интелект и предизвикателства пред защитата правата на човека

Най-напред следва да се изясни понятието „изкуствен интелект“ (ИИ). Според дадената дефиниция от Експертната група на високо равнище „системите с изкуствен интелект (ИИ) са софтуерни (а вероятно и хардуерни) системи, създадени от хора, които с оглед на дадена сложна цел действат в рамките на физическото или цифровото измерение, като възприемат заобикалящата ги среда чрез събиране на данни, тълкуват събраните структурирани или неструктурирани данни, разсъждават въз основа на познанието или обработват информацията, получена от тези данни, и вземат решение за предприемане на най-доброто (добрите) действие (действия) за постигане на дадената цел. Системите с ИИ могат или да използват символно представени правила, или да усвояват цифров модел и могат да адаптират поведението си, като анализират начина, по който средата е засегната от предишни техни действия. Като научна дисциплина ИИ включва няколко подхода и

[1] Американски писател и сценарист.

[2] Вж Янков, З. Изкуствен интелект – предизвикателства пред зачитането на правата на човека, (онлайн), 18.06.2023, (прегледан на 18.06.2023). Достъпен на: https://bcnl.org/news/izkustven-intelekt-predizvikatelstva-pred-zachitaneto-na-pravata-na-choveka

техники, като например машинно самообучение (специфични примери за което са дълбокото самообучение и обучението с утвърждение), машинно разсъждение (което включва планиране, изготвяне на график, моделиране на познанието и разсъждение, търсене и оптимизация) и роботика (която включва контрол, възприятие, сензори и задвижващи механизми, както и интегрирането на всички други техники в кибер-физически системи)“[3].

В Бялата книга за изкуствения интелект се възприе виждането за ИИ като „определен набор от технологии, които съчетават данни, алгоритми и изчислителна мощ“[4].

Според Стамфорд Джон Маккарти ИИ е „науката или инженерният процес по създаването на интелигентни машини, особено интелигентни компютърни програми, които могат да се използват за изучаване и разбиране на човешкия интелект“[5].

Посочените дефиниции обхващат различни интелигентни системи, вкл. т.нар. „чатботове“ за създаване на съдържание (Chatbots), приложения, роботизирани системи и други технологии. Общото между тях е, че всички те представят т.нар. ИИ като **вид компютърна програма с възможност за автономни решения**. Специфичното на този вид технология е техническата способност да функционира по начин, наподобяващ човешкия механизъм на взимане на решения. Обработвайки огромен обем от информация (данни), посредством зададени алгоритми, ИИ за кратък интервал от време постига определени резултати.

Днес ИИ има потенциал да намери употреба в дейността на редица дейности, върху които е установен държавен монопол. Той намира приложение в извършването на извънпроцесуални проверки, в оперативно-издирвателната дейност, като в технологически по-развитите страни все по-открито се говори и за неговия потенциал в хода на разследването по наказателни дела. Не е тайна, че открито се говори, че ИИ може да е особено полезен в борбата с определени видове престъпни посегателства като престъпления срещу фи-

[3] Определение за Изкуствен интелект: Основни възможности и дисциплини. Определение, разработено за целите на документалните резултати на групата, Брюксел, 2018.,посетен на 18.06.2023. Достъпен на: https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:52021PC0206&from=EN.

[4] Вж Бяла книга за изкуствения интелект – Европа в търсене на високи постижения и атмосфера на доверие, публикувана на 19.02.2020, достъпна онлайн на следния линк: https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:52020DC0065&from=EN#footnote29

[5] Вж Енджов, В. Изкуственият интелект като предизвикателство пред правото (онлайн)18.06.2023, (прегледан на 18.06.2023). Достъпен на: https://news.lex.bg/Изкуственият-интелект-като-предизвикателство-пред-правото/

нансовата система на държавата, изпирането на пари, тероризъм, трафик на хора, сексуалното насилие над деца онлайн, киберпрестъпления и др.

Новите технологии намират все по-широка употреба и в дейността на правоприлагащите държавни органи, например когато се търси в наличната база данни потенциален извършител на престъпление, при установяване самоличността на жертвите на престъпления (трафик на хора и др.), при идентифициране на деца – жертви на сексуална експлоатация, и т.н. В сферата на правоохранителната и оперативно-изидрвателната дейност също се използват системи за автоматизирано разпознаване на регистрационни номера, за гласова идентификация, звуково наблюдение или компютърни информационни технологии за разчитане по устните. Известни са случаи на прогностика, с която да се установят т.нар. „горещи точки“ на престъпността, установяват се потенциални случаи на последващ рецидив или точното местонахождение на определени лица, които в образуваното наказателно производство имат качеството на свидетели очевидци, обвиняеми, пострадали и др.

Предимствата на ИИ са безспорни. Широкият капацитет на ИИ и възможностите му за обработка на голям обем данни с изключителна прецизност за кратко време повишава доверието в него. Подчертавайки „точността“ на извършените автоматизирани процеси посредством интелигентните системи, аргументирано може да се защитава идеята за необходимостта техните резултати да се ползват директно в процеса на доказване по наказателни дела. В тази връзка не може да се отмине без внимание обстоятелството, че вече се говори за „електронен обиск“, виртуална аутопсия на труп, следствен експеримент и др[6]. Налице са и научни изследвания, посветени на тема „дигитално разследване“, където се приветства идеята човешкият фактор да бъде заменен с изкуствен (технологичен)[7].

Успоредно с внедряването и употребата на ИИ нараства опасността от засягане на редица основни права, в това число и правото на справедлив процес по чл. 6 в неговия наказателен аспект. По този повод още през 2018 г. Съветът на Европа и Агенцията на Европейския съюз за основните права постави на дневен ред проблема за защитата правата на човека и изкуствения интелект. Подчертавайки необходимостта от изграждане на

[6] Lundberg, S.; Lee, S.I. A Unified Approach to Interpreting Model Predictions. 2017, (accessed on 15 February 2022), Available online: http://xxx.lanl.gov/abs/ 1705.07874

[7] Arianna Trozzea, Toby Daviesb, Bennett Kleinberg, Of degens and defrauders: Using open-source investigative tools to investigate decentralized finance frauds and money laundering, Forensic Science International: Digital Investigation. arXiv – CS – Cryptography and Security Pub Date: 2023-03-01, DOI:arxiv-2303.00810, Available online: file:///C:/Users/Аделина/Downloads/mathematics-10-00949-v3.pdf

балансиран подход и увеличаващо се доверие на обществото в новите иновативни приложения, бяха изведени основните права на човека, които могат да бъдат засегнати от ИИ.

През 2019 г. бяха публикувани и т.нар. „Десет стъпки за защита на правата на човека при употребата на изкуствен интелект“. Последните представляват изисквания, които предвиждат конкретни ангажименти към отделните държави членки, както следва: задължителна оценка на въздействието върху правата на човека при разработването и използването на ИИ и провеждане на обществени консултации, които да повишат доверието на обществото в ИИ; прилагането на стандарти за правата на човека в частния сектор; информираност и прозрачност на процесите; независим човешки надзор; зачитане принципите на недискриминация и равенство на гражданите; защита на данните и тяхната поверителност; правото на свобода на изразяване; спазване на правото на свобода на събиране и сдружаване; достъп до средства за защита; насърчаване на „грамотността сред обществото за ползите от изкуствения интелект.

2. ИИ и някои елементи от правото на справедлив процес по чл. 6 ЕКПЧ

Поначало ИИ се явява напълно съвместим с правото на всяко лице при решаването на правен спор относно… „основателността на каквото и да е наказателно обвинение срещу него, …на справедливо и публично гледане на неговото дело в разумен срок, от независим и безпристрастен съд, създаден в съответствие със закона“ (чл. 6 § 1 ЕКПЧ). Но осигуряването на правото на справедлив наказателен процес по чл. 6 ЕКПЧ поставя редица предизвикателства пред законодателя с цел осигуряване на ефективната му защита. В тази връзка научен интерес представлява какво е съотношението на новите технологии с някои от неговите основни елементи, по-конкретно с правото на лицето неговото дело да бъде разгледано и решено **от независим и безпристрастен съд, създаден в съответствие със закона.**

Известно е, че независимостта и безпристрастността са ключови компоненти на чл. 6 ЕКПЧ. Самото понятие „независим и безпристрастен съд“ предполага съдиите и съдебните заседатели да бъдат избрани въз основа на професионална компетентност и морална почтеност, по установения в закона ред. В този смисъл строгият процес за назначаване на съдии и съдебни заседатели е от съществено значение за обезпечаване на правото по чл. 6 § 1 ЕКПЧ. С оглед прозрачността на преразпределението на делата у нас отдавна е разпределението на делата и преписките в органите на съдебната власт се извършва на принципа на случайния подбор чрез равномерно

електронно разпределение съобразно поредността на постъпването им при спазване изискванията на чл. 360б от Закона за съдебната власт. Автоматизираната система може да се настрои и да разпределя делата съобразно зададен алгоритъм и критерии. В същото време обстоятелството, че системата е под човешки контрол и в този смисъл остава открита потенциалната заплаха да бъде манипулирана, винаги поставя под съмнение изискването за независимост и безпристрастност.

Ето защо с цел да се обезпечи правото по чл. 6 ЕКПЧ преразпределянето може да се запази и да се осъществява посредством ИИ, но само при наличието на всички необходими гаранции за това. На практика това означава да се предприемат мерки, изключващи възможността за злоупотреба и евентуално произволно заместване на съдии и съдебни заседатели чрез умишлено заличаване на съдии и/или съдебни заседатели заради отпуск, командироване, изтичане на мандат и т.н.

В противоречие с чл. 6 ЕКПЧ, по-конкретно някои основни негови елементи би било използването на ИИ в хода на разследването по наказателни дела. Вярно е, че ИИ може да улесни и ускори дейността на държавните органи, но винаги следва да се има предвид, че в редица случаи се засяга неприкосновеността на личния живот на лицата, участващи в едно или друго процесуално качество в наказателното производство[8]. Така например прилагането на система с ИИ за автоматизирано разпознаване на лицата в публичното пространство по походка, пръстови отпечатъци, ДНК, гласови и други биометрични показатели трябва да бъде забранена на национално ниво. Същевременно **подобно разпознаване представлява сериозна намеса в личната сфера на лицата.** Тя ще е в нарушение на чл. 8 ЕКПЧ, което поставя под съмнение автоматично и справедливостта на производството по чл. 6 § 1 ЕКПЧ.

Говорейки за ИИ и неговата употреба в наказателното производство, не може да се отмине без внимание обстоятелството, че съществуват компютърни информационни технологии с разработени алгоритми, които могат да отчетат редица грешки при обработката на голям обем данни. Това на практика означава, че може да се стигне до неоснователни и неправилни резултати. Изкуственият интелект сам по себе си е сложна система, незастрахована от пропуски. Освен това съществува риск от възникване на особен вид „зловредна ситуацията“, при която ИИ като всяка компютърна програма може да стане обект на „хакерска“ атака и да бъде „заразен“ с вирус, който до доведе до внедряване на неправилни данни с цел получат-

[8] Rigno, Ch. Using Artificial intelligence to address criminal justice needs, National Institute of Justice, Issue No. 280, 2019.

ване на необективни резултати под формата на правни и/или юридически изводи при постановяване на крайни решения. В тази връзка държавните органи следва да предприемат сериозни мерки, възпрепятстващи опасността от изтичане на данни или нерегламентиран достъп до лични данни и друга информация от значение за конкретно съдопроизводство. Това може да стане чрез предвиждане на конкретни изисквания за технологична сигурност и надеждност на новите интелигентни системи, като последните винаги са под човешки надзор.

В контекста на правото на справедлив наказателен процес предизвикателство е зачитането на **презумпцията за невиновност по чл. 6 § 2 ЕКПЧ**. Тя играе ключова роля за производствата по наказателни дела и се прилага с известния принцип „in dubio pro reo“, според който всяко съмнение следва да се тълкува в полза на обвиняемия. Спазвайки този постулат, ЕСПЧ приема, че същността на презумпцията за невиновност се свежда до изискването съдебният състав да не подхожда предубедено към обвиняемия, а прокуратурата да представи необходим обем доказателства срещу него[9]. В този смисъл тази процесуална гаранция е нарушена във всички случаи, когато е налице предубеденост от страна на магистрат или друг държавен орган, без преди това да е установена виновността на обвиняемия по безспорен начин. С оглед предварително зададените алгоритми и критерий, които правят възможно изготвянето на „прогностики“ за последващо поведение на процесуални фигури в процеса, струва ми се, че прилагането на ИИ винаги ще постави под съмнение презумпцията по чл. 6 § 2 ЕКПЧ.

Трудно би било обезпечено и **изискването за мотивираност на съдебните решения** като елемент на правото на справедлив процес по чл. 6 § 1 ЕКПЧ. Вярно е, че т.нар. Chatbots приложения могат да създават съдържание, т.к. разполагат с технически възможности да следват предварително определен количествен критерий за излагане на аргументи за всеки конкретен случай, съобразявайки обема на доказателствения материал. Но това не е достатъчна гаранция, за да е налице този ключов елемент по чл. 6 § 1 ЕКПЧ. Мотивираното решение означава не само описание на събрания и проверен доказателствен материал, но предполага от изложените мотиви те ясно да личи, че съдебният състав е разполагал със свободата да оцени доказателствения материал по вътрешно убеждение. Считам, че именно тук се откроява и най-силният аргумент за това, че ИИ няма място в нака-

[9] Вж Решение от 31 март 2016 по жалба № 45773/10 – *Петров и Иванова срещу България*; Решение от 31 март 2016 по жалба № 0336/10 – *Алексей Петров срещу България*; Решение по допустимост от 4 април 2017 по жалба № 19557/05г. – *Стоянов срещу България*; Решение от 28 ноември 2002 г. по делото *Marziano v. Italy*, № 45313/99.

зателното правораздаване, доколкото е несъвместим с принципа за взимане на решения въз основа на свободна оценка на доказателствения материал.

Допускането на интелигентната система да постанови крайно решение посредством автоматизиран процес на обработка на определен обем процесуално релевантни факти (данни за ИИ – б.м.), *de facto u de jure* означава **да се подмени вътрешното убеждение на компетентния държавен орган**. Дори ИИ да работи с „научни" правила и да разполага с възможност за автономно взимане на решения, оценъчният процес чрез него се осъществява въз основа на предварително зададени критерии и мащаби, като изходът от наказателното производство е предопределен.

Възможно е идеята ИИ да разглежда и решава наказателни дела да срещне привърженици, които дори да посочват като аргумент, че интелигентната система от ново поколение може да се научи на самоконтрол, да разпознава човешките емоции и да реагира на тях[10]. Но подобно твърдение следва да се отхвърли като несъстоятелно, т.к. води до „подмяна" на човешкия фактор и свободата на оценката при постановяване на крайното решение. Следвайки същите разсъждения, научно несъстоятелно би било в бъдеще ИИ да намери приложение не само при постановяване на крайните съдебни актове, но дори и когато следва да се взема решение за предварително задържане на конкретно лице.

Заключение

Внедряването и употребата на ИИ поставя редица предизвикателства пред законодателя. С цел запазване на общественото доверие в правоприлагащите органи на фона на нарастващото значение на новите иновативни приложения, добре би било на този етап държавите да се въздържат от прилагането им в наказателните производства.

Библиография:

1. Бяла книга за изкуствения интелект — Европа в търсене на високи постижения и атмосфера на доверие, публикувана на 19.02.2020, посетен на 18.06.2023, достъпна на: https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:52020DC0065&from=EN#footnote29
2. Определение за изкуствен интелект: Основни възможности и дисциплини. Определение, разработено за целите на документалните резултати на групата,

[10] Зад подобни съждения стои т. нар. теория на научната обективизация, която отдавна основателно е отхвърлена в процеса на доказване по наказателни дела.

Брюксел, 2018, посетен на 18.06.2023, достъпен на: https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

3. Енджов, В. Изкуственият интелект като предизвикателство пред правото (онлайн), (прегледан на 18.06.2023). Достъпен на: https://news.lex.bg/Изкуственият-интелект-като-предизвикателство-пред-правото/
4. Янков, З. Изкуствен интелект – предизвикателства пред зачитането на правата на човека, (онлайн), (прегледан на 18.062023). Достъпен на: https://bcnl.org/news/izkustven-intelekt-predizvikatelstva-pred-zachitaneto-na-pravata-na-choveka
5. Arianna Trozzea, Toby Daviesb, Bennett Kleinberg, Of degens and defrauders: Using open-source investigative tools to investigate decentralized finance frauds and money laundering, Forensic Science International: Digital Investigation. arXiv – CS – Cryptography and Security Pub Date: 2023-03-01, DOI:arxiv-2303.00810, Available online: file:///C:/Users/Аделина/Downloads/mathematics-10-00949-v3.pdf
6. Lundberg, S.; Lee, S.I. A Unified Approach to Interpreting Model Predictions. 2017, (accessed on 15 February 2022), Available online: http://xxx.lanl.gov/abs/1705.07874
7. Rigno, Ch. Using Artificial intelligence to address criminal justice needs, National Institute of Justice, Issue No. 280, 2019.

Съдебна практика:

Решение от 31 март 2016 по жалба № 45773/10 – Петров и Иванова срещу БългарияРешение от 31 март 2016 по жалба № 0336/10 – Алексей Петров срещу България.

Решение по допустимост от 4 април 2017 по жалба № 19557/05 г. – Стоянов срещу България.

Решение от 28 ноември 2002 г. по делото Marziano v. Italy, application № 45313/99.

Защита на личните данни в условията на електронно управление

Цветомир Панчев*

Предмет на настоящия доклад е въпросът за степента на постигнат баланс между спазването на динамичната нормативна регламентация за защитата на лични данни и осигуряването на реални условия за ефективно електронно управление. Във връзка с това е обърнато внимание на режима на предоставяне на лични данни от Национален автоматизиран информационен фонд за българските лични документи – „Национален регистър на българските лични документи“, с цел развитие потенциала на електронното управление, включително подобряване на бизнес средата.

Ключови думи: *администратор, документи за самоличност, лични данни, мерки срещу изпиране на пари*

* Доктор по наказателен процес от Академия на Министерството на вътрешните работи, зам.-директор на дирекция „Български документи за самоличност“ към Министерство на вътрешните работи, ел. поща: tzvetomir_panchev@abv.bg

Protection of personal data in the context of e-government

Tsvetomir Panchev*

The subject of this report is the issue of the degree of balance achieved between compliance with the dynamic regulatory regulation for the protection of personal data and the provision of real conditions for effective e-government. In this regard, attention is drawn to the regime of providing personal data by the National Automated Information Fund for Bulgarian Personal Documents – "National Register of Bulgarian Personal Documents" in order to develop the potential of e-government, including improving the business environment.

Keywords*: administrator, identity documents, measures against money laundering, personal data*

* PhD in Criminal Justice, Academy of the Ministry of Interior, e-mail: tzvetomir_panchev@abv.bg

От 25 май 2018 г. всички държави – членки на Европейския съюз, следва да прилагат 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), въвеждащ по-високи стандарти за защита на данните, разширени права на физическите лица и нови задължения на администраторите на лични данни.

Част от принципите, които са водещи в националната и европейската нормативна уредба за защита на лични данни, са постигане на законосъобразност, добросъвестност и прозрачност; свеждане на данните до минимум; ограничение на съхранението и отчетност. Те следва да бъдат реализирани чрез модернизирането на правилата за защита на личните данни с оглед на новите технологии, даване по-голям контрол на лицата върху личните им данни в дигиталния свят, повече яснота и правна сигурност и по-малка бюрократична тежест за бизнеса. Предоставянето на лични данни е законосъобразно само ако и администраторът, който предоставя данните, и администраторът, който ги получава, разполагат с правно основание за обработване на данните. Необходимо е стриктно съблюдаване на всички принципи при обработване на личните данни. Посочените изисквания са сериозно предизвикателство за публичния сектор, който следва да постига баланс между защитата на личните данни и осигуряването на ефективност в бързо развиващите се технологични процеси.

В същото време пред Република България все още стои предизвикателството за полагане на системни усилия за изграждането на електронно правителство и преминаване към цифрова администрация. Във връзка с това моделът на електронното правителство, регламентиран в Закона за електронното управление (ЗЕУ)[1], е основан на принципа на еднократно създаване и съхраняване на данни, който е закрепен в законодателствата и на други държави, напр. Белгия, Нидерландия, Германия, Испания.[2] Прилагането на принципа води до отпадане на необходимостта от предоставяне на данни, които вече са предоставени или са създадени от държавни органи чрез създаване на задължение за служебен обмен на такива данни.

От изключително значение е изработването на ефективна уредба на обществените отношения между административните органи, свързани с

[1] Обн. ДВ, бр. 46 от 12 юни 2007 г., в сила от 13.06.2008 г., посл. изм. и доп. ДВ, бр. 15 от 22 февруари 2022 г.

[2] Хубенова, М. (2016). Вътрешни електронни административни услуги – актуална уредба и предлагани изменения. – Норма, № 1, 1–10.

работата с електронни документи и предоставянето на административни услуги по електронен път, както и обмена на електронни документи между административните органи. Съгласно ЗЕУ обменът се извършва като вътрешна електронна административна услуга и намира приложение по отношение на дейността на лицата, осъществяващи публични функции, и на организациите, предоставящи обществени услуги, доколкото в друг закон не е предвидено друго. Те са длъжни да предоставят помежду си вътрешни електронни административни услуги, свързани с осъществяването на правомощията им и с извършването на електронни административни услуги на гражданите и организациите. Позволява се обмен на данни за нуждите на всички административни процеси, а не само тези, свързани с предоставянето на административни услуги**.**

Административните органи, лицата, осъществяващи публични функции, и организациите, предоставящи обществени услуги, не могат да изискват от гражданите и организациите представянето или доказването на вече събрани или създадени данни, а са длъжни да ги съберат служебно от първичния администратор на данните. Последният е административен орган, който по силата на закон събира или създава данни за гражданин или организация за първи път и изменя или заличава тези данни. Наред с това предоставя достъп на гражданите и организациите до цялата информация, събрана за тях.

Към настоящия момент е в ход реализацията на целите на регистрова реформа, свързана с оптимизиране на организацията на регистрите в държавната администрация; поддръжката им с възможно най-малко разходи; служебния обмен на информация и данни за предоставяне на качествени услуги; възможността за предоставяне на услуги, базирани на регистрите, водени от други административни органи; качеството, пълнотата и всеобхватността на данните; осигуряване на възможности за използване и повторно използване на вече налични данни в публичния сектор от всички заинтересовани страни и т.н.[3]

В ЗЕУ е предвидено, че доставчиците на електронни административни услуги са длъжни да събират, обработват и предоставят само лични данни, които са необходими за извършването на електронни услуги по смисъла на този закон. Събраните данни не могат да се използват за цели, различни от посочените, освен с изричното съгласие на лицето, за което се отнасят (арг. чл. 16 ЗЕУ).

Условията за автоматизиран обмен на електронни документи като вътрешни електронни административни услуги са уредени в Наредбата

[3] Концепция за регистрова реформа, приета с РМС № 546 от 18.08.2019 г.

за общите изисквания към информационните системи, регистрите и електронните административни услуги, приета на основание чл. 7г, ал. 6, чл. 12, ал. 4 и чл. 43, ал. 2 от Закона за електронното управление (Наредбата)[4], като съгласно чл. 2, ал. 1 от Наредбата министърът на електронното управление води регистър на регистрите, в който се вписват регистри и бази данни на първичните администратори на данни. Достъпът до регистрите и базите данни се осъществява чрез подаване на заявление, съдържащо минимум данни за произхода на заявлението – юридическото лице – заявител и информационната система; основанието за получаването на данните, включително номер на преписка, ако има такава; длъжностното лице, извършващо заявяването, ако има такова. Първичният администратор на данни отказва достъп до данни на лицата, които ги заявяват, когато в заявлението за достъп липсва един или повече от изискуемите реквизити или заявителят няма право да получи данните съгласно закон.

На пръв поглед и видно от засегнатата нормативна регламентация би могло да се констатира, че **е налице особено противоречие между задължението за автоматично предоставяне на данните и един от основните принципи на правото на защита на личните данни, а именно данните да не се използват за цели, различни от целите, за които са първоначално създадени, освен с изричното съгласие на лицето**.

От една страна, по дефиниция автоматичното предоставяне на данните се извършва, за да бъдат използвани за цел различна, от онази, за която са събрани, а от друга – такава обработка не е допустима без съгласието на лицето.[5] Съгласие обаче не би следвало да се изисква, когато общата цел на обработването следва да бъде спазването на правно задължение, разписано конкретно в националното законодателство или в правото на Европейския съюз.[6] В този смисъл администраторът следва да може да идентифицира въпросното задължение или чрез позоваване на конкретната правна разпоредба, респективно по друг начин, като посочи относим източник. Така например в изпълнение на законово задължение по чл. 53 от Закона за мерките срещу изпирането на пари (ЗМИП)[7] всяка финансова институция по

[4] Приета с ПМС № 3 от 09.01.2017 г., обн. ДВ, бр. 5 от 17.01.2017 г., в сила от 01.03.2017 г., изм. ДВ, бр. 47 от 24 юни 2022 г.

[5] Хубенова, М. (2016). Вътрешни електронни административни услуги – актуална уредба и предлагани изменения. – Норма, № 1, 1–10.

[6] Обработването на лични данни от администратори както в публичната, така и в частната сфера е законосъобразно, ако е налице някое от следните алтернативни и равнопоставени основания: съгласие; изпълнение на договор; законово задължение; жизненоважни интереси; обществен интерес/официални правомощия; легитимни интереси.

[7] Обн. ДВ, бр. 27 от 27 март 2018 г., посл. изм. ДВ, бр. 32 от 26 ьприл 2022 г.

смисъла на Закона за кредитните институции[8] следва да идентифицира свой потенциален или настоящ клиент чрез представяне на официален документ за самоличност и снемане на копие от него.

Информационната дейност в Министерството на вътрешните работи (МВР) е дейност по събиране, обработване, систематизиране, съхраняване, използване и предоставяне на информация на потребители от министерството, на държавни органи, организации, юридически лица и граждани. За осъществяването ѝ се осигуряват функционирането и развитието на комуникационни и информационни системи, взаимодействието с национални и международни такива и защитата на информационния обмен на ведомството и други държавни органи. В министерството се изграждат фондове и звена за събиране, обработване, систематизиране, съхраняване, анализиране, изготвяне и предоставяне на информация. Те се изграждат при съответните структури на МВР съобразно функционалната им компетентност.

Личните данни се обработват в автоматизирани и неавтоматизирани информационни фондове като същите са регистри с лични данни по смисъла на Общия регламент относно защитата на данните и Закона за защита на личните данни (ЗЗЛД).[9] Националният автоматизиран информационен фонд за българските лични документи – „Национален регистър на българските лични документи“ (НАИФ НРБЛД) е информационен фонд на МВР представлява един от регистри с лични данни. Фондът е гръбнакът на всички информационни системи, експлоатирани в МВР и данните от него се използват с цел осигуряване основните дейности на министерството, а именно: оперативно-издирвателна; охранителна; разследване на престъпления; информационна; контролна; превантивна; административнонаказателна и предоставяне на административни услуги.

Първичен администратор на данните от НАИФ НРБЛД, в който за пръв път се въвеждат данни за лична карта и паспорт на български граждани, Единен регистър на чужденци, в който първично се въвеждат данни за български лични документи на чужденци и Регистър на водачите на моторни превозни средства, в който първично се въвеждат данни за свидетелствата за управлението им, е министърът на вътрешните работи. Отговорности по първично събиране и въвеждане на данни в посочените регистри имат различни структури на министерството, като дирекция „Български докумен-

[8] Обн. ДВ, бр. 59 от 21 юли 2006 г., в сила от 01.01.2007 г., посл. изм. и доп. ДВ, бр. 51 от 1 юли 2022 г.

[9] Обн. ДВ, бр. 1 от 4 януари 2002 г., в сила от 01.01.2002 г., посл. изм. и доп. ДВ, бр. 11 от 2 февруари 2023 г.

ти за самоличност“, дирекция „Миграция“, Главна дирекция „Национална полиция“ и областните дирекции на министерството.

Поради спецификата на своят характер НАИФ НРБЛД не е публичен регистър и данните от него с изключение на пръстовите отпечатъци се предоставят на държавни органи и организации съобразно законоустановените им правомощия, както и на лица, на които е възложено със закон да изпълняват държавни функции; граждани, притежаващи български лични документи, само ако данните не засягат трети лица; юридически лица на основата на закон или с акт на съдебната власт (арг. чл. 70 Закона за българските лични документи).[10]

I. Проверка на идентификацията като мярка срещу изпирането на пари

Материята, свързана с определянето на мерки срещу изпирането на пари, организацията и контрола по тяхното изпълнение е правно уредена в ЗМИП и правилника за неговото прилагане. **Целта, която се преследва с посочената правна уредба е чрез установяване на комплекс от мерки да се постигне предотвратяване на изпирането на пари, респективно повишаване на степента на неговата разкриваемост.**

Мерките за превенция на използването на финансовата система за целите на изпирането на пари са регламентирани в чл. 3 от ЗМИП, като една от основните от тях е комплексната проверка на клиентите. Комплексната проверка на клиентите включва изчерпателно посочени дейности, включително идентифициране на клиенти и проверка на тяхната идентификация въз основа на документи, данни или информация, получени от надеждни и независими източници. Мерките срещу изпирането на пари намират приложение по отношение на посочените в чл. 4 ЗМИП правни субекти, дори когато последните са обявени в несъстоятелност и в ликвидация.

През призмата на засегнатата нормативна уредба е важно да се отговори на въпроса дали предоставянето на данни от НАИФ НРБЛД е допустимо въз основа на посочените по-горе разпоредби в качеството на независим източник по смисъла на чл. 10, т. 1 ЗМИП и външна база от данни съгласно чл. 42 ЗМИП. Ако това е така, е интересно да се уточни дали е налице легитимен интерес на попадащите под регулацията на ЗМИП субекти да достъпват данни от посочения информационен фонд. Последното предполага изследване на въпроса за наличието на пропорционалност между

[10] Обн. ДВ, бр. 93 от 11 август 1998 г., в сила от 01.04.1999 г., посл. изм. и доп. ДВ, бр. 8 от 25 януари 2023 г.

необходимостта от обработването на лични данни и преследваните цели, поради което е наложително да се направи оценка по следните показатели:

- **Специфика на преследваната цел и наличие на легитимен интерес на администратора да обработва лични данни.**
- **Необходимост от обработване на конкретни лични данни за постигането на преследваната цел** – обективно изследване на въпроса дали е възможно целта да бъде постигната, без да се обработват лични данни, респективно да се обработват данни в по-малък обем.
- **Наличие на пропорционалност между степента на намеса в личната сфера на субекта на данни и важността на идентифицирания легитимен интерес на администратора.**

II. Съотношение между преследвана цел и наличие на легитимен интерес при използване на лични данни

Измамата със самоличност е в основата на редица престъпления, вариращи от организирана престъпност до тероризъм, чието разпространение притежава потенциал да породи сериозни опасения за сигурността и безопасността в световен мащаб. Националните власти непрекъснато надграждат своите системи за проверка на документите за самоличност и пътуване, с цел подобряване сигурността. От друга страна е налице закономерност, при която с повишаването на степента на защита на документите за самоличност и пътуване, се повишава делът на опитите за неправомерно използваните истински документи.

Въз основа на натрупаната през годините практика може да се констатира, че една от основните групи престъпления, свързани с документи за самоличност, е използване на истински документ, издаден на друго лице. С цел превенция на този род престъпления и предотвратяване на злоупотреби при идентификация на лица на редица административните органи, организации, осъществяващи публични функции, и лица, предоставящи обществени услуги, е предоставен достъп до част от данните за издадени документи за самоличност.

Изпирането на пари, финансирането на тероризма и организираната престъпност често се извършват в международен план и са проблеми, по които следва да се работи както на национално равнище, така и в рамките на Европейския съюз, респективно и в международен план. Потоците от пари с незаконен произход могат да навредят на целостта, стабилността и репутацията на финансовия сектор и да застрашат вътрешния пазар на Съюза и международното развитие. С приетия през 2018 г. изцяло нов ЗМИП

в българското законодателство бяха въведени изискванията на Директива (ЕС) 2015/849 на Европейския парламент и на Съвета от 20 май 2015 година за предотвратяване използването на финансовата система за целите на изпирането на пари и финансирането на тероризма, Международните стандарти за превенцията на изпирането на пари и финансирането на тероризма (Препоръките на FATF), Конвенцията на Съвета на Европа относно изпиране, издирване, изземване и конфискация на облагите от престъпления и финансиране на тероризма (CETS 198), подписана във Варшава на 16 май 2005 г.[11], както и на резолюции на Съвета за сигурност на Организацията на обединените нации за превенция на тероризма и финансирането му.

Основните цели, които се преследват с прилагане на уредбата на ЗМИП са:

- превенция на изпирането на пари и финансирането на тероризма чрез ефективно използване на ресурсите, включително с отчитане на конкретни рискове по отношение на отделните сектори на финансовата система и икономиката, отделни услуги, продукти и клиенти, на национално и наднационално ниво;
- увеличаване на капацитета на компетентните национални институции да събират, анализират и обменят информация свързана с потенциални случаи на изпиране на пари и финансиране на тероризма, включително и международен обмен;
- повишаване на прозрачността и отчетността на юридическите лица и другите правни образувания, които са регистрирани на територията на страната или управляващи имущество в страната и не на последно място – повишаване на капацитета за противодействие на финансиране на тероризма.

В закона е определен кръгът задължени лица в съответствие с правото на Европейския съюз, което изисква от държавите членки да гарантират, че мерките се прилагат от всички субекти, ангажирани с дейности, за които е особено вероятно да бъдат използвани за целите на изпирането на пари или финансирането на тероризма.

Всяко лице, което попада в регулацията на ЗМИП, е длъжно да разработва ефективни вътрешни системи, които да му позволят да установи идентификацията на потенциален клиент, съществуващ клиент или действителен собственик на клиент юридическо лице или друго правно образу-

[11] Ратифицирана със закон, ДВ, бр. 103 от 2012 г., обн. ДВ, бр. 51 от 2013 г., в сила от 1.06.2013 г.

вание. Тези вътрешни системи могат да се основават на един или повече от следните източници на информация:

- информация, получена чрез прилагане на мерките за разширена комплексна проверка;
- писмена декларация, изискана от клиента, с цел установяване дали лицето попада в някоя от категориите по чл. 36 ЗМИП;
- информация, получена чрез използването на вътрешни или външни бази от данни.

Предвид изложеното е извън всякакво съмнение огромното значение на преследваната цел, а именно осигуряването на превенция на използването на финансовата система за целите на изпирането на пари. Налице е легитимен интерес на всички задължение лица по ЗМИП да осъществяват ефективна идентификация на своите клиенти, като насрещната проверка на всички събрани идентификационни данни е част от нея.

Както вече беше споменато, НАИФ НРБЛД е създаден на основата на автоматизираните информационни фондове за издаване, ползване и съхраняване на българските лични документи.[12] Ето защо в този регистър се съдържа най-актуална информация, която може да бъде използвана за насрещна проверка на валидността и редовността на представените документи за самоличност. В процедурата по издаване на български лични документи лицата са информирани за необходимостта по предоставяне на съответен набор от лични данни и целта на тяхната обработка, но не и за използването им като мярка за препятстване изпирането на пари. В същото време в Общия регламент относно защитата на данните е предвидено, че обработването на лични данни за цели, различни от тези, за които първоначално са събрани личните данни, следва да бъде разрешено единствено когато обработването е съвместимо с целите, за които първоначално са събрани личните данни. В такъв случай не се изисква отделно правно основание, различно от това, с което е било разрешено събирането на личните данни.

Ако обработването е необходимо за изпълнението на задача от обществен или легитимен интерес, респективно е свързано с упражняването на официални правомощия, които са предоставени на администратора на лични данни по силата на действащото право, могат да бъдат определени и уточнени задачите и целите, за които по-нататъшното обработване следва да се счита за съвместимо и законосъобразно.

[12] Съгл. чл. 1, ал. 5 от ЗБЛД българските лични документи включват документите за самоличност; свидетелството за управление на моторно превозно средство и документите за пребиваване.

III. Необходимост от обработване на лични данни за постигането на противодействие на изпирането на пари

Съгласно действащата нормативна регламентация идентифицирането на клиентите на задължените субекти по чл. 4 от ЗМИП следва да се извършва чрез представяне на официален документ за самоличност и снемане на копие от него, като при идентифицирането на физически лица се събират данни за: имената;

- датата и мястото на раждане;
- официален личен идентификационен номер или друг уникален елемент за установяване на самоличността, съдържащ се в официален документ за самоличност, чийто срок на валидност не е изтекъл и на който има снимка на клиента и др.[13]

Проверката на идентификацията се извършва **чрез използване на документи, данни или информация от надежден и независим източник** (арг. чл. 52 от ЗМИП). На нормативно равнище е уредено извършването на проверка на вече събрани идентификационни данни чрез използването на съответни способи за това, а един от тях е извършване на справки в електронни страници и бази от данни на местни и чуждестранни компетентни държавни и други органи, предоставени за публично ползване за целите на проверката на валидността на документи за самоличност и на други лични документи или на проверката на други данни, събрани при идентификацията.

Видно е, че посочената правна рамка е твърде обща и е предпоставка за твърде широко тълкуване. Наред с това е необходимо да се отбележи, че при определяне на методите за проверка на идентификация следва да бъдат съблюдавани изискванията на действащите правни актове в областта на защитата на личните данни в Република България, в Европейския съюз и в международното право.

С известна категоричност може да се заключи, че когато се извършва проверка на вече събрани данни при идентифицирането на физически лица, не бива да се събират данни извън определените в чл. 53, ал. 2 ЗМИП, а именно имената; датата и мястото на раждане; официален личен идентификационен номер или друг уникален елемент за установяване на самоличността, съдържащ се в официален документ за самоличност; гражданство; държава на постоянно пребиваване и адрес.

Вече беше посочено, че НАИФ НРБЛД не представлява база от данни на държавен орган, предоставена за публично ползване, т.е. **не е налице основание за ползване на лични данни на основание чл. 55, ал. 1, т. 3 от**

[13] Вж. чл. 53, ал. 2 ЗМИП.

ЗМИП, а именно когато проверката на събраните идентификационни данни се извършва чрез извършване на справки в електронни страници и бази от данни на местни и чуждестранни компетентни държавни и други органи, предоставени за публично ползване за целите на проверката на валидността на документи за самоличност.

В съдебната практика се приема, че непублични регистри с лични данни могат да се приемат за надежден и независим източник по смисъла на чл. 52 ЗМИП, а информацията от тях представлява външна база по чл. 42, ал. 2, т. 3 от ЗМИП. Налага се изводът, че тези непублични регистри могат да осигурят възможността задължените по чл. 4 ЗМИП лица да изпълнят законовото си задължение за комплексна проверка на своите клиенти, респ. идентифицирането им.[14]

IV. Наличие на пропорционалност между степента на намеса в личната сфера на субекта на данни и значението на легитимния интерес на администратора

Защитата на личните данни на етапа на проектирането е ново задължение за администраторите на лични данни, въведено за първи път с Общия регламент относно защитата на данните и се изразява в задължението им да въведат подходящи технически и организационни мерки преди започването на обработката на лични данни (на етапа определяне на целите и средствата за обработване), като осигурят тяхното прилагане през целия жизнен цикъл на данните. Това задължение е особено важно в контекста на новите технологии и предоставянето на услуги на информационното общество.

Защита на личните данни по подразбиране изисква администраторите да прилагат механизми, които гарантират изпълнението на следните изисквания:

- биват обработвани само минималното количество лични данни и операции по обработване, които са абсолютно необходими за постигането на всяка специфична цел;

[14] Вж. Решение № 1091 от 22.02.2022 г. по адм. д. № 1549/2021 г. на Административен съд – София-град. В посоченото решение се приема, че независим източник по чл. 52 ЗМИП и външна база данни по чл. 42, ал. 2 т. 3 от ЗМИП е Национална база данни „Население“ и Класификатор на постоянни и настоящи адреси, като справките от посочените регистри дават възможност да се установят случаи на предоставени неверни, фалшифицирани данни или използване на документи за самоличност на клиенти и свързаните с тях лица.

- данните са съхранявани за минималния срок, абсолютно необходим за постигане на целите на обработване и след това заличени при спазване на съответните правила и процедури;
- всеки достъп, предаване или споделяне на данни е допустим само при наличие на валидно правно основание за това (например съгласието на субекта на данни, правни задължения на администратора и т.н.).

Когато се касае за обработване на биометрични данни (в НАИФ НРБЛД такива са изображението на лицето на гражданина и пръстовите му отпечатъци), би следвало да бъде отчетено, че съгласно ЗЗЛД това е разрешено с цел уникално идентифициране на физическото лице само когато: това е абсолютно необходимо; съществуват подходящи гаранции за правата и свободите на субекта на данни; предвидено е в правото на Европейския съюз или в законодателството на Република България.

Предоставянето от НАИФ НРБЛД на биометрични данни под формата на снимково изображение на притежателя на съответния документ за самоличност ще допринесе за препятстване измамите, свързани с използване на чужд документ. Същевременно снимката не е предвидена в обхвата от данни, които се събират при идентифицирането на физически лица по реда на чл. 53, ал. 2 ЗМИП и се проверяват съгласно чл. 55 ЗМИП. Снимките, когато се обработват чрез специални технически средства, позволяващи уникална идентификация или удостоверяване на автентичността на дадено физическо лице, са включени в специалните категории лични данни в Общия регламент за защита на лични данни. Като такива те се приемат като особено чувствителни от гледна точка на основните права и свободи, поради което за тях се полага специална защита, тъй като контекстът на тяхното обработване би могъл да създаде значителни рискове за основните права и свободи.[15]

Следователно има основание да се смята, че предоставяне на биометрични данни от НАИФ НРЛД под формата на изображение на лицето по реда на чл. 52 ЗМИП е непропорционално на преследваната цел. Този извод не може да бъде разколебан и от обстоятелството, че справките от НАИФ НРБЛД действително дават възможност да се установят случаи на предоставени неверни, фалшифицирани данни или използване на чужди идентификационни данни (документи за самоличност) на лицето, като по

[15] Вж. съображение 51 на 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.

този начин ще се допринесе за изработване на ефективна вътрешна система за изпълнение изискванията по чл. 41, ал. 3, т. 1 и 2 от ППЗМИП.[16]

Администраторът, респ. обработващият личните данни, следва да документира решението си за позоваване на легитимен интерес при обработване на личните данни, демонстрирайки съответствие с Регламент (ЕС) 2016/679 и стриктно да спазва т.нар. „принцип на отчетност". В изпълнение на този принцип администраторът трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни, вкл. поддържане на регистър на дейностите по обработване на лични данни, приемане на вътрешна инструкция/правила/процедури/политика за защита на личните данни, актуализиране на формите за документиране на съгласие, актуализиране на договореностите с обработващите лични данни и др. Наред с това субектите на данни следва да са информирани в детайли относно позоваването на относимото правно основание.

Оценката на въздействието е важен инструмент за отчетност, чрез който да се идентифицира спазването на изискванията на Общия регламент за защита на лични данни и се изразява в задължение за администратора на данни да опише обработването на лични данни; да оцени необходимостта и пропорционалността на обработката; да спомогне за избора на най-подходящите технически и организационни мерки за защита и т.н.

В чл. 16 ЗМИП е регламентирано задължените по закона лица да поддържат актуална събраната чрез прилагането на мерките за комплексна проверка информация за своите клиенти и за извършваните от тях операции и сделки, като периодично преглеждат и актуализират при необходимост поддържаните бази от данни и клиентски досиета. Във връзка с това задължение за поддържане на актуални данни нееднократно в МВР са правени запитвания за осигуряване на възможността за автоматизирано актуализиране на лични данни на стотици хиляди граждани, получени от НАИФ НРБЛД, които са използвани за насрещна проверка на идентификационни данни по реда на ЗМИП. Считам допускането на подобна актуализация за незаконосъобразно, тъй като данните от НАИФ НРБЛД са получени единствено за процедурата по проверка на идентификация на съответния клиент. С осъществяване на тази проверка се изчерпва възможността и правното основание за достъп на данни до посочения информационен фонд.

В допълнение е редно да се посочи, че с Общия регламент за защита на лични данни е възприет подходът за изследване на риск за правата и свободите на физическите лица при обработване на лични данни. В този

[16] Приет с ПМС № 357 от 31.12.2018 г., обн. ДВ, бр. 3 от 8 януари 2019 г., посл, изм. и доп. ДВ, бр. 21 от 13 март 2020 г.

смисъл се приема, че операции по обработване, които по правило пораждат висок риск, са например извършването на автоматично вземане на решения или мащабно обработване на данни.

Заключение

Електронното управление е основната платформа за цифрова трансформация на публичните институции, за повишаване на качеството на административните услуги, за преминаването към рационални електронни процеси на функциониране и управление в публичния сектор и за достъп по електронен път на информацията, с която разполагат публичните институции. То е средство за всеобхватно повишаване ефективността на процесите в администрацията и за облекчаване взаимодействието между администрацията, гражданите и бизнеса.[17] В този непрекъснат процес и всички предприети и предстоящи инициативи в областта на е-управлението обаче следва да съблюдават следните основни принципи, а именно принципът за неприкосновеност на личността и личния живот по подразбиране, съгласно който всички инициативи следва да се основават на правната рамка за защита на личните данни и неприкосновеността на личния живот още на етапа на проектиране на е-услуги.

Действително на национално и международно ниво се генерира все по-нарастващо количество данни и начините и моделите, по които те се събират, съхраняват, управляват, използват и гарантират, трябва да се поставят на първо място в процеса на цифрова трансформация. За практическата необходимост на хора, организации, общество, медии и държава ежедневно да обработват, съхраняват, използват и предоставят лични данни следва да се отчита действието на действащото национално и европейско законодателство.

Както беше посочено, превенцията срещу изпирането на пари е основната цел, към която е насочена възможността за предоставяне на лични данни от НАИФ НРБЛД на държавни органи и организации, предоставящи обществени услуги за проверка на идентификацията на техните клиенти по ЗМИП. Тази проверка може да бъде реализирана чрез използването на лични данни, които са събрани в процедурата по издаване на съответните документи за самоличност. Същевременно има сериозни основания да се смята, че предоставянето на лицата, задължени по ЗМИП, на пълния обем от

[17] Актуализирана Стратегия за развитие на електронното управление в Република България 2019 – 2025 г., приета с Решение № 298 на Министерския съвет от 02.04.2021 г.

лични данни (включително лицеви изображения), с които разполага НАИФ НРБЛД, би надхвърлило пропорционалността.

Нещо повече, в електронния сайт на МВР е разработена функционалността „Справка за български лични документи“, която позволява при въвеждане на конкретни данни за документ (тип документ, номер на документа, дата на раждане на притежателят му) да се установи в реално време неговият статус на валидност. Чрез посоченото средство би било възможно извършването на насрещна проверка на представения документ за самоличност от клиента по време на неговата идентификация пред съответната кредитна институция.

Макар на пръв поглед да се констатира противопоставяне между регулацията за защита на личните данни и дейностите, които следва да обезпечат електронно управление, това съвсем не е така. Свеждането на обема на обработваните лични данни до минимум, ограниченията, свързани с тяхното съхранение и правилата за отчетност са принципни изисквания, които да допринесат за ефективното изпълнение на нормативно регламентираните цели на задължените по ЗМИП субекти. Ето защо в настоящия доклад са представени аргументи в подкрепа на тезата, че нормативните изисквания за защита на лични данни са насочени към уреждане на необходимата среда, в която да се развият процесите на електронно управление. В този смисъл режимът за защитата на личните данни не трябва да се схваща като препятствие, а едно от средствата за изграждане на електронно управление, основано на защита на личната неприкосновеност и интегритет.

Библиография:

1. Актуализирана Пътна карта за изпълнение на Актуализирана стратегия за развитие на електронното управление в Република България 2019–2023 г., приета с Решение № 546 от 18.09.2019 г.
2. Актуализирана Стратегия за развитие на електронното управление в Република България 2019 – 2025 г., приета с Решение № 298 на Министерския съвет от 02.04.2021 г.
3. Концепция за регистрова реформа, приета с Решение № 546 на Министерския съвет от 18.08.2019 г.
4. Хубенова, М. (2016). Вътрешни електронни административни услуги – актуална уредба и предлагани изменения. – Норма, № 1, 1–10.

Правни проблеми при обучението на модели на генеративен изкуствен интелект със защитено от авторско право съдържание

Ана Лазарова*

Използването на системи за изкуствен интелект (ИИ), които генерират различни форми на художествено съдържание, повдига редица актуални въпроси в сферата на прилагането на авторското право и сродните му права. Тези въпроси и проблеми могат да бъдат групирани в две основни направления, които обхващат съответно правния статус и режима на използване, от една страна, на материалите, върху които т.нар. голям базов модел се обучава (проблеми „на входа“), и от друга – на материалите, които ИИ системата генерира (проблеми „на изхода“). Докато проблемите „на изхода“ са по-познати на широката общественост и въпросът за авторството на ИИ генерирано съдържание ангажира активна дискусия със силен етичен оттенък, настоящият доклад се фокусира върху проблемите „на входа“ – свързани с използването на съдържание за целите на обучението на съответния модел в основата на генеративния ИИ. За да се обучат тези големи базови модели, те трябва да обработят огромни количества съдържание, от което да извлекат определени зависимости и информация. Технологията по обработка на съдържанието обикновено включва дейности, които са част от правомощията на носителите на авторско и сродните му права, като възпроизвеждане и преработка. Настоящият доклад изследва степента, в която използването на технологии, асоциирани с ИИ системите, като извличане на информация от текст и от данни и машинното самообучение, засягат правата върху защитено съдържание и възможностите, която наличната правна уредба дава за законосъобразното им използване както в световен, така и в регионален, на ниво ЕС, и в национален аспект.

Ключови думи: *авторско право, генеративен ИИ, голям базов модел, извличане на информация от текст и данни, изключения и ограничения от авторското право, изкуствен интелект, машинно самообучение*

* Ана Лазарова е адвокат, преподавател в катедра Европеистика на Софийски университет „Св. Климент Охридски“ и председател на сдружение Цифрова република, ел. поща: ana@digrep.bg

Legal implications of training generative AI models on copyrighted content

Ana Lazarova*

The use of artificial intelligence (AI) systems generating creative content in various forms raises a number of issues in the field of copyright and related rights. These questions and problems can be grouped into two main categories, which cover the legal status and the regime of use of, on the one hand, the materials on which the so-called large foundation model is trained (input) and, on the other hand, the materials that the AI system produces (output). While the 'output' issues are more familiar to the general public and the question of authorship over AI generated content in subject to an active discussion with strong ethical implications, this report shall focus on the 'input' issues, related to the use of copyrighted content for the purpose of training the model underlying generative AI. In order for these large foundation models to be trained, massive amounts of data and content must be processed for certain patterns and information to be extracted. The text or data mining technology usually implies activities that are part of the domain of copyright and related rights holders, such as acts of reproduction and adaptation. The report studies the extent to which the use of technologies associated with AI systems, such as text and data mining and machine learning, affects the rights over protected content, as well as the opportunities that the existing legal framework globally, at the regional (EU) level, as well as nationally, provides for said content's lawful use.

Keywords: *artificial intelligence, copyright, exceptions and limitations, generative AI, large foundation models, machine learning, text and data mining*

* Ana Lazarova is an attorney at law, lecturer at the Department of European Studies at Sofia University „St. Kliment Ohridski" and chair of Digital Republic association, e-mail: ana@digrep.bg

В последните няколко години развитието на системите с изкуствен интелект (ИИ) е една от основните теми в сферата на цифровите политики. Подготовката на хоризонтално законодателство, което да регулира ИИ системите на ниво Европейски съюз[1], както и предоставянето на достъп на широката публика до ChatGPT през ноември 2022 г.[2], накараха всички да заговорят за предстоящите регулации в сферата на ИИ, както и за етичните проблеми, придружаващи неизбежното навлизане на този тип технологии във всички сфери на обществения живот.

В този контекст някои анализатори твърдят[3], че преобладаващият дискурс относно бъдещите етични и регулаторни предизвикателства при използването на ИИ целенасочено измества фокуса на обществеността от актуалните правни проблеми при създаването и функционирането на тези системи.

Всъщност използването на ИИ системи и на технологиите, асоциирани с изкуствения интелект, има напълно осезаем регулаторен аспект дори с оглед на съществуващото към настоящия момент законодателство на международно, регионално – в Европейския съюз – и национално ниво. В частност т.нар. „базови модели“ се обучават върху данни, чиято автоматизирана обработка е предмет на разнообразно секторно законодателство. Така например данните, от които моделът извлича зависимости и информация, биха могли да бъдат лични данни. В такъв случай тяхната обработка би се подчинила на актуалното законодателство за защита на личните данни, съответно на ниво ЕС би се приложил Общият регламент относно защитата на данните (ОРЗД)[4]. Нерядко ИИ системи използват и чувствителни лични данни, чиято обработка е обект на още по-стриктен режим[5].

[1] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts [8115/21 – COM(2021) 206 final]

[2] https://openai.com/blog/chatgpt.

[3] Вж. напр. Chowdhury, R. (2023). Generative AI: Hype, Harms, and the Responsible Tech Community (video). Available at: https://www.linkedin.com/events/7048711724547354624/comments/.

[4] В края на м. март 2023 г. италианският орган за защита на личните данни – *Garante per la protezione dei dati personali*, наложи на OpenAI временна забрана да обработва лични данни, в резултат на което компанията геоблокира ChatGPT за Италия. Вж. GPDP (2023) Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori. Available at: https://www.garanteprivacy.it/home/autorita/collegio. Вж. още Kristi Hines, Exploring Italy's ChatGPT Ban And Its Potential Impact. Available at: https://www.searchenginejournal.com/chatgpt-ban-italy/484157/.

[5] Така напр. в края на 2022 г. TikTok уреди извънсъдебно заведен срещу компанията

Разбира се, творческите материали, базите данни, софтуерът и т.н., върху които се обучава ИИ, могат да бъдат и обект на авторско и сродни права. В такъв случай неоторизираното им използване от съответния базов модел би могло да представлява нарушение на тези права.

Взаимовръзката между машинното самообучение (*machine learning*), съответно – обучението на базови модели на генеративен ИИ, от една страна, и авторското право, от друга, не винаги е самоочевидна. Обичайната житейска нагласа е, че след като субектът има достъп до определено съдържание и може да го прочете физически, то би следвало да има право и да го „прочете“ и машинно. Тази логика обаче е недостатъчна в контекста на основните концепции за авторскоправна защита, и особено с оглед крайно формализираната уредба в Европейския съюз, където не е налице гъвкаво изключение за допустимо използване от типа на *fair use* доктрината. Прилагайки формалните изисквания на авторскоправната закрила, определени действия, включени в процеса по извличане на информация от текст или от данни, биха могли да представляват действия на използване на чужди произведения или други обекти, напр. неоригинални бази данни. Съответно за всички тези действия е необходимо разрешението на автора или, в зависимост от случая, друг правоносител, и ако такова не е налице, е възможно да има правонарушение.

1. Извличане на информация от текст и данни

1.1. Същност на технологичния процес и легална дефиниция

За целите на преценката до каква степен обучението на т.нар. „базови модели“ в основата на генеративния ИИ може да бъде предмет на авторскоправната уредба, следва да уточним каква е използваната за тази цел технология, и дали – и ако да, то как използването на тази технология би могло да засегне правомощията на правоносителя, предвидени в закона.

Изследователската техника за събиране на информация и извличане на зависимости от големи количества цифрови данни чрез автоматизирани софтуерни инструменти се нарича „извличане на информация от текст и данни“ (на англ.: *text and data mining* или *TDM*). Технологията се определя

колективен иск в щата Илинойс заради незаконна обработка на биометрични данни на нейните потребители. Според медиите TikTok е платила обезщетение в размер на 92 млн. долара. Вж. NBC 5 (2022) Judge Approves $92 Million TikTok Settlement, With Illinois Claimants Receiving Biggest Share. Available at: https://www.nbcchicago.com/news/local/judge-approves-92-million-tiktok-settlement-with-illinois-claimants-receiving-biggest-share/2921881/.

още като „процес на използване на компютри и автоматизация за претърсване на големи набори от данни с цел установяване на зависимости/модели и тенденции“[6]. Тя обхваща следните последователни операции: (i) идентифициране на входни материали, които трябва да бъдат анализирани, напр. произведения или данни, индивидуално събрани или организирани в съществуваща база данни; (ii) копиране на значителни количества материали – което включва: (ii.a) предварителна обработка на материалите чрез превръщането им в машинно четим формат, съвместим с технологията, така че структурираните данни да бъдат извлечени и (ii.b) евентуално, но не задължително, качване на предварително обработените материали на платформа в зависимост от техниката на извличане, която ще се използва; (iii) извличане на данните и (iv) рекомбинирането на данните за идентифициране на модели в крайния резултат[7].

На практика има разлика между извличане на информация от данни (*data mining*), което е изчислителният процес на откриване и извличане на знания от структурирани данни, и извличане на информация от текст (*text mining*) – изчислителният процес на откриване и извличане на знания от неструктурирани данни. Във втория случай обикновено се има предвид информация, създадена от човек на естествен език, в машинно нечетим формат. Текстови данни могат да бъдат създавани и от софтуерни програми.

Извличането на информация от текст и данни е в основата на методи за анализ на данни като скрейпинг на данни (*data scraping*), машинно самообучение (*machine learning)* и машинен анализ на изображения (*computer vision*)[8]. Съответно това е технологията, по която базовият модел в основата на генеративния ИИ се „обучава“, за да може след това да възпроизведе извлечените зависимости в новосъздадено съдържание.

През 2019 г. в Европейския съюз, като част от Стратегия за цифров единен пазар за Европа, бе приета Директивата относно авторското право в цифровия единен пазар[9], която въведе легална дефиниция на понятието

[6] Rutgers Bootcamps. (2022). What Is Data Mining? A Beginner’s Guide. Available at: https://bootcamp.rutgers.edu/blog/what-is-data-mining/.

[7] Geiger, C., Frosio, G., & Bulayenko, O. (2019). Text and data mining: Articles 3 and 4 of the directive 2019/790/EU. Propiedad intelectual y mercado único digital europeo, Valencia, Tirant lo blanch, 27–71.

[8] За подробно изследване на уредбата, засягаща тези процеси, вж. Kretschmer, M., Margoni, T., & Oruc, P. (2021). D3.6 Interim study on the state of harmonisation of the rights of reproduction and adaptation and connected exceptions. Zenodo. Available at: https://doi.org/10.5281/zenodo.5069507.

[9] Директива (ЕС) 2019/790 на Европейския парламент и на Съвета от 17 април 2019 година

извличане на информация от текст и данни. Това е „автоматизиран аналитичен способ, чиято цел е да анализира текст и данни в цифрова форма, за да се създаде информация, включваща, но без да се ограничава до това – модели, тенденции и взаимовръзки“[10]. Съгласно Съображение 8 от директивата, „извличането“ е технология, която позволява обработването на големи обеми информация с оглед придобиване на нови знания и разкриване на нови тенденции“.

Терминът, който проектът за Законът за изменение и допълнение на българския Закон за авторското право и сродните му права (ЗАПСП)[11] използва за означаване на технологията, е *автоматизиран анализ на текст и информация*. Новото понятие е дефинирано в нова т. 3а от § 2 от Допълнителните разпоредби на ЗАПСП, както следва: „автоматизиран анализ на текст и информация“ е който и да е автоматизиран аналитичен способ, използван за анализ на текст и данни в цифрова форма, за създаването на модели, тенденции, взаимовръзки и друга информация“.

1.2. Приложение

Дали при извличането рискуваме потенциално авторскоправно нарушение зависи от конкретния метод на анализ и използваните инструменти. В някои случаи технологията не ангажира действия в правомощията на автора и съответно не може да представлява нарушение. Такъв е случаят, когато извличането използва инструменти, предвиждащи минимално копиране на няколко думи или т.нар. обхождане (*crawling*) на данни и обработка на отделни „парчета“ информация[12].

В повечето случаи обаче при обработката на големите масиви от данни за целите на извличане на зависимости и информация от тях биха се осъществили действия по временно или трайно *възпроизвеждане* – вид използване на данни и съдържание, което, когато тези данни и съдържание са защитени с авторски или сродни права – е част от имуществените правомощия на правоносителя. Правото на възпроизвеждане е хармонизирано

относно авторското право и сродните му права в цифровия единен пазар и за изменение на директиви 96/9/ЕО и 2001/29/ЕО (PE/51/2019/REV/1, OJ L 130, 92–125).

[10] Вж. чл. 2 параграф 2 от Директива ЕС/2019/790.

[11] Закон за изменение и допълнение на Закона за авторското право и сродните му права (ЗИД на ЗАПСП) с цел транспонирането на Директива 2019/789 и Директива 2019/790 в българското законодателство (внесен в 49 НС със сигнатура 49-302-01-21).

[12] Според някои автори възпроизвеждането в контекста на автоматизирания анализ поначало не засяга правомощията на правоносителите, т.е. изобщо не е налице използване по смисъла на авторското право. Вж. напр. Carroll, M. (2019). Copyright and the Progress of Science: Why Text and Data Mining Is Lawful’. UC Davis Law Review 53: 89.

на ниво ЕС, като член 2 от Директива 2001/29/ЕО[13] го дефинира като „изключителното право [на правоносителите] да разрешават или забраняват пряко или непряко, временно или постоянно възпроизвеждане по какъвто и да е начин и под каквато и да е форма, изцяло или частично“. Правото се предоставя за авторите – върху техните произведения, за артистите изпълнители – върху фиксирането на изпълненията им, за продуценти на звукозаписи – върху техните звукозаписи, за продуцентите – върху първото фиксиране на филм, и за радио– и телевизионните организации – за фиксирането на техните излъчвания, независимо дали са предавани по жичен път или по въздуха, чрез кабел или спътник. С член 15 от Директива 2019/790 правото на възпроизвеждане бе предоставено и на нова група носители на сродни права – издателите на публикации в пресата.

Българският закон урежда правото на възпроизвеждане като част от имуществените правомощия на автора в чл. 18, ал. 2, т. 1 от ЗАПСП, съгласно който „възпроизвеждането на произведението“ е вид използване. Легалната дефиниция за възпроизвеждане се съдържа в § 2, т. 3 от Допълнителните разпоредби на ЗАПСП, и го определя като „прякото или непрякото размножаване в един или повече екземпляри на произведението или на част от него, по какъвто и да е начин и под каквато и да е форма, постоянна или временна, включително запаметяването му под цифрова форма в електронен носител“. Към настоящия момент в теорията и практиката е безспорно, че цифровизирането на съдържание представлява действие по възпроизвеждане. Като възпроизвеждане се квалифицира и създаването на временни (ефимерни) копия.

В някои случаи процесът по автоматизиран анализ може да ангажира и други правомощия на автора – например преработка. Така напр. предварителната обработка на масивите от данни за целите на извличането може да включва преформатиране на данни, премахване на данни, които не са релевантни за анализа, и в този смисъл да засегне и правото за създаване на адаптации и преработки на оригиналния правоносител. В случая е важно да се подчертае, че в процеса на обучение на базовите модели и генериране на съдържание от ИИ, *изходните данни не са резултат от директна преработка на входните данни по смисъла на авторското право*[14]. Алгоритъмът

[13] Директива 2001/29/ЕО на Европейския парламент и на Съвета от 22 май 2001 година относно хармонизирането на някои аспекти на авторското право и сродните му права в информационното общество (OJ L 167, 22.6.2001, 10–19).

[14] Guadamuz, A. (2023). A Scanner Darkly: Copyright Infringement in Artificial Intelligence Inputs and Outputs. Available at SSRN 4371204, p. 7.

„чете“ съответните материали и „се обучава“, като извлича зависимости от тях, които зависимости после възпроизвежда в ново съдържание[15].

2. Генеративен ИИ и свободно използване на защитени произведения

Както е добре известно, авторскоправната закрила върху произведение възниква автоматично и без формалности върху всяко произведение на литературата, изкуството и науката, което е (i) обективирано и (ii) оригинално, в смисъл, че е „собствено интелектуално творение на неговия автор“[16], „отразява личността на автора“[17] и „авторът е успял да изрази своите творчески способности в производството на произведението, като е направил свободен и креативен избор“[18]. Доколкото обработката на данни с цел техния автоматизиран анализ в рамките на базовия модел включва действия по възпроизвеждане и преработка по смисъла на авторското право, то такова използване на входните данни, когато включват защитени произведения или други обекти на сродни права, следва да се основава или на разрешение от страна на правоносителя[19], или на основание изключения и ограничения от авторското право – случаи, в които законът разрешава използването на чуждо защитено произведение в обществен интерес и без разрешение от страна на правоносителя[20].

---

[15] Въпреки че едно от обвиненията към CoPilot на OpenAI е, че възпроизвежда големи „парчета“ съществуващ в платформата GitHub авторски код. Вж. Vaughan-Nichols, S. (2022). GitHub’s Copilot flies into its first open source copyright lawsuit. It won’t be the last. Available at: https://www.theregister.com/2022/11/11/githubs_copilot_opinion/.

[16] Вж. напр. Решение на Съда на ЕС по дело C-5/08, Infopaq International A/S срещу Danske Dagblades Forening [2009] ECLI:EU:C:2009:465, и Решение на Съда на ЕС по дело C-145/10, Eva-Maria Painer срещу Standard VerlagsGmbH и др. [2011], ECLI:EU:C:2011:798.

[17] Вж. член 6 и Съображение 16 от Директива 2006/116/ЕО на Европейския парламент и на Съвета от 12 декември 2006 година за срока за закрила на авторското право и някои сродни права (OJ L 372).

[18] Решение на Съда на ЕС по дело C-604/10, *Football Dataco Ltd и др. срещу Yahoo UK Ltd и др.,* ECLI:EU:C:2012:115.

[19] Такова разрешение може да се твърди, че е налице при използване на „отворено“ съдържание, като напр. произведения, публикувани под свободен лиценз.

[20] Т.нар. „изключения и/или ограничения от авторското и сродните му права“, още наречени „свободно използване“, „разрешени употреби“ и „ползвателски права“, са основният инструмент, който както на ниво ЕС, така и на национално ниво служи за прокарване на справедливо равновесие между насрещните интереси в горния контекст. Това са заложени в закона хипотези, в които при определени условия даден кръг бенефициери, а в някои случаи – всички граждани, имат право да използват защитени от авторско и сродни права произведения без съгласието на правоносителя, а в много

Когато говорим за свободно използване за целите на обучение на базовите модели на генеративния ИИ, следва да се държи сметка за това, че решенията, които различните юрисдикции предлагат в това отношение, не се основават на единен подход. Въпреки че усилията на международната общност по разработване и хармонизиране на наднационалното законодателство в сферата на авторското право до настоящия момент са довели до чувствително сближаване на англо-американската концепция за *copyright* и континенталната европейска доктрина за *droit d'auteur*, това, към което и до ден днешен двете системи запазват коренно различен подход, е логиката при уреждането на изключенията и ограниченията. Докато континенталното право предвижда затворен каталог с изключения, англо-американската традиция позволява отворена *fair use* система, която предоставя на съдилищата задачата по идентифициране на отделни случаи на законосъобразно неразрешено използване.

2.1. Справедлива употреба

Преобладаващата част от вече инициираните съдебни дела по повод неразрешено използване на защитени произведения за обучение на модели на генеративен ИИ са в компетентността на съдилищата в САЩ. Към юни 2023 г. срещу компании, разработили и експлоатиращи генеративен ИИ, са заведени два колективни и два индивидуални иска за нарушение на авторски права върху съдържанието, използвано за обучение на съответните модели. Един от предявените искове засяга използването на компютърни програми, съхранявани в хранилището за свободен софтуер GitHub, при тренирането от OpenAI на Codex и Copilot – две „асистиращи" системи, базирани на ИИ. Ищците по това дело твърдят, че ответниците OpenAI, Microsoft и GitHub са нарушили, на първо място, договорните условия по шест лицензa, под които в GitHub е публикуван отворен софтуер, и на второ място, са нарушили права на интелектуална собственост[21]. Останалите три дела са заведени

случаи – и без да дължат заплащане на възнаграждение. Класически изключения и ограничения от авторското право са цитатът, използването за илюстриране при обучение, свободното разпространение на новини, използването на закриляни творби за целите на карикатурата и пародията и пр. Изключението като механизъм определя граници на упражняването на авторското право като ограничава монопола на правоносителя и абсолютния му контрол върху съдбата на творбата в полза на обществения интерес.

[21] Doe 1 et al v. GitHub et al, Case No. 4:2022cv06823 (N.D. Cal.).

по повод използването на защитени изображения за обучение на моделите Stable Diffusion[22] и Midjourney[23].

Настоящият коментар не навлиза в проблематиката на използването на съдържание, публикувано под отворен лиценз, за целите на обучение на ИИ системи, във въпросите за спазването на съответните договорни условия, при които са публикувани данните „на входа“, нито в етичните проблеми, свързани с такова използване[24]. Следва да се има предвид, че за момента изглежда, че по нито едно от заведените дела ползвателите не са се ограничили до използването на съдържание, публикувано под отворен лиценз. Това е видно и от генерираното от базовите модели съдържание – от една страна, Copilot възпроизвежда означението „All rights reserved” в генерирания от ИИ системата код, а от друга – случва се Stable Diffusion да възпроизведе водния знак на Getty Images в генерираните от ИИ изображения[25]. Независимо от тези въпроси, част от защитата на ответниците по тези дела неминуемо ще включва възражение за законно използване на защитеното съдържание по силата на „справедлива“ неоторизирана употреба.

Доктрината за справедливата употреба (*fair use*) на САЩ е най-известният пример за отворена разпоредба, съдържаща гъвкави критерии за преценка кога една употреба на защитено произведение е разрешена от закона. Тази доктрина, отразена в раздел 107 от Закона за авторското право на САЩ, позволява на съдилищата да извършват анализ за всеки отделен случай, за да определят дали дадена употреба може да бъде изключени от контрола на правоносителя, включително използване за целите на цитиране, пародия и други преработки. В разпоредбата на раздел 107 от Закона за авторското право на САЩ американският законодател залага четири критерия за преценка на „справедливостта“ на неоторизираното използване[26]. От тези

[22] Вж. Getty Images v. Stability AI, Case No. 1:2023cv00135 (D. Del.); и Getty Images v Sability AI (England), Case IL-2023-000007.

[23] Andersen et al v. Stability AI et al, Case No. 3:23-cv-00201 (N.D. Cal.).

[24] И двата споменати по-горе колективни иска съдържат „обвинения“ към отворените платформи GitHub и DeviantArt за това, че са предали принципите и ценностите на отворената общност.

[25] Broz, M. (2023). Original research: More watermarks found in Stable Diffusion’s images. Available at: https://photutorial.com/stable-diffusion-watermarks-investigation/.

[26] Разпоредбата, разписваща *fair use* в Закона за авторското право на САЩ (17 U.S.C. § 107) задава следните четири критерия за преценка: (i) целта и характера на използването, включително дали това използване е с търговско естество или е за образователни цели и с нестопанска цел; (ii) естеството на защитеното произведение; (iii) количеството и значимостта на използваната част по отношение на защитеното произведение като цяло; и (iv) ефекта от използването върху потенциалния пазар или стойността на защитеното произведение. Фактът, че дадено произведение не е

четири критерия, два – първият и последният – се ползват със сравнително по-голяма тежест.

От една страна, американският съд консистентно търси да установи, че съответната употреба е „трансформираща“. Практиката по този въпрос се е развила до степен съдът в определени случаи да приравнява дори буквалното възпроизвеждане на „трансформиращо“ използване – когато копирането е „систематично и институционално“ с цел да „позволи изчислително изследване“[27] или когато копирането служи за „неекспресивни“ цели.[28] Последният критерий, „ефектът на използването, доколкото той може да се измери с пазарната си стойност“, гарантира неналичието на т.нар. „пазарно заместване“ (*market substitution*) във вреда на правоносителя. Според някои автори това пазарно заместване трябва да е „съществено“ (*substantial*)[29], т.е. неоторизираното използване следва да нанася „разпознаваема пазарна вреда“ (*cognizable market harm*), за да бъде квалифицирано като нарушение.

Макар почти сигурно обработката от базовия модел на съдържанието „на входа“ да представлява „трансформираща употреба“, основният проблем, с който системите на генеративен ИИ могат да се сблъскат при прилагате на *fair use* доктрината, е именно този последен критерий, доколкото генерираното „на изхода“ съдържание вероятно пряко се конкурира с продукцията на авторите, върху която моделът се обучава.

2.2. Европейският подход

За разлика от англосаксонския подход към разрешените употреби на защитено съдържание, континенталната правна традиция се характеризира с липса на гъвкавост на хипотези на свободно използване. ЕС регулира разрешените употреби съгласно строго формулирани изключения, които са (i) изчерпателно изброени и (ii) предоставят права на използване на ползвателите в ограничени хипотези. Неоторизираното използване извън тези хипотези представлява нарушение на авторското право или сродните му права, независимо от наличието или липса на съществени щети за правоносителя

публикувано, сам по себе си не възпрепятства констатацията за наличие на справедлива употреба.

[27] Вж. напр. *Kelly v. Arriba Soft Corp*., 336 F.3d 811, 822 (9th Cir. 2003); *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1169 (9th Cir. 2007); *A.V. ex rel. Vanderhye v. iParadigms*, LLC, 562 F.3d 630, 640 (4th Cir. 2009).

[28] *Authors Guild, Inc. v. Google, Inc*., 804 F.3d 202 (2d Cir. 2015).

[29] Sun, H. (2021). Creating a Public Interest Principle for the Adjudication of Fair Use and Fair Dealing Cases. The Cambridge Handbook of Copyright Limitations and Exceptions (Cambridge Law Handbooks, pp. 233–266). Cambridge: Cambridge University Press. doi:10.1017/9781108671101.019.

или от значението на обществения интерес, отразен в съответната употреба. В контекста на европейското *acquis* държавите членки нямат дискрецията да предвиждат хипотези на свободно използване извън случаите, уредени в правото на ЕС[30].

В този контекст законодателят на ЕС констатира, че е налице правна несигурност в европейски мащаб по отношение на използването на защитено съдържание за целите на машинното самообучение. Съгласно Съображение 8 на Директива (ЕС) 2019/790 „в Съюза […] организации и институции се сблъскват с правна несигурност относно степента, до която могат да извличат съдържание при извличането на информация от текст и данни. […] Когато не е предвидено приложимо изключение или ограничение, се изисква разрешение от правоносителите, за да се предприемат такива действия“. В този смисъл в хода на европейската авторскоправна реформа се наложи и въвеждането на изключения за целите на машинното извличане.

В резултат Директива (ЕС) 2019/790 въвежда в своите членове 3 и 4 две отделни, задължителни изключения за целите на извличане на информация от текст и данни. Двете разпоредби предвиждат различен кръг субекти, които могат да се възползват от съответното изключение, и различни условия за прилагане на изключението.

2.2.1. Изключение в полза на научноизследователските организации

Първото изключение за извличане на информация от текст и данни в директивата се съдържа в член 3. То беше и единственото такова в първоначалното предложение на Европейската комисия от 2016 г.

Изключението съгласно член 3 се въвежда единствено в полза на *научноизследователски организации* и *институциите за културно наследство*, при това единствено за *целите на научни изследвания*. Заявената цел на това ограничение е да бъде подпомогната работата на тези институционални ползватели, действащи в обществен интерес, в областта на големите данни и изкуствения интелект. Директивата изброява неизчерпателно различни видове организации, като допълнителните уточнения в член 2 определят кръга на бенефициерите като предимно публично финансирани лица. Съ-

[30] Съгласно Съображение 32 на Директива 2001/29/ЕО, последната „съдържа изчерпателен списък на изключенията и ограниченията по отношение на правото на възпроизвеждане и правото на публично разгласяване“. Забраната държавите членки да отиват отвъд този списък при въвеждането на национални изключения е била нееднократно потвърждавана по съдебен път. За изчерпателни разсъждения по тази тема, вж. Заключение на генералния адвокат по дело C-516/17, *Spiegel Online GmbH срещу Volker Beck* [2019] ECLI:EU:C:2019:16.

ображение 11 предвижда изрична възможност използването в рамките на изключението да се случва и в рамките на публично-частни партньорства. Подходът на директивата при дефиниране на бенефициерите на изключението е донякъде объркващ. Явното желание на законодателя да ограничи риска от нечестен „преференциален“ достъп на търговски играчи до механизма, съчетан с обясненията в съображенията на документа, че научноизследователски организации все пак трябва да могат да си партнират с частни играчи, като използват частни ресурси, води до неяснота относно кръга на субекти, които могат да имат достъп до изходни или нормализирани данни.

Член 3 предвижда автоматизиран анализ да може да бъде провеждан върху обекти на авторското право, но също така и на сродни права – това включва и новото сродно право на издателите на публикации в пресата съгласно член 15 от Директивата. Обектите, обхванати от член 3 включват и неоригинални бази данни. За разлика от член 4, член 3 не препраща изрично към Софтуерната директива[31], но не е известно дали това е умишлено или се касае по-скоро за пропуск на текста. Тук е важно да се уточни, че научноизследователските организации и институциите за културното наследство, включително свързаните с тях лица, попадат в обхвата на изключението за извличане на информация от текст и данни единствено по отношение на *съдържание, до което имат правомерен достъп*[32]. Съгласно Съображение 14 от ДАПЦЕП, правомерният достъп следва да се разбира като обхващащ достъпа до съдържание въз основа на *политика за свободен достъп или чрез договорни споразумения* между правоносители и научноизследователски организации или институции за културно наследство, като например *абонаменти*, или чрез други законни средства.

Разпоредбата на член 3 не обхваща всички авторски правомощия. Това, което изключението покрива, е (i) възпроизвеждане и (ii) извличане и повторно използване на части от бази данни. Според някои анализатори действията по „възпроизвеждане”, освен сваляне на използваните материали на машината, обхващат и цифровизиране на аналогови материали, копиране с оглед нормализиране на данните преди извличане или създаването на производни набори от данни, технологии като *оптично разпознаване на символи* (*Optical Character Recognition – OCR*) или *преобразуване на речта в текст* (*speech to text*). В този смисъл се приема, че се обхващат и

[31] Директива 2009/24/ЕО на Европейския парламент и на Съвета от 23 април 2009 година относно правната закрила на компютърните програми (ОВ L 111, с. 16–22).

[32] Подробно относно изискването за правомерен достъп вж. Лазарова, А. (2022). Преодоляване на действието на изключенията от авторското право по договорен път. – Съвременно право, № 4/2021, 25.

действия, формално квалифицирани като преработка, доколкото те са част от технологичния процес по извличане[33].

Важен момент по отношение обема на това изключение е изричната забрана за ограничаването му по договорен път или с технически средства за защита[34].

В проекта за ЗИД на ЗАПСП, с цел транспонирането на Директива 2019/789 и Директива 2019/790, изключението е пренесено в нов член 26ж, с наименование „Автоматизиран анализ на текст и информация за научни цели".

2.2.2. Общо изключение по отношение на извличането на информация от текст и данни

Второто изключение, уредено в член 4 от Директивата, ползва всички участници на цифровия пазар. То обаче позволява действия по използване в по-малък обем и при по-ограничителни условия в сравнение с изключението в полза на научноизследователските организации съгласно предходния член 3. Въведеният на късен етап от законодателния процес допълнителен член 4 не съдържа ограничение по отношение на бенефициерите на изключението. Всяка „извличаща" организация, която не може да се впише в обхвата на предходния член 3, защото дейността ѝ ни може да се квалифицира като чисто научноизследователска или защото се ползва от частно финансиране, може да се възползва от разпоредбата на член 4. Освен за качеството на бенефициерите, няма ограничение и по отношение на целите на извличането.

По-нататък, член 4 предвижда провеждане на автоматизиран анализ върху всички обекти на авторското право и сродни права. За разлика от член 3, член 4 изрично препраща и към Софтуерната директива, т.е. няма спор, че по реда на член 4 може да се осъществява автоматизиран анализ и на софтуерен код. Както и при член 3, и тук задължително условие за прилагане

[33] Следва да се уточни, че европейското *acquis* по принцип не се простира върху правото на преработка. Последното се приема за правомощие на автора с по-силен личен елемент от правомощията за копиране и разгласяване на едно произведение такова, каквото е. То също така има силна връзка с неимуществените права на автора, като например неимущественото право на запазване на интегритета на произведението. Освен че моралните авторски правомощия в континенталното право също не са хармонизирани на ниво ЕС и се смятат за материя извън компетенциите на Съюза, налице са и много големи разлики между държавите членки по отношение на „интензитета" на връзката между имущественото право на преработка и моралното право на интегритет.

[34] Вж. Лазарова, А. (2022). Преодоляване на действието на изключенията от авторското право по договорен път. – Съвременно право, № 4/2021, 25.

на изключението е наличието на *правомерен достъп*. За да се осъществи законосъобразно извличане на информация от определени материали, обект на авторско право, трябва да последните да могат да бъдат достъпени законосъобразно – т.е. или трябва да са свободно достъпни онлайн, или да достъпът до съответната база, хранилище, колекция и т.н. да е възможен по силата на различни форми на отворен достъп или абонамент.

Член 4 също въвежда изключение за *възпроизвеждане* или *извличане на откъси* от произведения или други обекти, до които лицата имат правомерен достъп, за целите на извличането на информация от текст и данни, като специално за компютърните програми директивата позволява и действия по преработка. Разпоредбата не съдържа специални изисквания за съхраняването на копията, запазени в резултат на машинно четене.

В проекта за ЗИД на ЗАПСП изключението е транспонирано в нов член 26е – „Автоматизиран анализ на текст и информация“.

Важен елемент от това изключение е, че то се прилага единствено доколкото използването на произведенията и друго защитено съдържание „не е запазено по подходящ за това начин от правоносителите“. Това означава, че авторът или носителят на сродни права може изрично да обяви, че не желае обектът на авторските му или сродни права да се използва за целите на извличането, т.е. действието на *изключението може да се обезсили едностранно от правоносителя*[35]. Когато става дума за извличане онлайн, Директивата препоръчва упражняването на тази възможност за забрана за използване да се извършва чрез машинно четими средства. С оглед прецизиране на това изискване, се приема за добра практика прилагането на *стандартни технически протоколи* за сигнализиране кога едно произведение може да бъде подлагано на извличане. Тъй като всеки уебсайт има различни общи условия, начинът да се улесни извличането онлайн е използването на протокол като *robots.txt*, който създава двоично правило „извличай“ и „не извличай“. Използването на *Robots Exclusion Standard* по

[35] Механизмът не е непознат за авторското право. Право едностранно да обезсилят законно изключение правоносителите имат открай време в контекста на изключението за *преглед на печата*. Това изключение съществува в подобен вид още в Бернската конвенция и е въведено на ниво ЕС от член 5 параграф 3, б. в), първа хипотеза от Директива 2001/29/ЕО. Европейската норма гласи, че „без съгласието на носителя на авторското право и без заплащане на възнаграждение“ е допустимо възпроизвеждането от средствата за масово осведомяване на вече разгласени статии по актуални икономически, политически или религиозни теми, *в случай, че такова използване не е било изрично забранено*, при посочване на източника и името на автора, освен когато това е невъзможно. Изключението за *преглед на печата* в чл. 5 параграф 3, б. в), първа хипотеза, е транспонирано в член 24, алинея 1, точка 5 от ЗАПСП.

отношение на съдържанието, свободно достъпно онлайн, беше и акцентът на дискусиите в Съвета и в Парламента. Този стандарт се използва широко от средата на 90-те години и се спазва от най-големите операции по извличане в интернет, включително *Google*, *Bing*, *Baidu*, *DuckDuckGo*, *Yahoo!* и *Yandex*. Поради ангажимента на търсачките да спазват тези правила, повечето уебсайтове по света следват стандарта, за да контролират какво може да се извлича от ботове. Чрез използването на машинночетим файл *robots.txt* се уточняват ограниченията за достъп, които предотвратяват или позволяват индексиране и извличане на ниво уебсайт и на ниво отделен елемент. В допълнение, правоносителите имат гъвкавостта да създават правила като напр. черни списъци, предотвратяващи обхождането от конкретно наименувани ботове (*crawlers*) или възможността да се зададат правила за ботове, които правоносителят не познава. Тези правила могат да се приложат и на ниво индивидуален документ в сайта, като се използва HTML етикет. *Robots.txt* също има възможност да посочи интервал в секунди между обхожданията (*crawls*), за да информира извличащите как могат да избегнат отрицателен ефект върху ефективността на уебсайта в резултат на обхождането.[36]

Същевременно фиксирането на определен технически подход, какъвто е *Robots Exclusion Standard*, в националното законодателство също е рисковано, доколкото може да компрометира технологичната неутралност на закона.

Горните съображения бяха взети предвид от екипа на Министерство на културата при изготвянето на текста на ЗИД на ЗАПСП в българското законодателство. В резултат на дебатите, провели се в рамките на работната група, Министерството предложи елегантно решение, което успява да повиши сигурността за извличащите ползватели, без да застраши технологичната неутралност на разпоредбата. Още в обявения за обществена консултация на 15.09.2021 г. проект за ЗИД[37], изискването на Съображение 18 е пренесено в алинея 4 на новия член 26е както следва: „Носителите на права могат да забранят използването на произведения, други обекти на закрила или части от тях при условията на алинеи 1 и 2 преди те да бъдат достъпени. В случаите на обекти, до които е предоставен електронен дос-

[36] Горните съображения се отнасят за извличането в отворената мрежа. Когато става въпрос за извличане в бази данни на издатели, и когато защитените обекти се лицензират от правоносителите, последните, ако желаят да забранят извличането от тях, следва да имат задължение ясно да посочат това ограничение в съответните лицензионни споразумения.

[37] Министерство на културата. (2021). Проект на Закон за изменение и допълнение на Закона за авторското право и сродните му права. Достъпен на: https://www.strategy.bg/PublicConsultations/View.aspx?lang=bg-BG&Id=6348.

тъп, забраната има действие само ако е *установена с технически средства*, *незабавно разпознаваеми* от софтуера, извършващ автоматизиран анализ.“

Заключение

Темата на настоящия доклад са правнотехническите аспекти на извличането на информация от текст и данни в контекста на използването на закриляни от авторското право материали. Самата технология по „извличане“ е очертана на ниво Европейски съюз от нова легална дефиниция в Директива 2019/790. В съображенията на директивата технологията се описва още като „автоматизиран изчислителен анализ на информация в цифрова форма, като например текст, звук, изображения или данни“.

В контекста на системите на генеративен изкуствен интелект, обучаването на съответния базов модел върху съдържание и данните, обект на авторско право и сродни права, ангажира действия по възпроизвеждане и преработка, които представляват използване по смисъла на авторското право. Тези действия изискват или разрешение от страна на правоносителите, или наличие на законова възможност за неоторизирано използване по силата на изключение или ограничение от авторското право. Когато говорим за гъвкавост на хипотезите на разрешена употреба, на преден план излиза естественото сравнение между континенталния и англо-американския подход при проектирането на изключения. Англо-американските концепции за *fair use* и *fair dealing* отчитат редица гъвкави критерии, които помагат на съда във всеки конкретен случай да направи преценка доколко дадена неразрешена употреба е „справедлива. В контекста на европейската континентална правна традиция, неоторизирано извличане на информация от текст и данни може да се извършва единствено на базата на изрично изключение.

Първоначалният текст на Директива 2019/790, предложен през 2016 г. от Европейската комисия, предвижда подобно извличане да се случва единствено за научноизследователски цели от институционални ползватели в обществен интерес. Проектодирективата изобщо не съдържа разпоредба, аналогична на сегашния член 4. За да не останат извън обхвата на разрешителния режим не само европейските технологични компании, използващи машинното самообучение, но и някои субекти, които биха могли успешно да се възползват от олекотен режим за извличане в общественополезната си дейност, каквито са например журналистите в хода на своите разследвания, бе добавено допълнително изключение, позволяващо извличане и за търговски цели, без ограничение по отношение на бенефициерите. Параграф 2 на член 4, обаче уточнява, че възпроизвеждането и извличането на откъси,

извършени съгласно параграф 1, могат да бъдат *запазени, докогато това е необходимо* за целите на извличането на информация от текст и данни, т.е. правоносителите могат едностранно да отменят действието на изключението.

Това е и основният механизъм, от който системи на генеративен ИИ на европейско ниво могат да се възползват, за да обработват законно защитено съдържание за целите на „захранване“ на съответния модел.

Библиография:

1. Директива 2001/29/ЕО на Европейския Парламент и на Съвета от 22 май 2001 година относно хармонизирането на някои аспекти на авторското право и сродните му права в информационното общество (OJ L 167, 22.6.2001, стр. 10–19).
2. Директива 2006/116/ЕО на Европейския парламент и Съвета от 12 декември 2006 година за срока за закрила на авторското право и някои сродни права (OJ L 372).
3. Директива 2009/24/ЕО на Европейския парламент и на Съвета от 23 април 2009 година относно правната закрила на компютърните програми (ОВ L 111, стр. 16–22).
4. Директива (ЕС) 2019/790 на Европейския парламент и на Съвета от 17 април 2019 година относно авторското право и сродните му права в цифровия единен пазар и за изменение на директиви 96/9/ЕО и 2001/29/ЕО (PE/51/2019/REV/1, OJ L 130, стр. 92–125).
5. Решение на Съда на ЕС по дело C-5/08, Infopaq International A/S срещу Danske Dagblades Forening [2009] ECLI:EU:C:2009:465.
6. Решение на Съда на ЕС по дело C-145/10, Eva-Maria Painer срещу Standard VerlagsGmbH и др. [2011], ECLI:EU:C:2011:798.
7. Решение на Съда на ЕС по дело C-604/10, Football Dataco Ltd и др. срещу Yahoo UK Ltd и др., ECLI:EU:C:2012:115.
8. Заключение на генералния адвокат по дело C-516/17, Spiegel Online GmbH срещу Volker Beck [2019] ECLI:EU:C:2019:16.
9. Проект за Закон за изменение и допълнение на Закона за авторското право и сродните му права (ЗИД на ЗАПСП) с цел транспонирането на Директива 2019/789 и Директива 2019/790 в българското законодателство (внесен в 49 НС със сигнатура 49-302-01-21).

10. Министерство на културата. (2021). Проект на Закон за изменение и допълнение на Закона за авторското право и сродните му права. достъпен на: https://www.strategy.bg/PublicConsultations/View.aspx?lang=bg-BG&Id=6348
11. Kelly v. Arriba Soft Corp., 336 F.3d 811, 822 (9th Cir. 2003).
12. Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1169 (9th Cir. 2007).
13. A.V. ex rel. Vanderhye v. iParadigms, LLC, 562 F.3d 630, 640 (4th Cir. 2009).
14. Authors Guild, Inc. v. Google, Inc., 804 F.3d 202 (2d Cir. 2015).
15. Doe 1 et al v. GitHub et al, Case No. 4:2022cv06823 (N.D. Cal.)
16. Andersen et al v. Stability AI et al, Case No. 3:23-cv-00201 (N.D. Cal.)
17. Getty Images v. Stability AI, Case No. 1:2023cv00135 (D. Del.).
18. Getty Images v Sability AI (England), Case IL-2023-000007.
19. Broz, M. (2023). Original research: More watermarks found in Stable Diffusion's images. Available at: https://photutorial.com/stable-diffusion-watermarks-investigation/.
20. Carroll, M. (2019). Copyright and the Progress of Science: Why Text and Data Mining Is Lawful'. *UC Davis Law Review* 53: 89.
21. Chowdhury, R. (2023). Generative AI: Hype, Harms, and the Responsible Tech Community (video). Available at: https://www.linkedin.com/events/7048711724547354624/comments/.
22. Geiger, C., Frosio, G., & Bulayenko, O. (2019). Text and data mining: Articles 3 and 4 of the directive 2019/790/EU. *Propiedad intelectual y mercado único digital europeo*, Valencia, Tirant lo blanch, 27–71.
23. Kretschmer, M., Margoni, T., & Oruc, P. (2021). D3.6 Interim study on the state of harmonisation of the rights of reproduction and adaptation and connected exceptions. Zenodo. Available at: https://doi.org/10.5281/zenodo.5069507.
24. GPDP (2023). Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori. Available at: https://www.garanteprivacy.it/home/autorita/collegio. Вж. още Kristi Hines, Exploring Italy's ChatGPT Ban And Its Potential Impact. Available at: https://www.searchenginejournal.com/chatgpt-ban-italy/484157/.
25. Guadamuz, A. (2023). A Scanner Darkly: Copyright Infringement in Artificial Intelligence Inputs and Outputs. Available at SSRN 4371204.
26. NBC 5 (2022). Judge Approves $92 Million TikTok Settlement, With Illinois Claimants Receiving Biggest Share. Available at: https://www.nbcchicago.com/news/local/judge-approves-92-million-tiktok-settlement-with-illinois-claimants-receiving-biggest-share/2921881/.

27. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts [8115/21 – COM(2021) 206 final]

28. Rutgers Bootcamps. (2022). What Is Data Mining? A Beginner's Guide. Available at: https://bootcamp.rutgers.edu/blog/what-is-data-mining/.

29. Sun, H. (2021). Creating a Public Interest Principle for the Adjudication of Fair Use and Fair Dealing Cases. *The Cambridge Handbook of Copyright Limitations and Exceptions* (Cambridge Law Handbooks, pp. 233–266). Cambridge: Cambridge University Press. doi:10.1017/9781108671101.019.

30. Vaughan-Nichols, S. (2022). GitHub's Copilot flies into its first open source copyright lawsuit. It won't be the last. Available at: https://www.theregister.com/2022/11/11/githubs_copilot_opinion/.

31. Лазарова, А. (2022). Преодоляване на действието на изключенията от авторското право по договорен път. – Съвременно право, № 4/2021, 25.

Решенията на Съда на ЕС за обработване на лични данни в сектора на електронните съобщения

Д-р Огнян Стоичков*

Изследвана е практиката на Съда на ЕС за обработване на лични данни в сектора на електронните съобщения, като накратко са анализирани основните актове на Европейския съюз в предметната област и тяхната проекция в националните правни системи на държавите членки.

Основният пробем, поставен в доклада, е необходимостта от спешна актуализация на нормативната ни уредба, съобразно Решение по дело C 350/21 от 17 ноември 2022 г. за България, с което Съдът на ЕС постановява, че Директива 2002/58 трябва да се тълкува в смисъл, че не допуска:

- национално законодателство, което предвижда превантивно общо и неизбирателно запазване на данни за трафик и на данни за местонахождение;
- национална правна уредба, която предвижда достъп до запазени данни за трафик и данни за местонахождение, без да гарантира, че лицата са били уведомени за това в степента, предвидена от правото на Съюза, и без посочените лица да разполагат с правно средство за защита срещу неправомерен достъп.

Ключови думи: *Електронни съобщения, Закон за електронните съобщения, лични данни, Наказателно-процесуален кодекс, Съд на Европейския съюз, трафични данни*

* Д-р Огнян Стоичков, член на Национално бюро за контрол на специалните разузнавателни средства, ел. поща: stoichkov111@gmail.com

The decisions of the Court of Justice of the EU on the processing of personal data in the electronic communications sector

Ognyan Stoichkov, PhD*

The case law of the Court of Justice of the European Union (CJEU) on the processing of personal data in the electronic communications sector is examined, with a brief analysis of the main European Union acts in the subject area and their projection into the national legal systems of the Member States. The main issue raised in the report is the need to urgently update our legal framework, in line with the judgment in Case C 350/21 of 17 November 2022. for Bulgaria, whereby the Court of Justice of the EU ruled, that Directive 2002/58 must be interpreted as precluding:

- national legislation which provides for the preventive general and non-selective retention of traffic data and location data;
- national legislation which provides for access to stored traffic and location data without ensuring that the persons concerned have been informed to the extent provided for by Union law and without those persons having a legal remedy against unlawful access.

Keywords*: Electronic communications, Electronic Communications Act, personal data, Criminal Procedure Code, Court of Justice of the European Union, traffic data*

* Ognyan Stoichkov, PhD, member of of the National Bureau for Control of Special Intelligence Means, e-mail: stoichkov111@gmail.com

Съдът на Европейския съюз е институция на ЕС със значим принос за развитието както на съюзното право, така и на националното право на всяка държава членка.

В Договора за функциониране на ЕС е уреден статутът на СЕС[1], състоящ се от две юрисдикции – Съд и Общ съд (учреден през 1988 г.)[2].

От създаването си през 1952 г. Съдът на Европейския съюз има за задача да осигурява „спазването на правото при тълкуването и прилагането“ на Договорите, като има следните по-съществени правомощия: упражнява контрол за законосъобразност на актовете на институциите на Европейския съюз; следи за спазването от държавите членки на задълженията им по договорите и тълкува правото на Съюза по искане на националните съдилища[3].

Редът за преюдициалното запитване е регламентиран в чл. 276 от ДФЕС. Относно действието на решението на СЕС по отношение на националното производство, по което е направено запитване, съдът е имал случай да се произнесе, че разпоредбите на чл. 4, параграф 3 и чл. 19, параграф 1 ДЕС, както и чл. 267 ДФЕС във връзка с чл. 47 от ХОПЕС трябва да се тълкуват в смисъл, че *допускат процесуални разпоредби* на държава членка[4], които са съобразени с принципа на *равностойност* и водят до това, че когато върховната административна юрисдикция на тази държава членка постанови съдебен акт за решаване на спор, в рамките на който тя е сезирала Съда с преюдициално запитване, страните по този спор *не могат да поискат отмяна* на този влязъл в сила съдебен акт на националната юрисдикция с

[1] Договор за ЕС и Договор за функциониране на ЕС (Консолидирани текстове), раздел 5, чл. 251–281. (В протокол № 3 към Договора е уреден статутът на СЕС.) https://eur-lex.europa.eu/legal-content/bg/TXT/?uri=celex:12016ME/TXT

[2] Пак там, чл. 256 параграф 3. Общият съд е компетентен да разглежда и да се произнася по преюдициални въпроси, отправени към него, по силата на член 267 в специфични сфери, определени от статута.
Когато Общият съд прецени, че делото изисква принципно решение, което може да засегне единството или съгласуваността на правото на Съюза, той може да препрати делото към Съда, който да се произнесе.
Решенията, постановени от Общия съд относно преюдициални въпроси, могат по изключение да бъдат преразглеждани от Съда съгласно условията и ограниченията, предвидени от статута, в случай на сериозен риск от засягане единството или съгласуваността на правото на Съюза.

[3] Съд на Европейския съюз – CURIA, https://curia.europa.eu/jcms/jcms/Jo2_6999/bg/

[4] Виж Вучков, В. Доказателствени средства в наказателното производство. София: Фенея, 2006, с. 32–38, ISBN 954-8214-90-3; 978-954-8214-90-2

мотива, че тя не се е съобразила с тълкуването на правото на Съюза, дадено от Съда в отговор на това запитване[5].

С **Решение по дело C 350/21 от 17.11.2022 г**. за България Съдът на

ЕС се произнася относно Преюдициално запитване – Обработване на лични данни в сектора на електронните съобщения – Конфиденциалност на комуникациите – Доставчици на електронни съобщителни услуги – Общо и неизбирателно запазване на данни за трафик и на данни за местонахождение за период от шест месеца – Борба с тежката престъпност – Достъп до запазените данни – Уведомяване на съответните лица – Право на жалба – **Директива 2002/58/ЕО** – Член 15, параграфи 1 и 2 – **Директива (ЕС) 2016/680** – Членове 13 и 54 – Харта на основните права на Европейския съюз – Членове 7, 8, 11 и 47 и член 52, параграф 1[6].

С оглед точното прилагане на решението за България, включително и съобразяването му при наложителната законодателна промяна на ЗЕС и НПК[7], накратко е представена практика на СЕС по релевантно национално законодателство и на други държави.

I. Относими актове на ЕС

1. Директива 2002/58/ЕО *на ЕП и на Съвета* 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)[8].

Съгласно чл. 15, § 1 от Директивата държавите членки могат да приемат законодателни мерки, за да ограничат обхвата на правата и задълженията, предвидени в чл. 5 (конфеденциалност), чл. 6 (данни за трафик), чл. 8, параграф 1, 2, 3, и 4 (идентификация на линия) и чл. 9 (данни за местонахождение) от настоящата директива, когато такова ограничаване представлява **необходима, подходяща и пропорционална мярка** в рамките на демократичното общество, *за да гарантира националната сигурност,*

[5] Виж Решение на СЕС от 07.07.2022 г. по дело C-261/21 относно тълкуването на чл. 4, § 4 от ДЕС и чл. 267 от ДФЕС, https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:62021CJ0261

[6] Решение на Съда на ЕС по дело C 350/21 от 17.11. 2022 г., https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:62021CJ0350

[7] Виж Велчев, Б. Международно наказателно право. София: Сиела, 2015, с. 45–50, ISBN 978-954-28-1720-8

[8] Директива 2002/58/ЕО на Европейския парламент и на Съвета, https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32002L0058&qid=1606395563171

отбраната, обществената безопасност и превенцията, разследването, разкриването и преследването на престъпления или неразрешено използване на електронна комуникационна система. В тази връзка държавите членки могат, *inter alia*, да одобрят законодателни мерки, предвиждащи съхранението на данни за ограничен период, оправдани на основанията, изложени в настоящия параграф.

В решението е цитиран и ***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 – GDPR)[9].

Съгласно член 2, параграф 2, буква г) от регламента, **той не се прилага** за обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазване от заплахи за обществената сигурност и тяхното предотвратяване.

2. ***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.[10]

В разпоредбата на чл. 13 от Директивата е предвидена **Информация, до която се осигурява достъп или която се предоставя на субекта на данните**[11], като в параграф 3 се допуска държавите членки да могат

[9] Регламент (ЕС) 2016/679, https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32016R0679

[10] Директива (ЕС) 2016/680, https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=celex%3A32016L0680

[11] Директива 2016/680, **чл. 13, параграф 1**. Държавите членки предвиждат администраторът да предоставя на субектите на данни най-малко следната информация**: а)** данни за идентифициране и координатите за връзка на администратора; **б)** координатите за връзка на длъжностното лице по защита на данните, когато е приложимо; **в)** целите на обработването, за които са предназначени личните данни**; г)** правото да бъде подадена жалба до надзорен орган и да бъдат предоставени неговите координати за връзка; **д)** съществуването на право да се изиска от администратора достъп до коригиране или изтриване на лични данни и ограничаване на обработването на

да приемат законодателни мерки, които забавят, ограничават или водят до пропускане на предоставянето на информация на субекта на данните съгласно параграф 2, до такава степен и за толкова време, за колкото тази мярка е необходима и пропорционална в едно демократично общество, като надлежно се вземат под внимание основните права и легитимните интереси на засегнатото физическо лице, за да**: а)** се избегне възпрепятстването на официални или съдебни проучвания, разследвания или процедури; **б)** не се допусне неблагоприятно влияние върху предотвратяването, разкриването, разследването или наказателното преследване на престъпления или изпълнението на наказания; **в)** се защити обществената сигурност; **г)** се защити националната сигурност; **д)** се защитят правата и свободите на други лица.

II. Съдебна практика на СЕС за релевантно национално законодателство на други държави

1. Решение от 8 април 2014 г. Digital Rights Ireland and Others (C-293/12 и C-594/12, EU:C:2014:238)[12]

СЕС е сезиран от Върховния съд на Ирландия и от Конституционния съд на Австрия във връзка с национални производства, съответно за оспорване на част 7 от Закона за наказателно правораздаване (терористични престъпления) от 2005 г. и за оспорване на член 102а от Закона за далекосъобщенията от 2003 г.

Във връзка с оспорването пред двете национални съдилища и на Директива 2006/24 СЕС обявява същата за невалидна поради нарушаване на принципа на пропорционалност, съгласно чл. 7, 8 и 52, параграф 1 от Хартата на основните права на ЕС.

лични данни, свързано със субекта на данните; **параграф 2.** Освен информацията, посочена в параграф 1, държавите членки предвиждат със закон администраторът да предоставя на субекта на данните, в конкретни случаи и с цел да му се даде възможност да упражни правата си, следната допълнителна информация: **а)** правното основание на обработването; **б**) срока, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок; **в)** когато е приложимо, категориите получатели на личните данни, включително в трети държави или международни организации; **г)** когато е необходимо, допълнителна информация, по-специално когато личните данни са събрани без знанието на субекта на данните.

[12] Решение от 8 април 2014 г. *Digital Rights Ireland and Others* (C-293/12 и C-594/12, EU:C:2014:238) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293

2. Решение на СЕС от 21.12.2016 г. (Tele2 Sverige and Watson and Others, C-203/15 и C-698/15, EU:C:2016:970)[13]

Въз основа на преюдициални запитвания на Административен апелативен съд Стокхолм, Швеция и Апелативен съд (Англия и Уелс) Съдът на ЕС постановява решение, подобно на решението, постановено шест години по-късно за България, а именно: **член 15, параграф 1** от Директива 2002/58/ЕО във връзка с членове 7, 8 и 11 и член 52, параграф 1 от ХОПЕС трябва да се тълкува в смисъл, че не допуска национална правна уредба, която за целите на борбата с престъпността предвижда общо и неизбирателно запазване на всички данни за трафик и данни за местонахождение на всички абонати и регистрирани ползватели на всички електронни съобщителни средства.

В съображение 121 от решението СЕС приема, че *компетентните национални органи, на които е предоставен достъп до запазените данни, следва да уведомят за това засегнатите лица* в рамките на приложимите национални производства веднага щом това е възможно, без да се възпрепятстват водените от тези органи разследвания. Тази информация фактически е необходима, за да им се позволи да упражнят правото си на жалба съгласно чл. 15, параграф 2 от Директива 2002/58, чл. 47, първа алинея от ХОПЕС, във връзка с чл. 79, параграф 1 от Регламент 2016/679.[14]

3. Решение от 6.10.2020 г. (La Quadrature du Net and Others, C-511/18, C-512/18 и C-520/18, EU:C:2020:791)[15]

Съдът на ЕС постановява решението си след преюдициално запитване на Държавния съвет на Франция и Конституционния съд на Белгия, като потвърждава практиката си до момента, допълва и следното:

1) Допуска следните **законодателни мерки:**

- позволяващи с оглед опазването на **националната сигурност** да се разпореди на доставчиците на електронни съобщителни услуги да извършват *общо и неизбирателно запазване* на данни за трафик и на данни за местонахождение в положения, при които съответната държава членка е изправена пред сериозна заплаха за националната

[13] Решение на СЕС от 21.12. 2016 г. (*Tele2 Sverige and Watson and Others*, C-203/15 и C-698/15, EU:C:2016:970), https://curia.europa.eu/juris/liste.jsf?num=c-203/15

[14] Виж по аналогия решения от 7 май 2009 г., Rijkeboer, C-553/07, EU:C:2009:293, т. 52 и от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 95.

[15] Решение от 6.10.2020 г. (La Quadrature du Net and Others, C-511/18, C-512/18 и C-520/18, EU:C:2020:791), https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18

сигурност, *която е действителна и настояща или предвидима*, като решението, предвиждащо това разпореждане, трябва да подлежи на ефективен контрол от юрисдикция или от независима административна структура, като посоченото разпореждане може да бъде издадено само за ограничен до строго необходимото период от време, който може да бъде удължен, ако заплахата продължи да съществува,

- предвиждащи за целите на опазването на **националната сигурност, борбата с тежката престъпност** и предотвратяването на **сериозни заплахи срещу обществената сигурност** *целево запазване* на данни за трафик и на данни за местонахождение, което да е ограничено въз основа на обективни и недискриминационни критерии в зависимост от категориите *засегнати лица или посредством географски критерий*, за ограничен до строго необходимото период от време, който може да бъде удължен,
- предвиждащи за целите на **опазването на националната сигурност, борбата с тежката престъпност** и предотвратяването на **сериозни заплахи срещу обществената сигурност** *общо и неизбирателно запазване* на ***IP адреси***, дадени на източника на свързване с интернет, както и ***запазване на данни относно самоличността*** на ползвателите на електронни съобщителни средства за ограничен до строго необходимото период от време, и
- позволяващи, за целите **на борбата с тежката престъпност** и *a fortiori* **за опазване на националната сигурност** да се разпореди на доставчиците на електронни съобщителни услуги чрез решение на компетентния орган, подлежащо на ефективен съдебен контрол, ***да извършват за определен период бързо запазване на данните за трафик и на данните за местонахождение***, с които разполагат тези доставчици на услуги, при положение че тези мерки гарантират с ясни и точни правила, че запазването на разглежданите данни е подчинено на спазването на съответните материални и процесуални условия и че засегнатите лица разполагат с ефективни гаранции срещу рисковете от злоупотреби.

2) Член 15, параграф 1 от Директива 2002/58 трябва да се тълкува в смисъл, че допуска национална правна уредба, която задължава доставчиците на електронни съобщителни услуги, от една страна, да използват автоматизиран анализ, както и **да събират в реално време** по-

специално данни за трафик и данни за местонахождение, и от друга страна, да събират в реално време технически данни за местонахождението на използваните крайни устройства, ако:

- използването на автоматизирания анализ се ограничава до положения, при които държава членка е изправена пред ***сериозна заплаха за националната сигурност***, която е действителна и настояща или предвидима, като прибягването до този анализ трябва да подлежи на ефективен контрол от юрисдикция или от независима административна структура и
- прибягването до събиране в реално време на данни за трафик и на данни за местонахождение се ограничава до лицата, за които съществува основателна причина да се подозира, че участват по един или друг начин в ***терористични дейности***, и подлежи на предварителен контрол от юрисдикция или от независима административна структура.

3) Директива 2000/31/ЕО (Директива за електронната търговия) не е приложима в областта на защитата на поверителността на съобщенията и на физическите лица, като тази защита се урежда от Директива 2002/58 – чл. 23, параграф 1 от Регламент 2016/679 трябва да се тълкува в смисъл, че не допуска национална правна уредба, която налага на доставчиците на достъп до обществени съобщителни услуги в интернет и на доставчиците на хостинг услуги задължение за общо и неизбирателно запазване по-специално на лични данни, свързани с тези услуги.

4) Национална юрисдикция не може да прилага разпоредба от националното си право, която я оправомощава *да ограничи във времето последиците на възложено ѝ по силата на това право обявяване на незаконосъобразността на национално законодателство*, което налага на доставчиците на електронни съобщителни услуги с оглед по-специално на опазването на националната сигурност и борбата с престъпността общо и неизбирателно запазване на данни за трафик и на данни за местонахождение в разрез с член 15, параграф 1 от Директива 2002/58. Разпоредбата на член 15, параграф 1, тълкуван в светлината на принципа на ефективност, изисква националният наказателен съд ***да не взема предвид данни и доказателства, получени чрез несъвместимо с правото на Съюза*** общо и неизбирателно запазване на данни за трафик и на данни за местонахождение в рамките на наказателно производство, образувано срещу заподозрени в престъпни деяния лица, ***ако тези лица не са в състояние да обсъдят*** ефективно тези

данни и доказателства от област, в която са необходими специални познания, каквито съдът няма, и които данни и доказателства могат да окажат ***съществено влияние*** върху преценката на фактите и обстоятелствата.[16]

4. Решение от 2 март 2021 г., Prokuratuur (Условия за достъп до данните за електронните съобщения, C-746/18, EU:C:2021:152)[17]

По съдебно производство в Естония и дадени разрешения за достъп от прокуратурата СЕС постановява, че чл. 15, параграф 1 от Директива 2002/58 трябва да се тълкува в смисъл, че не допуска национална правна уредба*, която оправомощава прокуратурата*, чиято задача е да ръководи наказателното разследване и евентуално да представлява държавното обвинение в последващо производство, *да разреши достъпа* на публичен орган до данните за трафик и до данните за местонахождение за целите на наказателно разследване.

5. Решение от 5 април 2022 г., Commissioner of An Garda Síochána и др. (C-140/20, EU:C:2022:258)[18]

Във връзка със запитване на Върховния съд на Ирландия СЕС излага следните съображения:

- Държавите членки могат да приемат мерки за запазване по отношение на лица, спрямо които – във връзка с такова идентифициране – се провежда *разследване* или се прилагат други текущи мерки за наблюдение, или за които в националния регистър за *съдимост* е посочена предишна присъда за тежки престъпления, която може да предполага повишен риск от извършване на ново престъпление;
- От друга страна, мярка за целево запазване на данни за трафик и на данни за местонахождение може да се основава и на *географски критерий,* когато компетентните национални органи установят, че в една или в няколко географски зони съществува повишен риск от подготвяне или извършване на тежки престъпления. Тези зони могат да бъдат по-специално места, характеризиращи се с *голям брой*

[16] Виж Вучков, В. Образуване на досъдебно производство: актуални проблеми. София: Сиби, 2015, с.12–17, ISBN 978-954-730-947-0

[17] Решение от 2 март 2021 г., Prokuratuur (Условия за достъп до данните за електронните съобщения, C 746/18, EU:C:2021:152), https://curia.europa.eu/juris/liste.jsf?language=en&num=c-746/18

[18] Решение от 5 април 2022 г., Commissioner of An Garda Síochána и др. (C-140/20, EU:C:2022:258), съображения 78, 79, 85, 91 и 100, https://curia.europa.eu/juris/liste.jsf?num=C-140/20

тежки престъпления, места, особено изложени на извършването на тежки престъпления, като места или инфраструктури, редовно посещавани *от много голям брой хора, или стратегически места* като летища, гари, морски пристанища или зони за събиране на пътни такси;

- По принцип такива данни трябва да бъдат изтрити или да се направят анонимни след изтичане на законовите срокове, в които трябва да се извършва обработването и съхранението им. Съдът обаче приема, че по време на това обработване и съхранение могат да възникнат положения, при които е налице *необходимост от запазване на посочените данни след изтичането на тези срокове* с цел разкриването на тежки престъпления или посегателства върху националната сигурност както когато тези престъпления или посегателства върху националната сигурност вече са били установени, така и когато след обективна преценка на всички релевантни обстоятелства може разумно да се подозира, че съществуват[19];
- Допуска компетентните национални органи да разпоредят мярка за бързо запазване *още на първия етап от разследването* на сериозна заплаха за обществената сигурност или на евентуално тежко престъпление;
- Когато тези данни по изключение са били предмет на общо и неизбирателно запазване за целите на *опазването на националната сигурност* от действителна и настояща или предвидима заплаха, националните органи, компетентни в областта на разследването на престъпления, *не биха могли да получат достъп до посочените данни в рамките на наказателно преследване*, тъй като в противен случай би се лишила от всякакво полезно действие забраната за такова запазване за целите на борбата с тежката престъпност.

6. Решение от 20 септември 2022 г. (Bundesrepublik Deutschland v SpaceNet AG и Telekom Deutschland GmbH, съединени дела C-793/19 и C-794/19)[20]

По преюдициално запитване на Федералния административен съд на Германия СЕС приема следното:

[19] Виж в този смисъл решение от 6 октомври 2020 г., La Quadrature du Net и др., C-511/18, C-512/18 и C-520/18, EU:C:2020:791, т. 150, 160 и 161.

[20] Решение от 20 септември 2022 г. (*Bundesrepublik Deutschland v SpaceNet AG и Telekom Deutschland GmbH*, съединени дела C-793/19 и C-794/19), съображения 86, 92, 93 и 94. https://curia.europa.eu/juris/liste.jsf?num=C-793/19

- В случая тези срокове, които съгласно § 176 от Закона за съобщенията (TKG)[21] са *четири седмици за данните за местонахождение и десет седмици за другите данни*, са значително по-кратки от приетите в други националните правни уредби;
- Що се отнася до довода на Европейската комисия, че *особено тежката престъпност би могла да бъде приравнена на заплаха за националната сигурност*, Съдът вече е постановил, че целта за опазване на националната сигурност съответства на първостепенния интерес от защита на съществените функции на държавата и основните интереси на обществото чрез предотвратяването и преследването на *дейности, които могат сериозно да дестабилизират основните конституционни, политически, икономически или социални структури на дадена страна, и по-специално да заплашват пряко обществото, населението или самата държава, като например терористични дейности*[22];
- За разлика от престъпността, дори и особено тежка, заплахата за националната сигурност трябва да бъде *действителна и настояща или поне предвидима, което предполага настъпването* на достатъчно конкретни обстоятелства, за да може да се обоснове общо и неизбирателно съхраняване на данни за трафик и на данни за местонахождение през ограничен период от време. Следователно такава заплаха се различава – по своето естество, тежест и специфика на свързаните с нея обстоятелства – от общия и постоянен риск от тежки престъпления или от възникване на напрежение или смущения на обществената сигурност дори ако те са сериозни[23];
- Престъпността, дори особено тежка, не може да се приравни на заплаха за националната сигурност. Всъщност подобно приравняване би могло да въведе *междинна категория* между националната сигурност и обществената сигурност, така че към *обществената сигурност да се приложат изискванията, които са свързани с националната сигурност*.

21 Закон за съобщенията (TKG) на ФРГ, § 176, https://dejure.org/gesetze/TKG/176.html

22 Виж Денчев, Ст. Информация и сигурност, изд. „За буквите – О писменехъ“, УНИБИТ, 2019, с. 123–138, ISBN:978-619-185-369-4

23 Виж Решение от 5.04.2022 г., Commissioner of An Garda Síochána и др., C-140/20, EU:C:2022:258, т. 61, 62 и 63.

III. Приложимо национално право

1. Закон за електронните съобщения – чл. 251б–262

2. Наказателно-процесуален кодекс – чл. 159а.[24]

3. Закон за защита на личните данни

Съгласно ДР, § 1а. (Нов – ДВ, бр. 91 от 2006 г., изм. ДВ, бр. 17 от 2019 г.) ЗЗЛД предвижда мерки по прилагане на Регламент (ЕС) 2016/679 , както и въвежда изискванията на Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г.

Съответно в Глава седма са регламентирани правата на субектите на данните и средствата за правна защита, съгласно Регламента и в Глава осма, чл. 42–83 се транспонира Директивата.

4. Решение № 2 по к. д. № 8/2014 г. на Конституционния съд[25]

След обявяването на Директива 2006/24 за невалидна (виж т. 1.2.1) КС обявява за противоконституционни чл. 250а–250е, чл. 251 и чл. 251а ЗЕС.

Конституционният съд постановява, че Българската конституция по принцип допуска общо и неизбирателно запазване на данни с цел наказателно преследване на тежки престъпления, при условие че срокът на запазване не е прекомерно дълъг, какъвто според него е случаят със срока от шест месеца. По-специално, като признава, че такова общо и неизбирателно запазване е засягало всички лица, а не само онези, за които има данни или улики, че са извършили тежко престъпление, Конституционният съд приема, че на практика не съществува друг способ, който може да осигури необходимите сведения за целите на борбата с тежката престъпност относно времето, предшестващо престъпното деяние.

5. Решение № 15 по к. д. № 4/2020 г. на Конституционния съд[26]

Обявяват се за противоконституционни разпоредби, свързани със запазване и предоставяне на данни при условията на пандемично положение.

КС обсъжда в тази връзка и горецитираните решения на СЕС – Digital Rights Ireland, *Tele2 Sverige и Watson* и др., без да променя позицията си, изложена в Решение № 2/2015 г.

---

[24] Виж Вучков, В. Предмет и тежест на доказване в наказателното производство. София: Сиби, 2008, с. 55–60, ISBN 978-954-730-528-1

[25] Решение № 2 от 2015 г. по к. д. № 8/2014 г. на Конституционния съд, https://www.constcourt.bg/bg/act-4467

[26] Решение № 15 по к.д. № 4/2020 г. на Конституционния съд, https://www.constcourt.bg/bg/act-6866

Съдът е приел имплицитно, че общото и неизбирателно запазване на данни за трафик и за местонахождение е в съответствие с Българската конституция. Освен това българската правна уредба съдържала допълнителни гаранции, които евентуално са ефективен балансиращ фактор и оправдават такова общо запазване на данните.

IV. Решение по дело C 350/21 от 17.11. 2022 г. за България

1. Основни принципи в решението на СЕС

В съображения към решението съдът приема, че национално законодателство относно запазването на лични данни и достъпа до тях трябва да предвижда разпоредби, които ясно и точно да сочат, че достъпът до запазените данни трябва да се ограничи *до строго необходимото за постигане на преследваната цел.* В случая националното законодателство се ограничава до изискването този достъп *да се отнася само до разумен период* от време, който не надвишава шест месеца.

Съдът излага в мотивите си, че са налице две процедури относно обработване на лични данни, а именно: *предоставянето на данни от доставчиците* на електронни съобщителни услуги, които са ги запазили; *използването на така предоставените данни* от националните органи, компетентни в областта на наказателното преследване. Първата процедура попада в приложното поле на Директива 2002/58, а втората – в приложното поле на Директива 2016/680.

Въз основа на принципа на ***процесуална автономия*** вътрешният правен ред на всяка държава членка трябва да уреди процесуалните правила, които страните в процеса черпят от правото на Съюза, при условие обаче че те не са по-неблагоприятни от правилата, които уреждат подобни вътрешноправни положения ***(принцип на равностойност)***, и не правят практически невъзможно или прекомерно трудно упражняването на правата, предоставени от правото на Съюза ***(принцип на ефективност)*** .

Съдът стига до извода, че принципът на ефективност не е спазен. Разглежданата национална правна уредба предвижда, че разрешение се предоставя само въз основа на искане от страна на компетентните национални органи, ***без съответните лица да са били изслушани*** и следователно без юрисдикцията да е могла да вземе предвид възможните възражения на тези лица.[27]

[27] Решение по дело C 350/21 от 17.11.2022 г. за България, съображения 65, 66, 68, 69, 74 и 75.

2. Уведомяване на засегнатото лице

В решението си СЕС приема, че българската правна уредба не гарантира, че лицата, до чиито данни е осъществен достъп, са били уведомени за това в степента, предвидена от правото на Съюза.

Както бе посочено по-горе, с редакцията на Закона за защита на личните данни от 2019 г. в Глава седма са регламентирани правата на субектите на данните и средствата за правна защита, съгласно Регламент (ЕС) 2016/679, и в Глава осма, чл. 42–83, се транспонира Директива (ЕС) 2016/680.

Осъществяване на предвидените в ЗЗЛД права на лицата е въпрос на двустранно активно поведение – на засегнатите лица и на органите, които дължат уведомяване. Упражняването на контролните правомощия на трите органа – Комисията за защита на личните данни, Инспектората към ВСС и компетентната комисия на Народното събрание (съгласно ЗЕС и Правилника за дейността на НС), явно не отговаря на зададените стандарти.

Заключение

Безспорна е необходимостта от спешни законодателни промени в ЗЕС и НПК в основните насоки, определени в решенията на СЕС, както за другите държави, така и за България.

Към момента се нарушават не само правата на засегнатите лица, участващи в електронната комуникация, но се поставя под въпрос и доказателствената стойност на приобщените трафични данни в наказателния процес.

Библиография:

1. Велчев, Б. Международно наказателно право. София: Сиела, 2015, ISBN 978-954-28-1720-8
2. Вучков, В. Доказателствени средства в наказателното производство. София: Фенея, 2006, ISBN 954-8214-90-3; 978-954-8214-90-2
3. Вучков, В. Предмет и тежест на доказване в наказателното производство. София: Сиби, 2008, ISBN 978-954-730-528-1
4. Вучков, В. Образуване на досъдебно производство: актуални проблеми. София: Сиби, 2015, ISBN 978-954-730-947-0
5. Денчев, Ст. Информация и сигурност, изд. „За буквите – О писменехъ“, УНИБИТ, 2019, ISBN:978-619-185-369-4

Изкуствен интелект – формиране на вина за умишлени противоправни деяния

Даниел Делчев*

Извършването на умишлени противоправни деяния и формирането на вина от страна на изкуствения интелект е една все още сравнително непозната тематика за съвременното право. Тя търпи динамично развитие във връзка с все по-широко навлизащото понятие за електронно лице и налагането му като субект на правото в съвременната правна теория. Способността на изкуствения интелект да притежава необходимите качества, за да успее да формира интелектуален и волеви момент на вината при извършването на противоправни деяния, е донякъде спорна към днешна дата, но развитието на технологиите и постоянната дигитализация на обществените отношения налагат все повече мнението, че възможността това да се реализира е все по-близка до настоящия момент. Публикацията има за цел да насочи вниманието към все по-всеобхватните възможности на изкуствения интелект, да разгледа понятията свързани с него, електронното лице като субект на правото и възможностите за формиране на вина от страна на изкуствения интелект при извършването на противоправни деяния.

Ключови думи: *вина, електронно лице, изкуствен интелект, наказателна отговорност, противоправно деяние*

* Д-р Даниел Делчев, старши преподавател, катедра „Публичноправни науки“ към факултет „Полиция“, Академия на Министерство на вътрешните работи, ел. поща: daniel1001d@gmail.com

Artificial intelligence – formation of fault for intentional unlawful actions

Daniel Delchev*

The commission of intentional unlawful actions and the formation of fault by artificial intelligence is still a relatively unknown topic for modern law. It is undergoing a dynamic development in connection with the increasingly widespread concept of the electronic person and its imposition as a subject of law in the modern legal theory. The ability of artificial intelligence to possess the necessary qualities to be able to form an intellectual and volitional moment of fault during committing unlawful actions is somehow controversial to date, but the development of the technologies and the constant digitalization of the social relations increasingly impose the opinion that the possibility, this to be accomplished is ever closer to the present moment. The purpose of this publication is to draw attention to the increasingly comprehensive potential of the artificial intelligence, to examine the concepts related to it, to examine the electronic person as a subject of law and the possibilities for the formation of fault by the artificial intelligence in committing unlawful actions.

Keywords: *fault, electronic person, artificial intelligence, criminal liability, unlawful actions*

* Daniel Delchev, PhD, senior lecturer, Department of Public Law at the Faculty of Police, Academy of the Ministry of the Interior,
e-mail: daniel1001d@gmail.com

Умисълът при извършване на престъпления е формата на вина, която се проявява по-често в сравнение с непредпазливостта, но за да може да се стигне до ангажиране на наказателна отговорност на извършителя, следва да е налице съответният интелектуален и волеви момент. Възникването на наказателна отговорност на изкуствения интелект (чието определяне като евентуален субект на правото може да бъде под формата на т.нар. „електронно лице“) има за предпоставка наличието на способност на изкуствения интелект да отговаря на изискването за формиране на интелектуален и волеви момент на вината при извършване на умишлени противоправни деяния. Способността за формирането на вина от страна на изкуствения интелект и в частност на електронното лице може да бъде основата, която да обуслови, в един близък до настоящето момент, възможността изкуственият интелект да бъде реално признат като същински правен субект, заедно с традиционните такива. В действителност вече е факт съществуването на машини, функциониращи на базата на и поставени под контрола на изкуствен интелект, които биха могли да причиняват реални вреди. Същото пък от своя страна неминуемо води до необходимостта от правното регламентиране на юридическата отговорност, която би възникнала в тази връзка. Макар способността на изкуствения интелект да притежава необходимите качества, за да успее да формира интелектуален и волеви момент на вината при извършването на противоправни деяния да е все още спорна, технологичното развитие и постоянната дигитализация на обществените отношения постепенно ще доведат до острата необходимост от изясняването на този придобиващ все по-голям интерес въпрос.

Така наречените „интелектуален момент“ при вината се формира от субекта на правото, който може да носи наказателна отговорност, когато той съзнава характера на извършваното от него противоправно деяние и предвижда настъпването на съответните общественоопасни последици. Важна за интелектуалния момент при вината е способността за формиране в съзнанието на представа за причинно-следствената връзка между деянието и последиците от него.[1] При различните форми на вина формирането на тази представа има своите особености. Самото деяние представлява обективен израз на намерението на дееца да изпълни състава на дадено престъпление. Без обективиране на психичните процеси на дееца, изразяващи се в желание да породи определени противоправни последици, той не би могъл да носи наказателна отговорност, тъй като не е налице каквото и да е материализиране на волята му за предизвикване на отрицателни изменения в

[1] Horwitz, M. (1998) The Rise and Early Progressive Critique of Objective Causation, The politics of law: a progressive critique, 3rd edition.

обективната действителност. За да бъде нанесена телесна повреда например, е необходимо извършителят на деянието да извърши такива действия, които по своята същност засягат нормалното функциониране на тялото на пострадалия от престъплението. Отговорност за извършителя не може да бъде търсена единствено на основата на неговото субективно желание да нанесе телесната повреда, без на практика да се е стигнало до отрицателното повлияване върху телесната неприкосновеност на пострадалия.

Тогава възможно ли е изкуственият интелект да обективира „волята“ си за извършване на престъпление посредством извършване на такива действия, които по своята същност да повлияят върху определени обществени отношения? На този въпрос може да бъде отговорено положително, когато изкуственият интелект е инсталиран например в робот. Докато роботът движи своите ръце или други части от механичната си структура, той може да извърши деяние под формата на действие. Това действие, осъществено от робота, може да е резултат както от самостоятелни изчисления, които се реализират въз основа на действието на изкуствения интелект, но може да бъде резултат и от управлението на робота от страна на човешко същество. Когато роботът бива управляван от човешко същество, той отново извършва действие, но в такъв случай няма как да бъде коментиран въпросът за неговата наказателна отговорност, защото самият факт на управлението му от човек означава, че роботът не формира вина като субективно отношение към извършеното от него противоправно деяние.

Действието и бездействието като начини, по които може да се реализира едно противоправно деяние, се различават. При действието е налице система от телодвижения, които се осъществяват под контрола на съзнанието (при изкуствения интелект думите „телодвижения“ и „съзнание“ имат по-различно съдържание отколкото при физическото лице, като „стандартен“ субект на правото). Бездействието, обратно, представлява непредприемането на действие, което субектът на задължение е трябвало да предприеме, конкретен пример в тази насока може да бъде чл. 139 от Наказателния кодекс.[2] Бездействието по смисъла на правото представлява въздържане от действие, което субектът е бил правно задължен да предприеме. Ако едно физическо лице бездейства, но за него не е налице правно задължение да извърши дадено действие, то това физическо лице няма как да отговаря наказателно за бездействието си. Например лекар, който

[2] Чл. 139 НК (изм. ДВ, бр. 28 от 1982 г., в сила от 01.07.1982 г., изм. ДВ, бр. 10 от 1993 г., изм. ДВ, бр. 92 от 2002 г., изм. ДВ, бр. 103 от 2004 г., в сила от 01.01.2005 г.) – Който при непосредствена опасност за живота на другиго не се притече на помощ, която е могъл да му даде без опасност за себе си или за другиго, се наказва с пробация до шест месеца или с глоба от сто до триста лева.

не окаже медицинска помощ на лице, което спешно се нуждае от такава, ще отговаря за бездействието си. Задължението на лекаря да окаже медицинска помощ не е пожелателно, а произтича от характера на изпълняваната от него професионална дейност, регулирана от Закона за здравето и съпътстващите го подзаконови нормативни актове. Изкуственият интелект би могъл да бездейства (в смисъла на втората форма на деянието – бездействие), защото бездействието изисква от него да не прави нищо. Това бездействие би било противозаконно, когато задължението за действие в конкретния случай е скрепено в правна норма.

Възможността на изкуствения интелект да осъществява и двете форми на деянието означава, че фактически той би могъл да осъществи състава на едно престъпление (от обективна страна). Това обаче не означава, че фактическото осъществяване на деянието е достатъчно, за да може да бъде ангажирана наказателна отговорност спрямо изкуствения интелект, независимо че деянието е предизвикало съответния престъпен резултат. Фактическото поведение на изкуствения интелект трябва да е обвързано с определено негово субективно отношение към извършеното.[3] Тук се явяват затрудненията в разбирането за това как може да бъде дефинирано „субективно отношение“ на изкуствения интелект, защото той не притежава сетивна система, която да функционира като човешката. Хората формират възприятия на базата на външни стимули, които се възприемат от сетивната система (звуци, визуални изображения, студ, топлина и др.).[4] Сигнали за тези външни стимули стигат до мозъка, който ги обработва и благодарение на това човек формира оценка за даден стимул. Външните стимули обикновено са повече от един, което означава, че мозъкът действа в известен смисъл избирателно при тяхното обработване. Т.е. той обработва някои стимули с предимство, като игнорира тези, които в даден момент не се явяват толкова важни. Това става в процеса на насочване на вниманието към информация, която се явява важна в конкретната ситуация. Това не означава, че всяка друга информация спира да бъде обработвана, просто тя остава „на заден план“ до момента, в който ще се превърне във фокус за работата на мозъка. Мозъкът се явява основният фактор в обработването на информация и осъществяването на оценъчен процес.[5] Това може да бъде обяснено и с един стандартен процес като виждането с очи. Мозъкът съз-

[3] Winograd, T. (2006) Thinking Machines: Can There Be? Are We, Derek Pertridge & Yorick Wilks eds.

[4] Gardner, H. (1987) The mind’s new science: a history of the cognitive revolution, Basic Books Inc. Publishers/New York.

[5] Searle, John R. (1984) Minds, Brains & Programs, Department of Philosophy, University of California, Berkeley, Calif.

дава изображението, докато очите са единствено „сензорите“, чрез които информацията стига до мозъка.

От гледна точка на правото, за да може един човек да осъзнава свойството на това, което извършва, е необходимо на първо място да има сензорна система, чрез която информацията да бъде възприета, и на второ място, тази информация да придобие „реален“ вид посредством обработката в мозъка. Ако едно от тези условия липсва, не бихме могли да говорим за способност на физическото лице да формира вина. Реално извършителят на противоправното деяние няма да е наясно с това, което върши, ще се сблъскаме с липсата на причинно-следствена връзка.[6] Налице ли са обаче при изкуствения интелект тези условия за формиране на вина? Притежава ли той както физическото лице сензори, които възприемат информацията, и „мозък“, който да я обработи? Без съмнение изкуственият интелект може да е оборудван с камери, които подобно на очите при човека да възприемат фактически данни от заобикалящата среда. Микрофони пък могат да възприемат звуци и също както камерите да предават информацията към процесорите, които да я обработват.

Изкуственият интелект обаче не притежава биологичен мозък както човека, но притежава изкуствен такъв. Той се състои от процесора, паметта и като цяло хардуерната конфигурация на съответния компютър.[7] Ако например един робот, който функционира на база на изкуствен интелект е създаден с идеята да информира правоприлагащите органи в случай на нарушаване на сигурността на даден обект, този робот ще извърши подобно информиране чрез обработване на данните за нарушителя, възприети посредством хардуерни сензори. Тези сензори трябва да са достатъчно ефективни, за да не объркат правонарушител с правоприлагащ орган (напр. полицейски орган). Роботът може да е кодиран например да различава предполагаеми цветове, които би носил един нарушител и предполагаеми цветове на униформата на правоприлагащ орган. Роботът би могъл да различава звуци и евентуално използвани изречения от правонарушителя или предполагаемото съдържание на заповеди, които се издават от правоприлагащия орган. Т.е. в посочения пример роботът би могъл да възприема фактически данни от заобикалящата го среда, да ги анализира и да създаде изображение на съответния субект, който го интересува за изпълнение на заложените му функции (в случая осъществяването на охранителни мероприятия спрямо определен обект). Следователно може да бъде направен изводът, че един

[6] Stapelton, J. (1988) Law, Causation and Common Sense, Oxford j. legal stud.

[7] Schank, C. R. (2006) What is ai, Anyway?, In the foundations of artificial intelligence 3, 4–6, Derek Pertridge & Yorick Wilks eds.

подобен робот „разбира“ относимата информация, т.е. да е съзнателен. За нуждите на настоящия материал е необходимо да бъде направо уточнението, че вижданията за изкуствения интелект като „съзнателен“ са обвързани с разбиранията на юридическата наука. Тук не говорим за стриктно тълкуване на понятието за съзнание в психологически и/или философски смисъл.

Разбиранията за съзнание в българското административнонаказателно и наказателно право са по-праволинейни, защото са обвързани с постигането на ограничени по своя обем цели, а именно реализиране на съответния вид юридическа отговорност. За да може да понесе юридическа отговорност, едно физическо лице трябва да разбира свойството и значението на извършваното от него и да може да ръководи своите действия. Физическото лице трябва да осъзнава, че чрез действията си влияе отрицателно върху съответното обществено отношение. Разбирането за отрицателно влияние се свързва с мотивите, които извършителят има. Физическото лице може да извършва правонарушението поради „зли“ мотиви. Затова тук възниква въпросът дали изкуственият интелект трябва да формира знание за такова отрицателно влияние върху обществените отношения. Ако под „знание“ се разбира вътрешното усещане, че бива извършвано нещо нередно, то не можем да говорим за такова при изкуствения интелект. Но нужно ли е действително вътрешно усещане, т.е. чувстване, за да е налице знание за отрицателния характер на извършеното противоправно деяние? Отговорът тук следва да е по-скоро отрицателен. Едно физическо лице, извършител на противоправно деяние, може да отговаря на всички изисквания, за да бъде постановен съдебен акт, в който да е отразено становището на съдията, че деецът е действал в условията на пряк умисъл, като форма на вина. Деецът може да отговаря на психологическите изисквания, за да формира пряк умисъл, но това не означава, че той ще се чувства виновен, т.е. че въпреки че е проявил дадена форма на вина, самият той ще изпитва угризения на съвестта или каквито и да било отрицателни чувства. Т.е. чувството, че върши нещо нередно, не е нужно да е налице, за да бъде ангажирана отговорност за противоправното деяние. В кода на изкуствения интелект може да бъде заложено, че извършването на дадено действие от негова страна е „нередно“ и въпреки това той да го извърши, защото именно в кода му да е заложено да извършва „нередни“ неща. В този случай не е нужно изкуственият интелект да се чувства виновен за това, което е извършил, за да понесе юридическа отговорност.

Друг е въпросът за волята. Субектът на едно правонарушение може да желае да настъпят отрицателните последици; да не желае тяхното настъпване; да е безразличен към тяхното настъпване. Тук трудност се явява положението на изкуствения интелект и неговата способност да проявява воля. Разбирането за воля може да бъде различно в различните сфери на човешко познание.

В теологията например волята да бъде направено нещо добро съобразно съответните правила на дадена религия ще се различава от волята да бъде извършено правонарушение (съобразно вижданията на юридическата наука). В правото най-силният израз на волята е намерението/желанието нещо да бъде извършено, съответно да настъпят отрицателните последици (когато волята е насочена към извършването на правонарушение). Желанието да настъпят отрицателните последици може да има различна степен на конкретика в зависимост от осъществения престъпен състав, състав на административно нарушение или състав на дисциплинарно нарушение. Желанието да бъде извършено едно престъпление например може да е с цел да бъде отправено послание към обществото – например при терористичен акт.

Желанието пък да бъде извършено административно нарушение може да е с висока степен на конкретизация по отношение на неговата цел. Например едно лице с правомощия в сферата на обработването и защитата на лични данни да се интересува и неправомерно да обработва личните данни на конкретен гражданин с цел да узнае интимни подробности за нея/него.

Поведението на субекта на правонарушението е юридически укоримо още от момента, в който предприеме действия към постигането на своята цел, но не и от момента, в който противоправните последици възникнат в съзнанието му. Защото каквото и да си представя едно лице, дори и да фантазира как извършва възможно най-зверското престъпление, поведението му не може да бъде санкционирано. Това е така, защото мисълта му не е материализирана по никакъв начин. Той не е започнал процеси (не е създал предпоставки за започването на процеси), които да доведат до отрицателни изменения в обществените отношения. Това, което се случва в неговото съзнание, може да е укоримо по правилата на морала и етиката, но правото защитава това, което се случва в обективната действителност, т.е. това, което има реални материални измерения или още това, което може обективно да бъде възприето не само от този, който осъществява елементите на едно правонарушение, но и от останалите субекти – от пострадалия от правонарушението и от обществото като цяло. За да бъде ангажирана юридическа отговорност, правото изисква волята да бъде превърната в поведение.

Като цяло можем да обособим следните процеси, които водят до материализиране на едно отрицателно поведение. На първо място, възниква идеята за извършване на правонарушението. Субектът може в сравнително спокойна обстановка и при възможност да прецени „хладнокръвно“ мотивите „за“ и „против“ извършването на едно престъпление и да вземе крайното решение да извърши същото. Субектът може внезапно да вземе решение да извърши престъплението. Тази внезапност може да е породена и от това, че

субектът е афектиран от поведението на бъдещата жертва на същото това престъпление. Във всички случаи и варианти, които могат да възникнат, за да кажем, че се е стигнало до взимане на решение за извършване на престъпление, важното е, че самото вземане на решение все още не е основание да бъде ангажирана юридическа отговорност. Дотук обособихме желанието за извършване на правонарушение и вземането на решение за извършването на същото поради наличието на различни по своя характер предпоставки и мотиви. Мотивите за вземането на решение не във всички случаи трябва да бъдат отрицателни, т.е. обществено укорими. Един извършител на грабеж по смисъла на чл. 198 от наказателния кодекс[8] може да вземе решение да извърши това общественоопасно деяние, защото има нужда от парите, за да осигури лечението на свой роднина, който страда от тежко заболяване. Тук мотивът явно води до това поведението на дееца да не бъде в такава степен порицано от обществото, но това не означава, че последиците от взетото решение не влияят по тежък начин върху нормалното протичане на обществените отношение, свързани с гарантирането на правото на собственост. След като деецът си представи измеренията на своето деяние и след като вземе решение да извърши същото, е необходимо реалното поставяне на началото на протичане на отрицателни обществени процеси. От този момент обществото в лицето на правоприлагащите органи вече се противопоставя на поведението на дееца и възпира реализирането на съответното противоправно деяние. Тук следва обаче да направим уточнението, че материализирането на действията при извършването на едно правонарушение не във всички случаи е свързано с материалното влияние върху един обект. Например при обидата по смисъла на Наказателния кодекс[9] думите, които съдържат едно неприятно за обидения послание, нямат материален характер в смисъла, че те не се материализират в изображения извън съзнанието на обидения и в съзнанието на тези членове на обществото, които са чули обидата. Волята за извършване на едно правонарушение не е нужно да бъде добре обмислена. Това означава, че един субект просто може да „чувства“, че трябва/иска да извърши престъплението. Например чувства, че трябва да убие жертвата, защото цялостната му ценностна система го насочва към това, че убийството в случая е справедливо (без интелектуално да осмисля това чувство и субективното

[8] Чл. 198 НК (1) (изм. ДВ, бр. 10 от 1993 г.) – Който отнеме чужда движима вещ от владението на другиго с намерение противозаконно да я присвои, като употреби за това сила или заплашване, се наказва за грабеж с лишаване от свобода от три до десет години.

[9] Чл. 146 НК (1) (изм. ДВ, бр. 28 от 1982 г., в сила от 01.07.1982 г., изм. ДВ, бр. 10 от 1993 г., изм. ДВ, бр. 21 от 2000 г.) – Който каже или извърши нещо унизително за честта или достойнството на другиго в негово присъствие, се наказва за обида с глоба от хиляда до три хиляди лева. В този случай съдът може да наложи и наказание обществено порицание.

разбиране за справедливост). Или пък извършителят на едно административно нарушение чувства, че желае да наруши правилата за движение по пътищата, защото конкретното ограничение на скоростта на конкретната пътна отсечка се явява несправедливо (отново без цялостно да осмисля защо смята, че е налице несправедливост). Не винаги човек може да контролира желанията си, но за да може да ги контролира, той трябва да ги осъзнава. Тоест волята към извършване на едно правонарушение може да бъде осъзната и неосъзната. Когато тази неосъзнатост е резултат от медицинска неспособност на извършителя правилно да оценява заобикалящата го среда, тогава същият се явява невменяем и не може да носи юридическа отговорност. Когато обаче е осъзната, поведението му ще бъде укоримо, независимо че е могъл да се контролира и да не извърши съответното правонарушение, но в конкретния случай самоконтролът му не е бил налице (например при извършването на някой състав на престъпление против половата неприкосновеност).

При изкуствения интелект проявата на воля е въпрос, който зависи от това доколко той може да изпита влечение или липсата на такова към последиците от едно противоправно деяние. Съществуват програми, които много успешно могат да играят и печелят игри на шах. Използваният в тях изкуствен интелект преценява възможните си ходове и прави оценка на ходовете на своя противник. Прецизността, с която такъв тип програми работят, е впечатляваща, а успехите им в игри на шах печелят все по-голяма популярност. Ако един човек играе на шах, се предполага, че той проявява воля към победа. Няма как със сигурност да знаем, че той наистина иска да спечели, но от поведението на тялото му и ходовете, които играчът предприема, можем да направим извод, че цели победа. Когато изкуствен интелект участва в игра на шах, отново можем да направим извод, че цели да спечели, защото всичките му ходове се предприемат, за да може да бъде постигнат крайният успех. От тази изходна позиция можем да твърдим, че подобно на човека изкуственият интелект проявява воля към постигане на победа. Т.е. за да говорим за проява на воля, можем да вземем предвид следното: един човек/изкуствен интелект, който преценява няколко различни възможности и избира съзнателно една от тях, очевидно прави това, защото желае чрез конкретно избраната опция да бъде постигнат крайният резултат – независимо дали той е обществено-приемлив или общественонеприемлив. Предвиждането на настъпването на противоправни последици е свързано с проявата на воля от страна на субекта. Когато един робот движи своята стоманена ръка с цел да удари едно човешко същество, защото така е програмиран, тогава той предвижда, че чрез удара ще постигне целта, за която е програмиран (както казах, например да нарани един човек). Изкуствен интелект, който се използва за робот, който например е създаден за нуждите на армията, може с много по-голяма точност да

прецени, че изстреляният от държано от него оръжие куршум би довел до настъпването на смъртта на един човек, отколкото един човек би могъл да прецени това спрямо друг човек.

Вижданията за проявата на воля от страна на изкуствения интелект, които са описани дотук, следва да бъдат взимани предвид в контекста на юридическата наука. Нормално е за някои читатели думите „воля“ и „желание“ да бъдат отхвърляни, когато става въпрос за изкуствен интелект. По-широкото виждане за воля и желание, с които сме запознати като качества, проявявани от човешки същества, трябва да бъде преценявано по различен начин, когато става въпрос за изкуствен интелект. Правото е наука, която се занимава с постигането на точно определени цели посредством регулирането на законосъобразното развитие на обществените отношения в различните сфери на обществения живот. Затова и понятията, които се използват в юридическата наука, са строго обвързани с нейните цели. Когато говорим за доказателства, чрез които трябва да бъде анализирано доколко е проявена воля от страна на изкуствен интелект, трябва да имаме предвид, че за анализиране на тези доказателства трябва да имаме пълен достъп до процесите на вземане на решения в конкретната машина. Тук положителна се явява възможността за пълен достъп до компютърните архиви на дадената компютърна информационна система. Нещо, което не може да стане по отношение на човешкия мозък (или поне не на този етап от развитие на обществото). Във всички случаи, след като успешно бъдат анализирани съответните доказателства, бихме могли да ангажираме съответният вид отговорност. Тук възникват редица нови въпроси по отношение на това кой следва да понесе отговорността за действията/бездействията, проявени от страна на изкуствения интелект, които се явяват противоправни. Защото поначало наказателната и административнонаказателната отговорност са лични. Тоест само субектът, който е извършил престъплението/административното нарушение, може да понесе съответния вид отговорност. Но какво се случва, когато изкуственият интелект е програмиран от човек да действа или бездейства по определен начин и при определени условия? Тогава по-логично е да мислим, че отговорността трябва да бъде понесена от този, който е програмирал ИИ. Но това отново крие неизвестности, защото не програмиращият е извършил лично действията, които са довели например до смъртта на някого. Аналогично един родител няма да носи отговорност за извършено от неговия пораснал син или дъщеря престъпление само защото ги е възпитавал да бъдат агресивни. Това, че той е създал погрешни представи у тях за някои обществени процеси, не означава, че лично той е извършил дадено престъпление. За да се даде конкретен отговор на въпроса за личната отговорност при изкуствения интелект, е необходимо да продължат изследванията относно това доколко действията, които той е

извършил, са резултат от постоянния процес на учене/оценяване на нова информация. Не бива да забравяме, че изкуственият интелект е първоначално кодиран от човек, но през времето на своето съществуване самостоятелно се учи и открива различни начини на разсъждение и различни ценности, чиято валидност и тежест непрекъснато преценява.

Заключение

Темата за изкуствения интелект и все по-широкото му навлизане във всяка една обществена сфера, включително и в обществените отношения, отнасящи се до правоотношенията между лицата, както на публичноправо ниво, така и в частноправната сфера, поставя акцент върху необходимостта от изясняването на все още неясните момент, свързани с изкуствения интелект в неговата цялост. Въпросите, свързани с формирането на вина при извършването на противоправни деяния от страна на изкуствения интелект са само един от аспектите, които предстои да се наложи да бъдат засегнати с цел избягване възникването на правни усложнения в бъдеще. С оглед постоянната динамика в развитието на съвременния свят, произтичаща както, от една страна, от дигиталните технологии, така и от друга, от контекста на съвременните правоотношения, следва да бъде обърнато сериозно внимание на разгледаните по-горе въпроси. Навременното създаване на правна регулация и запълването на наличните към момента празноти в правото по тематиката, свързана с изкуствения интелект, утвърждаването на понятието за електронно лице и законовата регламентация на юридическата отговорност на същото са само част от стъпките, които могат да бъдат предприети.

Библиография:

1. Gardner H. (1987), *The mind's new science: a history of the cognitive revolution*, Basic Books Inc. Publishers/New York.
2. Horwitz M., (1998), *The Rise and Early Progressive Critique of Objective Causation*, The politics of law: a progressive critique, 3rd edition.
3. Schank C. R. (2006), *What is ai, Anyway?*, In the foundations of artificial intelligence 3, 4 – 6, Derek Pertridge & Yorick Wilks eds.
4. Searle John R. (1984), *Minds, Brains & Programs*, Department of Philosophy, University of California, Berkeley, Calif.
5. Stapelton J. (1988), *Law, Causation and Common Sense*, Oxford j. legal stud.
6. Winograd T. (2006), *Thinking Machines: Can There Be? Are We*, Derek Pertridge & Yorick Wilks eds.

Предизвикателства пред наказателноправната закрила на подрастващите при използването на информационните технологии

Гергана Андонова*

Информационните технологии стават все по-развити и трансформират всички сфери на обществения живот, като предлагат нова дигитална култура не само на възрастните, но и на подрастващите. Ненавършилите 18-годишна възраст следва по необходимост да овладеят актуалните тенденции в усъвършенстването на компютърните технологии, тъй като те вече се използват като платформа за образование, забавление и социална комуникация.

Действително използването на електронното пространство сред подрастващите има толкова много положителни страни като виртуални класни стаи, разширяване на социалните кръгове, увеличаване на визуалното мислене, креативността и подобряване на техническите умения и самочувствието. Не може да се пропусне обаче и обстоятелството, че цифровите технологии имат не само положителен, но и отрицателен ефект върху психическото и физическото развитие на младото поколение. Дори научните изследвания показват, че отрицателното въздействие е много по-силно от положителното им влияние. Прекомерната употреба на социалните медийни платформи може да доведе до различни негативни последици – кибертормоз, ниско самочувствие, пристрастяване към игри и др. Електронната среда и електронните устройства нанасят достатъчно сериозни и трудно поддаващи се на обобщение вреди при формиране на личността на подрастващите. Различни видеоигри в социалните платформи, музикални видеоклипове и филми, в които се демонстрира открито насилствено поведение, повишават агресията и тревожността сред подрастващите. Подобно влияние на информационните технологии е един от факторите, които водят до формиране или задълбочаване на техните противообществени прояви.

Потребността от наказателноправна защита на обществените отношения във виртуалното пространство е отразена от законодателя в правните конструкции на престъпните състави, които все още не обхващат пълноценно всички форми на незаконното и неправилно експлоатиране с електронната информация, засягащи интересите на подрастващите.

Ключови думи: *информационни технологии, наказателноправна закрила, непълнолетни*

* Главен асистент, д-р, Правно-исторически факултет към Югозападен университет „Неофит Рилски“, ел. поща: gergana_andonova@law.swu.bg.

Challenges to the criminal protection of adolescents in the use of information technologies

Gergana Andonova*

Information technologies are becoming more and more developed and transforming all spheres of public life, offering a new digital culture not only to adults, but also to adolescents. Adolescents must necessarily master the current trends in the advancement of computer technology as it is already being used as a platform for education, entertainment and social communication.

Indeed, the use of electronic space among adolescents has so many positives such as virtual classrooms, widening social circles, increasing visual thinking, creativity and improving technical skills and self-esteem. However, the fact that digital technologies have not only a positive but also a negative effect on the mental and physical development of the young generation cannot be overlooked. Even scientific studies show that the negative impact is much stronger than their positive influence. Excessive use of social media platforms can lead to various negative consequences-cyberbullying, low self-esteem, gaming addiction, etc. The electronic environment and electronic devices cause sufficiently serious and difficult to generalize damages in the formation of the personality of adolescents. Various video games on social platforms, music videos and movies that demonstrate overtly violent and sexual behavior increase aggression and anxiety among adolescents. Such an influence of information technologies is one of the factors that lead to the formation or deepening of their anti-social manifestations.

The need for criminal protection of public relations in the virtual space is reflected by the legislator in the legal constructions of criminal structures, which still do not fully cover all forms of illegal and improper exploitation of electronic information affecting the interests of adolescents.

Keywords: *information technology, criminal protection, juveniles*

* Chief Assist. Prof., PhD, Faculty of Law and History, South-West University "Neofit Rilski", e-mail: gergana_andonova@law.swu.bg.

Интернет и другите достижения на информационните технологии предоставят изключително големи възможности за търсене, анализ и споделяне на информация, но същевременно водят и до множество деяния, които драстично накърняват правата на подрастващите – изпращане на заплашителни съобщения, преследване през електронните устройства, разпространение на материали с порнографско съдържание и др.

Взаимодействието на подрастващите с информационните технологии и излъчваните от тях послания оказва много по-дълбоко и сериозно влияние върху техните *разбирания и емоции,* отколкото се предполага при по-ранни изследвания на влиянието на електронната среда върху психиката им.[1]

Особено разпространено през последните години е умишленото и многократно осъществяване на негативно въздействие по отношение на лица, навършили 15, 16 и 17-годишна възраст. Технологичните възможности на сайтове на социални медии в интернет и социални медийни платформи, особено Facebook (Facebook Messenger, Facebook Watch), за съжаление, се използват за осъществяване на *психическо насилие по отношение на непълнолетни лица (cyberbullying).* Много често тези деяния включват не само директни вербални заплахи, но и заплахи чрез качване в електронна среда на видеоклипове с подобно съдържание. Осъществяват се също и индиректни действия на манипулиране на приятелства и целенасочено изключване на непълнолетни от определени дейности в електронна среда. Разпространено сред подрастващите е и *преследването в електронното пространство (cyberstalking).*[2] Използват се интернет, имейли или други електронни комуникационни средства за преследване на подрастващи.

Особено обезпокоително е и обстоятелството, че много от тези деяния се извършват също от лица, ненавършили 18-годишна възраст, което в значителна степен променя концепцията за личността на непълнолетния извършител.

Изясняването на въздействието и ролята на цифровите технологии в живота на подрастващите осигурява по-задълбочено разбиране за това как цифровите технологии влияят върху личността им и допринася за изясня-

[1] Bell, D.R., Tokovska, M., Eg, R. (2021) Exploring Adolescents Experiences with Personalized Content on Social Media: A Qualitative study. Journal of Adolescents and Adult Literacy [online], vol.10 (4), 1-10 [viewed 10 June]. Available from: https://www.researchgate.net/journal/Journal-of-Adolescent-Adult-Literacy-1936-2706

[2] Siegel, L. J., Welsh, B. (2015). Juvenile Delinqency. Theory, practice and law. United States: Cengage Learning.

ване на проблемите, които възникват при използването на тези технологии от младежите.

Огромните бази данни, възможностите за търсене и анализ, изкуственият интелект (AI), телекомуникационните мрежи са мощно средство за развитието на обществените отношения. Концепцията за информацията, съхранявана в електронна форма, е значително по-сложна и възможностите за нейното създаване, насочване и пренасочване са много големи. Създаването на информационните технологии е резултат от продължителната еволюция на обществените отношения и сложните процеси по изграждането на дигиталните технологии. Електронната форма осигурява бърз и евтин обмен на информацията без оглед на нейния обем и разстоянията. Създадени са и гаранции за сигурността на информацията. Всички тези особености на електронното изявление го превръщат и в източник на отрицателно въздействие върху подрастващото поколение (насилие, преследване, разпространение на информация с неморално съдържание и др.). Двойствените възможности на електронното общуване водят и до амбивалентни преживявания при младежите.

Характерните за съвременното общество форми на общуване, свързани с информационните технологии, не винаги съдействат за тяхната успешна социализация. Действително, те са мощно средство за осъществяване на връзки и приятелства. Общуването в електронното пространство помага на подрастващите да *повишат* увереността си, дава им възможност да се почувстват значими и желани в референтната група от виртуални приятели. Особено привлекателни за ненавършилите 18-годишна възраст са възможностите за получаване на много и интересна информация, развиването на технически умения и на въображението. Електронното общуване разнообразява социалния живот на подрастващите и до известна степен редуцира стреса и психичния дискомфорт, които биха могли да възникнат при реалното общуване. Същевременно информационните технологии имат и своето *отрицателно влияние върху психиката на подрастващите.* Сравнително свободният достъп до информация им позволява да се запознават и с такава, която не е подходяща за тяхната правилна интелектуализация и емоционално развитие. Развлекателният характер на информацията в интернет, както и не особено сложното ѝ и издържано съдържание водят до ограничаване на мисловните процеси и понижаване на чувството за отговорност. Електронното пространство осигурява на подрастващите възможност да реализират защитния механизъм на его-бягството от действителността, като се изолират от реалния свят с неговите емоционални проблеми (стрес,

безпокойство, учебна натовареност и др.). Това обаче възпира развитието на тяхната личност, която ограничава уменията си за преодоляване на трудности и на възможностите за справяне с житейските ситуации. Под влияние на информационните технологии се формират специфични форми на зависимости, свързани с интернет търсене на информация от различни бази данни, изграждане на виртуални взаимоотношения, в основата на които е като цяло зависимостта към използване на електронни устройства.[3]

Продължаващото увеличаване на т.нар. „електронно време“, което прекарват подрастващите, предизвиква голяма загриженост и тревога сред изследователи и практикуващи специалисти в редица научни области.

Научните изследвания в глобален аспект са особено детайлни по отношение на това как лицата от 15- до 18-годишна възраст използват социалните медийни платформи и какво е влиянието на последните върху структурата на младата личност. Медийното потребление вече не е пасивен процес, но взаимен и активен процес на информация, което поставя изисквания и към дигиталната компетентност на тази възрастова група, свързана с технологиите на социалните медии. От значение е също така и как се ориентират потенциално уязвимите подрастващи в техните персонализирани интернет реалности и какъв е опитът им с *персонализираното съдържание в социалните медии*.[4] Изследванията акцентират и върху корелациите между времето пред екрана и психичното здраве на подрастващите, т.е. как те преживяват социалните медии. Основните причини за присъединяване към социалните медии, които подрастващото поколение споделя, са необходимостта да поддържат връзка с приятелите, както и страх да не бъдат отхвърлени от общността, към която принадлежат. Повечето от тях предприемат действия за проучване на персонализирано съдържание предимно под влияние на приятели и по-рядко на инфлуенсъри.

Осъзнаването и разбирането за целевото и персонализираното съдържание се различава до известна степен в зависимост от пола и възрастовите групи. Участниците от 17 до 19 години изразяват по-широко

[3] По тези въпроси вж по-подробно Чонова, Р., Ганева, В. (2008) Свободното време на подрастващите в новата информационна среда. В: Смикаров, А., Везиров, Ч., В. Иванов, Ю. Попова, съст. Научни трудове на Русенския университет. Русе: Русенски университет „Ангел Кънчев“, 94–98.

[4] Bell, D. R., Tokovska, M., Eg, R. (2021) Exploring Adolescents Experiences with Personalized Content on Social Media: A Qualitative study. Journal of Adolescents and Adult Literacy [online], vol.10 (4), 1-10 [viewed 10 June]. Available from: https://www.researchgate.net/journal/Journal-of-Adolescent-Adult-Literacy-1936-2706

разбиране и по-голяма осведоменост за целевото и персонализираното съдържание в сравнение с по-ниските възрастови групи. Наред с това по-широко разбиране и по-голяма осведоменост за посоченото съдържание на социалните медии (платформи) се наблюдава при подрастващите от женски пол в сравнение с тези от мъжки пол.[5] Повечето от тази възраства група споменават, че са наблюдавали целенасочено и персонализирано съдържание в популярните социални медийни платформи (преди всичко TikTok и Facebook) още преди да им бъдат поставени въпроси, свързани с персонализиране. Установено е, че някои от алгоритмите, които персонализират съдържанието, се разпознават по-лесно от други. Например, когато са означени като „предложения за Вас“, съдържанието може да бъде по-лесно разпознато като персонализирано в сравнение с по-фината, по-завоалирана персонализация. Съдържанието в социалната медийна платформа TikTok е уникално подбрано и съобразено с индивидуалните предпочитания на потребителите. Същевременно са налице онлайн действия, водещи да целенасочено рекламиране в различни платформи (например новинарския канал на Facebook), което води до смесване на комерсиално и обикновено съдържание и за подрастващите може да е трудно да разграничат дали са повлияни от социалните медии.

Повечето от участниците обобщават, че им е харесало проучването на специализирано съдържание, защото то е имало уместно и интересно съдържание и смятат, че то има положително влияние върху тяхното ежедневие. Не биха могли да бъдат пренебрегнати и противоположните емоции, които това съдържание предизвиква в потребителите, ненавършили 18-годишна възраст. Някои заявяват, че не приемат добре целево и персонализирано съдържание. Тревожните преживявания на подрастващите са свързани с това, че приложенията кумулират информация за техните интереси чрез проследяване във виртуалното пространство. Някои от участниците имат амбивалентно отношение към персонализираното съдържание, което произтича от това, че те не могат да контролират всички ситуации и не винаги попадат на приемливо съдържание.[6]

Подобни преживявания на подрастващите показват, че те *не са достатъчно дигитално компетентни*, тъй като платформите имат и опция за премахване на избора или блокиране на съдържание. Тенденцията да се

[5] Ibidem.

[6] Young, S., Greer, B., Church, R. (2017) Juvenile delinquency, welfare, justice and therapeutic interventions: a global perspective. BJPsychBulletin, № 2, 21–29.

игнорира, а не да се блокира съдържанието отразява липсата на критичност, рефлексия и дигитална компетентност. В този смисъл персонализираното съдържание оформя дигиталната култура на подрастващите както в положителна, така и в отрицателна насока.

Сериозна загриженост в глобален аспект предизвикват и някои много сериозни прояви на подрастващите, които са обществено опасни и водят до използването на информационните технологии за извършването на престъпления. Значителната свобода и анонимността във виртуалното пространство в съчетание с недостатъчните етични стандарти в личността на подрастващите са предпоставка за въвличането им в редица обществено опасни и противоправни деяния и взаимодействия. Дори в някои по-развити държави, като например САЩ, вече се смята, че съществува *фигурата на извършващия компютърни престъпления непълнолетен* и необходимо федерално преследване на непълнолетни за компютърни престъпления. Този извод се налага от наказателноправния и криминологичния анализ на следните деяния с по-висока степен на обществена опасност. Младеж на 16 години от окръг Честърланд, Вирджиния, прониква в системата на интернет доставчика в щата Масачузетс и причинява имуществени вреди на стойност над 20 000 долара. Двама непълнолетни на 15 и 17-годишна възраст създават подправени парични знаци с помощта на компютърните технологии в окръг Бедфорд, Вирджиния. Извършители на някои по-драстични прояви са и малолетни лица. Момче на 13 години от Помпона, Калифорния, отправя заплахи чрез използване на компютър към 13-годишно момиче. Малолетният извършител създава уебсайт, който включва игра със снимка с надпис: „Побързайте! Кликнете на спусъка, за да я убия!“. Уебсайтът включва и петиция, призоваваща за нейната смърт.[7]

Подобни тенденции се наблюдават и в нашата страна, макар такива деяния да не се реализират в такъв обем и с толкова сериозни обществено опасни последици, както в развитите либерални демокрации.[8] Така 16–17-годишни момчета са проникнали в системата за експериментално машинно гласуване през 2015 г.[9] Непълнолетен ученик от Русе през 2021 г. е

[7] Artur, L., Bowker, M. A. (1999) Juveniles and computers: Should We Be Concerned? *Uscourts,* № 40, 40–43 [online] [viewed on 16 June 2023]. Available from: https://www.uscourts.gov/sites/default/files/63_2_7_0.pdf

[8] Национален статистически институт на Република България [онлайн] [прегледан на 16.06.2023]. Достъпен на: www.nsi.bg

[9] Непълнолетни хакери са пробили системата за експериментално машинно гласуване. Questona. [онлайн], 25 август 2015 [прегледан на 16.06.2023]. Достъпен на: https://questona.com/nepalnoletni-hakeri-sa-probili-sistemata-za-mashinno-glasuvane/

осъществил хакерска атака на профили на хора от различни населени места на страната и е използвал данните от дебитните им карти, за да извършва покупки от интернет.[10]

Множество фактори в своето съчетание водят до извършване на престъпни деяния от подрастващите през електронните устройства. На първо място, непълнолетните са технологично много по-развити в сравнение с предходните поколения. Технологичните открития като персоналния микрокомпютър и интернет вече играят ролята и на фактори за развитието на личността. В резултат на това съвременните млади хора овладяват и използват потенциала на новите технологии. Същевременно лицата, ненавършили 18-годишна възраст, не са овладели в достатъчна степен *етичните правила* по отношение на използването на информационните технологии.

Както и при другите видове противообществени прояви, един от основните фактори за компютърната престъпност сред непълнолетните е общуването с приятели, които извършват такива престъпни деяния. Приятелският кръг е по-склонен да споделя такъв опит и да провокира включването в онлайн игри, програми и технологии. С навлизането на интернет обаче връстниците вече не оказват толкова силно влияние. В съвременните условия многобройни уебсайтове провокират педофилия, разпространение на наркотици, омраза и формиране на расистки групи. Освен това има уебсайтове и чат стаи, които са посветени или най-малко имплицитно подкрепят проникването в компютърни системи.[11]

Очевидно правилният подход е да се вземат превантивни мерки и да се предпазят подрастващите от гравитиране към компютърната престъпност. Информационните системи и социалните платформи предоставят на извършителите многобройни възможности, които не са съществували в близкото минало. Използването на компютри през интернет може да прикрие възрастта и създава степен на анонимност, която не е съществувала преди. Това също разширява обхвата и възможностите за делинквентно поведение сред ненавършилите пълнолетие извършители.

Очевидно най-добрият подход е да се вземат превантивни мерки и да се предпазят подрастващите от гравитиране към компютърната прес-

[10] Непълнолетен ученик от Русе е хакнал онлайн чужди дебитни карти. РусеМедиа [онлайн], 21 юни 2021 [прегледан на 16.06.2023]. Достъпен на: https://www.rusemedia.com/

[11] Artur, L., Bowker, M. A. (1999) Juveniles and computers: Should We Be Concerned? *Uscourts,* № 40, 40–43 [onlain] [viewed 16 June 2023]. Available from: https://www.uscourts.gov/sites/default/files/63_2_7_0.pdf

тъпност. Изключително бързото навлизане на компютрите, софтуеъра и свързаните технологии в домакинствата, училищата и институциите води до необходимост от изучаване на технологиите и как те да бъдат използвани. Необходимо е в обучението на подрастващите да се постави акцент върху етичните ценности, свързани с използването на информационните технологии – уважение към другите, тяхната собственост и право на личен живот. Необходимо е и включването в учебната програма на уроци относно етиката при използване на информационните технологии и проявните форми на компютърната престъпност, за да могат подрастващите ясно да разграничат правилното използване на компютърните технологии от деянията с висока степен на обществена опасност, които накърняват неприкосновеността на компютърните информационни данни.

Особено внимание се отделя на правата на децата в електронна среда в Общ коментар 25 от 2021 г. към Конвенцията на ООН за правата на детето.[12]

В посочения коментар е проучено и мнението на подрастващите, които обобщават, че цифровите технологии заемат изключително важно място в техния живот и че от информационните технологии до голяма степен зависи и тяхното бъдеще. Тези изводи се потвърждават и от развитието на обществените отношения, тъй като електронната среда непрекъснато се усъвършенства и развива, обхващайки информационни и комуникационни технологии, включително цифрови мрежи, съдържание, услуги и приложения, свързани устройства и среди, виртуална и разширена реалност, изкуствен интелект, роботика, автоматизирани системи и алгоритми и анализ на данни, биометрия и технология на имплантиране и др. Същевременно децата, които участват в консултирането, изразяват загриженост за безопасността на дигиталната среда и изискват от държавите, технологичните компании и училището да им създадат условия за управление и ограничаване на ненадеждната информация онлайн.

В съответствие с притесненията на подрастващите Общият коментар подлага на анализ доколко са защитени правата на детето в електронна среда с оглед специфичните особености на информацията и изявленията в електронна форма. Коментарът обобщава докладите на държавите – страни по Конвенцията, юриспруденцията на органите по правата на човека, препоръките на Съвета по правата на човека и специалните процедури на Съвета. Коментарът е съобразен и с други общи коментари на Комитета

[12] General comment No. 25 (2021) on children,s rights in relation to the digital environment. [onlain] [viewed 17 June 2023] Available from: https://docstore.ohchr.org/

и неговите насоки относно прилагането на Факултативния протокол към Конвенцията относно продажбата на деца, детската проституция и детската порнография.

Фундаменталните изводи, залегнали в общите принципи са, че правата на детето трябва да се зачитат, защитават и осъществяват и в цифровата среда. Защитата на правата на децата в електронна среда е анализирана от гледна точка на *принципите на недискриминация, най-добрия интерес на детето, правото на живот, оцеляване и развитие, уважение към възгледите на детето.*

Правото на недискриминация изисква държавите членки да гарантират, че всички деца имат равен и ефективен достъп до цифровата среда по начини, които са значими за тях. Това включва предоставяне на безплатен и безопасен достъп за деца на специални обществени места и инвестиране в политики и програми, които подкрепят достъпа на всички деца до цифровите технологии в образователната среда, в общността и в домовете им. Децата могат да бъдат дискриминирани, като бъдат изключени от използването на цифровите технологии и услуги или чрез получаването на *неподходящи съобщения или чрез несправедливо отношение при използването на тези технологии.* Други форми на дискриминация могат да възникнат, когато автоматизирани процеси, които водят до филтриране на информация, профилиране или вземани на решения, се основават на необективни, частични или несправедливо получени данни относно дете. Необходимо е и преодоляване на дискриминацията в електронното пространство, основаваща се на дискриминационни критерии.

Най-добрият интерес на детето в електронна среда според Коментара е динамична концепция, която изисква оценка, подходяща за конкретния контекст. Държавите членки трябва да гарантират, че във всички действия, свързани с използването на цифровата среда, най-добрият интерес на детето е от първостепенно значение. При отчитане на най-добрия интерес на детето те трябва да зачитат всички права на децата, включително правата им да търсят, получават и предават информация. Необходимо е също, съобразно коментара, националните и местните органи на държавите членки да следят за спазването на правата на децата при подобни действия.

В коментара се обобщават и рисковете, свързани с взаимодействието с електронната среда – информация с насилствено и сексуално съдържание, киберагресия и тормоз, подбуждане към самоубийство, въвличане в организирани престъпни групи за извършване на терористични действия и

др. В заключение се посочва, че следва да се избегне вредното използване на информационните технологии. Постигането на тази сложна цел изисква да се обърне специално внимание на въздействието на технологиите в най-ранните години от живота, когато пластичността на мозъка е много голяма и социалната среда, по-специално отношенията с родителите, са от решаващо значение за оформяне на конгнитивното, емоционалното и социалното развитие на децата.

В българския Наказателен кодекс[13] са регламентирани редица състави на престъпления, свързани с компютърни информационни данни, които гарантират наказателноправна защита при използването на информационните технологии. Законните състави на компютърна измама (чл. 212а НК), както и тези на компютърните престъпления (гл. IXа от Особената част на НК) предоставят достатъчно всеобхватна наказателноправна защита на обществените отношения, гарантиращи нормалното функциониране на компютърните системи и технологии. Те безспорно отразяват актуалността, важността и значимостта на проблема за компютърната престъпност в съвременните обществени условия в нашата страна.

На първо място, съставите на компютърната измама и компютърните престъпления отразяват обстоятелството, че престъпните деяния накърняват съществени обществени отношения – те засягат стопанството, икономиката, търговските отношения, функционирането на държавните и обществените институции, отношенията, свързани със създаването, ползването и опазването на документите. На второ място, някои от признаците на законните състави отразяват обстоятелството, че неправомерният достъп до компютърна информация в електронна форма се използва и за извършването на други престъпления. Така организираната престъпност използва все повече различни информационни технологии – от обикновени персонални компютри до глобални информационни мрежи, включително и интернет.[14] На трето място, възможностите на компютърните технологии позволяват дистанционно извършване на престъпления, без да е необходимо физически да се проникне в помещенията на учреждения, предприятия и организации, за да се получи достъп до съответната база данни. [15]

[13] Обн. ДВ, бр. 26 от 2.04.1968 г., в сила от 01.05.1968 г., посл. изм. ДВ, бр. 10 от 31.01.2023 г.
[14] Kerr, S. (2022) Computer Crime Law. United States: West Academic Publishing
[15] Hill, J., Marian, N. (2016) Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century. United States: Praeger Security International.

Анализът на правната регламентация на компютърната измама и на компютърните престъпления показва, че инкриминирането на този нов вид деяния не осигурява достатъчно адекватна защита на обществените отношения. Признаците на законните състави все още *не отразяват достатъчно пълноценно техническите специфики на информационните технологии.* В този смисъл липсва и достатъчно адекватна наказателноправна закрила и в случаите, в които непълнолетните лица са извършители или пострадали от подобни деяния. Създаването на електронната форма качествено променя съдържанието на понятието „средства за осъществяване на престъпното деяние“, изменя и неговия обхват и начин на осъществяване. Концепцията за електронната форма и среда е по-сложна и тези особености би трябвало да заемат основно място при криминализирането на престъпните деяния.

Същевременно законните състави *не отчитат и особеностите на престъпното поведение на подрастващите*, доколкото последните имат наказателноправно значение. Неправомерният достъп до информационни системи от непълнолетни извършители обикновено се осъществява без особени затруднения, като същевременно в някои случаи води до съществени обществено опасни последици. Подрастващите са способни да проникнат в информационните системи, гарантиращи осъществяването на дейности, които са от обществен интерес. Наред с това те проникват и в данни от електронните профили на отделни хора, като злоупотребяват с тях. Престъпните действия най-често се осъществяват под формата на хакерски атаки, което свидетелства за изключителната дързост на подрастващите.

Ето защо е уместно законните състави на компютърните престъпления да отразяват подхода на непълнолетните извършители при извършване на тези специфични престъпни деяния, както и особеностите на тяхната личност. Непълнолетният извършител на компютърни престъпления, наред с непосредствената цел за проникване и манипулиране на компютърни информационни данни, много често се стреми да извлече и облага от противоправното манипулиране. Това показва, че личността на подрастващия извършител на компютърни престъпления е с по-висока степен на обществена опасност в сравнение с непълнолетните извършители на други категории престъпления.

Заключение

Необходимо е да се осигурят ефективни механизми за защита на подрастващите при използване на информационните технологии и в електронна среда. Те следва също така да гарантират защитата на правата на децата в електронна среда. Проникването в компютър или електронна мрежа през хакерска атака е възможно да създаде много голям риск за обществените отношения и е необходимо непълнолетните извършители на подобен род деяния да бъдат преследвани по подходящ начин.

Активното използване на социалните медии от подрастващите неизбежно оказва влияние върху тяхната *осъзнатост, разбиране и емоции.* Взаимодействието със социалните медии и изобщо с информация и послания в електронна форма е предмет на особена загриженост и научни изследвания, а в някои държави и на законодателна инициатива. Използването на информационните технологии е особено обезпокоително поради увеличаването на т.нар. „електронно време“, а и поради недостатъчната дигитална компетентност на някои от тази възрастова група, поради което те по-лесно могат да бъдат въвлечени в престъпления или да станат жертва на такива.

Законните състави на компютърните престъпления съгласно НК на Република България не отразяват в достатъчна степен специфичните особености на компютърните системи и мрежи. Поради това тези състави не могат да обхванат достатъчно пълноценно всички деяния, осъществени от непълнолетни по отношение на информационните технологии, както и личностните особености на извършителите.

Библиография:

1. Чонова, Р., Ганева, В. (2008) *Свободното време на подрастващите в новата информационна среда.* В: Смикаров, А., Везиров, Ч., В. Иванов, Ю. Попова, съст. Научни трудове на Русенския университет. Русе: Русенски университет „Ангел Кънчев“.
2. Artur, L., Bowker, M. A. (1999) Juveniles and computers: Should We Be Concerned? Uscourts, № 40, 40-43.
3. Bell, D. R., Tokovska, M., Eg, R. (2021) Exploring Adolescents Experiences with Personalized Content on Social Media: A Qualitative study. Journal of Adolescents and Adult Literacy online, vol.10 (4), 1–10.
4. Hill, J., Marian, N. (2016) Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century. United States: Praeger Security International.
5. Kerr, S. (2022) Computer Crime Law. United States: West Academic Publishing.
6. Siegel, L. J., Welsh, B. (2015) Juvenile Delinqency. Theory, practice and law. United States: Cengage Learning.
7. Young, S., Greer, B., Church, R. (2017). Juvenile delinquency, welfare, justice and therapeutic interventions: a global perspective. BJPsychBulletin, vol.2, 21–29.

Етични и правни нарушения при използването на AI срещу публични фигури за целите на черния PR

Радостина Михайлова*

Въвеждането на някои AI приложения за анализ на средата и синтезирането и обрботването на огромни по обем компресирани (и не само) данни информация, като Deepfake Voice Generators и Deepfake Video Maker, би могло грубо и неправомерно да разруши имиджа на публични фигури от обществено-политическия ни живот и да доведе до тежки репутационни и лични кризи и нарушаване на личните им свободи. Този факт е в разрез с конкретни права, които FRA идентифицира и публикува още през 2018 г.; с Етичните насоки за използването на AI от 2021 г. и действащия Регламент (ЕС)2016/697. Въпреки приетата Концепция за развитието на AI в България до 2030 г., правната регулация, свързана с човешките права в този контекст, все още е проблематична.

***Ключови думи**: AI, Deep fake Voice Generators, Deep fake Video Maker, FRA, PR, публичен имидж, човешки права*

* Радостина Михайлова, главен асистент доктор, Правно-исторически факултет, Югозападен университет „Неофит Рилски“,
ел. поща: radost_mihaylova@swu.bg; rkm72@abv.bg

Ethical and legal violations in using ai against public figures for black pr purposes

Radostina Mihaylova*

The introduction of some AI applications for analyzing the environment and synthesizing and processing huge volumes of compressed (and not only) data information, such as Deepfake Voice Generators and Deepfake Video Maker, could grossly and unlawfully destroy the image of public figures from our socio-political life and lead to severe reputational and personal crises and violation of their personal freedoms. This fact is in contrast to specific rights that FRA identified and published back in 2018; with the Ethical Guidelines for the Use of AI from 2021 and the current Regulation (EU) 2016/697. Despite the adopted Concept for the development of AI in Bulgaria until 2030, the legal regulation related to human rights in this context is still problematic.

Keywords*: AI, Deep fake Voice Generators, Deep fake Video Maker, FRA, PR, public image, human rights*

* Radostina Mihaylova, Chief Assistant PhD, Faculty of Law and History, Southwest University "Neofit Rilski",
e-mail: radost_mihaylova@swu.bg; rkm72@abv.bg

Изкуственият интелект (Artificial Iintelligence) обхваща компютърни системи, които са в състояние да изпълняват задачи, изискващи човешки интелект, като решаване на проблеми, вземане на решения, учене и разбиране на език – човешки или изкуствено програмиран.

Според европейското законодателство Artificial Iintelligence е системи с интелигентно поведение, което се изгражда на базата на анализ на големи обеми от данни, взети от тяхното обкръжение, които са способни да действат с известна степен на автономност в името на някакви предварително зададени специфични цели, като тези системи могат да бъдат софтуерно или хардуерно базирани – първият тип действа във виртуалното пространство, вторият – в интернет приложения, дронове, роботи и др. подобни.[1]

Хардуерно базираните системи са реактивни. Те са най-старите форми на AI системи, които имат изключително ограничени възможности. Те подражават на способността на човешкия ум да реагира на различни видове стимули и нямат функционалност, която да е базирана на паметта. Следователно подобни системи не са в състояние да натрупват информация и да се базират на предишен опит, за да форматират действията си, а само реагират автоматично. Популярен пример за реактивна AI система е Deep Blue на IBM, която победи на шах Гари Каспаров през 1997 г.

Софтуерно базираните системи, от своя страна, са с ограничена памет и освен че могат да са реактивни, са способни да се обогатяват непрекъснато от вече натрупани данни, за да могат да оформят референтен модел за реакция на бъдещи проблеми и да взимат решения с постоянно нарастваща надеждност и точност. Почти всички AI приложения се включват в тази категория системи.

Разбира се, чисто концептуално, съществуват и още два вида Artificial Iintelligence – Theory of mind AI и Самоосъзнаващ се AI – следващото ниво на развитие на системите за изкуствен интелект, който ще е натоварен със сложната задача да може да разбира по-добре субектите, с които си взаимодейства, техните нужди, емоции, вярвания, цялостния им мисловен процес. Развиването на собствено самосъзнание е може би крайно еволюиралата форма на AI, напълно близка по форма до човешкия разум и следователно – със собствени мисли, нужди и желания.

Алтернативната система за класификация, която се използва по-общо на технологичен език, е класификацията на технологията на изкуствен тесен

[1] Илиева, И. (2020) Върховенството на правото и изкуственият интелект. В: Известия. Списание на Икономически университет – Варна. 64 (3), 210–226, 211

интелект (ANI), изкуствен общ интелект (AGI) и изкуствен суперинтелект (ASI).

Има още няколко разновидности, но на този етап това са главните четири типа ИИ, които са обяснени като кратък наръчник за етапите на еволюция, през които минава една такава сложна система.[2]

Анализът тук е съсредоточен главно върху етичните и правните проблеми, които възникват от използването на софтуерно базирани системни приложения за изкуствен интелект с все още ограничена памет, които обаче успешно могат да причинят репутационна криза в политическото поле и да се превърнат в сериозен инструмент за целите на черния PR.

Между 50-те и 90-те години на отминалия вече XX век класиците на комуникационната теория (Уилбър Шрам, Пол Лазарсфелд, Брус Уестли и Майкъл Маклийн, Франк Данс, Джон Кеъри, Евърет Роджърс и Лорънс Кинкейд, Самюел Бекер, Денис Макуейл, Джей Блек и Дженингс Браянт, Елит Николов и много други) усилено анализираха изместването на постулатите от старата „Куршумена теория“ за всевластието на медиите над пасивната публика, от новата тогава „революция“ в медийната среда, породена от напредъка в технологиите и „овластяването“ на медийния реципиент чрез дистанционното устройство. Коментираше се как изведнъж цялата схема на обществения комуникационен процес е преобърната поради ключовата роля на аудиторията и нейните нива за разбиране и интерпретация, на начините, по които тя би могла евентуално да филтрира информационните потоци, да ги осмисля, запаметява в дългосрочно или краткосрочно или пък директно да ги игнорира.

Цялото медийно съдържание се получаваше първично и вторично обработено, структурирано, програмирано, предварително зададено и надлежно фокусирано към определени таргети, докато цифровият телевизионен и радиоформат не постави въпроса за тоталния аудиторен контрол над медийните съдържания. Защото медията се превърна в интерактивна. Реципиентите започнаха да контролират времето, ракурсите, поредността на съдържанията и утвърдиха постоянното диалогизиране с медията в ефира. Синхронизацията, интерактивността, едновременността на общуването

[2] Naveen, Joshi, 7 Types Of Artificial Intelligence, достъпно на https://www.forbes.com/sites/cognitiveworld/2019/06/19/7-types-of-artificial-intelligence/?sh=8f43ce3233ee&fbclid=IwAR1b-t2DPzuRbro9Lqv1Xpn3cIPUO75kqIRnszUJ00UXGqWY8_GZBkg-0-8, с. 1, [последно посетена на 9.05.23]
Coursera articles, 4 Types of AI: Getting to Know Artificial Intelligence, достъпно на https://www.coursera.org/articles/types-of-ai, с. 1, [последно посетена на 9.05.23]

през медиите, аудиторният контрол завинаги белязаха цялостната световна медийна система.

Появата на AI в сегашния XXI век революционизира съвременната медийна реалност отново и драстично, доколкото от реципиента вече не се очаква само да контролира съдържанието и стиловете на работа и неговото поднасяне, времевата му рамка и последващия „шлейф от ефекти“. От него вече се очаква да осмисля (доколкото му е възможно) в мащаб социалните и политическите въздействия от своите автономни авторски намеси в медийния поток, различните етични и законови норми при неговото конструиране, форматиране, споделяне и пресподеляне, защото така или иначе им влияе – позитивно или негативно. И най-вече защото с еволюцията на информационните технологии той вече е в центъра на медийната система в ролята на автор. И когнитивната власт, която изкуственият интелект връчи в ръцете на редовия автор и доставчик на съдържания в интернет, създава условия за творчество, но и за значителни злоупотреби, които би трябвало да са наказуеми по силата на действащото законодателство.

AI някак успя да пренареди структурата на медийното влияние и днес от самостоятелен играч на терена на публичността, особено когато става дума за полето на политиката, медийният сектор се превръща в рефлекторна отразяваща акустична и визуална кутия на персонализираните потребителски „Аз“ канали за съдържания, които не винаги са точно информация по смисъла на журналистическото понятие за информация, но все едно – диктуват все по-усилено облика на днешното глобализирано дигитално информационно поле.

И изглежда все по-парадоксален фактът, че именно на фона на този контекст, изграден от Аз-говореното на обикновения човек в медиите, особено в тяхната интернет битност, свободата на словото расте за сметка на свободата на медиите, защото между двете свободи очевидно има съществена разлика. Усеща се известна неспособност на ЕС да се справи с регулацията на медиите онлайн, както и със свободата на медиите в някои страни членки като цяло, което се дължи на липсата на адекватни ресурси за влияние върху промените, които медиите изживяват особено в източноевропейските страни след 2001 г., когато Съюзът се разшири с тях. Всеки ангажиран в медия, който си позволява критика, авторска интерпретация на актуалните събития, разследване, огласяване на неудобни факти, бива маргинализиран и изтласкан силово към периферията на медийното прос-

транство, за да се влее в извъннорменото малцинство без право на достъп до рейтинговите пояси на влияние[3].

Общественото доверие в класическите медии също се срива и отразяването и изчезването от публичното пространство на знакови имена се приема с безразлично мълчание от страна на аудиториите, които вече сами генерират своя контент и все повече се дистанцират от професионално структурираните медийни послания.

По този начин днес наблюдаваме една трайна тенденция към неистово и упорито усилие от страна на медийните редакции да са „в крак с времето“. Да са уж „в тон“ със стила на мисленето и нуждите на аудиториите си – да са техни сенки и огледални образи, а всъщност подвластни на други финансови и политически кръгове. Наблюдаваме и отчуждението на тези аудитории от професионално списваната и снимана журналистика, особено когато е ангажирана със сериозни социални и политически тематики. Това отдръпване на аудиториите от „студените“ тежки новинарски съдържания е всъщност белег и за умора от големите социални и обществени проблеми на деня, които ги поддържат перманентно тревожни и неудовлетворени и умишленото им „потапяне“ във всекидневно-битовото, локалното, дори персоналното като рефлекс за самосъхранение и търсене на убежище от травматичните фактологии на съвремието ни.

Антоний Тодоров неслучайно подчертава, че политическата информация много рядко е освободена от манипулативни елементи и поради това никак не е безобидна, защото внушава конкретни заключения, често съдържа полуистини или е умишлено фрагментарна.[4] Така осакатеното комуникиране между публичното и публиките капсулира всяка от групите в самите тях, което води до драстични загуби на легитимност и крайни жестове на нетолерантност и незачитане на другата страна.

В сферата на политическия живот тези тенденции се открояват особено ярко. И ако доскоро за висша форма на нетолерантност и отхвърляне се считаха компроматите, слуховете, инсинуациите, които влизаха в инструментариума на негативния „сив“ PR, използван главно от политически централи срещу други политически централи, днес оръжието е друго, въоръжените – също.

[3] Вълков, И. (2022) Фактори и форми на натиск в медийната среда в България – В: Проблеми на постмодерността, № 3, 385–417.

[4] Тодоров, А., Д. Канев. (2012) Информация и анализи в политиката. – В: Учебник по политически мениджмънт 1. София: Фондация „Фридрих Еберт“, 13–14.

Понеже политиците все по-малко осъзнават, че имат проблем с комуникациите по отношение на своите аудитории извън твърдите партийни ядра, те не полагат особени усилия и да я развиват, ако изключим режимите на предизборно говорене. Така не се осъзнава и фактът, че цялостното медийно присъствие на публичните политически фигури в медийното пространство или се филтрира умишлено от вниманието на широките аудиторни маси, или се възприема като форма на реалити шоу, което забавлява, но не убеждава достатъчно в полза на една или друга политика, не дават работещи аргументи, които да мотивират публиките да отстояват един или друг избор за политическа сила. Пренасочването на политическото усилие и внимание в превземането на медийни територии чрез закупуване, вместо към електората и неговите все по-втвърдяващи се антинагласи на просто публика на шоуто, девалвира респекта и вярата в политическото като цяло в свят, в който имиджът е значително по-важен от репутацията на честно изградената биография и ситуационната представа е по-определяща от задълбочения дебат за политики, а личният интерес се оказва по-определящ от социалната отговорност.

Именно поради тази девалвация на публичното и политическото, поради този тежък срив на доверие и професионално менажиран чрез техниките на PR плуралистичен диалог[5], днешният стоящ в центъра на медийната система реципиент – автор провидя в някои от приложенията на AI удобен и дори забавен инструмент, с който едновременно да се заяви и да осмее допълнително политиците и политическото. Да ги преиначи гротесково, да ги извади от обичайния им публичен контекст и да им прикачи чужда реч и чуждо поведение, за да „донапише“ шоуто, едновременно да си отмъсти и да се надсмее над публично овластените, които го игнорират комуникативно. Резултатът често се прихваща от т.нар. „черен“ PR[6] и вторично се употребява в публичните битки между политически лидери и техните централи.

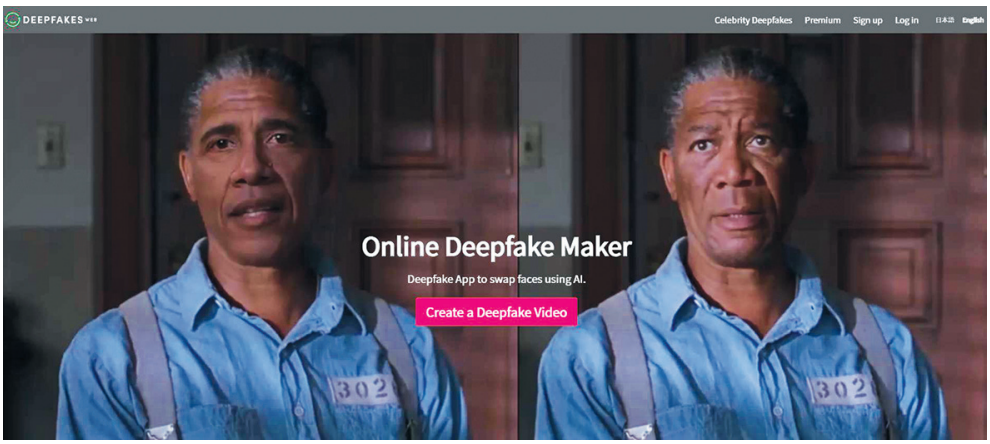
Удачна е тезата на Иванка Цонева, че „връзките с обществеността не са PR, а само част от него, не са негов абсолютен синоним, а само компонент, при това не най-яркият. Те са видимо положителните послания към обществеността, чрез които се изграждат положителни образи; предназ-

[5] Ковачева, С. За произхода на публик рилейшънс. – В: Годишник на Софийския университет „Св. Климент Охридски“, Факултет по журналистика и масова комуникация 1, 223–240, особено 238–239.

[6] Вж. по-подробно Цонева, И. (2007) Черен или негативен PR – средство за конкурентна борба. – Диалог, № 2, 61–90.

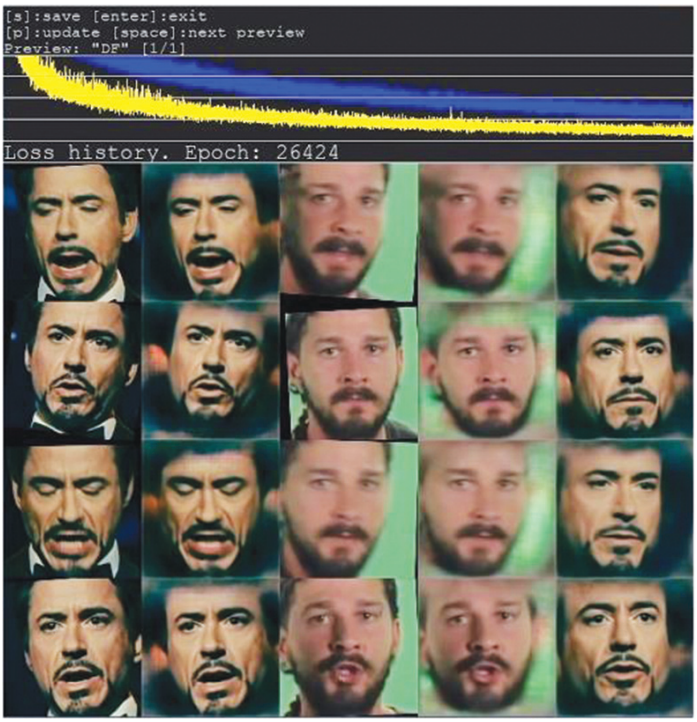
начението на „черния“ PR е да руши тези образи“. Авторката допълва, че „между понятията „черен“ и „негативен“ ПР се поставя знак за равенство. Те еднакво се тълкуват като отрицателна публичност, като изобличаване или компрометиране на конкурента, имащо за източник явен или анонимен, но винаги заинтересован зложелател. Оттук произтича склонността на практиката да разпространява чрез разговорния език понятието „черен“ PR, когато става дума за дискредитиране на публични лица и организации. Смисълът на тази част от връзките с обществеността обаче е по-широк по обхват, по-многообразен и разнопосочен, защото не се определя само като антипод на имиджмейкърството... Точно тази област на активните връзки с обществеността е най-непрозрачна, именно тук същността е много различна от видимостта“[7].

Така Deepfake Voice Generators[8] и Deepfake Video Maker[9] (фиг. 1), като едни от най-използваните за целта AI приложения, започнаха грубо и на практика неправомерно да разрушават имиджа на конкретни публични фигури от обществено-политическия ни живот с цел тежки репутационни и лични кризи и нарушаване на личните им свободи.



Фиг. 1

[7] Пак там, 61–62.
[8] Напр. https://www.resemble.ai/
[9] Напр. https://deepfakesweb.com/
https://speechify.com/blog/top-five-deepfake-voice-generators/?landing_url=https%3A%2F%2Fspeechify.com%2Fblog%2Fdeepfake-voice%2F The top five deepfake voice generators.



Фиг. 2 DeepFaceLab

„Deepfake“ се появява за първи път в интернет през 2017 г., като се базира на иновативен тогава метод за т.нар. „дълбоко учене“, известен като GAN – генеративни конкурентни мрежи. Deepfakes са генерирани от AI изображения, реч, музика или видеоклипове, които изглеждат истински. Те работят, като изучават и анализират софтуерно съществуващи изображения или аудио от реалния свят, картографират ги в детайли, след което ги манипулират, за да създадат художествени произведения, които са обезпокоително идентични на реалните. Често обаче има някои издайнически знаци, които ги отличават от реалността. В подобни видеа гласовете може да звучат малко роботизирано или образите на хората може да изглеждат леко неестествено или да повтарят еднотипни жестове с ръцете си. Освен да ги генерира, AI може и да открива подобни несъответствия и да маркира манипулирани видеа и гласове.

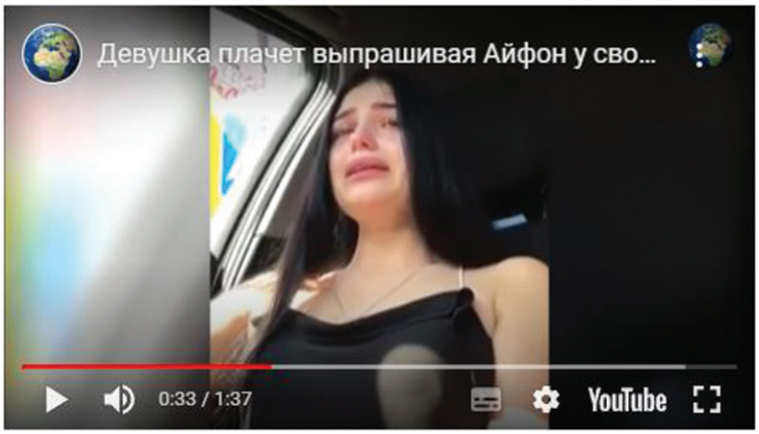
Гласовото клониране, известно още като Deepfake Voice или синтетични гласове, създава клонирани гласове с помощта на AI технология и алгоритми за машинно обучение. Създаването на клониран глас с добро качество изисква компютър от висок клас с мощни графични карти и из-

числителна мощност в облак, както и достатъчно данни, тоест записи на гласа на целевия човек, чийто глас ще се клонира. Така AI може да създаде автентични гласове, които ще кажат всичко, което потребителят напише, като използва технологията за текст към реч или технологията за реч към реч.

Сега изкуственият интелект може да клонира човешки глас въз основа само на един час запис на говор, но колкото по-голям е гласовият вход, толкова по-лесно е на изкуствения интелект свърши поставената задача.

Един от най-знаковите и особено показателни образци за използването на подобно обработено видео с политик от световна величина е това с Барак Обама[10]. През април 2018 г. режисьорът Джордан Пийл (Jordan Peele) направи видео във FakeApp на бившия президент на САЩ Барак Обама, за който се твърди, че обижда настоящия лидер на САЩ Доналд Тръмп. Така Пийл решил да покаже до какво може да доведе развитието на технологиите и как ще изглеждат фалшивите новини.

Друга такава мишена е украинският президент Володимир Зеленски и неговото семейство. Deepfake Video показва плачеща млада жена, която уж била 17-годишната дъщеря на украинския президент Олександра Зеленска. Твърди се, че тя нарича баща си „нацист“ и „убиец на украинския народ“ и че казва, че го „мрази“. Кадърът е разпространен на различни езици и в различни държави, включително и в българските социални мрежи, където се твърди, че Олександра Зеленска нарича баща си „изнасилвач на деца“[11] (фиг. 3).



Фиг. 3

[10] Deepfake Video – Обама се обажда на Тръмп. – достъпно на https://www.youtube.com/watch?v=_gVTvlTMjV4

[11] Достъпно на https://gospodari.com/tag/дийп-фейк/

Семейството му също е обект на дезинформационни кампании: в социалните мрежи бе публикувана снимка, за която се твърди, че показва съпругата на Зеленски в Ница. Украинският президент отрече и потвърди, че съпругата му е с него в Украйна.

Фиг. 4

Прокуратурата все още разследва скандалния запис с гласа, за който се смята, че е на бившия премиер Бойко Борисов[12]. 29.07.2020 г. беше публикуван в сайта на „Афера“, като записът е със заглавие „Баце и Томи“, на който предполагаемо Борисов и Томислав Дончев разговарят за президента Радев в особено вулгарен стил (фиг. 4).

През октомври миналата година впрочем в Русия се появи и първият Deepfake сериал пародия – „ПМЖейсон“[13], сътворен изцяло с тази технология (фиг. 5, 6). Той е от 10 серии, всяка по 5 мин. Заснет е от Agenda Media Group[14] за около 3 месеца.

Фиг. 5, 6

В него известни американски артисти като Киану Рийвс и Джейсън Стейтъм „играят“ главните роли. Фабулата е особено показателна – действието се развива през 2027 г. и те решават да останат в Русия за постоянно.[15]

[12] Новина https://www.youtube.com/watch?v=ZTnvsMe-fjM
[13] ПМЖ – „Постоянно местожителство“.
[14] https://agenda.media/pmgason
[15] Виж ппо-подробно на https://dzen.ru/b/Y0VSkPnAFzmjkh_t

Фиг. 7

Продуцентът на компанията – Мария Артьомова, както и шефът ѝ – Алексей Парфун, твърдят, че все още не съществуват юридически ограничения за използването на лицата на актьори (в случая от Холивуд) за създаване на някакво пародийно съдържание, стига то да не накърнява по някакъв начин честта, достойнството и деловата репутация на съответната личност. Но дали наистина деловата репутация и правата на тези актьори са ненакърнени на практика? Защото контекстовите внушения на „иновативния“ сериал, разбира се, имат ясни политически послания, които са далеч от коректните на фона на течащата война с Украйна и ролята, която САЩ и Русия играят в нея.

Фиг. 8

Същата е подтекстовата и контекстна заигравка с политическото – в навечерието на мисията на НАСА след 11-годишно затишие, полета на „SpaceX Demo-2“ с двустепенната ракета Falcon-9 от компанията *SpaceX* на Илон Мъск, се появи знаково Deepfake Video със самия Илон Мъск (фиг. 8), който пее още по-знаковата песен на група „Земляне“ – „Трава у дома“ („Земля в илюминаторе“), която винаги се свързва асоциативно точно с руската космонавтика, която дълги години доминираше в сектора.[16]

Още по-обезпокоителен от посочените (зло)употреби с AI за публични внушения чрез обществената комуникация за целите на черния PR е фактът, че изкуственият интелект на практика не може да „разсъждава“ етично.

Преди 7 години Microsoft дебютира AI личност в Twitter на име Тай с амбицията тя да участва в онлайн разговори с потребители на социалната

[16] https://trud.bg/илън-мъск-пее-земля-в-илюминаторе/ Труд онлайн – Илън Мъск пее „Земля в илюминаторе“.

медия като забавна интерактивна демонстрация на NLP (Natural Language Processing) технологията на Microsoft. Само за часове обаче интернет троловете накараха Тай да публикува доста стряскащи обидни съобщения, като например „Хитлер беше прав“ и „Мразя феминистките и всички те трябва да умрат и да горят в ада“. Microsoft набързо премахна бота Тай от интернет. Основният проблем с Тай не беше, че е неморална, а това, че на AI системите им липсва стабилно изградена концепция за „правилно“ и „погрешно“. Тай не разбра, че това, което публикува в социалната мрежа, е неприемливо, просто защото се оказа редови резултат от обичайния за нея статистически анализ на данни, циркулиращи в нета, при който анализ липсва възможност да оцени неетичността на въпросните публикувани изречения.

Заключение

Изредените особено драстични примери за употреби на AI приложения за анализ на средата и синтезирането и обработването на огромни по обем компресирани (и не само) данни информация като Deepfake Voice Generators и Deepfake Video Maker илюстрира тоталната апатия на аудиториите към реалността и в същото време стратегическото манипулиране с похватите на технологията и чрез контекстови внушения на устойчиви нагласи с цел постоянно „рефрешване“ на политически аргументи, които обаче подкрепят вече устойчиви нагласи по водещи теми и политики, които се пързалят по ръба на закона.

Европейските законодателни институции упорито се опитват да наложат на страните членки регламентация на употребата на изкуствен интелект чрез различни координирани планове и актове[17], които чрез съдържанието си демонстрират цялостната визия на Европейския съюз за дигитализацията и приложенията на AI.

В този процес явно се осъзнава, че рестрикциите за подобни употреби трудно кореспондират с юридическите постановки за свободата на словото. В същото време толкова лесно манипулируемите аудио и видеозаписи чрез изкуствен интелект биха могли изключително сериозно да нарушат личните права на потърпевшите. Защитата срещу клевета и набедяване, срещу публично опозоряване или дори подбуждане към нарушаване на обществения

[17] Съобщение на Комисията до Европейския парламент, Европейския съвет, Съвета, Европейския икономически и социален комитет и Комитета на регионите. Координиран план за изкуствения интелект, Брюксел, 7.12.2018, COM(2018) 795 final, достъпно на https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:52018DC0795&from=EN

ред чрез подобни фейк провокации обаче остава проблематична, предвид неустойчивите постановки в различните законодателства в Европа и някои части на САЩ и висящия проблем с анонимността на произведеното съдържание. Въпреки това подобни употреби на изкуствения интелект са в състояние да предизвикат сериозни гражданскоправни последици с широк диапазон – от увреждане на общите права на „мишената“ (потърпевшия), до застрашаване на националната сигурност или инспирирането на тежки дипломатически конфликти от недоразумения и умишлено дискредитиране на политически фигури от различен мащаб, които ги правят високорисково занимание.

В унисон с тези усилия у нас беше изработена Концепция за развитието на изкуствения интелект в България 2030 от ресорното Министерство на транспорта, информационните технологии и съобщенията[18], която беше приета неоднозначно най-вече заради отчетливата липса на фокус именно върху сектора „Правосъдие“, който на практика регулира правата и свободите на гражданите, заради недотам прецизните дефиниции и най-вече заради трудните за изпълнение на практика конкретни указания за социална отговорност, разписани в нея.

Едно от решенията, на фона на правните усилия по регламентирането на AI, би могло да бъде разширяването на обхвата на самата законодателна рамка, която сега стеснява периметъра на правен коментар върху опазването на основните права на гражданите и защитата на личните данни, в съответствие и с действащия Регламент (ЕС)2016/697.

В медийната среда, която е твърде особена и сложна за подобна рамкова регулация, особено в онлайн пространството, работеща би била по-скоро саморегулацията, която би могла да се изрази в няколко направления:

- осъвременяване на Етичния кодекс на българските медии с акценти върху цифровата среда;
- налагане на процеси на устойчиво оздравяване на сектора чрез приобщаването на конкретни приложения на AI с цел подобряване на работата на журналистите и повишаване на качеството на информацията;
- краудсорсинг наместо аутсорсинг или тяхното разумно съчетаване;

[18] Концепция за развитието на изкуствения интелект в България 2030 на Министерство на транспорта, информационните технологии и съобщенията, достъпно на https://www.mtc.government.bg/sites/default/files/koncepciyazarazvitienaiivbulgariyado2030.pdf

- целенасоченото повишаване на обществента ангажираност за ролята и опасностите от Deepfake и AI в социума чрез поддържането на постоянен публичен дебат за всички социални и политически рискове от неправомерното използване на изкуствен интелект, включително и в сенчестата PR практика;
- по-нататъшното развитие на data и decision журналистиката и изграждане на доверие към професията и технологиите, с които тя борави, както и към дигиталната медийна система като цяло.

Библиография:

1. Вълков, И. (2022) Фактори и форми на натиск в медийната среда в България – В: Проблеми на Постмодерността, № 3.
2. Ковачева, С. (2019) За произхода на публик рилейшънс. – В: Годишник на Софийския университет „Св. Климент Охридски“, Факултет по журналистика и масова комуникация , Т. 1.
3. Концепция за развитието на изкуствения интелект в България 2030 на Министерство на транспорта, информационните технологии и съобщенията, [онлайн] [посетена на 19.06.23] достъпно на https://www.mtc.government.bg/sites/default/files/koncepciyazarazvitienaiivbulgariyado2030.pdf
4. Петрова, А. (2022). Туитър срещу политиката – нова ера в политическия дискурс в САЩ. – В: Медии и комуникации. Т. 2, София: УИ „Св. Климент Охридски“.
5. Съобщение на Комисията до Европейския парламент, Европейския съвет, Съвета, Европейския икономически и социален комитет и Еомитета на регионите. Координиран план за изкуствения интелект, Брюксел, 7.12.2018, COM(2018) 795 final, [онлайн] [посетена на 19.06.23] достъпно на https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:52018DC0795&from=EN
6. Тодоров, А., Д. Канев. (2012) Информация и анализи в политиката.В: Учебник по политически мениджмънт 1. София: Фондация „Фридрих Еберт“, с.13-14.
7. Цонева, И. (2007) Черен или негативен PR – средство за конкурентна борба. – Диалог, № 2.
8. Naveen, J. (2023). Types Of Artificial Intelligence, [онлайн] [посетена на 9.06.23] Достъпна на: https://www.forbes.com/sites/cognitiveworld/2019/06/19/7-types-of-artificial-intelligence/?sh=8f43ce3233ee&fbclid=IwAR1b-t2DPzuRbro9Lqv1Xpn3cIPUO75kqIRnszUJ00UXGqWY8_GZBkg-0-8

9. Coursera articles (2023). 4 Types of AI: Getting to Know Artificial Intelligence, [онлайн] [посетена на 18.06.23] Достъпна на: https://www.coursera.org/articles/types-of-ai

Илюстративни онлайн ресурси:

Илън Мъск пее „Земля в илюминаторе“, Труд онлайн [посетен на 19.06.23] достъпно на https://trud.bg/илън-мъск-пее-земля-в-илюминаторе/

The top five deepfake voice generators[онлайн] [посетена на 19.06.23] достъпно на https://speechify.com/blog/top-five-deepfake-voice-generators/?landing_url=https%3A%2F%2Fspeechify.com%2Fblog%2Fdeepfake-voice%2F

Deepfake Video – Обама се обажда на Тръмп – [онлайн] [посетена на 18.06.23] https://www.youtube.com/watch?v=_gVTvlTMjV4

ПМЖ – „Постоянно местожителство“ [онлайн] [посетена на 19.06.23] достъпно на

https://agenda.media/pmgason

https://deepfakesweb.com/

https://gospodari.com/tag/дийп-фейк/

https://www.youtube.com/watch?v=ZTnvsMe-fjM

https://dzen.ru/b/Y0VSkPnAFzmjkh_t

Ролята на изкуствения интелект при извършване на оценка на риска от изпиране на пари

Андрей Михайлов*

Изкуственият интелект има потенциал да бъде полезен инструмент за разкриване и предотвратяване на дейности, свързани с изпиране на пари. Системите, управлявани от изкуствен интелект, могат да анализират огромни количества данни, за да идентифицират необичайни модели или аномалии при правни сделки или трансакции, които могат да бъдат индикатор за дейности по изпиране на пари. Следващата стъпка е да „предупредят“ регулаторните и правни екипи за извършване на по-нататъшно проучване (разширени проверки). Изкуственият интелект може да се използва за търговия с финансови инструменти, а това е един високотехнологичен механизъм за изпиране на пари. Алгоритмичната търговия е пример за това, тя включва прилагането на компютърни алгоритми за автоматично изпълнение на сделки въз основа на предварително определени правила и критерии. Тези алгоритми могат да бъдат проектирани така, че да анализират големи количества данни и да вземат решения за търговия въз основа на фактори като пазарни тенденции, медийни събития и технически показатели. Извършителите на престъплението „изпиране на пари“ много бързо ще осъзнаят технологичното предимство на изкуствения интелект, особено в сферата на модерните и актуални способи за изпиране на пари като търговията с финансови инструменти. Поради тази причина противодействието също следва да разчита на модерни и високотехнологични средства.

Ключови думи: *противодействие на изпирането на пари, изкуствен интелект, риск*

* Андрей Михайлов, докторант във ВА „Г. С. Раковски“,
ел. поща: andrew_mihaylov@abv.bg

The role of artificial intelligence in money laundering risk assessment

Andrey Mihaylov*

Artificial intelligence has the potential to be a useful tool for identifying and preventing money laundering activities. AI-driven systems can analyze vast amounts of data to identify unusual patterns or anomalies in legal deals or transactions that may be an indicator of money laundering activities. The next step is to "alert" regulatory and legal teams to conduct further investigation (enhanced due diligence). Artificial intelligence can be used to trade financial instruments, and this is a high-tech money laundering mechanism. Algorithmic trading is an example of this, it includes the application of computer algorithms to automatically execute trades based on predetermined rules and criteria. These algorithms can be designed to analyze large amounts of data and make trading decisions based on factors such as market trends, media events and technical indicators. The perpetrators of the crime of money laundering will very quickly realize the technological advantage of AI, especially in modern and current money laundering methods such as trading financial instruments. For this reason, countermeasures should also rely on modern and high-tech means.

Keywords: *Anti-money laundering, artificial intelligence, risk*

* Andrey Mihaylov, PhD Candidate at the G.S.Rakovski Military Academy, e-mail: andrew_mihaylov@abv.bg

Изпирането на пари е сериозен проблем, с който се сблъскват финансовите институции, регулаторните и правоохранителните органи по света, поради което е изключително важно да се разработят ефективни мерки за противодействието му. Най-новите постижения в областта на изкуствения интелект (ИИ) доведоха до иновативни техники за идентифициране на риска и предотвратяване на изпирането на пари. В настоящия доклад ще бъде разгледана ролята, която ИИ може да играе в противодействието на изпирането на пари, етичните и правните проблеми, свързани с използването на ИИ, и потенциалните пречки пред прилагането му.

Изкуственият интелект има потенциал да бъде полезен инструмент за разкриване и предотвратяване на дейности, свързани с изпиране на пари, поради което не бива да се лишаваме от него. Системите, управлявани от ИИ, могат да анализират огромни количества данни, за да идентифицират необичайни модели или аномалии при правни сделки или трансакции, които могат да бъдат индикатор за дейности по изпиране на пари. След това те могат да „предупредят“ регулаторните и правни екипи за извършване на по-нататъшно проучване (разширени проверки). Например системите, управлявани от ИИ, могат да маркират трансакции с необичайни места (рискови юрисдикции) на произход на средствата или местоназначение, модели на плащане или други характеристики (необичайно усложнени сделки, многоходови разплащателни операции), които могат да индикират извършването на противоправна дейност.

Моделите за *deep learning* са много ефективни при идентифицирането на **типизация (модели) в трансакциите**, които показват опити за изпиране на пари. Алгоритмите за *deep learning* могат да се „учат“ от големи масиви от исторически данни за трансакции, за да установят модели на противоправно поведение в последващи трансакции. Такива системи биха могли да подобрят откриването на незаконни дейности и да помогнат на финансовите институции (основно банкови) да изпълнят задълженията си при спазване на законодателството.

Друго предимство на системите с изкуствен интелект е способността им да откриват възникващи заплахи в реално време. За разлика от традиционните системи (като например *rule-based systems*), които разчитат на предварително дефинирани правила, моделите на ИИ могат да се адаптират и обучават към нови ситуации и да откриват постоянно променящи се модели на незаконни дейности, като същевременно свеждат до минимум процента на фалшивите положителни резултати (при идентифициране на риск от изпиране на пари).

Изкуственият интелект може да се използва за търговия с финансови инструменти, а това е един удобен и високотехнологичен механизъм за изпиране на пари. Пример за това е използването на **алгоритмична търго-**

вия, която включва прилагането на компютърни алгоритми за автоматично изпълнение на сделки въз основа на предварително определени правила и критерии. Тези алгоритми могат да бъдат проектирани така, че да анализират големи количества данни и да вземат решения за търговия въз основа на фактори като пазарни тенденции, медийни събития и технически показатели.

Алгоритмичната търговия под формата на процес за изпълнение на поръчки, използващи автоматизирани и предварително програмирани инструкции за търговия, за да отчитат променливи като цена, време и обем, е известна и използвана отдавна. Тя не е новост, но добавянето на системи с елементи на изкуствен интелект ще я превърне в бъдещето на търговията с финансови инструменти. По този начин изкуственият интелект ще взема решения за сключване на много на брой и изключително бързо реализирани сделки, а това е удобен способ за изпиране на пари – особено приложим във фазата „разслояване". Не е нужно да се пояснява, че утвърденото разбиране за стадиите (фазите) на процеса на изпиране на пари включва: пласиране, разслояване и интегриране на средства, придобити по незаконосъобразен начин. Разслояването има за цел да укрие произхода на средствата и за това най-често се използва именно серия от сделки, ако тези сделки са на сравнително малка стойност – те няма да направят впечатление и да привлекат внимание. Същевременно обаче процесът на „разслояване" ще стане по-ефективен за осъществяване на престъпния замисъл на извършителите, ако сделките са много на брой, т.е. с висока честота, извършени чрез алгоритмична търговия.

На извънборсов пазар (*over-the-counter* или OTC пазар) използването на алгоритмична търговия е много удобно, т.е. това е нецентрализиран финансов пазар, при който трансакциите се извършват бързо и ефективно чрез двустранни споразумения между различните участници. Това означава, че изкуственият интелект ще навлезе първо на OTC пазара на деривативни финансови инструменти, а след това на регулирания/организиран борсов пазар, оттук може да се направи заключение, че потенциално изпиране на пари с помощта на системи, управлявани от изкуствен интелект, може да се „засече" на извънборсовите пазари (те са носители на по-висок риск).

Алгоритмичната търговия ще става все по-популярна през следващите години, тъй като може да помогне за повишаване на ефективността и намаляване на разходите по сделките. Важно е обаче да се отбележи, че алгоритмичната търговия подлежи на законови и регулаторни изисквания точно както всеки друг вид търговска дейност с финансови инструменти. Финансовите институции трябва да спазват разпоредбите, свързани с търговията с вътрешна информация и противодействието на изпирането на пари. Що се отнася до риска от изпиране на пари при системите с ИИ, съществува потенциална опасност алгоритмите с ИИ да бъдат използвани

за улесняване на престъплението по същия начин, по който това може да стане с традиционните системи за търговия. Например извършителите на престъпления биха могли да използват алгоритмичната търговия за бързо прехвърляне на средства между различни сметки или на различни пазари с цел „изпиране“ на незаконни средства. Както посочихме, това е особено приложимо в етапа на т.нар. „разслояване“ на средствата, които се „изпират“.

Противодействието на изпирането на пари чрез използване на системи, управлявани от ИИ, може да се осъществи чрез прилагането на два подхода:

а) надзор и сертифициране на системите и платформите за търговия, т.е. използване на човешкия фактор, знания и опит за надзорна дейност. Този подход обаче едва ли е достатъчно надежден, поради липсата на достатъчно капацитет и човешки ресурси в регулаторните органи и пазарите по света. Не може да се очаква, че ще изчезне елементът на проверка, извършвана от хора – много държавни органи имат правомощия да извършват проверки по спазване на режима за изпиране на пари и тези проверки се подчиняват на специален ред за откриване и провеждане, този режим ще се запази и в бъдеще, но вероятно с променен профил[1];

б) внедряване на нови проучващи и анализиращи риска системи, които също са базирани на ИИ. По този начин се използва един и същи инструмент за извършване на деянието (изпиране на пари чрез търговия с финансови инструменти) и за противодействието – изкуственият интелект вероятно в близко бъдеще ще бъде важна част от инструментариума за разкриване на сделки за изпиране на пари, както и на пазарни злоупотреби. Може да се използва (макар и извън научната и професионална терминология) изразът, че ИИ ще бъде едновременно „отрова и противоотрова“ при изпирането на пари и неговото разкриване.

За да намалят риска, финансовите институции трябва да гарантират, че техните системи с изкуствен интелект са проектирани и внедрени по начин, който е в съответствие с разпоредбите за противодействие на изпирането на пари. Това може да включва въвеждането на проверки за противодействие на изпирането на пари в процеса на алгоритмична търговия, като например

[1] Повече за тактиката на извършване на проверки от КФН вж. Михайлов, А. (2006) Проверки на инвестиционни посредници, правомощия на Комисията за финансов надзор. – Пазар и право, № 9. Същият автор разглежда и извършването на измами с финансови инструменти, които са както предикатно престъпление на изпирането на пари, така и възможен инструментариум, използван за самостоятелно изпиране на пари при избягване на работа с банки, чийто контрол може да е на по-високо ниво. За повече детайли вж. Михайлов А. (2006) Измами с ценни книжа. – Пазар и право, № 1, 66–74.

наблюдение за подозрителни модели на търговия или извършване на проверки за надлежна проверка на клиента.

Отворен остава въпросът кой ще сертифицира и проверява системите с ИИ – вероятно най-лесният отговор би бил Комисията за финансов надзор (или съответно в други страни – органът, наблюдаващ небанковия сектор), но дали е налице необходимият капацитет за това – към момента това е въпрос без категоричен отговор. Сертифициране може да се извършва и от външни организации, отговарящи на предварително зададени стандарти, включително с опит и знания в областта на противодействието на изпирането на пари.

Като цяло, въпреки че съществуват потенциални рискове, свързани с използването на ИИ в търговията с финансови инструменти, тези рискове могат да бъдат контролирани чрез подходящи мерки за управление на риска и спазване на регулаторните изисквания. Тези мерки ще са основани на използване на технически средства – софтуер с елементи на ИИ, – ефектът ще е своеобразно противодействие на престъпното използване на изкуствения интелект именно чрез изкуствен интелект.

Финансовите институции трябва да гарантират, че техните системи с ИИ са проектирани и внедрени по начин, който е в съответствие с правните и регулаторните изисквания (именно върху тях ще тежи това задължение), и че са налице подходящи предпазни мерки за предотвратяване на изпирането на пари и други незаконни дейности.

Изкуственият интелект вече е доказал своя потенциал в противодействието на изпирането на пари (на пазара са налични софтуерни решения с елементи на ИИ) и използването му ще се увеличи в бъдеще. Изкуственият интелект може да повиши ефективността на програмите за борба с изпирането на пари и да даде възможност на финансовите институции да спазват нормативните изисквания по-ефективно. Все пак при внедряването на решения с ИИ трябва да се вземат предвид правните и етичните съображения и да се намери баланс между предотвратяването на финансови престъпления и неприкосновеността на личната информация на клиентите.

Прилагането на ИИ в борбата с изпирането на пари без съмнение поражда някои етични и правни проблеми. Един от тях е свързан с точността на алгоритмите, използвани в системата. Въпреки че моделите на ИИ биха могли да се учат от големи масиви от данни и да идентифицират подозрителни дейности, те все пак могат да доведат до фалшиви положителни резултати, т.е. до неправилно обозначаване на законни трансакции като подозрителни. Това би могло да причини затруднения в търговския оборот или дори вреди на засегнатите клиенти и да се разглежда като нарушение на личните права (правото на свободна стопанска инициатива). Оттук възниква въпросът за отговорността при причинени вреди поради погрешна прецен-

ка на система, управлявана от ИИ – тя ще бъде за търговското дружество, приложило системата.

Друг етичен въпрос е потенциалът за предубеденост в моделите на ИИ. Предубеденост може да възникне, ако данните, използвани за обучение на системата, отразяват типични пристрастия или дисбаланси в набора от данни. Това би могло да доведе до неточни прогнози с непропорционално въздействие върху определени групи хора или региони (например автоматично се маркират като рискови сделки със средства от определени юрисдикции, лица с определен произход или поведение). По този начин търговията от/към определени рискови юрисдикции е предварително „обречена“ и тези географски райони или държави постепенно ще се превърнат в своеобразно икономическо гето. За да се намалят подобни рискове, трябва да се положат усилия – да се гарантира, че системите с ИИ, използвани за предотвратяване на изпирането на пари, са проектирани така, че да бъдат безпристрастни и обективни (колкото и странно да звучат тези категории, употребени по отношение на компютърна система с ИИ).

Не на последно място, проблемите със спазването на законодателството са сред пречките пред широкото прилагане на ИИ в борбата с изпирането на пари. Разработването и внедряването на система с ИИ изисква спазване на приложимите разпоредби за защита на личните данни, както и с действащото законодателство срещу изпирането на пари. Поради това търговските дружества (главно банки, но и небанкови институции) следва да бъдат внимателни при внедряването на решения за ИИ, за да не се нарушава действащият регулаторен режим.

Сред примерите за използване на ИИ в борбата с изпирането на пари е внедряването на Falcon X на FICO, който използва система за машинно обучение, за да идентифицира моделите на все по-сложни опити за изпиране на пари. Освен това и друг продукт – Watson AI на IBM, може да анализира значителни количества неструктурирани данни от различни източници, за да открива модели на неправомерни дейности.

Ще нараства ролята на системите с ИИ в проверките на клиентите (KYC – know-your-customer, по-общо казано, „познавай своя клиент“), това е процес, използван от задължени да противодействат на изпирането на пари лица за идентифициране и проверка на самоличността и финансовото състояние на насрещната страна по сделката. С все по-широкото използване на цифрови технологии във финансовата сфера, прилагането на ИИ при проверките не е въпрос на близко бъдеще – това е настоящето. Въпреки че използването на ИИ има много потенциални ползи, съществуват и някои съществени трудности и предизвикателства, които трябва да бъдат преодолени. Предвид изложеното, могат да бъдат обобщени ползите при използването на ИИ:

1. Повишаване на ефективността – използването на ИИ може значително да намали времето и ресурсите, необходими за завършване на процеса. Алгоритмите на ИИ могат бързо да анализират големи количества данни и да маркират потенциални рискове или подозрително поведение, което да спести на финансовите институции значително количество средства и време;
2. Подобрена точност – алгоритмите на ИИ са проектирани да бъдат изключително точни и последователни, което може да помогне за намаляване на риска от грешки и подобряване на качеството на проверките на KYC. Това може да помогне на финансовите институции да идентифицират и управляват по-добре рисковете, както и да спомогне за предотвратяване на измами и други незаконни дейности;
3. Повишена сигурност – използването на ИИ може да помогне за подобряване на сигурността на финансовите трансакции и за намаляване на риска от противоправни действия. Алгоритмите на ИИ анализират големи количества данни, което може да помогне за идентифициране на потенциални заплахи за сигурността.

Наред с отбелязаните по-горе ползи, следва да се посочат и недостатъци при използването на ИИ:

1. Липса на прозрачност – едно от най-големите предизвикателства при използването на ИИ е липсата на прозрачност в начина на работа на алгоритмите. За финансовите институции би било трудно да разберат как алгоритмите вземат решения, което може да затрудни идентифицирането и справянето с потенциални пристрастия или грешки;
2. Използването на изкуствен интелект поражда опасения за неприкосновеността на личния живот, особено във връзка със събирането и използването на лични данни. Финансовите институции трябва да гарантират, че спазват съответните разпоредби за защита на личните данни и че използват ИИ по отговорен и етичен начин. Ако приемем факта, че системите с ИИ събират значителен обем информация за конкретен клиент, то в социалните мрежи например може да има лична информация за конкретни съдружници или акционери на търговското дружество клиент. По този начин ще се обработват и съхраняват данни за обстоятелства като: членове на семейството, обичайни предпочитания, почивки, дестинации, закупени скъпи вещи, имуществено състояние, дори публикувани слухове и непроверени данни в таблоидни издания. Вземането на решения от ИИ въз основа на всичко това е най-малкото притеснително;

3. Ограничен обхват – въпреки че ИИ може да бъде много ефективен при анализа на структурирани данни, той може да изпитва затруднения с неструктурирани данни или данни, които не се категоризират лесно. Това означава, че може да има ограничения в обхвата на проверките, които могат да се извършват с помощта на алгоритми на ИИ. Ограниченият обхват е преходен – може да се заключи, че ИИ много бързо ще преодолее първоначалните трудности и ограничения в обхвата и ще си създаде „свобода“ на действие;
4. Киберсигурност – използването на ИИ в проверките на клиентите и оценката на риска може да увеличи опасността от кибератаки, тъй като системите, използвани за събиране и обработване на данни, често са сложни и взаимосвързани. Финансовите институции трябва да гарантират, че техните системи с ИИ са сигурни и защитени от кибератаки. Може да се предположи, че те ще се превърнат в първостепенна цел за извършители, които биха искали да прикрият произхода на средствата си и за целта ще използват кибератаки по отношение на банкови и небанкови финансови институции.

Всичко посочено по-горе позволява да се направят някои изводи и заключения:

1. Използването на системи с изкуствен интелект при оценка на риска от изпиране на пари е високоефективно и неговият обхват ще се увеличава в бъдеще. Банкови и небанкови институции ще инвестират повече в разработката или закупуването на такива системи.
2. Извършителите на престъплението „изпиране на пари“ много бързо ще осъзнаят технологичното предимство на ИИ, особено в модерните и актуални способи за изпиране като търговията с финансови инструменти.
3. Противодействието на изпирането на пари с високотехнологични средства е възможно единствено с подобен инструментариум. Човешкият фактор, особено в първоначалния етап на борбата с изпирането на пари (най-вече в сфери като търговията с финансови инструменти) бързо ще губи своето значение за сметка на самообучаващи се платформи с елементи на изкуствен интелект.
4. По отношение на строго правните действия, като образуване на административни и наказателни производства, извършване на процесуални действия, повдигане на обвинение и неговото доказване, във връзка с престъплението „изпиране на пари“, все още сме много далеч от изместване на човешкия фактор. Субектът на престъплението е общ, т.е. всяко наказателно отговорно физическо

лице, поради това, че извършителите са лица (макар и използващи високотехнологични системи), същите заключения могат да бъдат направени и по отношение на извънпроцесуалните (оперативни) способи за събиране на информация – човешкият фактор при тях ще остане незаменим[2].

5. Финансовите институции (банкови и небанкови), както и регулаторните органи следва да работят съвместно за разработване на национални/международни стандарти и правила за използването на ИИ при оценката на риска – към момента такива няма. Стандартите следва да гарантират, че използването на ИИ в оценката на риска не нарушава правата на физически лица по отношение на упражняването на свободна стопанска инициатива. Чрез решаването на тези въпроси в професионалната юридическа общност ще можем да използваме силата на ИИ, за да подобрим борбата с изпирането на пари и да насърчим по-сигурна и стабилна национална икономика.

Библиография:

1. Ethics Guidelines for Trustworthy AI, European Commission, High-Level Expert Group on Artificial Intelligence, 2019.
2. Implementation of Fairness Principles in Financial Institutions Use of Artificial Intelligence/Machine Learning, Information paper, Monetary Authority of Singapore, 2022.
3. Floridi, L. (2019) What the Near Future of Artificial Intelligence Could Be. Philosophy & Technology, 32, 1–15.
4. Russell, S., Norvig, P. (2021) Artificial Intelligence: A Modern Approach, 4th US ed. Pearson.
5. Turner, J. (2018) Robot Rules Regulating Artificial Intelligence, Palgrave Macmillan Cham.
6. Кутейников, Д., Ижаев, О. (2023) Системы искусственного интеллекта – обзор определений, AI How to Comply
7. Михайлов, А. (2006) Измами с ценни книжа. – Пазар и право, № 1.
8. Михайлов, А. (2006) Проверки на инвестиционни посредници, правомощия на Комисията за финансов надзор. – Пазар и право, № 9.
9. Михайлов, А. (2022) Работата с информатори в американските военни и цивилни агенции. Поуки за Република България, София: За буквите.

[2] За тактиката на използване на информатори и извънпроцесуални способи виж Михайлов, А. (2022) Работата с информатори в американските военни и цивилни агенции. Поуки за Република България, ISBN 978-619-1855-23-0, София: За буквите.

Правна регулация на дигиталната трансформация в онлайн комуникациите. Новости в регулацията на онлайн платформите в ЕС

Мария Илиева*

Приемането на т.нар. „законодателен пакет“ под формата на две законодателни предложения – Законодателен акт за цифровите услуги и Законодателен акт за цифровите пазари, бяха дългоочаквани мерки, които имат за цел да осигурят по-голяма правна сигурност за потребителите в областта на цифровите услуги и да гарантират отговорно поведение на онлайн платформите. Предложенията бяха разработени след открита обществена консултация, включваща широк кръг от заинтересовани страни като академични среди, цифрови компании, асоциации, публични органи и др. Необходимостта от създаване на нови законодателни рамки е налице поради бързото технологично развитие и факта, че сегашната Директива 2000/31/ЕО на Европейския парламент и на Съвета от 2000 г. за електронната търговия не отговаря на съвременните предизвикателства. С оглед на значителното преместване на дейностите в онлайн средата, цифровите платформи придобиват все по-голямо значение в нашия живот. Целта на този доклад е да направи кратко проучване на съответните регламенти в контекста на конкурентните правила и въздействието им върху нарастващата употреба на онлайн платформите. В доклада се предоставя и кратко сравнение с настоящата правна уредба, за да се разберат практическите последици, които ще настъпят при въвеждането на новото законодателство.

***Ключови думи**: дигитални комуникации, Директива 2000/31/ЕО на Европейския парламент и на Съвета от 8 юни 2000 година за някои правни аспекти на услугите на информационното общество, и по-специално на електронната търговия на вътрешния пазар (Директива за електронната търговия), Законодателен акт за цифровите услуги, Законодателен акт за цифровите пазари, онлайн платформи, правни регулации*

* Мария Илиева, докторант в департамент Медии и комуникация, Нов български университет, ел. поща: mariya.ilieva89@gmail.com

Legal Regulation of Digital Transformation in Online Communications. New Developments in the Regulation of Online Platforms in the EU

Mariya Ilieva*

The adoption of the so-called legislative package in the form of two legislative proposals, the Digital Services Act and the Digital Marketplaces Act, were long-awaited measures aimed at providing greater legal certainty for consumers in the area of digital services and ensuring responsible behaviour by online platforms. The proposals were developed following an open public consultation involving a wide range of stakeholders such as academics, digital companies, associations, public authorities and others. There is a need for new legislative frameworks due to rapid technological developments and the fact that the current Directive 2000/31/EC of the European Parliament and of the Council of 2000 on electronic commerce does not meet today's challenges. In view of the significant shift of activities to the online environment, digital platforms are becoming increasingly important in our lives. The purpose of this report is to briefly examine the relevant regulations in the context of competition rules and their impact on the growing use of online platforms. The report also provides a brief comparison with the current legal framework in order to understand the practical implications that will arise when the new legislation is introduced.

Keywords: *Digital communications, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Digital Services Act, Digital Markets Act, online platforms, legal regulations*

* Mariya Ilieva, PhD student at the Department of Media and Communications in New Bulgarian University, e-mail: mariya.ilieva89@gmail.com

Дигиталните технологии промениха света и начина, по който живеем, превръщайки много аспекти от него в цифрови данни, които спомогнаха за бързото развитие на новите технологии и трансформацията на нашето общество. Цифровите технологии се утвърждават като неотменима компонента от нашата съвременна същност, като тяхното експоненциално разрастване е съпътствано от глобалната пандемия, породена от COVID-19. Всеки ден пренасяме все по-голяма част от дейностите си в онлайн пространството, като не изключваме служебните задължения, закупуването на стоки от първа необходимост, общуването с близки хора или извършването на административни услуги. Що се отнася до прехвърляне на нашите дейности в онлайн среда, съществуват много пречки и открити правни въпроси и неизвестни, които несъмнено са свързани с действията в онлайн пространството. Несъмнено част от правните въпроси, свързани с времето, прекарано в онлайн пространството, обхващат защитата на личните данни, защитата на потребителя, блокирането на достъпа до определено съдържание (независимо дали по търговски или правни причини), режима на отговорност за съдържание, публикувано онлайн, както и широк кръг аспекти, свързани с функционирането на цифровите онлайн платформи. По отношение на цифровите платформи, онлайн платформите или платформите за сътрудничество, както често ги използват като взаимозаменяемо, са обект на експертни дискусии по отношение на няколко аспекта. Тези аспекти включват отговорността на платформите във връзка с предоставянето на услугите, техният пазарен статут, отношенията им с обичайните доставчици на услуги, както и позицията на отделните платформи една спрямо друга.

Нелоялната конкуренция, свързана с бизнес условията, „неписаните практики“ и възможното антиконкурентно поведение на цифровите платформи, представлява актуален проблем. Един от съществените въпроси, които се обсъждат, е определението на онлайн платформите и параметрите, които ги класифицират като такива, както и последиците от тази дефиниция.

Връзката между онлайн платформите и института на конкуренцията отразява както публични, така и частни аспекти. При разглеждането на частноправните аспекти особено се фокусира върху бизнес условията, които влияят както на крайните потребители, така и на лицата, които предоставят услугите чрез платформите. Остава и въпросът дали платформата сама предоставя услугата или просто действа като посредник между прекия доставчик на услугата и „клиента“ като краен получател. Обичайно онлайн платформите се разглеждат като посредници, заемайки позицията между прекия доставчик на услуги и клиента като адресат, краен получател на услугата. През 2016 г., с предприемането на нови политики и стратегии, Европейската комисия отбеляза, че е необходимо да се проучи за всеки отделен случай дали отделна платформа предоставя услуги или е просто посредник.

За да отговори на всички тези предизвикателства, Европейският съюз (ЕС) предприе действия по приемане на т.нар. „законодателен пакет“ под формата на две основни предложения за законодателни актове, предназначени да прилагат дигиталната стратегия на ЕС. Заедно Законодателният акт за цифровите услуги (Digital[1] Service Act) и Законодателният акт за цифровите пазари (Digital Markets Act[2]) имат за цел да създадат по-безопасно дигитално пространство и да установят равни условия за насърчаване на иновациите и растежа както в ЕС, така и в световен мащаб.

Актуалното приемане от Европейския парламент на Законодателния акт за цифровите услуги представлява значителна стъпка в регулирането на онлайн платформите в правото на Европейския съюз (ЕС). Това предложение за законодателство, заедно с предходно приетия Законодателен акт за цифровите пазари, създава всестранна рамка за регулиране на онлайн платформите, което е първообразно в Европа и в световен мащаб.

1. Ретроспекция и съвремие на правната рамка за онлайн платформите

До приемането на Законодателния акт за цифровите пазари и Законодателния акт за цифровите услуги, който ще се прилага пряко в целия ЕС от 17 февруари 2024 г., регулирането на онлайн платформите беше предоставено на отделните държави членки. Като основна правна рамка за онлайн платформите и услугите се използваше Директива 2000/31/ЕО на Европейския парламент и на Съвета от 8 юни 2000 г., която обхваща различни правни аспекти на информационното общество и по-конкретно електронната търговия на вътрешния пазар (Директива за електронната търговия). Поради факта, че тази директива е приета през 2000 г., както и вследствие на динамиката на развитие на социалните процеси в резултат на дигитализацията, стана ясно, че в сегашната ера на цифровизация, е необходима нова законодателна уредба, която да отразява променливостта и развитието ѝ в тази област.

Важно е също така да се отбележи, че понастоящем във връзка с онлайн платформите и посредническите услуги имаме и Регламент 2019/1150 на Европейския парламент и на Съвета от 20 юни 2019 г. за насърчаване на спра-

[1] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) as known as DSA.

[2] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) as known as DMA.

ведливостта и прозрачността за бизнес потребителите на онлайн посреднически услуги. Този регламент по същество е първият правен акт, който урежда конкретни аспекти, свързани с онлайн платформите. Този регламент може да се нарече регламент за взаимоотношенията между предприятията (Business to Business a.k.a. B2B[3]), тъй като неговата роля е да регулира справедливите и прозрачни условия за бизнес потребителите. Регламент (ЕС) 2021/784 от 29 април 2021 г. относно справянето с разпространението на терористичното съдържание онлайн има за цел да предотврати и противодейства на разпространението на терористично съдържание в онлайн пространството. Това е една от инициативите на Европейския съюз за борба с тероризма и насърчаване на сигурността в дигиталната среда. Регламентът съдържа различни задължения за онлайн платформите и интернет доставчиците, с които се регламентират техните действия по отношение на терористичното съдържание. Някои от ключовите мерки и задължения включват:

- Бързо премахване на терористичното съдържание: онлайн платформите и интернет доставчиците трябва да премахват терористичното съдържание в рамките на един час от получаването на официално уведомление от компетентните органи в съответната държава въз основа на приложимото право. Това се отнася както за активно разпространявано съдържание, така и за съдържание, което е било предишно премахнато и се появява отново.
- Използване на автоматични инструменти за откриване и премахване на съдържание: онлайн платформите и интернет доставчиците трябва да използват автоматични инструменти за откриване и премахване на терористичното съдържание, като прилагат мерки за предотвратяване на негативни последици върху законното съдържание.
- Разработване на политики и средства за съобщаване и сътрудничество: Онлайн платформите трябва да разработят и публикуват политики и механизми за съобщаване на терористично съдържание от страна на потребителите. Те трябва също да установят средства за сътрудничество с компетентните органи.

В България Законът за електронната търговия (ЗЕТ) в известна степен, но не единствено и изчерпателно, е правният акт, който регулира електронната търговия в дигиталната сфера. В своята приложимост Законът за електронната търговия обхваща различни ключови сфери, които подлежат на негово регулиране, като същевременно се насърчава взаимодействието с дигиталните комуникации и онлайн платформите. Един от съществените

[3] Business to Business (B2B): What it is and how it`s used, https://www.investopedia.com/terms/b/btob.asp

аспекти, които ЗЕТ регулира, са електронните договори. В съответствие с акта се определят правилата за извършване на електронни договори, които могат да се сключват посредством използването на онлайн платформи. Включват се условията за валидност на електронните договори, механизмите за приемане на предложенията и други аспекти, свързани с електронната форма на такива договори.

Освен това Законът за електронната търговия урежда и информационните изисквания, които се прилагат към онлайн платформите и търговците. Онлайн платформите, респективно търговците подлежат на задължение да предоставят ясна и изчерпателна информация относно предлаганите от тях продукти и услуги. Важната информация, която трябва да е публично достъпна, е тази, която позволява на потребителите да се осведомят за цени, условия на доставка, потребителските им права и др.

ЗЕТ също така урежда и защита на потребителите, които извършват онлайн пазаруване, и определя задълженията на онлайн платформите и търговците в тази сфера. Той осигурява правни инструменти за защита срещу недобросъвестни практики, предлага механизми за отказ и възстановяване на плащания и регулира други важни аспекти, свързани със защита на интересите на потребителите.

Също така ЗЕТ има приложимост и към електронните съобщения, които включват електронна поща, мобилни съобщения, факсове и други форми на комуникации. Този аспект на законодателството е свързан с дигиталните комуникации, като установява правила за изпращане на нежелани съобщения (спам), задържане на комуникациите и други въпроси, свързани с комуникациите в електронен формат.

В заключение, ЗЕТ регламентира различни аспекти на електронната търговия, включително правилата за сключване на договори, информационните изисквания, защитата на потребителите и електронните съобщения, като същевременно има и своето отражение върху дигиталните комуникации и онлайн платформите.

2. Цели и принципи на новите законодателни предложения – Законодателен акт за цифровите пазари и Законодателен акт за цифровите услуги

В рамките на приоритета на Европейската комисия „Европа, пригодена за цифровата ера“[4] се предвижда въвеждането на ново законодателство в

[4] A Europe fit for the digital age. Empowering people with a new generation of technologies, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en

областта на цифровите технологии. Това разкрива намерението на Европейския съюз да бъде законодателно подготвен за настъпващата цифрова ера, въпреки че контурите ѝ ще станат напълно ясни през следващите години. Онлайн пространството представя определени особености, които не са присъщи на офлайн средата и офлайн комуникационните модели. Тези особености създават правна несигурност в множество аспекти, особено във връзка с факта, че при сключване на договори чрез електронни средства (т.нар. „онлайн или виртуални договори“) нямаме достатъчна възможност за проверка на самоличността на другата страна. Въпросите за „онлайн сигурност“ и сигурност на онлайн пазаруването често биват предизвикани, тъй като все още се наблюдават различни измамни практики. Въпреки това въпросът за сигурността на онлайн пазаруването и осигуряването на плащания за закупените стоки онлайн са изключително комплексни.

С оглед смекчаване на правния вакуум и нелоялните практики, създаването на регулаторна рамка заляга сред приоритетите на ЕС поради значимостта на цифровата икономика и важната роля на онлайн платформите. В този смисъл решаването на тези проблеми е от съществено значение. Европейският съюз проявява интерес към бизнеса и търговията, като насочва усилията си към хармонизиране на законодателството на държавите членки.

Акцентирайки върху онлайн съдържанието, е важно да бъдат изтъкнати инициативите, предприети от Европейския съюз с цел преодоляване на географските пречки, познати като „географско блокиране“, със стремеж да се уравновеси достъпът до онлайн услугите. Представените законодателни инициативи имат за цел създаването на по-безопасно цифрово пространство, където основните права на всички потребители на цифрови услуги да бъдат защитени, и създаването на равни условия за насърчаване на иновациите, растежа и конкурентоспособността както в единния европейски пазар, така и в глобален мащаб[5]. В следващите раздели от доклада ще се опитам да откроя основни новости в правната рамка на двата регламента – Законодателен акт за цифровите услуги (Digital Service Act) и Законодателен акт за цифровите пазари (Digital Markets Act).

[5] EU Digital Markets Act and Digital Service Act explained, https://www.europarl.europa.eu/news/en/headlines/society/20211209STO19124/eu-digital-markets-act-and-digital-services-act-explained?&at_campaign=20234-Digital&at_medium=Google_Ads&at_platform=Search&at_creation=RSA&at_goal=TR_G&at_audience=digital%20markets%20act%20european%20commission&at_topic=DMA_DSA&at_location=BG&gclid=CjwKCAjwvpCkBhB4EiwAujULMpXpvauBjOnKmEH82irUSL_567Qy-QkbLctBfoI0mJM_Q-jmw-BFxoCgnoQAvD_BwE

3. Преглед на предложение за Законодателен акт за цифровите услуги (Digital Service Act)

Основна цел на Законодателния акт за цифровите услуги е да създаде правна рамка и възможност за по-добра защита на потребителите и техните основни права онлайн, да създаде макет за висока прозрачност и ясна отчетност на онлайн платформите и да насърчи иновациите[6]. Законодателният акт за цифровите услуги влезе в сила на 16 ноември 2022 г. и ще се прилага пряко в целия ЕС от 17 февруари 2024 г. За да разберем действително каква е целта, предмета и обхвата на Законодателния акт за цифровите услуги, трябва да се обърнем към дефиницията, така сме свикнали от теорията в правото, но и във всяка друга дисциплина. Съгласно предмета на регламента, дефиниран в член 1, параграф 2 „С настоящия регламент се установяват хармонизирани правила относно предоставянето на посреднически услуги на вътрешния пазар. По-специално с него се установяват:

а) рамка за условно освобождаване от отговорност на доставчиците на посреднически услуги;

б) правила относно специални задължения за дължима грижа, съобразени с особеностите на някои специални категории доставчици на посреднически услуги;

в) правила за изпълнението и осигуряване на спазването на настоящия регламент, включително по отношение на сътрудничеството и координацията между компетентните органи“.

Целта на Законодателния акт за цифровите услуги (ЗАЦУ) е определена в член 1, параграф 1, а именно: „допринася за правилното функциониране на вътрешния пазар за посреднически услуги чрез установяване на хармонизирани правила за безопасна, предсказуема и надеждна онлайн среда, която улеснява иновациите и в която основните права, залегнали в Хартата, са ефективно защитени“.

Досега като основна регулаторна рамка се възприемаше Директива 2000/31/ЕО на Европейския парламент и на Съвета от 8 юни 2000 г., която, както споменах по-горе, обхваща различни правни аспекти на информационното общество и по-конкретно електронната търговия на вътрешния пазар (Директива за електронната търговия). В Законодателния акт за цифровите услуги в член 2, параграф 3 европейският законодател е записал, че „Настоящият регламент не оказва въздействие върху прилагането на

[6] Digital Service Act: ensuring a safe and accountable online environment https://www.eurojust.europa.eu/publication/digital-services-act-ensuring-safe-and-accountable-online-environment#:~:text=The%20Digital%20Services%20Act%20(DSA,safe%20and%20trusted%20online%20environment.

Директива 2000/31ЕО“. Интересното в ЗАЦУ е, че в заключителните разпоредби и чл. 89 е записано, че със Законодателния акт за цифровите услуги се изменя Директива 2000/31/ЕО и се заличават текстовете в чл. 12–15 от Директивата за електронната търговия. Цитираните по-горе разпоредби от Директивата за електронна търговия създават основата на правната структура, регулираща отговорността на онлайн платформите. От друга страна, режимът на отговорност е детайлно обсъден в текста на представения Законодателен акт за цифровите услуги (Digital Service Act). Формулировка за отговорността на онлайн платформите е разписана в член 3, 4, 5 и 7, с тази разлика, че съгласно чл. 8 от ЗАЦУ се предвижда, че на доставчиците на посреднически услуги не се налага общо задължение за наблюдение на информацията, която те пренасят или съхраняват, нито за активно търсене на факти или обстоятелства, указващи на незаконна дейност.

Текстовете на Законодателния акт за цифрови услуги (Регламент (ЕС) 2022/2065) преодолява въпроси, свързани с отговорността на посредническите платформи и предвижда редица нови задължения, произтичащи от тяхната позиция. С Регламент (ЕС)2022/2065 се въвеждат нови институции и механизми в контекста на онлайн платформите. Обхватът на задълженията е широк и надвишава обхвата на сегашната регулация на Директива 2000/31/ЕО за електронната търговия. В заключение оценявам, че Законодателният акт за цифрови услуги (Регламент (ЕС) 2022/2065) притежава потенциал да създаде правна сигурност и да задълбочи европейския вътрешен пазар, едновременно надграждайки изискванията за отговорност и защита на потребителите. Същевременно остава и въпросителната в уравнението къде ще падне тежестта и отговорността дали незаконно съдържание няма да мигрира към по-малки и по-малко регулирани платформи, като това е въпрос, който предстои да бъде обследван и посредством практиката на Съда на ЕС[7].

4. Преглед на предложение за Законодателен акт за цифровите пазари (Digital Markets Act)

Законодателният акт за цифровите пазари (ЗАЦП) влезе в сила на 1 ноември 2022 г., но започна да се прилага шест месеца след влизането си в сила, от 2 май 2023 г. Този законодателен акт заедно със Законодателния акт за цифрови услуги са два от основните елементи и опорни документи, има-

[7] Broadbent, M. The Digital Service Act, the Digital Markets Act, and the New Competition Tool, Center for strategic and international studies, November 20 2021, p. 8, available at: https://www.csis.org/analysis/digital-services-act-digital-markets-act-and-new-competition-tool

щи ключово значение по отношение на Европейската цифрова стратегия.[8] В член 3 от ЗАЦП за първи път се появява и новото понятие – „контролиращи достъпа предприятия или т.нар. „gatekeepers“. Законодателният акт за цифровите пазари въвежда конкретни и обективни критерии за големите онлайн платформи, които отговарят на понятието „контролиращи достъпа предприятия/gatekeepers“. Тези критерии имат за цел да се акцентира върху проблемите, свързани с големите и системни онлайн платформи, които имат значително икономическо влияние върху вътрешния пазар и оперират в няколко държави – членки на Европейския съюз. Също така тези платформи трябва да притежават силна посредническа роля, свързвайки значителен брой потребители с множество предприятия. Освен това те трябва да имат установена и стабилна позиция на пазара, което се доказва чрез спазването на определени критерии за последните три финансови години. Такива мерки са важни за създаването на равни условия, защита на потребителите и насърчаване на иновациите в цифровата среда. Основна разлика между двата законодателни акта се състои в това, че с въвеждане на понятието „пазачи на информационния вход“ се цели да се установят хармонизирани правила, с които да се гарантират конкурентни пазари в цифровия сектор в Европейския съюз. Платформите, които действат като „пазачи на информационния вход“, трябва да изпълняват няколко важни условия, които ще изложа по-надолу в текста. Първо, те трябва да предоставят възможност на трети страни да взаимодействат със собствените им услуги в определени ситуации. Това включва отварянето на платформата за външни участници, които могат да предлагат свои продукти или услуги на платформата. Второ, те трябва да осигурят на своите бизнес ползватели достъп до данните, генерирани при използването на платформата. Това включва предоставянето на информация за потребителското поведение и предпочитания, които могат да бъдат полезни за бизнес развитието на тези ползватели. Трето, платформите трябва да предоставят на дружествата, които рекламират върху техните платформи, достъп до инструменти и информация, които им позволяват да извършват собствена проверка на своите реклами. Това включва даването на възможност на рекламодателите и издателите да проследят ефективността и съответствието на рекламните си материали. Накрая, платформите трябва да позволяват на своите бизнес ползватели да популяризират и продават своите продукти или услуги извън рамките на платформата. Това създава

[8] The Digital Markets Act: ensuring fair and open digital markets. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

възможност за бизнес разширение и пряко взаимодействие с клиентите извън онлайн средата на пазача на информационния вход. Всички тези мерки имат за цел да създадат равни условия за участниците и да насърчат конкуренцията и иновациите в цифровата среда.

Респективно платформите, действащи като „пазачи на информационния вход“, вече няма да могат да третират собствените си услуги и продукти по по-благоприятен начин при класирания в сравнение със сходни продукти или услуги, предлагани от трети страни на платформата на пазача на информационния вход. Също така няма да разполагат с възможността да възпрепятстват свързването на потребители с предприятия извън техните платформи, както и да им възпрепятстват деинсталацията на предварително инсталиран софтуер или приложения, ако те желаят това. Накрая, но не по-маловажно, без изричното съгласие на крайните потребители, платформите няма да бъдат в състояние да проследят потребителите извън своите основни платформени услуги с цел насочена реклама.

Законодателният акт за цифровите пазари предвижда прилагането на санкции съгласно определени критерии в случай на нарушения. Тези санкции могат да достигнат до 10% от общия годишен световен оборот на дружеството или до 20% в случай на повторни нарушения. При периодични имуществени нарушения санкциите са ограничени до 5% от средния дневен оборот. Освен финансовите санкции, в случай на системни нарушения от страна на „пазачи на информационния вход“ могат да се приложат и допълнителни корективни мерки след провеждане на пазарно разследване. Възлагането на такива мерки трябва да бъде пропорционално на извършеното нарушение. Ако е необходимо, като последна инстанция, могат да се наложат нефинансови мерки, като например продажба на (части от) предприятието, което да осигури подходяща корекция и справедливост.

5. Практика на Съда на Европейския съюз

5.1. Решение на съда от 22 юни 2021 г. по съединени дела C-682/18 и C-683/18[9]

Във връзка с гореизложеното интересен и релевантен пример, обхващащ няколко законодателни акта на ЕС, е Решение на съда от 22 юни 2021 г. по съединени дела C-682/18 и C-683/18. Делата са с предмет две

[9] Решение на съда от 22 юни 2021 г. по съединени дела C-682/18 и C-683/18. Достъпно на: https://curia.europa.eu/juris/document/document.jsf?text=&docid=243241&pageIndex=0&doclang=BG&mode=req&dir=&occ=first&part=1&cid=3623813#Footnote*

преюдициални запитвания, отправени на основание член 267 ДФЕС от Bundesgerichtshof (Федерален върховен съд, Германия) съответно с актове от 13 септември 2018 г. и от 20 септември 2018 г., постъпили в Съда на 6 ноември 2018 г., в производствата по дела: *Frank Peterson срещу Google LLC, YouTube Inc*., *YouTube LLC, Google Germany GmbH* (дело C-682/18) и *Elsevier Inc. срещу Cyando AG* (дело C-683/18).

В един виртуален свят, изпълнен с безкрайни потоци от цифрово съдържание, едно съдебно разглеждане засяга сърцевината на интелектуалната собственост. В центъра на това разглеждане се намират платформите, които служат за кръстопът на информационни потоци, където потребителите споделят своето съдържание. Но каква е отговорността на тези Директиви, играещи ролята на „дигитални стражи", когато става дума за авторски права? Едно преюдициално запитване подхвърля тази тема в ръцете на съдиите в Съда на ЕС, изследвайки какви мерки трябва да се предприемат, за да се избегне нарушаване на закони – Директиви на ЕС. Именно това е фокусът на доклада, който разглежда фините юридически нюанси и задълженията, които съпътстват управлението на онлайн платформи в сянката на авторското право.

Запитванията са отправени в рамките на спорове, единият от които се води между г-н Франк Петерсон, музикален продуцент, и Google във връзка с публикуването в YouTube през 2008 г. на записи на Сара Брайтман, за които се твърди, че притежава различни права. Твърди се още, че записите са били публикувани в нарушение на изключителните права на Франк Петерсон от потребители на тази платформа без негово разрешение (дело C-682/18). Компанията YouTube не е отстранила или блокирала незабавно, въпреки че е била уведомена, че тези произведения са били незаконно предоставени на публично разположение чрез платформата.

Другият спор, по който е образувано дело C-683/18 касае издателя Elsevier, който предявява иск пред германските съдилища за неправомерно публикувани в платформа за съхраняване и споделяне „Uploaded" произведения. Cyando поддържа платформата Uploaded, която предлага на всеки интернет потребител безплатно място за съхраняване, за да качва (*upload*) файлове, като се твърди, че е качена медицинска литература, за която изключителни права има Elsevier. Връзката между двете дела и отправените преюдициални запитвания, по които после съдът дава разяснения, касаят отговорността на операторите на онлайн платформите по отношение на произведения, защитени с авторско право, които са незаконно публикувани онлайн на тези платформи от потребители на същите. Според заключението на генералния адвокат операторът на платформа за споделяне на видеоклипове и операторът на платформа за съхраняване и споделяне на файлове по

принцип могат да се ползват от предвиденото в тази разпоредба освобождаване от всяка отговорност, която може да произтече от файловете, които съхраняват по молба на потребителите на платформите си.

В рамките на спора по двете дела са съставени 6 преюдициални въпроса. Първият търси отговор дали се счита за публично разгласяване дейността на оператора на онлайн платформа по смисъла на член 3, параграф 1 от Директивата за авторското право[10], когато там се качват видеоклипове със защитено авторско съдържание без разрешението на носителите на авторските права, особено когато операторът на платформата извлича доходи от реклама и процесът на качване е автоматизиран без предварителен преглед или контрол от страна на оператора. Ако отговорът на първия въпрос е отрицателен, то целта на втория въпрос е да разясни, ако операторът на онлайн платформата не се счита за извършващ публично разгласяване по Директивата за авторското право, попада ли дейността му под режима на освобождаване от отговорност за посреднически услуги съгласно чл. 14, параграф 1 от Директивата за електронната търговия? Това преюдициално запитване поставя под въпрос ключови аспекти от регулацията на онлайн платформите и отговорността им в контекста на авторските права. Отговорите на тези въпроси от Съда на ЕС ще бъдат решаващи за бъдещето на регулирането на интернет пространството и защитата на интелектуалната собственост в цифровата епоха. Важно е да се намери правилен баланс, който да позволява и защита на авторските права и свобода на изразяване и иновациите.

По преюдициалните запитвания съдът е заключил, че тълкувайки Директива 2001/29/ЕО, оператор на платформа за споделяне на видеа или файлове не се счита за извършващ „публично разгласяване“ на защитено съдържание, освен ако активно допринася за нарушението на авторските права. Това важи, когато операторът има ясна информация за незаконно качено съдържание и не предприема действия за неговото премахване, не прилага необходимите технически мерки за предотвратяване на нарушения или подпомага нарушенията, например чрез предлагане на инструменти за споделяне или привличане на потребители към незаконно споделяне. Съдът дава тълкувание и на чл. 14, пар. 1 от Директива 2000/31/ЕО, като обосновава, че операторите на онлайн платформи за споделяне на видео и файлове се вписват в параметрите на Директивата, стига да не участват активно в знанието или контрола на незаконно каченото съдържание. Те могат да се ползват от освобождаване от отговорност, ако не са наясно с конкретни незаконни действия на своите потребители свързани със защитено съдържание

[10] Директива 2001/29/ЕО на Европейския парламент и на Съвета от 22 май 2001 година относно хармонизирането на някои аспекти на авторското право и сродните му права в информационното общество.

на техните платформи. Член 8, пар. 3 от Директива 2001/29/ЕО позволява постановяването на съдебни забрани срещу посредници, използвани за нарушаване на авторски права, дори без те да имат знание за нарушението, стига да са били уведомени и да не са предприели действия за премахване на въпросното съдържание или за предотвратяване на повторните нарушения. Националните съдилища трябва да гарантират, че тези мерки не причиняват несъразмерни вреди на притежателя на правата.

За да задълбочим и обогатим правните изводи така, че да звучат убедително и да привлекат вниманието на читателите, трябва да анализираме детайлно и да подчертаем баланса, постигнат от Съда на Европейския съюз. В заключение документът съдържа изводите на Съда на ЕС по делата C-682/18 и C-683/18, които обсъждат въпроси, свързани с авторските права в контекста на интернет платформите. Тези изводи уточняват обхвата на „публичното разгласяване“ и условията, при които операторите на платформите могат да бъдат освободени от отговорност. Съдът подчертава важността на активната роля на операторите при надзора на съдържанието и необходимостта от бърза реакция при получаване на конкретна информация за нарушение. Съдът разглежда сложното взаимодействие между защитата на интелектуалната собственост и насърчаването на технологичните иновации и обмена на информация. Важно е да се акцентира на изискванията за платформите да предприемат активни мерки срещу нарушенията на авторските права и да разработят системи за превенция и контрол в реално време. Този анализ ще обсъди и потенциалното въздействие на решенията върху развитието на цифровите услуги и бъдещето на управлението на цифровите права в контекста на съдържанието, генерирано от потребителите. Мисля, че тези решения имат значително въздействие върху регулаторната рамка, като налагат строги изисквания към операторите на онлайн платформи и подсилват защитата на авторските права в дигиталната среда. На следващо място, това изисква от платформите не само да предприемат мерки срещу нарушенията на авторските права, но и да разработят и прилагат своевременно системи за превенция и надзор.

5.2. Решение по дело C-401/19 от 26 април 2022 г. на Съда на ЕС[11]

Интересна е също практиката на Съда на ЕС в горецитираното решение, с което съдът отхвърли иска на Република Полша за отмяна на член 17 от Директива 2019/790 относно авторското право и сродните му права в цифровия единен пазар. Полша предявява иск за отмяна на чл. 17 от Директива

[11] https://curia.europa.eu/juris/documents.jsf?nat=or&mat=or&pcs=Oor&jur=C%2CT%2CF&num=C-401%252F19&for=&jge=&dates=&language=en&pro=&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&oqp=&td=%3BALL&avg=&lgrec=en&page=1&lg=&cid=5340160

2019/790, като според нея този член нарушава свободата на изразяване на мнение и свободата на информация, гарантирани от Хартата на основните права на ЕС. Съдът постановява, че при изготвянето на член 17 законодателят на ЕС е предвидил подходящи гаранции за защита на свободата на изразяване/информация и е дал важни насоки относно прилагането на новия режим на отговорност на практика. Анализът на решението ще бъде обект в друго изследване, но междувременно в съвсем краткия финален обзор бих искала да насоча вниманието на аудиторията и към него. С член 17 от Директивата, приета на 17 април 2019 г., се определят нови правила за отговорността на някои доставчици на услуги, по-конкретно доставчици на услуги за споделяне на онлайн съдържание.

Чрез член 17 Директивата значително разширява правата на носителите на права спрямо доставчиците на услуги за споделяне на онлайн съдържание (определени като доставчици на услуги на информационното общество, чиято основна цел е да съхраняват и предоставят публичен достъп до голямо количество защитени с авторско право произведения или други защитени обекти, качени от техните потребители, които те организират и популяризират с цел печалба). В него ясно се посочва, че такива доставчици съобщават на обществеността произведения, качени от техните потребители, когато предоставят достъп до такива произведения. Това беше много спорен въпрос в рамките на Директива 2001/29, като по-горе съм дала пример с делото *YouTube и Cyando* (C-682/18 и C-683/18).

За да избегнат отговорността, доставчиците трябва да получат разрешение от носителите на права, например чрез лицензионно споразумение. При липса на такова разрешение те по принцип носят основна отговорност за съдържанието, освен ако не могат да докажат, че са положили максимални усилия за получаване на разрешение, положили са максимални усилия, за да гарантират недостъпността на съдържанието, за което са били уведомени от носителите на права (това задължение е било оспорено изцяло от Република Полша) или са реагирали бързо на уведомленията за сваляне и са положили максимални усилия, за да гарантират, че това съдържание ще остане свалено (последното също е било оспорено от Полша).

В заключение решението на Съда на ЕС относно тълкуването на член 17 от Директива 2019/790 има значителни правни последици по отношение на отговорността на доставчиците на услуги за споделяне на онлайн съдържание. С тази правна уредба се налага по-голяма отговорност за доставчиците на услуги на информационното общество, като се изисква разрешение от носителите на авторски права за съдържанието, което потребителите им качват. Съдът на ЕС потвърждава, че този режим на отговорност се съобразява със свободата на изразяване и информация, предоставяйки

гаранции и насоки за защита на тези права. Този анализ, поднесен от съда на ЕС, подчертава важността на съответната регулация и съобразяване с новите изисквания на цифровата епоха, като същевременно подчертава необходимостта от сътрудничество между субектите, притежаващи авторски права върху произведенията и платформите за споделяне на съдържание, за да се осигури защита на авторските права и свободата на изразяване в дигиталното общество.

Заключение

Представените по-горе в изложението два законодателни акта, а именно Законодателен акт за цифровите услуги (DSA) и Законодателен акт за цифровите пазари (DMA), се считат за задължителни и неотложни в светлината на значимата позиция, която цифровите платформи заемат на пазара и бързият растеж на техните пазарни сили. Прогнозира се, че в бъдеще тяхната позиция ще продължи да се засилва. В този контекст е от съществено значение да се осигури на потребителите висока степен на правна сигурност и ясен набор от правила, които онлайн платформите следва да спазват. Въпреки фрагментарността на двата законодателни акта, необходимо е тяхното еднакво и прецизно тълкуване и прилагане в съответствие с буквата на закона, предимно поради нуждата от правно регулиране на цифровите платформи, особено в областта на конкуренцията, с цел предотвратяване на различни подходи за регулация на ниво Европейски съюз. Различни тълкувания и липса на хармонизиране на правоприлагането на европейските регламенти може да доведе до разнообразни подходи към онлайн платформите и съответно до нелоялна конкуренция на пазара. Поради тази причина е наложително законодателството да бъде приспособено към бизнес моделите на XXI век и да се предостави възможност на цифровите платформи да функционират на пазара в полза на потребителите, съчетана с гаранция за висока степен на защита на техните интереси.

Библиография:

1. Стоянов, Р. К. (2016) Комуникационна демокрация, София, издателство НБУ.
2. Terry Flew, Fiona R. Martin, Digital Platform Regulation. Global Perspectives on Internet Governence. Publisher Global Perspective on Internet Governance.
3. Alexandra Gnach, Wibke Weber, Martin Engebretsen and Daniel Perrin, (2022), Digital Communication and Media Linguistics. Cambridge University Press.
4. Петков, С. (2011) Крос-медийна комуникация, Научен електронен архив на НБУ.

5. Стоянов, Р. К. (2014) Субкултурите в дигиталната реалност, сборник от XVI Лятна школа по PR „Комуникация и култура“, НБУ.
6. Стоянов, Р. К. (2019) Хиперсоциализация в дигитална среда. – В: Европейските ценности – новата констелация, НБУ.
7. Papakonstantinou, V. (2023). States as platforms following the new EU regulations on online platforms. Wilfried Martens Centre for European Studies.

Цитиране на уебсайт:

1. Online portal for access to European Union law. Available at: https://eur-lex.europa.eu/legal-content/BG/ALL/?uri=CELEX:52020PC0825
2. Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions Shaping Europe's digital future. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020DC0067
3. Europe`s Digital Decade: digital targets for 2030. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en
4. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925&qid=1683547214296
5. *Europe fit for the Digital Age: new online rules for platforms*. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-platforms_en?fbclid=IwAR0WqE5F4BYFak02hej3Jljqjqd3r5v05NjeJaB81F49lZ0N1vyM6DIgNi8
6. *The new EU digital regulations: Explained*. Available at: https://www.bruegel.org/podcast/new-eu-digital-regulations-explained?fbclid=IwAR0wIyN9h1n8aFAKK29VwxTx178jQOOUWKFlDQcuZXMRsTWvGKLRWqhViBg
7. *The Digital Service Act: ensuring a safe and accountable online environment.* Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

8. *The EU Digital Markets Act: A Report from a Panel of Economic Experts*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3783436&fbclid=IwAR1y_B-6iAtCPlAsW0M9rPBoX9WH8Zi4TQOBQwK3m6ZYZDjRQSCDOd_HxxM

9. *A Europe fit for the digital age. Empowering people with a new generation of technologies.* Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en?fbclid=IwAR3AfjipHURss4oYTgZI90bU8zckWJklWDhaiqSvLCQ04Kqs3UT7xXc4qs

10. Broadbent M*., The Digital Service Act, the Digital Markets Act, and the New Competition Tool, Center for strategic and international studies, November 20 2021*, available at: https://www.csis.org/analysis/digital-services-act-digital-markets-act-and-new-competition-tool

11. *The Digital Markets Act: ensuring fair and open digital markets.* Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

Съдебна практика:

1. Решение на съда (голям състав) 22 юни 2021 г. по съединени дела C-682/18 и C-883/18 – Frank Peterson срещу Google LLC, YouTube Inc.,YouTube LLC, Google Germany GmbH (C-682/18), и Elsevier Inc. срещу Cyando AG (C-683/18).

2. Решение по дело C-401/19 от 26 април 2022 г. на Съда на ЕС с предмет на жалба за отмяна на основание на член 263 ДФЕС, подадена на 24 май 2019 г. Република Полша срещу Европейски парламент и Съда на Европейския съюз.

Правообразуващи фактори в епохата на цифровата трансформация

Петранка Щерева*

В епохата на цифровата трансформация изпъкват правообразуващи фактори с различна значимост. И настоящото изследване представя въздействието им върху еволюцията на правото в новата среда. Настоящото изследване определя като водещи в тези процеси потребностите от формирането на специфични качества на правото, проявяващи се във виртуалната среда, чрез институционализиране на специфични ефективни регулативни механизми при отчитане на необходимостта от единство и приемственост в механизмите на правно регулиране преди, по време и след цифровата трансформация с оглед наличието на правообразуващи фактори, характеризиращи се с признака новост, други с надграден правообразуващ потенциал.

Ключови думи: *правообразуващ фактор, виртуална среда, качества, регулативни механизми*

* Петранка Щерева, докторант, Катедра „Публичноправни науки“, Правно-исторически факултет, Югозападен университет „Неофит Рилски“, ел. поща: pepishereva@abv.bg.

Legal factors in the age of digital transformation

Petranka Shtereva[1]

In the age of digital transformation, legal factors of different significance stand out. This study presents their impact on the evolution of law in the new environment. The present study identifies as leading in these processes the needs for the formation of specific qualities of law, manifested in the virtual environment, through the institutionalization of specific effective regulatory mechanisms, taking into account the need for unity and continuity in the mechanisms of legal regulation before, during and after the digital transformation in view of the presence of legal factors characterized by the attribute of novelty, others with upgraded legal potential.

Keywords: *legal factor, virtual environment, qualities, regulatory mechanisms*

* Petranka Shtereva, PhD student, Department of Public Law,
Faculty of Law and History, South-West University "Neofit Rilski" – Blagoevgrad,
e-mail: pepishereva@abv.bg.

Единството между виртуално пространство и информационно общество предполага адекватно правно институционализирано съдържание с насоченост към поддържането на устойчивост. Информационното общество използва общодостъпна информация и технологии за обработването на данни. Ето защо информацията и информационните технологии са фактор на промените в обществото и правото. Този вид общество се отличава, защото главен фактор на развитието са идеалните фактори – знание и информация, а не материалните.

Информационното общество въздейства върху правото въз основа на три направления. Първото от тях се формира от новите отношения, които се нуждаят от правна регламентация. Второто направление обхваща действието на правната система, както механизмите на правотворчеството, така и правната реализация. И третото от тях са правната наука и нейният концептуален апарат[1].

Понятие за виртуално пространство

Интернет като информационно пространство е съвкупност от обществени отношения в нефизическа среда, която действа чрез информационни и комуникационни технологии, ето защо се свързва с понятието „виртуално пространство“ или „виртуална реалност“. Това понятие обозначава нефизическа, идеална, изкуствена среда, образувана и действаща по замисъл на човека посредством информационни и комуникационни технологии[2].

Сложността на явлението констатира три групи разбирания към проблема „виртуалност“ или „виртуална реалност“. Първата от тях е разбирането на „термина „виртуалност“ от латинското *virtus* и английското *virtual*“[3], иначе казано, сходство с думата от латински произход. Към гледната точка на втората група е възприемането ѝ като термин, синоним на термините „електронен“ и „компютърен“[4]. И третата група включва подхода към виртуалността, а именно „съвкупност от програмно-технически средства, имитиращи пространството и поведението на субектите в него, създаващи у човека илюзия за местонахождение в моделирано от компютъра пространство“[5].

[1] Кискинов, В. (2019) Правната система. Част I Онтология и методология. София: УИ „Св. Климент Охридски“, 192.
[2] Пак там, 171–176.
[3] Цит. по: Кискинов, В. Цит. съч., 169.
[4] Колев, Т., Цакова, И. (2015) Право и интернет. Въведение в правото и правното регулиране на виртуалното пространство. София: УИ „Св. Климент Охридски“, 40.
[5] Пак там.

В контекста на обозначаване на това пространство, което не може да съществува без интернет, са термините „виртуално пространство“, „киберпространство“, цифрово и дигитално пространство. Върховният съд на САЩ определя киберпространството като: „Уникален носител, известен на неговите ползватели като киберпространство, който не се намира на определена територия, но е достъпен от всеки във всяка точка по света чрез интернет“[6]. Определение за „цифровизация“ и „дигитализация“ е дадено от Бренън и Крейс[7], а именно цифровизацията е дефинирана като „материален процес на преобразуване на отделни аналогови потоци информация в цифрови битове“ и „начина, по който много области на социалния живот се преструктурират около цифровите комуникационни и медийни инфраструктури“ за дигитализацията.

Правното регулиране на цифровото пространство

Правото в цифровата среда създава ново качество на механизма на правно регулиране като система от правни средства с оглед резултативно правно въздействие върху обществените отношения[8]. Тези процеси се свързват с приоритизиране на нормативното регулиране в контекста на пластичност[9].

Спецификата на това правно регулиране и изборът на адекватни средства за въздействие се обуславя както от единството и системността на използваните за регулиране средства, така и от спецификата на регулираните отношения, произтичаща от децентрализирания характер на инфраструктурата на това пространство и на процесите на регулиране[10].

Правообразуващи фактори на цифровата трансформация

Цифровата трансформация е „интеграцията на цифровите технологии от компаниите и отражението на технологиите върху обществото“[11]. Това неизбежно се отразява на условията за възникване, съществуване и

[6] Цит. по: Колев, Т., Цакова, И. Цит. съч., 41.

[7] Цит. по: Дигитална хуманитаристика, научноизследователски блог [онлайн]. [прегледан на 26.06.2023]. Достъпен на http://digitalna-humanitaristika.com/?p=107.

[8] Използвана е интерпретацията на Алексеев, С. С. в: Кискинов, В. Цит. съч., 219.

[9] Използвана е интерпретацията на Л. Лесиг в: Колев, Т., Цакова, И. Цит. съч., 117.

[10] Колев, Т., Цакова, И. Цит. съч., 117.

[11] Европейски парламент [онлайн]. [прегледан на 25.06.2023]. Достъпен на: https://www.europarl.europa.eu/news/bg/headlines/society/20210414STO02010/tsifrovata-transformatsiia-strateghiiata-na-es.

прекратяване на правно релевантни отношения. Процесите на цифрова трансформация релевират правно редица фактори, като им придават правообразуващи качества, а по отношение на други надграждат правообразуващия им потенциал. Тези особености изправят законодателя пред редица предизвикателства, осъществявайки правотворческа дейност в редица направления – интелектуална собственост, лични данни, изкуствен интелект, трудови права и др.

Защита на интелектуалната собственост

В процеса на цифрова трансформация ефективната защита на правата върху обекти на интелектуалната собственост предполага по-висока степен на интензивност с оглед наличието на повече възможности за лесен достъп до защитени обекти чрез използване на съвременните технологии. Правната рамка на защитата на интелектуалната собственост се формира от съдържанието на редица правни нормативни актове: Закон за авторското право и сродните му права (ЗАПСП), Закон за марките и географските обозначения(ЗМГО), Закон за патентите и регистрацията на полезните модели (ЗПРПМ), Закон за промишления дизайн (ЗПД), Закон за топологията на интегралните схеми (ЗТИС) и др.

В съответствие с членството на България в Европейския съюз е хармонизирано законодателството с наднационалното законодателство на общността в областта на защитата на интелектуалната собственост по смисъла на Директива 2001/29/ЕО на Европейския парламент и на Съвета от 22 май 2001 година при хармонизирането на аспекти на авторското право и сродните му права в информационното общество, Директива 93/83/ЕЕС от 27 септември 1993 година при координирането на правила за авторски и свързани с тях права, приложима към сателитно излъчване и кабелно препредаване и за правна закрила на базите данни Директива 96/9/ЕО на Европейския парламент и на Съвета от 11 март 1996 година[12].

Защита на личните данни

Регулаторната рамка с оглед защитата на личните данни в Европейския съюз е установена с регламент на Европейския парламент и на Съвета

[12] Вж. Димитров, Г. (2014) Право на информационните и комуникационните технологии. Гражданскоправни аспекти. Част I. София: Фондация „Право и интернет“, 242.

(ЕС)2016/679 от 27 април 2016 г.[13] за защита на физическите лица при обработването на лични данни, както и свободното движение на такива данни, така и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните). Този регламент е в сила от 25 май 2018 г. с предимство пред националното законодателство и приложението му е пряко.

Защитата на личните данни е еманация на правото на неприкосновеност на личността, а развитието на информационните и комуникационните технологии следва да бъде съпътствано и с развитие на правни механизми за защитата му.

Изкуствен интелект

Развитието на технологиите естествено доведе до създаването на изкуствен интелект и приложението му във все повече характерни за цифровата трансформация правно релевантни социални взаимодействия. Наред с отчитане на положителните резултати обществото е разделено в мнението си за еднозначност на ползите от приложението му. Обществен интерес представляват редици въпроси свързани с областите на приложението му. Дискусионна е и проблематиката следва ли да се признае правосубектност или не на изкуствения интелект.

Заключение

Живеем в бързо развиващ се свят, променящ правото поради обществото на информацията. Дефиницията на това общество е посочена в Постановление № 40 на Министерския съвест за създаване на Координационен съвет по въпросите на информационното общество (ДВ, бр. 22 от 17 февруари 1998 г.), че „..информационното общество е общество с качествено нова структура, организация и обществени отношения, основани на глобалния достъп и използване на информационни и комуникационни мрежи и услуги без национални, географски и други ограничения за обмен на информация, научни, духовни и други постижения“[14]. Правната система на това общество

[13] Официален вестник на Европейския съюз [онлайн]. [прегледан на 07.07.2023]. Достъпен на https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32016R0679&qid=1688693881918.

[14] Цит. по: Попова, М. (2005) Виртуалният човек: Социално-комуникационни особености на интернет потребителя. София: Изток-Запад, 51–52.

следва да е ефективна както в материална, така и във виртуална среда, за да поддържа хомеостазиса в него.

Правото на информационното общество в епохата на цифрова трансформация е динамично, защото виртуалното пространство е с нова специфика и съдържание. Различни са и правообразуващите фактори, обуславящи правотворческите процеси, относими към процесите във виртуалното пространство. Някои от тях се характеризират с признака новост, други са съществуващи, но с надграден правообразуващ потенциал. Обстоятелства, които подчертават необходимостта от единство и приемственост в механизмите на правно регулиране преди, по време и след цифровата трансформация.

Библиография:

1. Върбанов, Р. (2007) България в европейското информационно пространство. Свищов: Стопанска академия „Д. А. Ценов“.
2. Димитров, Г. (2014) Право на информационните и комуникационните технологии. Гражданскоправни аспекти. Част I. София: Фондация „Право и интернет“.
3. Дигитална хуманитаристика научноизследователски блог[онлайн].[прегледан на 26.06.2023]. Достъпен на http://digitalna-humanitaristika.com/?p=107.
4. Европейска комисия[онлайн].[прегледан на 25.06.2023]. Достъпен на https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_bg.
5. Европейски парламент[онлайн].[прегледан на 25.06.2023].Достъпен на: https://www.europarl.europa.eu/news/bg/headlines/society/20210414STO02010/tsifrovata-transformatsiia-strateghiiata-na-es.
6. Кискинов, В. (2019) Правната система. Част I Онтология и методология. София: УИ „Св. Климент Охридски“.
7. Кискинов, В. (2019) Правната система. Част II Състав и действие. София: УИ „Св. Климент Охридски“.
8. Кискинов, В. (2005) Българско и европейско информационно право. Том I. София: Сиела.

9. Колев, Т., Цакова, И. (2015) Право и интернет. Въведение в правото и правното регулиране на виртуалното пространство. София: УИ „Св. Климент Охридски“.

10. Официален вестник на Европейския съюз[онлайн].[прегледан на 07.07.2023]. Достъпен на https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32016R0679&qid=1688693881918.

11. Попова, М. (2005) Виртуалният човек: Социално-комуникационни особености на интернет потребителя. София: Изток-Запад.

Анализ на ролята на основните права в новия законодателен акт за изкуствения интелект на Европейския съюз

Мила Видина*

Законодателният акт за изкуствения интелект (Акт за ИИ) на Европейския съюз ще бъде първият международен правно обвързващ инструмент в света, целящ да установи хармонизирани правила за разработването, пускането на пазара и въвеждането в експлоатация на системи с изкуствен интелект (ИИ). На 8 декември 2023 Европейският парламент и Съветът постигнаха политическо споразумение по измененията на текста на предложението, като официалното приемане на окончателния текст на АИИ от Съвета и Парламента се очаква да приключи ориентировъчно към края на януари 2024. Две от общо четирите конкретни цели на АИИ касаят гарантиране на съответствие и подобряване прилагането на съществуващата правна уредба на Европейския съюз (ЕС) в областта на основните права. Обяснителният меморандум към предложението изрично посочва, че „ценностите на ЕС и основните права“ са в неговата основа и начинът, по който те са включени в новата нормативна уредба, до голяма степен би определил ефективността на тяхната защита. Настоящата статия предоставя общ преглед и анализ на основните компоненти на предложението за АИИ и разяснява ролята на основните права в неговата структурата. Въпреки че до момента АИИ е единственото законодателство за дигитални технологии на Европейския съюз, което толкова амбициозно и изрично включва защитата на основните права в своето приложно поле, анализът разкрива, че мястото и ролята на тези права в новата нормативна рамка са сравнително ограничени и неясни.

***Ключови думи**: дигитални технологии, изкуствен интелект, основни права, право на Европейския съюз, регулиране*

* Мила Видина, редовен докторант към катедра „Международно право и международни отношения“ при Правноисторическия факултет на Югозападния университет „Неофит Рилски“; специалист политики на Европейския съюз в Европейската мрежа на органите за равнопоставеност (European Network of National Equality Bodies, Equinet), ел. поща: milla.vidina@gmail.com

Analysis of the role of fundamental rights in the new European Union Artificial Intelligence Act

Milla Vidina*

The Artificial Intelligence Act (AIA) of the European Union will be the first international legally binding instrument in the world which sets out harmonized rules for the development, marketing, and use of AI systems. On 8 December 2023, the European Parliament and the Council of the European Union reached political agreement on the amendments of the proposal for AIA, with formal adoption of the final text indicatively anticipated to take place by the end of January 2024. Two of the four specific aims of the Act concern ensuring compliance and improving the implementation of the existing legal framework for the protection of fundamental rights in the EU. The Explanatory Memorandum to the proposal explicitly states that "EU values and fundamental rights" are at its core and the way these rights are incorporated in the new legislation would largely determine the effectiveness of their protection. The presents article provides an overview and analysis of the main components of the AIA and explains the role of fundamental rights in its structure. Despite the fact that the AIA is so far the only EU digital technology legislation that so ambitiously and explicitly includes the protection of fundamental rights in its scope, the analysis reveals that the place and role of these rights in its structure are relatively limited and unclear.

***Keywords**: Artificial intelligence, digital technologies, European Union law, fundamental rights,regulation.*

* Milla Vidina, Ph.D. student at the Department of International Relations and International Law, School of Law and History, Southwestern University „Neofit Rilski"; Senior Policy Officer in the European Network of National Equality Bodies, email: milla.vidina@gmail.com

Законодателният акт за изкуствения интелект (Акт за ИИ) на Европейския съюз ще бъде първият международен правно обвързващ инструмент в света, целящ да установи хармонизирани правила за разработването, пускането на пазара и въвеждането в експлоатация на системи с изкуствен интелект (ИИ). Настоящата статия предоставя общ преглед и анализ на основните компоненти на предложението за АИИ и разяснява ролята на защитата на основните права на ЕС в неговата структура. Обяснителният меморандум към предложението изрично посочва, че „ценностите на ЕС и основните права“ са в неговата основа и начинът, по който те са включени в новата нормативна уредба, до голяма степен би определил ефективността на тяхната защита. Настоящият анализ няма за цел да предостави задълбочена оценка на тази ефективност, нито обстойно да обсъди възможното въздействие на АИИ върху защитата на основните права на ЕС в цифровия контекст. Добавената стойност на анализа е в разясняването на общата структура и основни градивни елементи на предложението и ролята на основните права в тази структура.

На 8 декември 2023 Европейският парламент и Съветът постигнаха политическо споразумение по измененията на текста на предложението, въпреки реалната възможност споразумението да бъде осуетено под натиска на няколко държави членки и силно лобиране от страна на бизнес гиганти в последния критичен момент от преговорите. Официалното приемане на окончателния текст на АИИ от Съвета и Парламента се очаква да приключи ориентировъчно към края на януари 2024. Настоящият анализ се базира основно на предложението на Европейската комисия не само поради липсата на официално публикуван текст, но също и защото повечето от основните елементи и цялостната логика на предложението са запазени, а именно те са обект на анализ. В различни части на долу изложения текст са включени разяснения относно определени окончателни изменения, които станаха публично достояние[1].

През април 2021 г. Европейската комисия предложи Регламент за изкуствения интелект, известен като Законодателния акт за изкуствения интелект (Акт за ИИ). Разработването на предложението от Европейската комисия (ЕК) води началото си от 2018 г. с публикуването на актуализираната Стратегия на Европейския съюз за ИИ, последва-

[1] Прессъобщения на следните институции на ЕС и партийни групи в Европейския парламент: the Parliament, the Council, President von der Leyen, the Commission, Renew, S&D, EPP. Виж също следните статии: European Union squares the circle on the world’s first AI rulebook – EURACTIV.com и AI Act: EU policymakers nail down rules on AI models, butt heads on law enforcement – EURACTIV.com

на от Бялата книга на ЕС относно ИИ – „Европа в търсене на високи постижения и атмосфера на доверие“[2] и доклада на ЕК относно последиците за безопасността и отговорността на изкуствения интелект, интернет на нещата и роботиката[3]. Първата индикация за бъдещата законодателна инициатива на Европейската комисия във връзка с ИИ е дадена в политическите насоки на председателя на Европейската комисия Урсула фон дер Лайен за периода 2019–2024 г. „Съюз с по-големи амбиции“, в които се споменава законодателство за координиран европейски подход към човешките и етичните аспекти на ИИ.[4] Основните елементи на бъдещото предложение бяха изложени в гореспоменатата Бяла книга на ЕК – Европейски подход към високи постижения и доверие[5]. Бялата книга определя варианти за политиката на ЕС за това как да се постигне двойната цел за насърчаване на внедряването на технологии с ИИ (така наречената „екосистема на иновациите“) и за справяне с рисковете, свързани с определени употреби на такава технология (така наречената „екосистема на доверие“). Предложението за регулиране на ИИ има за цел да изпълни втората цел на Бялата книга, като предложи правна рамка за сигурен, надежден и етичен ИИ.

Концепцията за „надежден ИИ“ е в основата на законодателното предложение и отразява връзката на предложението с ценностите на ЕС и основните права, така че „хората да имат увереността, че технологията се използва по безопасен и съответстващ на закона начин, включително по отношение на зачитането на основните права“[6]. Две от общо четирите конкретни цели на предложението са пряко свързани със законодателството на ЕС в областта на основните права, а именно: „да гарантира, че системите с ИИ, които се пускат на пазара на Съюза и се използват, са безопасни и в съответствие с действащото законодателство в областта на основните

[2] Европейска комисия, Бяла книга за изкуствения интелект – Европа в търсене на високи постижения и атмосфера на доверие, COM(2020) 65 final, 2020.

[3] Европейска комисия. (2020) Доклад относно последиците за безопасността и отговорността на изкуствения интелект, интернет на нещата и роботиката. Достъпно на: https://ec.europa.eu/info/publications/commission-report-safety-and-liability-implications-ИИ-internet-things-androbotics-0_en

[4] Урсула фон дер Лайен, „Съюз, който се стреми към повече: моята програма за Европа“ (Политически насоки за следващата Европейска комисия 2019–2024 г., 2019 г.).

[5] Европейска комисия, Бяла книга за изкуствения интелект – Европейски подход към високи постижения и доверие, COM(2020) 65 окончателен, 2020 г.

[6] European Commission (2021), Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts Brussels, 21 April, COM(2021). Обяснителен меморандум, с. 1.

права и ценностите на Съюза“ и „да подобри управлението и ефективното прилагане на съществуващата правна уредба в областта на основните права и изискванията за безопасност, приложими към системите с ИИ“[7]. Обяснителният меморандум допълнително подчертава, че предложението е в съответствие с „Хартата на основните права на ЕС и съществуващото вторично законодателство на Съюза относно защитата на данните, защитата на потребителите, недискриминацията и равенството между половете“[8]. Особено внимание се обръща на допълване на съществуващото право на Съюза относно недискриминацията със специфични изисквания, целящи да сведат до минимум риска от алгоритмична дискриминация чрез набор от технически мерки „по отношение на проектирането и качеството на наборите от данни, използвани за разработването на системи с ИИ, както и със задължения за изпитване, управление на риска, документиране и надзор от страна на човека през целия жизнен цикъл на системите с ИИ“[9].

Въпреки горепосоченото изрично включване на основните права в две от конкретните цели на предложението, в Обяснителния меморандум, оперативната част на АИИ, споменава защитата на основните права основно в контекста на осигуряване на необходимото обществено доверие за прогресивното внедряване на ИИ технологиите и намаляване на търговските бариери за движението на ИИ продукти и услуги в ЕС. Това е отразено и в правното основание на предложението, което е член 114 от Договора за функционирането на Европейския съюз (ДФЕС), предвиждащ приемането на мерки за гарантиране на изграждането и функционирането на вътрешния пазар. Предложението е част от стратегията на ЕС за цифров единен пазар и неговата основна цел е да се гарантира правилното функциониране на вътрешния пазар чрез определяне на хармонизирани правила за разработването, пускането на пазара на Съюза и използването на продукти и услуги, използващи ИИ технологии или предоставени като самостоятелни ИИ системи. Член 16 от ДФЕС служи като допълнително, по-ограничено правно основание само във връзка със специфичните правни правила относно защитата на лицата по отношение на обработването на лични данни, по-специално ограниченията за използването на системи с изкуствен интелект за дистанционна биометрична идентификация в „реално време“ на обществено достъпни места за целите на правоприлагането.

[7] Обяснителен меморандум, с. 3.
[8] Пак там, с. 13.
[9] Пак там, с. 4.

Предложението за ЗИИ се основава на подхода на така наречената „нова законодателна рамка“ (НЗР) за промишлените продукти в ЕС, която включва пакет от законодателни мерки, приети през 2008 г., имащи за цел да подобрят вътрешния пазар на стоки чрез подобряване на надзора на пазара посредством актуализирани правила за сертифициране на „безопасни“ продукти и повишаване на качеството на оценките на съответствието.[10] Предложението е част от набор от нови законодателни актове на ЕС, които са свързани с регулирането на ИИ[11], включително:

- Законодателния акт за цифровите услуги[12] (пряко приложим от 1 януари 2024 г.; за особено големи онлайн платформи задължението да публикуват броя на активните си потребители важи до 17 февруари 2023 г.);
- Законодателния акт за цифровите пазари[13] (пряко приложим от началото на май 2023 г.);
- Регламент относно машините [14](преразглеждане на Директивата за машините във връзка с ИИ, здравето и безопасността и машините – в сила от юни 2023 г. и пряко приложима от 20 януари 2027 г.);
- Предложение за Директива за отговорността във връзка със системи с ИИ[15];

[10] Veale, Michael, и Frederick J. Zuiderveen Borgesius. 2021. „„Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach“.“ Computer Law Review International, vol. 22, no. 4: 97–112.

[11] Ibid., p. 99.

[12] Регламент (ЕС) 2022/2065 на Европейския парламент и на Съвета от 19 октомври 2022 г. относно единен пазар за цифрови услуги и за изменение на Директива 2000/31/ЕО (Закон за цифровите услуги) (Текст от значение за ЕИП). Достъпно на: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014

[13] Регламент (ЕС) 2022/1925 на Европейския парламент и на Съвета от 14 септември 2022 г. относно конкурентни и справедливи пазари в цифровия сектор и за изменение на Директиви (ЕС) 2019/1937 и (ЕС) 2020/1828 (Закон за цифровите пазари) (Текст от значение за ЕИП). Достъпно на: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC

[14] Регламент (ЕС) 2023/1230 на Европейския парламент и на Съвета от 14 юни 2023 г. относно машините и за отмяна на Директива 2006/42/ЕО на Европейския парламент и на Съвета и Директива 73/361/ЕИО на Съвета. Достъпно на: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2023.165.01.0001.01.ENG&toc=OJ%3AL%3A2023%3A165%3ATOC

[15] Предложение за директива на Европейския парламент и на Съвета за адаптиране на правилата за извъндоговорна гражданска отговорност към изкуствения интелект (Директива за отговорността за ИИ). Достъпно на: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496

- Европейският акт за управление на данните[16] (пряко приложим от септември 2023 г.).

Актът за цифровите услуги (АЦУ) и Актът за цифровите пазари (АЦП) са основно насочени към регулирането на много големи търговски онлайн платформи като Google, Amazon, Facebook и Apple, докато АИИ се фокусира върху проектирането, разработването и използването на технологии с ИИ в публичния и частния сектор.[17] Подобно на Общия регламент относно защитата на данните (ОРЗД), персоналният обхват на АИИ е широк, обвързваш със задължения не само ползвателите на системи с ИИ, намиращи се на територията на ЕС, но и доставчиците, които пускат на пазара или въвеждат в експлоатация системи с ИИ в ЕС, независимо дали тези доставчици са установени в Съюза или в трета държава.[18] Друга съществена прилика с ОРЗД са значителните глоби за нарушения, които са определени като процент от общия годишен оборот на дружеството нарушител през предходната финансова година или като предварително определена сума, в зависимост от това коя от двете стойности е по-висока. По-конкретно това съответства на 35 млн. евро или 7% за нарушения на забранените приложения с ИИ, 15 млн. евро или 3% за нарушения на задълженията по Акта за ИИ и 7,5 млн. евро или 1,5% за предоставяне на невярна информация. В предварителното споразумение обаче се предвиждат по-пропорционални тавани на административните глоби за малки, средни и стартиращи предприятия в случай на нарушения на разпоредбите на АИИ.[19]

Предложението има също така широк материален обхват, включващ системи с ИИ, разработени с една или повече от техниките и подходите, посочени в приложение I, които могат „по отношение на даден набор от цели, определени от човек, да генерира резултати, като съдържание, прогнози, препоръки или решения, които оказват въздействие върху средите, с които взаимодействат“[20]. АИИ обвързва със задължения предимно доставчиците на системи с ИИ, като определението за доставчици включва всяко „физическо

[16] Регламент (ЕС) 2022/868 на Европейския парламент и на Съвета от 30 май 2022 г. относно управлението на данните в Европа и за изменение на Регламент (ЕС) 2018/1724 (Закон за управление на данните) (Текст от значение за ЕИП). Достъпно на: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868

[17] Lilian Edwards. (2022). The EU AI Act proposal. Ada Lovelace Institute. Available at: https://www.adalovelaceinstitute.org/ resource/eu-ai-act-explainer

[18] АИИ, чл. 2.

[19] Прессъобщение на Съвета на ЕС: https://www.consilium.europa.eu/bg/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/

[20] АИИ, чл. 3(1).

или юридическо лице, публичен орган, агенция или друга организация, която разработва система с ИИ или която възлага разработването на система с ИИ с цел пускането ѝ на пазара или въвеждането ѝ в експлоатация със своето име или търговска марка, срещу заплащане или безплатно“[21].

Предложението разграничава различни нива на риск по отношение употребата на ИИ, които са класифицирани в четири категории: 1) неприемливи рискове (дял II); 2) високи рискове (дял III); 3) умерени рискове (дял IV); 4) ниски или минимални рискове (дял IX). Повечето системи с ИИ ще попаднат в категорията на минималния риск, където държавите членки и Комисията просто „насърчават“ и „улесняват“ доброволни кодекси за поведение.[22]

Защитата на основните права, заедно с осигуряване на здравето и безопасността, са крайъгълните камъни на основания на риска подход, тъй като продуктите и услугите с ИИ се класифицират в една от четирите категории въз основа на свързани с тези интереси рискове. Основен проблем на АИИ е липсата на критерии за оценка на риска, включително рискове за потенциално нарушаване на основните права, което означава, че системите с ИИ автоматично се класифицират в категориите на неприемлив, висок или умерен риск без каквато и да е било обосновка и прозрачност относно съображенията, на които се основава това решение. Също толкова проблематичен от гледна точка на осигуряване на ефективна защита на основните права е фактът, че предложението не съдържа отделно определение на „риск от неблагоприятно въздействие върху основните права“[23]. Съгласно член 65, параграф 1, „що се отнася до рискове за здравето, безопасността или *защитата на основните права на хората*“ за високорисков продукт със система с ИИ се счита „продукт, представляващ риск по смисъла на член 3, точка 19 от Регламент (ЕС) 2019/1020 относно надзора на пазара и съответствието на продуктите“.[24] Този регламент има за цел да защити здравето и безопасността на потребителите, околната среда и други обществени интереси чрез подобряване и модернизиране на системата за надзор на пазара на продукти в ЕС. Регламентът въвежда следното

[21] АИИ, чл. 3(2).
[22] ЗИ, чл. 69.
[23] АИИ, чл. 7.
[24] Регламент (ЕС) 2019/1020 на Европейския парламент и на Съвета от 20 юни 2019 г. относно надзора на пазара и съответствието на продуктите и за изменение на Директива 2004/42/ЕО и Регламенти (ЕО) № 765/2008 и (ЕС) № 305/ 2011 (Текст от значение за ЕИП). Достъпно на: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R1020

определение за риск, към което предложението за АИИ препраща: „продукт, представляващ риск“ означава продукт, който има потенциал да повлияе неблагоприятно върху здравето и безопасността на хората като цяло, здравето и безопасността на работното място, защита на потребителите, околната среда, обществената сигурност и други обществени интереси, защитени от приложимото законодателство на Съюза за хармонизация, до степен, която надхвърля тази, считана за разумна и приемлива във връзка с предназначението им или при нормални или разумно предвидими условия на използване на съответния продукт, включително продължителността на употреба, и когато е приложимо, пускането му в експлоатация, изискванията за монтаж и поддръжка“[25].

От това определение става ясно, че основните права до голяма степен се разглеждат през призмата на защита правата на потребителите, което може да създаде пропуски в защитата на основните права, тъй като съществуват известни разминавания и би могло да възникне противоречие между разпоредбите на законодателството за безопасност на ЕС и нормите на правото на ЕС за защита на основните права.

Ограниченият обхват на Регламент (ЕС) 2019/1020 по отношение на защитата на основните права е отразен в каталога от основни права и принципи, „признати по-специално от Хартата на основните права на Европейския съюз и присъстващи в конституционните традиции на държавите членки“, на които Регламентът се стреми да осигури пълно зачитане[26]: защитата на потребителите, свободата на стопанска дейност, свободата на изразяване и информация, правото на собственост и защитата на личните данни“. Показателен е фактът, че добре документираните рискове от дискриминация и погрешни или предубедени решения, подпомагани от ИИ[27], както и набор от други основни права[28] не са упоменати.

[25] Ibid., член 3, точка 19.

[26] Обяснителен меморандум, съображение 16.

[27] Xenidis, Raphaële and Senden, Linda, ‘EU non-discrimination law in the era of artificial intelligence: Mapping the challenges of algorithmic discrimination’ in Ulf Bernitz et al (eds), General Principles of EU law and the EU Digital Order (Kluwer Law International, 2020), pp. 151-182., Available at SSRN: https://ssrn.com/abstract=3529524; Zuiderveen Borgesius, FJ (2020), ‘Strengthening legal protection against discrimination by algorithms and artificial intelligence’ The International Journal of Human Rights 1; Резолюция на Европейския парламент от 20 октомври 2020 г. относно рамка за етичните аспекти на изкуствения интелект, роботиката и свързаните с тях технологии 2020/2012(INL);

[28] Musco Eklund, A. (2023). Rule of Law Challenges of ‘Algorithmic Discretion’ & Automation in EU Border Control: A Case Study of ETIAS Through the Lens of Legality. European Journal of Migration and Law, 25(3), 249-274. https://doi.org/10.1163/15718166-12340152;

Първата и най-тясна категория на риск са забранените системи с ИИ, които са „особено вредни и следва да бъдат забранени, тъй като противоречат на ценностите на Съюза за зачитане на човешкото достойнство, свободата, равенството, демокрацията и принципите на правовата държава и на основните права на Съюза, включително правото на недискриминация, защита на данните и неприкосновеността на личния живот, както и правата на детето“[29]. Тази категория включва строго ограничен набор от системи с ИИ, без да са дадени разяснения защо именно тези системи се считат за по-опасни от други[30] от гледна точка на нарушаване на основните права:

- Сублимални техники: „система с ИИ, която си служи с … техники отвъд рамките на съзнаваното от човек, с цел съществено да измени поведението на дадено лице по начин, който причинява или може да причини ... физически или психологическа вреда“[31];
- Манипулация: „система с изкуствен интелект, която използва което и да е от уязвимите места на конкретна група лица, дължащи се на тяхната възраст, физическо или умствено увреждане, с цел съществено да измени поведението на дадено лице, принадлежащо към тази група, по начин, който причинява или може да причини ... физически или психологическии вреди“[32];
- Социален ранкинг: кредитна система за социално поведение, създадена или използвана от публичнин органи „с цел оценка или класифициране на надеждността на физически лица …на базата на тяхното социално поведение или известни или прогнозирани лични или личностни характеристики“[33];
- Биометрични данни: „системи за дистанционна биометрична идентификация в „реално време“ на „обществено достъпни прос-

Langford, M (2020), ‘Taming the Digital Leviathan: Automated Decision-Making and International Human Rights’ 114 American Journal of International Law Unbound 141 available at: www.cambridge.org/core/journals/american-journal-of-international-law/article/taming-the-digital-leviathan-automateddecisionmaking-and-international-human-rights/5AFE96F03A1B75B63729D60F0F609609

[29] АИИ, съображение 15 и член 5.

[30] Edwards, L. (2022). Regulating AI in Europe: four problems and four solutions. Ada Lovelace Institute. Available at: https://www.adalovelaceinstitute.org/report/regulating-ai-in-europe/; Ada Lovelace Institute. (2022). Policy briefing: People, risk and the unique requirements of AI. Available at: https://www.adalovelaceinstitute.org/policy-briefing/eu-ai-act

[31] АИИ, член 5, параграф 1, буква а). Подчертаването е добавено от автора.

[32] АИИ, Член 5, параграф 1, буква б.

[33] АИИ, Член 5, параграф 1, буква в.

транства“, използвани от правоприлагащите органи [с големи изключения].[34]

Според постигнатото на 8 декември политическо споразумение между Парламента и Съвета горепосочените забранени практики със системи с ИИ ще бъдат допълнени чрез промяна на приложното им поле и добавяне на нови забрани. Очаква се АИИ да съдържа следния каталог от системи с умерен риск: разширяване на определението за системи с цел манипулация, като настоящата формулировка включва всички системи с „цел заобикаляне на свободната воля на потребителите, като играчки с гласов асистент“; системи, които насърчават опасно поведение от страна на малолетни или непълнолетни лица; системи, които дават възможност за социално оценяване от страна не само на държавното управление, но и от частни дружествата; някои приложения за прогнозиране в полицейската област. Освен това някои видове използване на биометрични системи ще бъдат забранени, например системите за разпознаване на емоции, използвани на работното място, и някои системи за категоризиране на хора или отдалечена биометрична идентификация в реално време за целите на правоприлагането на обществено достъпни места (с по-малки изключения спрямо предложението на ЕК).[35]

Основната категория системи с ИИ, регламентирани от АИИ, са така наречените „високорискови системи“, които подлежат на подробен режим на сертифициране, базиран на списък с правни изисквания (виж по-долу). Високорисковите системи са обособени в две основни категории:

1. В приложение II-A системи с изкуствен интелект, предназначени да бъдат използвани като защитен елемент на продукти или самите те са продукт, които вече са регулирани съгласно така наречената „нова законодателна рамка“[36] (напр. машини, играчки, медицински изделия) и в приложение II-B, други категории хармонизирано законодателство на ЕС

[34] АИИ, член 5, параграф 1, буква г) и член 5, параграф 2, параграф 4.

[35] Прессъобщение на Европейската комисия. Комисията приветства политическото споразумение относно Законодателния акт за изкуствения интелект https://ec.europa.eu/commission/presscorner/detail/bg/ip_23_6473

[36] Това включва следните три правни инструмента: Регламент (ЕО) 765/2008, определящ изискванията за акредитация и надзор на пазара на продукти; Решение 768/2008 относно обща рамка за пускане на пазара на продукти, което включва референтни разпоредби за включване в ревиАИИте на законодателството за продуктите, което подчертава бъдещото законодателство за хармонизиране на продуктите; и Регламент (ЕС) 2019/1020 относно надзора на пазара и съответствието на продуктите. Достъпно на: https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en

съгласно така наречения „стар подход“[37] (напр. лодки, железопътни превозни средства, моторни превозни средства, въздухоплавателни средства и др.). 2. В приложение III са изброени други самостоятелни системи с ИИ с последици предимно за *основните права*[38], които включват:

a. Критични инфраструктури (напр. в областта на водоснабдяването, газоснабдяването и електроснабдяването), които могат да изложат на риск живота и здравето на гражданите.

b. Биометрични системи за самоличност (виж по-горе).

c. Системи за определяне на достъпа до образователни институции и професионално обучение и оценяване на учащите се (напр. автоматизирано оценяване на изпити).

d. Заетост, управление на работниците и достъп до самостоятелна заетост (напр. автоматизирано набиране на персонал и софтуер за сортиране на CV).

e. Основни частни и обществени услуги (напр. автоматизирани системи за определяне достъпа и размера на социални помощи; системи за кредитен скоринг в частния сектор).

f. Системи, използвани в областта на правоприлагането (напр. автоматизирано оценяване на риска за освобождаване под гаранция).

g. Управление на миграция, убежище и граничен контрол (напр. проверка на автентичността на документите за пътуване; обработка на визи).

h. Административно управление на правораздавателната система и демократичните процеси (напр. „робосъдие“; автоматизирана помощ при постановяване на присъди).[39]

[37] Това обхваща така наречения „Стар подход“, който все още се използва в някои области на техническото законодателство на ЕС като автомобили, храни и козметика. Новата законодателна рамка (НЗР) е методът за хармонизация, използван за повечето индустриални продукти. За разлика от НЗР, старият подход е основан на връзка с конкретни на продукти (за разлика от НЗР, която е организирана на базата на по-всеобхватни категории от продукти като машини, строителни продукти и играчки), не създава механизми за тясно сътрудничество между надзорните органи и пазарните оператори и включва технически спецификации за това как да се изпълнят изискванията, така че даден продукт да бъде сертифициран като безопасен. За повече информация вижте: https://boss.cen.eu/reference-material/guidancedoc/pages/newapproach/

[38] Обяснителен меморандум. Акцент, поставен от автора.

[39] ИИА, Приложение III.

Съгласно първоначалното предложение Комисията може, с възможност за вето от страна на Парламента или Съвета, да добави нови високорискови практики в рамките на тези области, ако системите с ИИ „крият риск от увреждане на здравето и безопасността или риск от неблагоприятно въздействие върху основните права, който е – по отношение на своята сериозност и вероятност от възникване – равностоен на или по-голям от риска от увреждане или неблагоприятно въздействие, произтичащ от високорисковите системи с ИИ, които вече са посочени в приложение III“[40]. Докато невъзможността за добавяне на нови високорискови зони най-вероятно ще остане непроменена. В резултат на приключилите политически преговори Съветът и ЕП предложиха различни области, като застрахователни системи и допълнителни случаи на употреба на системи с ИИ в областта на критичната инфраструктура, да бъдат добавени към „високорисковите“ системи и които по всяка вероятност ще залегнат в окончателния текста на АИИ.

Ключово изменение, което бе предложено в преговорните позиции[41] и на двата съзаконодателя, и което ще присъства в текста на АИИ, касае класификацията на високорисковите системи чрез разпоредбите на член 6. В сравнение с това, което първоначално беше предложено от Европейската комисия, а именно всички системи, изброени в Анекс III, директно и безусловно да подлежат на проверка за съответствие с правните изисквания в Глава II от Раздел III, Европейският парламент и Съветът бързо постигнаха съгласие относно необходимостта за по-гъвкави правила за класифициране. В резултат на това доставчиците на системи, които се използват за специфични цели в гореизложените области, считани за критични от гледна точка защитата на основните права на ЕС и чиито системи следователно се считат за високорискови, могат при определени условия да бъдат освободени от задължението да демонстрират съответствието на системите с правните изисквания. За да има правото на това, доставчикът на високорискова система трябва да (1) докаже, че системата не представлява „значителен риск“ от увреждане на здравето, безопасността или основните права на лицата и (2) регистрира системата в публична база данни[42] на ЕС.

Третата категория на подхода, основан на риска, съдържа така наречените системи с изкуствен интелект „с умерен риск“, които представляват „специфичен риск за прозрачността“ и са изчерпателно дефинирани в Дял

[40] ЗИ, чл.7 и 73.

[41] Виж Legislative Train Schedule, Artificial intelligence act in “A Europe Fit for the Digital Age.” Достъпно на https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence

[42] АИИ, чл. 60.

IV „Задължения за прозрачност на някои системи с ИИ“[43]. Дял IV налага сравнително минимални задължения във връзка с осигуряване на прозрачност – две за ползвателите на системи с ИИ и едно за доставчиците. Също както при класифицирането на системите с изкуствен интелект като „забранени“ и „с висок риск“, няма критерии за оценка на риска и по отношение на тази категория. Освен това не е ясно каква е практическата добавена стойност на тази категория, тъй като тя се припокрива с изискванията за прозрачност във връзка с използването на профилиране и автоматизирано вземане на решения от операторите на лични данни съгласно Общия регламент относно защита на данните.

Спрямо предложението на ЕК, изискванията към тези системи с ИИ бяха завишени, отговаряйки в значителна степен на предложенията на ЕП. Окончателният текст на АИИ цели да подсигури, че когато използват системи с ИИ, като чатботове, потребителите следва да са наясно, че си взаимодействат с машина. Дълбоките фалшификати и друго създадено с ИИ съдържание ще трябва да бъдат обозначавани като такива, а потребителите трябва да бъдат информирани, когато се използват системи за биометрична категоризация или разпознаване на емоции[44]. Освен това доставчиците ще трябва да проектират системите така, че съдържанието под формата на синтетично аудио, видео, текст и изображения да е маркирано в машинно четим формат и да е отбелязано като изкуствено създадено или манипулирано[45].

Четвъртата и най-многобройна категория е тази на системи с ИИ „с минимален риск“, като например филтрите за спам, които са изцяло освободени от задължения. АИИ предвижда възможността дружествата да могат да се ангажират на доброволна основа с допълнителни кодекси за поведение за тези системи с ИИ.[46]

Актът за ИИ изисква доставчиците на високорискови системи да извършат предварителна оценка на съответствието на тези системи с правните изисквания, посочени в Дял III, Глава 2 преди да ги пуснат на пазара или въведат в експлоатация.[47] Тези изисквания се отнасят до данните и управлението им, съхраняването на документацията и записите, прозрачността и предоставянето на информация на ползвателите, човешкия надзор, на-

[43] Пак там.

[44] Прессъобщение на Европейската комисия: „Комисията приветства политическото споразумение относно Законодателния акт за изкуствения интелект“. Достъпно на https://ec.europa.eu/commission/presscorner/detail/bg/ip_23_6473

[45] Пак там.

[46] Обяснителен меморандум 5.2.7; чл. 69.

[47] АИИ чл. 16 и 43.

дждността, точността и сигурността. В съответствие с модела на новата законодателна рамка доставчиците извършват процедура за оценяване на съответствието, чрез която системите са сертифицират с маркировката за съответствие „CE" и могат да бъдат свободно внасяни и разпространявани в целия ЕС[48].

Доставчиците трябва да създадат система за управление на риска, която да идентифицира, прогнозира и оценява рискове през целия жизнен цикъл на системата с ИИ, когато системата се използва по предназначение или при условия на „разумно предвидима неправилна експлоатация"[49]. Рискове могат да бъдат добавени в резултат на задълженията за мониторинг и докладване на доставчиците на системи с ИИ след пускането им на пазара. В предложението става ясно, че целта на системата за управление на риска не е само отстраняването на риска, но и намаляването му до ниво на „приемлив остатъчен риск", без да предоставят каквито и да е насоки или критерии за оценка на това ниво. Доставчиците могат да използват „адекватни мерки за ограничаване и контрол", когато рисковете не могат да бъдат отстранени и са задължени да съобщят тези рискове на ползвателите на системата с цел осигуряване на ефективен надзор от страна на човека. На практика това оставя преценката дали рискове за основните права са били адекватно намалени, изцяло в ръцете на техническите разработчици на системи с ИИ или така наречените „доставчици", тъй като единствено доставчиците са обект на задължението за създаване на система за управление на риска и при изпълнението на това задължение няма външен контрол.

Както беше вече споменато в предходната част на настоящия анализ, АИИ създава задължения предимно за участниците нагоре по веригата за създаване на стойност в областта на ИИ, тоест доставчиците, а не за ползвателите на системи с ИИ, които са надолу по веригата, освен ако тези потребители не направят „съществена промяна" в система, в който случай те се считат за доставчици и същите задължения се прилагат спрямо тях. Това е особено проблематично, когато става дума за така наречения „ИИ с общо предназначение" (ОПИИ), които са системи с ИИ, които имат множество възможни приложения в различни контексти и включват системи в основата на чатботите ЧатДжиПиТи (ChatGPT) и Бард (Bard). По дефиниция всички възможни цели и условия, за които се ползва ОПИИ, не могат да бъдат предварително предвидени.[50] Това поражда противоречие с основания на риск

[48] АИИ, чл. 49.
[49] АИИ, чл. 9.
[50] Кобе, Дж. и Сингх, Дж. (2021). „Изкуственият интелект като услуга: правни отговорности,

подход, тъй като класификацията на системите с ИИ като високорискови се основава на използването на дадена система по предназначение или „в условия на разумно предвидима неправилна експлоатация“ в една от областите, изброени в Приложение III. Това би могло да доведе до съществен пропуск в обхвата на защитата на основни права, тъй като е възможно доставчиците на ОПИИ да не носят задължения за спазване на основните изисквания на глава 2. Системите с ОПИИ включват широко използвани големи езикови модели, използвани за генериране на текст или реч, разпознаване на текст или реч, анализи и модули за езиков превод.[51] Има все повече доказателства, че тези системи могат да манипулират и дискриминират хората, да позволяват разпространението на измами и дезинформация в тревожен мащаб и да нарушават неприкосновеността на личния живот.

Политическото споразумение между Европейския парламент и Съвета относно АИИ въведе специални правила за моделите на ОПИИ с цел да се гарантира прозрачност по веригата за създаване на стойност. Според специалния режим на регулиране, в допълнение към изискванията за доставчиците на ОПИИ, АИИ създава по-строги правно обвързващи задължения за много мощните модели, които биха могли да породят „системни рискове“. Тези по-всеобхватни задължения са свързани с управлението на рисковете и наблюдението на сериозни инциденти и с извършване на оценка на моделите и изпитване с подаване на неочаквано или вредно съдържание.[52] Задълженията за ОПИИ и ОПИИ със системни рискове ще бъдат приведени в действие чрез кодекси на добрите практики, разработени от промишлеността, научната общност, гражданското общество и други заинтересовани страни заедно с Комисията.[53] От съществено значение във връзка с регулаторния контрол върху системи с ОПИИ е, че понятието за „системен риск“ е заимствано от Акта за дигиталните услуги и включва в своето определение изрично позоваване на рискове по отношение защитата на основните права.[54]

отговорности и политически предизвикателства.“ Преглед на компютърното право и сигурността, том 42. Наличен на: https://www.sciencedirect.com/science/article/pii/S0267364921000467

[51] Lilian Edwards. (2022). The EU AI Act proposal. Ada Lovelace Institute,p. 18. Available at: https://www.adalovelaceinstitute.org/ resource/eu-ai-act-explainer

[52] Прессъобщение на Европейската комисия „Комисията приветства политическото споразумение относно Законодателния акт за изкуствения интелект“ https://ec.europa.eu/commission/presscorner/detail/bg/ip_23_6473

[53] Ibid.

[54] Виж статия на онлайн новинарския портал Euroactiv, 7 декември: https://www.euractiv.com/section/artificial-intelligence/news/ai-act-eu-policymakers-nail-down-rules-on-ai-models-butt-heads-on-law-enforcement/

Доставчиците на високорискови системи и на системи с ОПИИ подлежат на задължителна процедура за оценяване на съответствието със съответните изисквания за тези две категории системи, като за високорисковите системи тези изисквания са изложени в глава втора от Дял III на АИИ. Доставчиците и на двата вида системи демонстрират съответствие на база на самооценяване.[55] АИИ дава възможност на доставчиците на високорискови системи да докажат съответствие чрез разработване на собствен план за съответствие или чрез следване на съответен хармонизиран технически стандарт. Външно оценяване на съответствие от независима трета страна чрез така наречения „нотифициран орган“ се предвижда предимно само за системи, попадащи в Приложение II, които, за разлика от системите от Приложение III, са по-малко свързани с последици за основните права.

Единствено доставчиците на следните системи ще трябва да преминат външен независим одит за съответствие:

1. ИИ системи за биометрична идентификация или категоризация на физически лица[56], но само при условие, че не е разработен технически хармонизиран стандарт, което е малко вероятно.
2. Системи с ИИ, които са регулирани съгласно съществуващата НЗР или друго законодателство на ЕС, изброено в Приложение II, когато участието на нотифицирани органи е предвидено по силата на това законодателство.[57]

Актът за ИИ предвижда самосертифицирането от доставчиците на високорискови системи да се основава на хармонизирани технически стандарти за високорисков ИИ, които ще бъдат създадени от технически комитети. Високорисковите системи, които съответстват на техническите стандарти, се считат за отговарящи на основните изисквания на Глава 2[58]. Така наречената „презумпция за съответствие“ е разпоредба от особено ключово значение в текста на АИИ, тъй като посредством нея високорискови системи с ИИ се считат за безопасни по отношение на „риск от неблагоприятно въздействие върху основните права“ само на базата на технически спецификации, чиято връзка с основните права е доста неясна. Доставчиците имат възможност да изберат да не се придържат към тези стандарти и вместо това да докажат, че са възприели технически решения, които са най-малкото еквивалентни[59].

[55] АИИ, член 43, параграф 1, буква а).
[56] АИИ, член 43, параграф 1.
[57] АИИ, член 43, параграф 3).
[58] АИИ, чл. 40.
[59] АИИ, чл. 41.

Предвид лекотата на използване на готови официални стандарти е малко вероятно доставчиците да изберат намирането и предоставянето на доказателства за приемането на ефективни технически решения.

Сертифицирането на безопасността на системи с ИИ във връзка с основните права посредством технически стандарти[60] е силно обезпокоително, тъй като създаването на тези стандарти ще бъде възложено от Европейската комисия на европейските организации по стандартизация Европейски комитет по стандартизация (CEN) и Европейски комитет за стандартизация в електротехниката (CENELEC), които нямат опит и познания в областта на основните права и чиито процеси за разработване на стандарти не позволяват смислено участие на заинтересовани страни, свързани със защитата на основните права. Възможността за принос на тези страни е силно ограничена както поради тясно техническия и специализиран характер на работните процеси на организациите по стандартизация, така и поради липсата на прозрачност, свързана с защитата на стандартите от правото на интелектуална собственост[61].

След като дадена високорискова система е преминала предварителни проверки от доставчика посредством процедурите за оценяване на съответствие и бъде пусната на пазара или въведена в експлоатация, Актът определя система за мониторинг с цел да се осигури непрекъснато съответствие на системата през целия ѝ експлоатационен срок. Доставчиците са натоварени със задачата да „създават и документират система за мониторинг след пускането на пазара по начин, съобразен с естеството на технологиите за изкуствен интелект и с рисковете на високорисковата система с ИИ“[62]. Тази система за мониторинг ще „събира, документира и анализира съответните данни, предоставени от ползвателите … относно функционирането на системи с ИИ през целия им жизнен цикъл“[63]. От своя страна, предприятията или публичните органи, които използват високорискови системи (т.е. „ползвателите“) имат задачата да изпълняват „мерките за човешки надзор, посочени

[60] European Commission. (2022). Press Release: New approach to enable global leadership of EU standards promoting values and a resilient, green and digital Single Market. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_661

[61] Micklitz, H.W. (2023). The Role of Standards in Future EU Digital Policy Legislation, Research Report commissioned by ANEC and BEUC. Available at https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-096_The_Role_of_Standards_in_Future_EU_Digital_Policy_Legislation.pdf. C. Perarnaud (2023) ‘With the AI Act, we need to mind the standards gap’. Centre for European Policy Studies. Available at https://www.ceps.eu/with-the-ai-act-we-need-to-mind-the-standards-gap

[62] АИИ, член 61, параграф 1.

[63] АИИ, член 61(2).

от доставчика“ чрез изготвените от доставчика „инструкции за употреба“ и да докладват за нови рискове, „сериозни инциденти“ или „неизправности“[64]. Трябва да се отбележи, че определението за „сериозен инцидент“ изрично включва нарушение на правни задължения съгласно правото на Европейския съюз, защитаващо основните права.[65] Това е единствената препратка към законодателството на ЕС за защита на основните права в определенията на Акта и единствената разпоредба в текста на АИИ, която пряко се позовава на норми на ЕС в областта на основните права за създаване на правно обвързващи задължения. Информацията, събирана от ползвателите посредством системата за мониторинг след пускане на пазара на високорисковите системи с ИИ, бива препратена към доставчици или дистрибутори на тези системи, а не директно към определения от държавите членки национален орган за надзор върху прилагането и изпълнението на регламента (ННО).

Държавите членки ще трябва да определят един или повече национални компетентни органи и, измежду тях, национален надзорен орган, който ще има задачата да контролира пазара и да разследва спазването на задълженията и изискванията за всички високорискови системи с ИИ, които вече са пуснати на пазара. Европейският надзорен орган по защита на данните ще действа като компетентен орган за надзор на институциите, агенциите и органите на Съюза, когато те попадат в обхвата на настоящия регламент.[66]

За разлика от нотифицираните органи, надзорните органи са публични органи, притежаващи силни регулаторни правомощия, съпоставими с тези, вменени на националните органи за защита на личните данни по силата на ОРЗЛД.[67] Те имат значителни правомощия като например право на пълен достъп до данни и информация, включително достъп до изходния код на системата с ИИ, правото да изтеглят продукти от пазара и да задължават операторите на системи, които не съответстват на изискванията и задълженията, определени в Акта, да предприемат всички „необходими коригиращи действия, за да приведе в съответствие системата с ИИ, да я изтегли от пазара или да я изземе в съобразен с характера на риска разумен срок, който органът за надзор може да определи“[68].

Основните права подлежат на специфични предпазни мерки във фазата на мониторинг и докладване след пускането на пазара и разследването на

[64] АИИ, член 29(4).
[65] АИИ, член 3(44)(c).
[66] АИИ, чл. 59.
[67] АИИ, член 64, параграф 2.
[68] АИИ, чл. 65(2).

инциденти и неизправности, свързани с ИИ. Когато даден сериозен инцидент, причинен от система с ИИ, касае нарушаване на законодателството за защита на основните права, националният надзорен орган, който получава уведомлението за инцидента от доставчика, има задължението да информира националните публични органи, които „упражняват надзор или налагат спазването на задължения съгласно правото на Съюза за защита на основните права“ или така наречените „органи по член 64(3)“[69]. Уведомителното задължение има за цел да подобри ефективността на защитата на основните права, като избегне отслабване на тази защита посредством раздробяването ѝ на два потенциално разминаващи се механизма за правоприлагане, свързани със защитата на основните права, а именно надзорните органи по силата на АИИ и националните надзорни органи във връзка с основните права, като институцията на омбудсмана и органите за равнопоставеност.

Въпреки че Актът според предложението на Комисията не създава механизъм за подаване на жалби, чрез който засегнатите лица да докладват и да търсят средства за защита при нарушения на основните им права посредством системи с ИИ, член 64(3) от Акта се стреми да осигури по-ефективна защита на тези лица посредством осигуряване достъп до документация, създадена съгласно Акта, на съществуващи специализирани механизми за правна защита за защита на основните права.

Съгласно тази разпоредба „националните публични органи или структури, които упражняват надзор или налагат спазването на задълженията съгласно правото на Съюза за защита на основните права във връзка с използването на високорисковите системи с ИИ, посочени в Приложение III, имат правомощието да изискват и получават достъп до всяка документация, създадена или поддържана съгласно настоящия регламент, когато достъпът до тази документация е необходим за осъществяването на задачите им съгласно техните правомощия и в рамките на тяхната юрисдикция“. Когато органите по член 64(3) не разполагат с достатъчно документация, за да „се установи дали е извършено нарушение на задълженията, произтичащи от правото на Съюза, предназначено да защитава основните права“, те могат да отправят „обосновано искане до органа за надзор на пазара да организира изпитване на високорисковата система с ИИ чрез технически средства“. Съгласуването и ефективното сътрудничество между механизма за правоприлагане съгласно Акта и съществуващите публични органи за прилагане на правото на ЕС за основните права се гарантира допълнително чрез задължението на надзорните органи в Акта да организират изпитването на системата с „с

[69] АИИ, чл. 62(3) и чл. 64(3).

активното участие на отправилия искането публичен орган или структура в разумен срок след подаване на искането“[70].

Допълнителен механизъм за засилване на защитата на основните права се предоставя чрез участието на публичните органи по член 64(3) в специалната процедура по правоприлагане при високорискови системи с ИИ съгласно член 65. Когато надзорните органи идентифицират рискове за защитата на основните права, те трябва да информират съответните национални публични органи за надзор във връзка с основните права. От особена важност е, че участниците по веригата за създаване на стойност в областта на ИИ, които АИИ нарича „оператори“, ще имат задължението да си сътрудничат „при необходимост“ не само с надзорните органи, но и с обществените органи за защита на основните права. Това е единственото законодателство на Европейския съюз за цифровите технологии, което създава механизъм за координация и сътрудничество между собствената си система за управление и надзор на национално ниво и съществуващата национална система за надзор във връзка със защитата на основните права.

Вероятно най-съществените разпоредби с оглед подобряване на защитата на основните права касаят изменения в предложението на Комисията във връзка с осигуряване достъп до правосъдие и прозрачност. Тези ключови подобрения бяха внесени от Парламента и приети от Съвета с известни ограничения. В компромисното споразумение се пояснява, че физическо или юридическо лице може да подаде жалба до съответния орган за надзор на пазара относно неспазване на Законодателния акт за ИИ и може да очаква, че тази жалба ще бъде разгледана в съответствие със специалните процедури на този орган. С цел съгласуваност с механизмите за прозрачност, предоставени по силата на Общия регламент за защита на личните данни, Актът урежда право на смислено обяснение за жалбоподателите. Споразумението между съзаконодателите също така предвижда задължение на ползвателите на високорискови системи да извършат оценка на въздействието върху основните права преди пускане на пазара или въвеждане в експлоатация на тези системи. В предварителното споразумение също така се осигурява повишена прозрачност по отношение на използването на високорискови системи с ИИ чрез изменения, уточняващи, че определени ползватели на тези системи, които са публични органи, също ще бъдат задължени да се регистрират в базата данни на ЕС за високорисковите системи с ИИ. Освен това в добавените нови разпоредби се набляга на задължението на ползва-

[70] АИИ, чл. 64 (5).

телите на система за разпознаване на емоции да информират физическите лица, когато по отношение на тях се използва такава система.

На равнището на Съюза системата за управление и надзор върху прилагането на регламента ще се осъществява от нова Европейска служба за ИИ в рамките на Европейската комисия, която освен обща надзорна функция, ще отговаря за прилагането на новите правила за моделите на ИИ с общо предназначение. Във връзка с тези модели службата за ИИ ще бъде подпомагана от научна група от независими експерти, която ще подава сигнали за системни рискове и допринася за класифицирането и изпитването на моделите. Допълнителен елемент от системата за управление на равнището на Съюза е първоначално предложеният от ЕК като водещ надзорен орган Европейски съвет по изкуствен интелект („Съвета по ИИ“), съставен от представители на държавите членки и на Комисията. В хода на политическите преговори между Парламента и Съвета голяма част от правомощията на Съвета по ИИ бяха прехвърлени към новата Служба за ИИ, която бе въведена чрез измененията, предложени от Парламента в преговорната позиция от юни 2023. Някои от прехвърлените правомощия имат значителни последици за защитата на основните права. Така например Службата за ИИ ще поеме от Съвета по ИИ правомощието да съветва Комисията относно необходимостта от добавяне или премахване на високорискови системи чрез изменение на Приложение III, което съдържа системи с ИИ със сериозни последици за основните права.

Съветът по ИИ, който ще включва представители на държавите членки, ще продължи да бъде координационна платформа и консултативен орган към Комисията и ще предостави съдействие на държавите членки при прилагането на регламента, включително разработването на кодекси на поведение за базовите модели. В допълнение към системата за управление и с цел предоставяне на технически експертен опит на Съвета по ИИ, ще бъде създаден също така консултативен форум за заинтересованите страни, които включват представителите на промишлеността, малките и средните предприятия, стартиращите предприятия, гражданското общество и академичните среди.

Заключение

в заключение настоящият аналитичен преглед на основни елементи от предложението за АИИ и ролята на основните права в неговата структура разкрива, че предложението не дава ясни указания на доставчиците и ползвателите на системи с ИИ как да осигурят разработване и използване на

тези системи в съответствие с „ценностите, основните права и принципите на Съюза“[71]. Както предложението на Европейската комисия, така и позициите на Съвета и Европейския парламент не дават определение на риск за основните права, нито пък съдържат насоки и критерии за оценка на риска от нарушаване на едно или повече основни права чрез системи с ИИ. Анализът също така показа, че предложението не предлага систематична и достатъчно всеобхватна рамка за определяне, превенция и правоприлагане по отношение на рисковете за основните права. Вместо последователен и задълбочен подход спрямо тези рискове, проектът на АИИ съдържа ограничен брой, като че ли произволно посочени препратки към основните права, предимно свързани с мониторинга на системи с ИИ след пускането им на пазара или въвеждането им в експлоатация и свързания с този мониторинг, обмен на информация и надзор на пазара (Дял VIII).

Едно от основните противоречия и несъвършенства на предложението е именно фактът, че обект на регулиране са почти изцяло доставчиците, а не ползвателите на системи с ИИ, на които от своя страна са вменени задължения и произтичащите от тях отговорности съгласно правото на ЕС за защита на основните права. Определянето на конкретни изисквания, технически параметри и прочие насочени към доставчиците на системи с ИИ и свързани с проектирането и разработването на тези системи не гарантира автоматично ненакърняването на редица основни права, залегнали в правото на ЕС. Нещо повече, именно използването на тези системи от ползвателите би породило значителни рискове за нарушаване на тези права, както показва развиващата се съдебна практика в Европа и Съединените щати във връзка с изкуствения интелект.[72] Въпреки че две от общо четирите конкретни цели на предложението касаят съществуващата правна уредба на ЕС в областта на основните права, мястото и ролята на тези права в структурата на АИИ са ограничени и неясни.[73] Това до голяма степен се дължи на факта, че предложението почива на правната рамка на ЕС за продуктова безопасност, което води до дефакто приравняване на рискове от неблагоприятно въздействие върху основните права с рискове от увреждане на здравето и безопасността,

[71] Обяснителен меморандум, с. 1.

[72] Cortez, Elif Kiesow and Maslej, Nestor (2023). Adjudication of Artificial Intelligence and Automated Decision-Making Cases in Europe and the USA, European Journal of Risk Regulation, 14, 457–475. Available at: https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/adjudication-of-artificial-intelligence-and-automated-decisionmaking-cases-in-europe-and-the-usa/12C2C1E0F9A3A36F64A3C08CCA419946

[73] Обяснителен меморандум, с. 3.

без да се отчита специалният статут на основните права и свързаната с това необходимост от подсилени гаранции за тяхната защита.

Библиография:

1. Policy Briefing: People, Risk and the Unique Requirements of AI [онлайн]. London: Ada Lodevich Institute, 2022 [прегледан на 15 май 2023]. Достъпен на: https://www.adalovelaceinstitute.org/policy-briefing/eu-ai-act.
2. Almada, M., N. Petit. (2022). The EU AI Act: Between Product Safety and Fundamental Rights. Robert Schuman Center for Advanced Studies Research [онлайн], Paper No. 2023/59 [посетен на 25.08.2023]. Достъпен на: https://hdl.handle.net/1814/75982
3. De Gregorio, G., P. Dunn. (2022). The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age. Common Market Law Review, 59(2), 473–500.
4. Edwards, L. (2022). Regulating AI in Europe: Four Problems and Four Solutions. Ada Lodevich Institute [онлайн], 2022 [прегледан на 15 октомври 2023]. Достъпен на: https://www.adalovelaceinstitute.org/wp-content/uploads/2022/03/Expert-opinion-Lilian-Edwards-Regulating-AI-in-Europe.pdf
5. Cortez, E. K., N. Maslej. (2023). Adjudication of Artificial Intelligence and Automated Decision-Making Cases in Europe and the USA, European Journal of Risk Regulation, 14, 457–475. Visited on 10 December 2023. Available at: https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/adjudication-of-artificial-intelligence-and-automated-decisionmaking-cases-in-europe-and-the-usa/12C2C1E0F9A3A36F64A3C08CCA419946
6. Edwards, L. (2022). The EU AI Act Proposal, Ada Lodevich Institute [онлайн]. [прегледан на 10 юни 2023]. Достъпен на: https://www.adalovelaceinstitute.org/resource/eu-ai-act-explainer
7. Enqvist, L. (2023). Human Oversight in the EU Artificial Intelligence Act: What, When and By Whom?, Law, Innovation and Technology. Law, Innovation and Technology [онлайн]. Volume 15, Issue 2, 508–535 [прегледан на 10 ноември 2023]. Достъпен на: https://www.tandfonline.com/doi/full/10.1080/17579961.2023.2245683
8. Ethics Guidelines for Trustworthy AI [онлайн]. Brussels: European Commission, 2019. [прегледан на 15 май 2023]. Достъпен на: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
9. European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intel-

ligence (Artificial Intelligence Act) and amending certain Union legislative acts. COM/2021/206 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

10. European Commission. (2023). Press Release: Commission welcomes political agreement on Artificial Intelligence Act*. [прегледан на 11 декември 2023]. Достъпен на: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6473
11. European Commission. (2022). Press Release: New approach to enable global leadership of EU standards promoting values and a resilient, green and digital Single Market. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_661
12. Market Surveillance Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC, and Regulations (EC) No. 765/2008 and (EU) No. 305/2011 [2019] OJ L 169.
13. Franklin, M., P. Tomei, R. Gorman. (2023). Strengthening the EU AI Act: Defining Key Terms on AI Manipulation. ResearchGate [онлайн], [прегледан на 1 септември 2023]. Достъпен на: https://www.researchgate.net/publication/373552132_Strengthening_the_EU_AI_Act_Defining_Key_Terms_on_AI_Manipulation
14. Hildebrandt, M. (2021). The issue of bias. The framing powers of machine learning. In Pelillo, Marcello, T. Scantamburlo. In Machines We Trust: Perspectives on Dependable AI [online], Boston: MIT Press, Accessed on 1 September 2023. Available at: https://mitpress.mit.edu/books/machines-we-trust
15. Mazzini, G., S. Scalzo. (2022). The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts. In Camardi (ed), La via europea per l'Intelligenza artificiale, Visited on 15 July 2023, Available at SSRN: https://ssrn.com/abstract=4098809 or http://dx.doi.org/10.2139/ssrn.4098809
16. Micklitz, H. W. (2023). The Role of Standards in Future EU Digital Policy Legislation [online]. Brussels: European Association for the Co-ordination of Consumer Representation in Standardisation and the European Consumers' Organisation. Visited on 10 September. Available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023–096_The_Role_of_Standards_in_Future_EU_Digital_Policy_Legislation.pdf
17. Perarnaud, C. (2023). With the AI Act, we need to mind the standards gap. Brussels: Centre for European Policy Studies. Visited on 10 September. Available at: https://www.ceps.eu/with-the-ai-act-we-need-to-mind-the-standards-gap/

18. Veale, M., K. Matus, R. Gorwa. (2023). AI and Global Governance: Modalities, Rationales, Tensions. Annual Review of Law and Social Science [online] Issue 19, 255-275. Visited on 29 September 2023. Available at: https://www.annualreviews.org/doi/abs/10.1146/annurev-lawsocsci-020223-040749

19. Veale, M., F. J. Zuiderveen Borgesius. (2021). Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear elements of the proposed approach. Computer Law Review International [online], Vol. 22, no. 4: 97-112. Visited on 1 July 2023. Available at: https://www.degruyter.com/document/doi/10.9785/cri-2021-220402/html?lang=en

CONTENTS

Форум „Юридически изследвания“

Книга първа

Legal Research Forum

Book One

ISSN 3033-1129 (Print), 3033-1137 (online)

ISBN 978-619-233-336-2 (печатно издание)
ISBN 978-619-233-337-9 (електронно издание)

www.nbu.bg
bookshop.nbu.bg