ПРАВНИ ГАРАНЦИИ ПРИ ИЗПОЛЗВАНЕ НА НОВИТЕ ТЕХНОЛОГИИ ЗА ЦЕЛИТЕ НА ПРОТИВОДЕЙСТВИЕ НА ПРЕСТЪПНОСТТА И ТЕРОРИЗМА

Мартин Захариев
Университет по библиотекознание и информационни технологии
Фондация „Право и Интернет“
Адвокатско дружество „Димитров, Петров и Ко.“

Резюме: Динамиката на съвременните обществени отношения поставя нови заплахи пред сигурността и обществения ред. Ето защо компетентните органи следва да идентифицират подходящи механизми за противодействие на такива заплахи, отговарящи на съвременното технологично развитие на обществото. Такива механизми могат да бъдат някои нови технологии, като лицево разпознаване, изкуствен интелект, автоматизирано вземане на решения и профилиране. Настоящият доклад има за цел да анализира някои основни правни гаранции за правата и свободите при прилагането на посочените технологии в сферата на противодействието на престъпността и тероризма.

Ключови думи: гаранции, автоматизирано вземане на решения и профилиране, резервационни данни на пътници, изкуствен интелект, правова държава.

Въведение

Динамиката на съвременните обществени отношения поставя нови заплахи пред сигурността, обществения ред и конституционно установените принципи на функциониране на модерната държава, в центъра на която са гражданите с техните основни права и свободи. Усложнената международна обстановка, в частност военният конфликт в Украйна, създава условия за дестабилизация в сферата на вътрешния ред и сигурността. На този фон опасността от развитие на различни форми на тероризъм и тежка организирана престъпност не трябва да бъде пренебрегвана. Ето защо компетентните органи следва да идентифицират подходящи механизми за противодействие на такива заплахи, отговарящи на съвременното развитие на обществото. Това могат да бъдат новите технологии, които са мощен инструмент за опазване на обществения ред и сигурност.

Технологиите обаче – поради степента на проникване в ежедневието на хората – могат да служат за манипулиране на човешкото поведение, дискриминация, прекомерно навлизане в

личния и семейния живот, непозволено следене, профилиране и др. под. Поради това използването на технологии като автоматизирана алгоритмична обработка на данни, биометрично разпознаване, изкуствен интелект (ИИ) и др. трябва да бъде съобразено с достиженията на модерната държава в областта на защитата на правата на човека. По този начин опазването на сигурността няма да бъде за сметка на други фундаментални права и свободи, а правоприлагането ще бъде ефективен гарант за спазването и прилагането на законите.

Директива 2016/680[1], транспонирана в глава 8 от Закона за защита на личните данни (ЗЗЛД)[2], и Директива 2016/681[3], транспонирана в глава 6а от Закона за Държавна агенция „Национална сигурност“ (ЗДАНС)[4], съдържат ключови гаранции за основните права и свободи при обработване на лични данни за противодействието на престъпността и тероризма. Подобни правила се очаква да бъдат включени и в бъдещия Регламент за ИИ[5]. Независимо от ключовото си значение за основните права и свободи, правните гаранции, които тези актове въвеждат или планират да въведат, остават недостатъчно изследвани в българската литература. Разбира се, трябва да се отчете наличието на специфични методики, изследващи особеностите на обработването на лични данни в наричаните в теорията „полицейски и наказателни дейности“ и определянето на приложимата правна уредба към различни операции по обработване на лични данни [1]. Други изследвания са фокусирани върху отделни явления, като автоматизираното профилиране и правилата за законосъобразното му внедряване в различни сфери, включително правоприлагането. Те обаче са изготвени по стария режим, преди приемането на горепосочените директиви [2] или преди транспонирането им в българското законодателство [3].

Отделно наличната литература основно се фокусира върху изследването на Общия регламент относно защитата на данните (ОРЗД)[6] [4], [5], а обработката на данни за полицейски и наказателни дейности е извън приложното му поле. Това е и основният мотив за изготвянето на настоящия анализ.

Методология на изследването

Резултатите от настоящото изследване бяха получени след прилагане на научни методи като:

- **Документален метод** – изразяващ се в анализирането и синтезирането на информация относно приложението на горепосочените директиви от документални източници – например от докладите за преглед на директивите на

Европейската комисия (ЕК) и от други публично достъпни (включително онлайн) източници, както и в систематизирането и обобщаването на тази информация;

- **Сравнителен анализ** – този метод се изразява в сравняване на общото и различното между отделни явления. В настоящия доклад този метод е необходим, за да се направи съпоставка между правилата на анализираните директиви и съответно транспониращите ги разпоредби в ЗЗЛД и ЗДАНС и по този начин да се определи дали и доколко националният законодател се е придържал към, респективно отклонил от, правилата на ЕС, и дали има специални национални правила в тези области.

Ограничение на изследването

Извън обхвата на настоящото изследване остава използването на технологии и правни гаранции в сфери извън приложното поле на правото на ЕС, като националната сигурност на държавите членки (ДЧ) [5]. Тази проблематика може да бъде предмет на бъдещи изследвания.

Резултати

Автоматизирано вземане на решения и профилиране за полицейски и наказателни дейности по реда на ЗЗЛД и Директива 2016/680

Възможността за автоматизирано вземане на решения (АВР) и профилиране за полицейски и наказателни дейности следва от чл. 11 на Директива 206/680, като транспониращото я в националното ни законодателство правило е чл. 52 от ЗЗЛД. Тези текстове съдържат сериозни гаранции за защита на основните права и свободи на хората при алгоритмична обработка на техните данни в сферата на правоприлагането.

Като цяло, цитираната норма **забранява** АВР, включително профилиране, което:

- поражда неблагоприятни правни последици за субекта на данните или
- го засяга съществено.

Като примери за типични неблагоприятни последици Работната група по чл. 29 (WP29) посочва „прилагането на повишени мерки за сигурност или осъществяване на надзор от страна на компетентните органи“, а за съществено засягане – „случай, при който пътник не е допуснат да се качи на борда на самолет, тъй като е регистриран в черен списък“[6]. Единственото изключение, позволяващо

преодоляване на забраната, е, ако това е предвидено в правото на ЕС/България и са осигурени подходящи гаранции за правата и свободите на субекта на данните, най-малко – човешка намеса при вземането на решението. В допълнение, **забранено е тези решения да се основават на специални категории данни** (както са дефинирани в чл. 51, ал. 1 от ЗЗЛД), освен ако не са въведени подходящи мерки за защита на правата и свободите и законните интереси на субекта на данните. Забранено е и профилирането, което води до дискриминация на физически лица (ФЛ) въз основа на специалните категории лични данни.

Освен това ЗЗЛД се отклонява от Директива 2016/680 и предвижда **допълнителни национални гаранции** при АВР и профилиране. Първо, въведено е задължителното извършване на оценка на въздействието по чл. 64 от ЗЗЛД при подобен тип операции. Това е в съответствие и с препоръките на WP29. Второ, правото на засегнатия субект да получи човешка намеса от страна на администратора по Директивата, е доразвито и чл. 52, ал. 5 от ЗЗЛД регламентира и правата на субекта да получи информация за обработването, да изрази своето мнение, да получи обяснение за решението, взето в резултат на това обработване, както и да обжалва решението. Това разрешение следва да бъде оценено положително, доколкото отговаря на съображение 38 от Директивата и на стандарта за аналогичните операции по АВР и профилиране по чл. 22 от ОРЗД.

Автоматизирана обработка на резервационни данни на пътниците (РДП) за противодействие на тероризма и тежката престъпност по реда на ЗДАНС и Директива 2016/681

РДП за пътниците и екипажа на въздушните полети до, във или от Република България съгласно глава 6а от ЗДАНС, транспонираща Директива 2016/681, подлежат на специализирана автоматизирана обработка с цел противодействие на изчерпателно уредени тежки престъпления и тероризъм. България е разширила приложното поле на Директивата и е предвидила приложение на този режим и за вътрешните за ЕС полети. По данни на ЕК към 2020 г. само една ДЧ не бе предвидила приложението на този режим за вътрешни за ЕС полети[7].

Ключов орган в тази система е Националното звено за данни на пътниците (НЗДП) – специализирана структура в ДАНС, която получава РДП от въздушните превозвачи или упълномощени от тях доставчици на услуги. НЗДП може да съпоставя данните с информационни фондове на ДАНС, МВР и Агенция „Митници“ и да обработва получените резултати. Ако се идентифицират съвпадения

по предварително определени критерии, НЗДП е длъжно незабавно да предаде РДП и резултатите от тяхното обработване на изчерпателно изброени компетентни правоприлагащи органи. Методиката за определяне на посочените критерии и редът за предоставяне на данните на съответните органи се определят с инструкция на председателя на ДАНС, съгласувана с ръководителите на засегнатите ведомства, при спазване на принципа „необходимост да се знае“. Подобно на чл. 52 от ЗЗЛД, и ЗДАНС съдържа важни гаранции срещу автоматизираната обработка и съпоставянето на данните: решението на компетентните органи за предприемане на мерки спрямо конкретно лице, което може да има правни или други съществени последици за него, не може да се основава единствено на резултата от автоматизираното обработване на РДП. Всяко съвпадение вследствие на автоматизирано обработване на РДП се преглежда поотделно **по неавтоматизиран начин** (чл. 42ж[1]). Подобно изискване е въведено и преди предаването на получени от чужди ЗДП РДП/резултати от обработката им на компетентни органи (чл. 42л, ал. 5). Уредена е и възможност „фалшиво-позитивните резултати“, установени чрез човешка намеса, да се съхраняват с цел да се избегнат бъдещи недействителни съвпадения (чл. 42з, ал. 12).

Следва да се отбележи, че в момента са налице няколко преюдициални запитвания пред Съда на ЕС (СЕС) дали Директивата съответства на основните права и норми на ЕС (дело C-817/19 и съединени дела C-148/20 Ligue des droits humainains, C-149/20 и C-150/20 Deutche Lufhansa)[7]. По дело C-817/19 е налице становище на Генералния адвокат, което отчита някои несъвършенства на Директивата, но определя същата за съвместима с основните права по отношение на неприкосновеността на личния живот и защитата на личните данни. Това се критикува от някои автори, които призовават за обявяване на Директивата за невалидна[8]. Предстои да видим дали СЕС ще оцени стандартите по Директивата за достатъчни за опазване на основните права и свободи, или ще я обяви за невалидна.

Приложение на ИИ в сферата на правоприлагането

В допълнение, се очаква ЕС да утвърди и допълнителна правна рамка за използването на ИИ в различни сфери на обществения живот, включително правоприлагането. В момента на ниво ЕС се обсъжда проект на Регламент за ИИ (Регламентът/Проектът)[5]. Самият Регламент урежда важни гаранции при прилагането на ИИ в чувствителна сфера като правоприлагането, в която всяка грешка може да доведе до непропорционално ограничаване на правата и

свободите на хората – например тяхното следене, задържане и др. Ето няколко неизчерпателни примера в тази насока:

Първо, **предвижда се забрана публичните органи да използват системи за ИИ за социален ранкинг**, тоест за оценка или класифициране на надеждността на ФЛ на базата на тяхното социално поведение или известни/прогнозирани лични/личностни характеристики, ако това води до увреждащо и/или неблагоприятно третиране на определени ФЛ или групи. Това е гаранция за опазване на човешкото достойнство и правата на личността в едно демократично общество. Всяко подобно автоматизирано сегрегиране и оценяване на хората е несъвместимо с модерните разбирания на правовата държава.

Второ, Проектът предвижда **класифицирането на системите с ИИ в областта на правоприлагането** като **високорискови**. Това ще наложи съобразяване на редица изисквания по Регламента във връзка с пускането на пазара и въвеждането в експлоатация на подобни системи. Както е посочено в обяснителния меморандум към Регламента: „Подобни системи с ИИ ще трябва да отговарят на набор от хоризонтални задължителни изисквания за надежден ИИ и да преминат през процедури за оценяване на съответствието, преди да могат да бъдат пуснати на пазара на Съюза. По отношение на доставчиците и ползвателите на подобни системи се определят предвидими, пропорционални и ясни задължения за гарантиране на безопасността и спазването на съществуващото законодателство за защита на основните права през целия жизнен цикъл на системите с ИИ“[5].

Трето, възможността за използване на системи с ИИ за дистанционна биометрична идентификация в реално време на ФЛ на обществено достъпни места за целите на правоприлагането се ограничава **до три изчерпателно уредени хипотези**, а именно, ако е строго необходимо за:

- целево издирване на конкретни потенциални жертви на престъпления, включително изчезнали деца;
- предотвратяване на конкретна, значителна и непосредствена заплаха за живота или физическата безопасност на ФЛ или за терористично нападение;
- откриване, локализиране, идентифициране или преследване на извършител или заподозрян в извършването на определена категория тежки престъпления (очертани в Рамково решение 2002/584/ПВР на Съвета) и наказуемо в съответната ДЧ с лишаване от свобода/мярка за задържане с максимален срок не по-малко от 3 години.

Причината е, че използването на подобни системи „се счита за особено силно накърняващо правата и свободите на засегнатите лица, доколкото то може да засегне личния живот на голяма част от населението, да породи усещане за постоянно наблюдение и косвено да действа разубеждаващо по отношение на упражняването на свободата на събранията и други основни права“ (съображение 18). Въвеждат се специфични критерии при използването на тези системи, като естеството на ситуацията, последиците от използването на системата за правата и свободите на засегнатите лица и пр. Важно изискване, гарантиращо правата и свободите на хората, е всяко отделно използване на такава система да подлежи на предварително разрешение от съд или независим административен орган на ДЧ, в която ще се осъществи използването, след получаване на мотивирано искане и в съответствие с националното право. Изключение се допуска единствено при надлежно обосновани спешни случаи, в които разрешение може да се поиска едва по време на или след използването на системата. Допуска се ДЧ да разрешат изцяло или частично използването на подобна система за биометрична идентификация за целите на правоприлагането при горепосочените условия и хипотези, но тогава съответната ДЧ ще бъде длъжна да уреди в националното си законодателство необходимите подробни правила за ползване на тези системи, като подаване на искания, издаване на разрешения, изпълнението им, надзора спрямо тях, за кои цели и престъпления може да се използват тези системи. Това е своеобразна допълнителна гаранция, че използването на подобни системи ще бъде обект на детайлна законова регламентация – било на европейско, било на национално ниво.

У нас **българската Комисия за защита на личните данни (КЗЛД) също отчита рисковете, свързани със защитата на личните данни при използването на ИИ в различни сфери, включително в тази на правоприлагането**. КЗЛД посочва, че „ИИ и свързаните с него технологии в областта на правоприлагането и граничния контрол биха могли да подобрят обществената безопасност и сигурност“[9]. КЗЛД обаче отчита, че тези системи се нуждаят от всеобхватен и строг обществен контрол; от възможно най-високо равнище на прозрачност по отношение на оценката на риска за отделните приложения; от общ преглед за използването на ИИ, роботиката и свързаните с тях технологии в областта на правоприлагането и граничния контрол. КЗЛД призовава тези технологии да бъдат обмислени подобаващо, като се отчитат възможните неблагоприятни последици за хората, по-специално във връзка с техните права за неприкосновеност на личния живот, защита

на личните данни и недискриминация[9]. Подобни разяснителни документи също представляват гаранция при използването на нови технологии, като ИИ, в сферата на правоприлагането, тъй като дават рамка и насока какви аспекти на използването на тези технологии трябва да бъдат съобразени, за да бъдат новите технологии внедрени в съответствие със стандартите на модерните демократични държави.

Изводи/Дискусия

Бъдещето ще покаже дали ЕС и ДЧ ще успеят да постигнат ефективна регулация на новите технологии, като автоматизираната обработка на данни и ИИ. Като минимум, решенията на ИИ трябва да подлежат на преглед и контрол от човек, в противен случай се създават сериозни рискове пред правата и свободите на гражданите. Тепърва предстои и СЕС и националните съдилища да създадат практика по тези проблеми, която да бъде обект на бъдещи научни анализи.

Докладът е изготвен в рамките на научен проект „Колективните и националните политики за сигурност и отбрана в контекста на съвременната среда за сигурност“ по Договор № НИП-2022-06/18.04.2022 г.

Бележки

[1] **Direktiva** (ES) 2016/680 na Evropeyskiya parlament i na Saveta ot 27 april 2016 godina otnosno zashtita na fizicheskite litsa vav vrazka s obrabotvaneto na lichni danni ot kompetentnite organi za tselite na predovratyavaneto, razsledvaneto, razkrivaneto ili nakazatelnoto presledvane na prestapleniya ili izpalnenieto na nakazaniya i otnosno svobodnoto dvizhenie na takiva danni i za otmyana na Ramkovo reshenie 2008/977/PVR na Saveta, Obn. OJ L 119, 4.05.2016, s. 89 – 131.

[**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, Обн. OJ L 119, 4.05.2016, с. 89 – 131.]

[2] **Zakon** za zashtita na lichnite danni, obn. DV, br. 1 ot 4.01.2002 g., posl. izm. DV, br. 93 ot 26.11.2019 g. s Reshenie № 8 ot 15.11.2019 g. na KS na RB po k.d. № 4/2019 g.

[**Закон** за защита на личните данни, обн. ДВ, бр. 1 от 4.01.2002 г., посл. изм. ДВ, бр. 93 от 26.11.2019 г. с Решение № 8 от 15.11.2019 г. на КС на РБ по к. д. № 4/2019 г.]

[3] **Direktiva** (ES) 2016/680 na Evropeyskiya parlament i na Saveta ot 27 april 2016 godina otnosno izpolzvaneto na rezervatsionni danni na patnitsite s tsel predotvratyavana, razkrivane i nakazatelno presledvane na teroristitschni prestaplenya i tezhki prestaplenya, obn.OJ L 119, 4.05.2016, s. 132 – 149.

[**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, обн. OJ L 119, 4.05.2016, с. 132 – 149.]

[4] **Zakon** za Darzhavna agentsia „Natsionalna sigurnost“, obn. DV, br. 109 ot 20.12.2007 g., posl. dop. DV, br. 51 ot 5.06.2020 g.

[**Закон** за Държавна агенция „Национална сигурност“, обн. ДВ, бр. 109 от 20.12.2007 г., посл. доп. ДВ, бр. 51 от 5.06.2020 г.]

[5] **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.
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206> (16.04.2022).

[6] **WP29**, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), Adopted on 29 November 2017, WP 258.
<https://ec.europa.eu/newsroom/article29/items/610178/en> (16.04.2022), p. 11 – 14.

[7] **REPORT** FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime {SWD(2020) 128 final}. <https://ec.europa.eu/home-affairs/system/files/2020-07/20200724_com-2020-305-review_en.pdf> (16.04.2022).

[8] **Thönnes**, Ch. A cautious green light for technology-driven mass surveillance. <https://verfassungsblog.de/green-light/> (16.04.2022).

[9] **KZLD.** Savremenni zaplahi i predizvikatelstva pred zashtitata na lichnite danni w konteksta na tendentsiite w razvitieto na izkustvenya intelekt i novite tehnologii za litsevo razpoznavane. <https://www.cpdp.bg/index.php?p=element&aid=1342> (16.04.2022).

[**КЗЛД.** Съвременни заплахи и предизвикателства пред защитата на личните данни в контекста на тенденциите в развитието на изкуствения интелект и новите технологии за лицево разпознаване.
<https://www.cpdp.bg/index.php?p=element&aid=1342> (16.04.2022)].

References/Литература

1. **Feti**, N., D. **Toshkova-Nikolova**. Prilagane na zashtitata na lichnite danni. Sofia: Trud i pravo, 2020.

[**Фети**, Н., Д. **Тошкова-Николова**. Прилагане на защитата на личните данни. София: Труд и право, 2020.]

2. **Zahariev**, M., D. **Krusteva**. Avtomatiziranoto profilirane v konteksta na garantirane na natsionalnata sigurnost. – V: *Sbornik* nauchni trudove, Shumen, NVU „V. Levski“ – Fakultet „Artileria, PVO i KIS“, 2016, s. 101 – 112.

[**Захариев**, М., Д. **Кръстева**. Автоматизираното профилиране в контекста на гарантиране на националната сигурност. – В: *Сборник* научни трудове, Шумен, НВУ „В. Левски“ – Факултет „Артилерия, ПВО и КИС“, 2016, с. 101 – 112.]

3. **Zahariev**, M. Avtomatiziranoto profilirane i zashtitata na lichnite danni. Sofia: Za bukvite – O pismeneh, 2018.

[Захариев, М. Автоматизираното профилиране и защитата на личните данни. София: За буквите – О писменехь, 2018.]

4. **Tselkov**, V., D. **Petkov**, G. **Sredkov**, P. **Georgiev**. Zashtita na dannite. Printsipi i praktiki. Sofia: Za bukvite – O pismeneh, 2019.

[**Целков**, В., Д. **Петков**, Г. **Средков**, П. **Георгиев**. Защита на данните. Принципи и практики. София: За буквите – О писменехь, 2019.]

5. **Toshkova-Nikolova**, D., N. **Feti**. Zashtita na lichnite danni. Sofia: Trud i pravo, 2019.

[**Тошкова-Николова**, Д., Н. **Фети**. Защита на личните данни, София: Труд и право, 2019.]

За автора

Мартин Захариев завършва специалност „Право“ с отличие, като се дипломира в Юридическия факултет на Софийския университет „Св. Климент Охридски“ през 2014 г. Притежава образователната и научна степен „доктор“ от Университета по библиотекознание и информационни технологии (УниБИТ), а от 2021 г. е доцент към катедра „Национална сигурност“, Факултет „Информационни науки“ на УниБИТ. Работи като старши адвокат в една от водещите български кантори – Адвокатско дружество „Димитров, Петров и Ко.“, като старши правен експерт във фондация „Право и Интернет“, а също така е член на Софийската адвокатска колегия и Сдружението за международни състезания по право. Автор е на две монографии и на учебник в областта на защитата на личните данни, както и на множество статии и анализи в областта на защитата на личните данни, търговския арбитраж, трудовото и търговското право. Преподавател е по различни дисциплини в областта на правото и информационните технологии.

За контакт с автора: m.zahariev@unibit.bg

LEGAL GUARANTEES IN THE USE OF NEW TECHNOLOGIES FOR THE PURPOSE OF COUNTERING CRIME AND TERRORISM

Martin Zahariev
University of Library Studies and Information Technologies
Law and Internet Foundation
Dimitrov, Petrov & Co. Law Firm

Abstract: The dynamics of modern social relations pose new threats to security and public order. Therefore, the competent authorities should identify appropriate mechanisms to counter such threats, in line with the modern technological developments of society. Such mechanisms could be some new technologies such as facial recognition, artificial intelligence, automated decision making, and profiling. This paper aims to analyze some basic legal guarantees, for the rights and freedoms in the application of these technologies, in the field of combating crime and terrorism.

Keywords: guarantees, automated decision making and profiling, passenger name records, artificial intelligence, rule of law.

About the author

Martin Zahariev graduated with honors from Sofia University "St. Kliment Ohridski", Faculty of Law (LL.M.) in 2014. He has an educational and scientific degree "doctor" at the University of Library Studies and Information Technologies (ULSIT) and since 2021 has been appointed as "Associate Professor" with the Department of National Security, Faculty of Information Sciences, at ULSIT. He is a senior associate in one of the leading Bulgarian law firms – "Dimitrov, Petrov and Co." Law Firm, a senior legal expert in the "Law and Internet" Foundation, and is also a member of the Sofia Bar Association and the International Moot Court Competitions Association. Assoc. Prof. Zahariev is the author of two monographs and a students' book in the field of personal data protection, as well as numerous articles and analyzes in the field of personal data protection, commercial arbitration, labor and commercial law. He is a lecturer in various disciplines, in the field of law and information technologies.

To contact the author: m.zahariev@unibit.bg