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

доц. д-р Мартин Захариев

Университет по библиотекознание и информационни технологии

Фондация „Право и Интернет“, Старши правен експерт

Адвокатско дружество „Димитров, Петров и Ко.“, Старши адвокат

София

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.

- Подходящи механизми за противодействие на заплахи, отговарящи на съвременното развитие на обществото могат да бъдат **новите технологии**, които са мощен инструмент за опазване на обществения ред и сигурност.

Въведение

- **Съществуващи рискове:** технологиите могат да служат за манипулация на човешкото поведение, дискриминация, прекомерно навлизане в личния и семейния живот, непозволено следене, профилиране и др. под. (напр. чрез автоматизирана алгоритмична обработка на данни, биометрично разпознаване, изкуствен интелект (ИИ) и др.)

- **Ключови правни актове:** Директива 2016/680, транспонирана в глава 8 от Закона за защита на личните данни (ЗЗЛД) и Директива 2016/681, транспонирана в глава 6а от Закона за Държавна агенция „Национална сигурност“ (ЗДАНС) = съдържат важни гаранции за основните права и свободи при обработване на лични данни за противодействието на престъпността и тероризма.

Методология на изследването

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

- **Сравнителен анализ** – този метод се изразява в сравняване на общото и различното между отделни явления.

- **Ограничение на изследването** – не обхваща използването на технологии и правните гаранции в сфери извън приложното поле на правото на ЕС като националната сигурност на държавите членки

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

- Следва от чл. 11 на Директива 206/680, като транспониращото я в националното ни законодателство правило е чл. 52 ЗЗЛД

- Забранява АВР, включително профилиране, което:

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

- **Забранено е тези решения да се основават на специални категории данни** (както са дефинирани в чл. 51, ал. 1 ЗЗЛД), освен ако не са въведени подходящи мерки за защита на правата и свободите и законните интереси на субекта на данните

- **Допълнителни национални гаранции** при АВР и профилиране
  - задължителното извършване на оценка на въздействието по чл. 64 ЗЗЛД при подобен тип операции
  - правото на засегнатия субект да получи човешка намеса от страна на администратора по Директивата е доразвито и чл. 52, ал. 5 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

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

- Обработка на РДП от Националното звено за данни на пътниците (НЗДП) – специализирана структура в ДАНС, за целите на противодействие на изчерпателно уредени тежки престъпления и тероризъм

- 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).

- Подобно изискване е въведено и преди предаване на получени от чужди ЗДП РДП/резултати от обработката им на компетентни органи (чл. 42л, ал. 5)

- Уредена е възможност „фалшиво-позитивните резултати“, установени чрез човешка намеса, да се съхраняват с цел да се избегнат бъдещи недействителни съвпадения (чл. 42з, ал. 12)

Приложение на ИИ в сферата на правоприлагането

- В момента на ниво ЕС се обсъжда проект на Регламент за ИИ (Регламентът/Проектът):

1. Предвижда се забрана публичните органи да използват системи за ИИ за социален ранкинг, т.е. за оценка или класифициране на надеждността на ФЛ на база на тяхното социално поведение или известни/прогнозирани лични/личностни характеристики, ако това води до увреждащо и/или неблагоприятно третиране на определени ФЛ или групи

2. Класифициране на системите с ИИ в областта на правоприлагането като високорискови

Приложение на ИИ в сферата на правоприлагането

3. **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.

Приложение на ИИ в сферата на правоприлагането

- 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.
- Всяко отделно използване на такава система подлежи на предварително разрешение от съд или независим административен орган на ДЧ. 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.

Приложение на ИИ в сферата на правоприлагането

- **Комисията за защита на личните данни (КЗЛД) също отчита рисковете, свързани със защитата на личните данни при използването на ИИ в различни сфери, в т.ч. в тази на правоприлагането.**
  - *„ИИ и свързаните с него технологии в областта на правоприлагането и граничния контрол биха могли да подобрят обществената безопасност и сигурност“.*
- 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.

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

- ✓ 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

Благодаря за вниманието!

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.

За контакт:
E-mail: m.zahariev@unibit.bg
Телефон: тел. 02/ 421-42-01; +359 888 95 00 77
Уебсайт: www.dpc.bg