

НАЦИОНАЛНА СИГУРНОСТ

РАДИКАЛИЗАЦИЯ БЕЗ ВЕРБОВЧИК: ПОВЕДЕНЧЕСКИЯТ ДИГИТАЛЕН ДВОЙНИК НА ДЕТЕТО КАТО НОВ РИСК ЗА НАЦИОНАЛНАТА СИГУРНОСТ

КОМИСАР ПРОФ. Д-Р ИЛИН САВОВ, Д.Н.

ЗАМЕСТИНИК-РЕКТОР

АКАДЕМИЯ НА МИНИСТЕРСТВОТО НА ВЪТРЕШНИТЕ РАБОТИ



Резюме: Настоящата статия разглежда трансформацията на онлайн радикализацията при деца и младежи в среда, в която въздействието все по-често не се осъществява чрез един разпознаваем вербовчик, а чрез съчетание от системи за препоръчване, поведенческо профилиране, затворени дигитални общности и разговорен изкуствен интелект. На тази основа се предлага авторското понятие „поведенчески дигитален двойник на уязвимостта“ (Behavioural Vulnerability Twin - BVT). То обозначава динамична аналитична реконструкция на поведенчески сигнали, чрез които могат да бъдат изведени интереси, емоционални реакции, търсене на принадлежност, модели на внимание и възприемчивост към определени послания. Концепцията не предполага, че платформите поддържат буквален цифров двойник на всяко дете, а се използва като рамка за анализ на персонализираното цифрово въздействие. Разгледани са актуални

данни на Europol, UNICEF, eSafety Commissioner, Institute for Strategic Dialogue и съвременни научни изследвания за алгоритмична персонализация, Human Digital Twins и онлайн радикализация. Предлага се петстепенен авторски модел BVT-R за оценка на риска, както и принципи за превенция, които съчетават защита на детето, основни права, дигитална грамотност и институционална готовност.

Ключови думи: онлайн радикализация, деца, поведенчески дигитален двойник, изкуствен интелект, алгоритми, екстремизъм, превенция, национална сигурност

RADICALISATION WITHOUT A RECRUITER: THE CHILD'S BEHAVIOURAL DIGITAL TWIN AS AN EMERGING NATIONAL SECURITY RISK

COMMISSIONER PROF. ILIN SAVOV, PHD, DSC

DEPUTY RECTOR OF THE ACADEMY OF THE MINISTRY OF INTERIOR

Abstract: This article examines the transformation of online radicalisation among children and young people in a digital environment where influence is increasingly generated not by a single identifiable recruiter, but by the interaction of recommender systems, behavioural profiling, closed online communities and conversational artificial intelligence. It introduces the author's concept of a "Behavioural Vulnerability Twin" (BVT), understood as a dynamic analytical reconstruction of behavioural signals

from which interests, emotional responses, belonging needs, attention patterns and potential susceptibility to specific messages may be inferred. The concept does not claim that platforms maintain a literal digital twin of every child; it is proposed as an analytical framework for understanding personalised digital influence. The paper draws on current Europol, UNICEF, eSafety Commissioner and Institute for Strategic Dialogue findings, as well as recent academic research on algorithmic personal-

isation, Human Digital Twins and online radicalisation. A five-stage BVT-R conceptual model is proposed, alongside prevention principles combining child protection, fundamental rights, digital literacy and institutional preparedness.

Keywords: *online radicalisation, children, behavioural digital twin, artificial intelligence, algorithms, violent extremism, prevention, national security.*

ВЪВЕДЕНИЕ

В продължение на години един от първите въпроси при случай на радикализация на дете беше лесен за формулиране: кой го е намерил, кой му е говорил и кой го е убедил. Този въпрос остава важен, но вече не е достатъчен. В съвременната дигитална среда детето може да не познава конкретен вербовчик, да не е получавало пряка инструкция и въпреки това постепенно да се окаже в информационна среда, която последователно усилва гняв, чувство за унижение, недоверие, нужда от принадлежност или привличане към насилието. Влиянието не винаги започва с идеология. Понякога започва с любопитство, провокация, мем, видео, игрова общност или разговор, който изглежда личен и безопасен.

Това е съществена промяна. Интернет отдавна не е само пространство, в което съдържанието се публикува и потребителят сам го търси. Системите за препоръчване наблюдават поведенчески сигнали и непрекъснато пренареждат следващото съдържание. В същото време генеративният и разговорният изкуствен интелект добавят нов тип взаимодействие: диалог, който може да бъде постоянен, персонализиран и да запазва контекст. Така класическата схема „вербовчик – послание – цел“ започва да се допълва от по-сложна архитектура, в която алгоритми, групова динамика, дигитални субкултури и автоматизирани системи могат да работят едновременно.

Данните от най-новия доклад на Europol за тероризма в Европейския съюз показват колко сериозно е това развитие. През 2025 година 130 заподозрени за престъпления, свързани с тероризъм, които са били арестувани в ЕС, са на възраст 18 години или по-малко, като най-младият е на 12 години. Europol описва среда, в която насилствена екстремистка пропаганда, gaming общности и дигитални субкултури могат да въздействат едновременно чрез различни и дори смесени идеологически влияния. При част от младите лица се наблюдава не задълбочено приемане на една иде-

ология, а фрагментарно съчетаване на радикални наративи, срещнати онлайн.

Това поставя изследователски проблем с пряко значение за националната сигурност: възможно ли е процесът на радикализация да се развива без постоянен човешки вербовчик, когато дигиталната среда сама събира достатъчно поведенчески сигнали, за да персонализира съдържанието и взаимодействието? Настоящата статия предлага концептуален отговор чрез понятието „поведенчески дигитален двойник на уязвимостта“ – модел, който свързва поведенческото профилиране, системите за препоръчване, разговорния AI и динамиката на онлайн радикализацията. Целта не е да се технологизира или криминализира детското поведение, а обратното да се изгради по-точен език за превенция, преди рисковите сигнали да бъдат превърнати в насочено влияние.

ОТ ВЕРБОВЧИКА КЪМ СРЕДАТА: ПРОМЯНА В ЛОГИКАТА НА ОНЛАЙН РАДИКАЛИЗАЦИЯТА

Класическите модели на радикализация обикновено предполагат наличие на човек, група или организация, която идентифицира потенциална цел, установява контакт, изгражда доверие и постепенно въвежда идеологическа рамка. Дигиталната среда не премахва този модел, но го прави само една от възможностите. Днес първият контакт може да бъде алгоритмичен, а човешкият участник да се появи много по-късно, когато интересът вече е оформен, езикът на групата е усвоен и определени форми на насилие са нормализирани.

Оперативните наблюдения на Europol дават конкретна картина. При координирана европейска акция през май 2025 г. са насочени за действие над 2000 интернет връзки към джихадистко и крайнодясно насилствено екстремистко и терористично съдържание, насочено към непълнолетни. Сред използваните форми са кратки видеа, мемета, gaming елементи и съдържание, създава-

но с изкуствен интелект - изображения, текст и видео, пригодени към по-млада аудитория. Тук не става дума само за наличие на пропаганда, а за съзнателно адаптиране на формата към начина, по който децата консумират съдържание.

Още по-показателен е феноменът „The Com“, описан от Europol през 2026 г. Това е децентрализирана среда от крайни онлайн групи с нихилистична и мизантропска насоченост, в която насилието нерядко е ценност само по себе си, а не средство за постигане на стройна политическа цел. Групи от тази среда използват социални мрежи, приложения за съобщения и gaming платформи, за да привличат млади хора и да ги насочват към частни пространства. През месец юни и месец юли на 2026 г. в рамките на европейска операция са насочени за действие приблизително 4340 URL адреса, свързани с нихилистичен насилствен екстремизъм. Това е важен пример за радикализация, при която идеологията може да бъде разпокъсана, но механизмите на принадлежност, престиж, страх, принуда и ескалация остават силни.

Следователно изразът „радикализация без вербовчик“ не означава радикализация без хора. В повечето реални процеси хора, групи и общности продължават да имат значение. Новото е друго: за започването и поддържането на процеса вече не е необходимо един конкретен човек постоянно да води целта. Част от функциите на традиционния вербовчик е откриване на интерес, подбор на послание, повторение, създаване на чувство за значимост и насочване към следващо съдържание, за да могат да бъдат разпределени между технологични и социални механизми.

КОГАТО ДЕТЕТО СЕ ПРЕВРЪЩА В ПОВЕДЕНЧЕСКИ ДАННИ

В основата на тази промяна е фактът, че дигиталното поведение оставя много повече информация от видимото съдържание, което човек публикува. Времето, което потребителят задържа върху определено видео, кои материали пропуска, какво търси, в какъв часови диапазон е активен, към кои профили се връща, какви теми предизвикват реакция и как се променят контактите му, всичко това може да се превърне в сигнал за персонализация. Отделният сигнал е слаб. Натрупани във времето, сигналите образуват поведенческа картина.

Изследването на Martin Hilbert и съавтори, публикувано в Telematics and Informatics през 2025

г., е особено важно в този контекст. Чрез одит на препоръчващите системи на YouTube, Instagram и TikTok авторите установяват, че алгоритмите могат бързо да променят препоръките спрямо поведенчески характеристики, свързани с по-млада възраст и с уязвими тийнейджърски профили. Изследването не доказва намерение за причиняване на вреда и не следва да бъде интерпретирано като доказателство, че платформите „диагностицират“ децата. То обаче показва нещо принципно: поведението позволява да се извежда практически използвана информация за потребителя, дори когато той не я е заявил пряко.

Точно тук се появява връзката с по-широката научна дискусия за Human Digital Twins. Систематичният преглед на Gaffinet, Al Haj Ali, Naudet и Panetto (2025) показва, че понятието човешки дигитален двойник все още няма напълно еднозначно съдържание и е необходимо разграничаване между дигитален модел, дигитална сянка и истински дигитален двойник според вида и посоката на обмен на данни. В технически строг смисъл повечето платформени профили биха били по-близо до „дигитална сянка“, тъй като данните се натрупват от поведението и се използват за прогнозиране и персонализация.

В настоящото изследване терминът „поведенчески дигитален двойник“ се използва съзнателно като аналитична рамка, а не като твърдение за конкретна архитектура на информационните системи. Той насочва вниманието към практическата последица: дигиталната среда може да изгради функционално полезно отражение на това какво задържа вниманието на детето, какво предизвиква емоционален отговор и към какво е вероятно да се върне. Когато подобно отражение се срещне с вредно съдържание, рискът вече не е само „достъп до пропаганда“, а възможност за персонализирана последователност на въздействие.

ПОВЕДЕНЧЕСКИ ДИГИТАЛЕН ДВОЙНИК НА УЯЗВИМОСТТА - АВТОРСКА КОНЦЕПЦИЯ

За целите на настоящата статия се предлага понятието Behavioural Vulnerability Twin (BVT) или „поведенчески дигитален двойник на уязвимостта“. Под него се разбира динамична аналитична реконструкция на поведенчески сигнали, чрез които могат да бъдат изведени вероятни интереси, емоционални тригери, модели на внима-

ние, необходимост от принадлежност, чувствителност към определен език и възприемчивост към конкретни форми на дигитално въздействие.

BVT не е медицинска, психологическа или криминологична диагноза. Той не може да показва, че едно дете „ще се радикализира“, нито може да бъде използван като доказателство за бъдещо престъпно поведение. Концепцията описва рисковата информационна асиметрия: платформата или системата може да разполага с натрупана картина за предпочитанията и реакциите на детето, докато родителят, учителят и дори самото дете нямат видимост върху начина, по който тази картина влияе върху следващото съдържание.

В този модел значение имат най-малко пет групи сигнали. Първата е вниманието, какво се гледа, колко дълго и към какво потребителят се връща. Втората е емоционалната реакция, тоест теми, които водят до силно одобрение, възмущение, страх или любопитство. Третата е социалната ориентация са профили, групи и общности, към които потребителят постепенно се приближава. Четвъртата е езикът е промяната в използваните думи, символи, шегички и кодирани изрази. Петата е ритъмът на моментите и честотата на активност, особено когато взаимодействието се измества към затворени или по-интензивни пространства.

Тези сигнали не са сами по себе си доказателство за риск. Дете може да гледа насилствено съдържание от любопитство, изследователски интерес или случайна препоръка. Проблемът възниква при съчетанието на продължителност, повторемост, ескалация и социално укрепване. Именно затова концепцията BVT не следва да се използва за автоматично „етикетиране“ на лица. Нейната стойност е в разбирането как дигиталната среда може да превърне множество слаби сигнали в прецизно насочване.

АВТОРСКИ МОДЕЛ BVT-R: ПЕТ ЕТАПА НА РАДИКАЛИЗАЦИЯ В ПЕРСОНАЛИЗИРАНА ДИГИТАЛНА СРЕДА

Въз основа на разгледаните тенденции се предлага концептуален модел BVT-R (Behavioural Vulnerability Twin - Radicalisation), който описва пет взаимосвързани етапа. Моделът не представя радикализацията като задължителна линейна последователност. В реалността процесът може да се прекъсне, да се върне назад или изобщо да не пре-

мине към насилие. Неговото предназначение е да покаже къде възникват възможности за превенция.

Първи етап е дигиталната следа (Digital Trace). Детето използва социални мрежи, видео платформи, игри, чатове или AI услуги и оставя поведенчески данни. Това е нормална част от дигиталното участие. Рискът не е в самото наличие на данни, а в това колко подробно и продължително могат да бъдат свързвани в модел на поведение.

Втори етап е извеждане на уязвимост (Vulnerability Inference). Системите за персонализация започват да разпознават теми и формати, които задържат вниманието. В този етап „уязвимост“ не означава непременно психологически дефицит. Това може да бъде силен интерес към конфликт, търсене на признание, чувство за несправедливост, необходимост от групов идентичност или привличане към шоково съдържание. От гледна точка на риска същественото е, че различни сигнали могат да бъдат превърнати в прогноза за следващото съдържание.

Трети етап е адаптивно експониране (Adaptive Exposure). Потребителят получава съдържание, което все по-точно съвпада с установения модел на внимание. При нормално съдържание това е механизмът на персонализация. При екстремистки или насилствени наративи същата логика може да улесни постепенното придвижване към по-крайни материали. Европейската комисия признава този системен риск в Насоките от 2025 г. за защита на непълнолетните по Digital Services Act, като отделя специално внимание на препоръчващите системи и възможността те да усилят вредно съдържание.

Четвърти етап е синтетично валидиране и идентичност (Synthetic Validation and Identity). Тук влиянието вече не е само съдържателно. То може да бъде социално и разговорно. Затворена група, мрежа от профили или AI система може да потвърждава оплакванията, да предлага обяснения, да създава усещане за разбиране и да укрепва разграничението „ние - те“. Докладът на Institute for Strategic Dialogue от юли 2026 г. определя разговорния AI като качествено различна среда за риск от радикализация, защото взаимодействието може да бъде лично, продължително и едно към едно. Авторите изследват именно фазите на първоначално подготвяне, укрепване и поведенческа ескалация.

Пети етап е поведенческа мобилизация (Behavioural Mobilisation). Това е моментът, в който потребителят престава да бъде само консулатор. Започва да разпространява материали, да търси затворени групи, да изпълнява задачи, да създава съдържание, да упражнява натиск върху други или да обсъжда реални действия. Преминването към този етап не е автоматично. Именно тук човешките контакти често отново придобиват решаващо значение. Силата на модела BVT-R е в това, че показва как значителна част от подготовката за този преход може да се случи преди появата на разпознаваем вербовчик.

Моделът следва да се разбира и като обратна връзка. Всяко взаимодействие генерира нови данни, които променят следващата препоръка. Колкото по-дълго продължава цикълът, толкова по-персонализирана може да стане средата. Това е причината превенцията да бъде най-ефективна не когато се опитва да „познава бъдещия извършител“, а когато прекъсва механизмите на вредно усилване и връща възможност за избор, критична оценка и човешка подкрепа.

РАЗГОВОРНИЯТ ИЗКУСТВЕН ИНТЕЛЕКТ И РИСКЪТ ОТ „ЗАТВОРЕНА ОБРАТНА ВРЪЗКА“

Социалната мрежа препоръчва съдържание. Разговорният изкуствен интелект може да направи още една крачка, тоест да отговори. Тази разлика е фундаментална. При чатбот или AI companion потребителят не просто получава материал, а формулира въпроси, споделя преживявания и може да изгради усещане за постоянен разговор. Това създава нов тип лична дигитална среда, в която алгоритмичната персонализация се среща с езика на доверие.

UNICEF в политическия си документ от юни 2026 г. отбелязва, че децата използват AI чатботове не само за информация и учене, но и за съвет, подкрепа и понякога отношения, което поражда отделни и повишени рискове за детските права и безопасността. Австралийският eSafety Commissioner достига до сходна практическа картина. В национално проучване сред 1950 деца на възраст от 10 до 17 години, проведено през февруари и март 2026 г., 78% съобщават, че са използвали AI assistant, а 54% от използвалите AI assistant или companion са го правили и по лични или социални причини. Една пета от използвалите такива системи съобщават за потенциално непод-

ходящо или вредно взаимодействие, а около една трета, че са споделяли лични или потенциално чувствителни данни.

Тези числа не означават, че AI чатботовете радикализират деца. Такъв извод би бил научно некоректен. Те показват, че вече съществува мащабен канал за лично взаимодействие, който може да съдържа информация за емоционални състояния, конфликти и потребности. Именно затова рискът от „затворена обратна връзка“ трябва да бъде изследван предварително: когато една система едновременно получава чувствителен контекст, адаптира отговорите си и се възприема като доверен събеседник, грешката или вредният модел на взаимодействие може да има по-голямо значение от единична публикация в социална мрежа.

В този контекст изследването на Kenneth Yeو Yaoren от 2026 г. поставя следващия въпрос, а именно как AI agents биха могли да намалят традиционните затруднения при екстремисткото достигане до аудитория чрез автоматизиране на превод, генериране на съдържание и персонализирано взаимодействие. Към момента това следва да се разглежда преди всичко като развиващ се риск, а не като доказателство за масово автономно AI вербуване. Но именно периодът преди масовото разпространение е най-подходящ за изграждане на защиты.

КОГА ИНДИВИДУАЛНАТА УЯЗВИМОСТ СЕ ПРЕВРЪЩА В РИСК ЗА НАЦИОНАЛНАТА СИГУРНОСТ

Националната сигурност не следва да превръща всяко проблемно онлайн поведение на дете в „заплаха“. Подобен подход би бил едновременно неточен и опасен. Рискът за националната сигурност възниква на системно ниво, когато едни и същи технологични механизми позволяват едновременно въздействие върху голям брой уязвими потребители, бързо преминаване между платформи, създаване на транснационални общности и размиване на границата между идеологическа радикализация, криминална експлоатация, самоувреждане и насилие.

Точно тази хибридность е една от най-важните характеристики на новата среда. Европейската агенция Europol описва млади лица, които могат да бъдат едновременно жертви на манипулация и извършители на насилие. При „The Com“ например екстремистки елементи се смесват със сексу-

ална принуда, самоувреждане, култ към насилието и търсене на статус в групата. Това усложнява институционалния отговор, защото традиционно разделение между „тероризъм“, „киберпрестъпност“, „детска закрила“ и „превенция“ не винаги съвпада с реалния живот на детето онлайн.

Българската Стратегия за противодействие на радикализацията и тероризма 2026-2030 г., приета с Решение № 316 на Министерския съвет от 23 април 2026 г., вече отчита този преход. Документът поставя акцент върху ранното установяване на рискове, защитата на уязвими групи, включително подрастващи и малолетни, и използването на съвременни технологии за противодействие на екстремистко съдържание онлайн. Особено важно е, че стратегията разглежда онлайн радикализацията в контекста на използване на алгоритми и изкуствен интелект за персонализиране на съдържанието. Това създава добра национална основа, върху която могат да бъдат разработени по-конкретни механизми за детска дигитална устойчивост.

ПРЕВЕНЦИЯ БЕЗ ЦИФРОВО ПОДОЗРЕНИЕ: ПРАВНИ И ИНСТИТУЦИОНАЛНИ ГРАНИЦИ

Ако алгоритмите могат да извеждат поведенчески уязвимости, изкушението е държавата да отговори със същото, да събира повече данни и да се опитва да предвижда кои деца „могат да станат опасни“. Това би било грешна посока. Защитата от алгоритмично въздействие не може да бъде изградена чрез алгоритмично подозрение към детето.

Регламент (ЕС) 2024/1689 за изкуствения интелект задава важни граници. Сред забранените практики е използването на AI за експлоатиране на уязвимост, свързана с възрастта, когато чрез това съществено се изкривява поведението и се причинява или е вероятно да се причини значителна вреда. Същевременно регламентът ограничава използването на AI за оценка на риска от извършване на престъпление, когато прогнозата се основава единствено на профилиране или личностни характеристики. Това е принципно важно за всяка бъдеща система за превенция: BVT-R не трябва да се превръща в автоматизиран „скоринг“ на деца.

Digital Services Act поставя задължение платформите, достъпни за непълнолетни, да осигурят високо ниво на поверителност, безопасност и сигурност. Насоките на Европейската комисия от 2025 г. развиват тази логика, включително чрез мерки спрямо системите за препоръчване, които

могат да усилят вредно съдържание. Подходът е правилен, защото измества част от тежестта от детето към дизайна на средата. Детето не може да носи пълната отговорност да разпознава всяка манипулация в системата, която е създадена да се адаптира по-бързо от неговото внимание.

Регламент (ЕС) 2021/784 относно терористичното съдържание онлайн допълва тази рамка с механизъм за бързо премахване или блокиране на съдържание след валидна заповед, включително срок до един час за изпълнение. Но премахването на незаконно съдържание е само една част от решението. Значителна част от вредната траектория може да се развива чрез съдържание, което поотделно не достига прага на незаконност, но в комбинация, повторение и персонализация създава опасна ескалация.

Практическият отговор следва да се основава на пет принципа. Първо е безопасност по дизайн: системите за препоръчване и разговорният AI трябва да имат специални защитни механизми за непълнолетни. Второ е дигитална и социално-медийна грамотност, която учи не само „какво е фалшива новина“, а как работят персонализацията, груповият натиск и емоционалната манипулация. Трето е ранна човешка интервенция при видима промяна в поведението, без автоматично приписване на престъпни намерения. Четвърто са механизми за обмен на информация между образование, социална закрила, психолози и компетентни органи при ясно законово основание и защита на личните данни. Пето е научен и независим одит на платформените рискове, така че обществото да не разчита единствено на вътрешните оценки на технологичните компании.

ЗАКЛЮЧЕНИЕ

Следващият вербовчик може да няма име, профилна снимка и конкретен момент на първи контакт. В някои случаи той може да бъде заменен от среда, която се учи от всяко действие на детето, какво го задържа, какво го разгневява, към какво се връща и къде търси принадлежност. Това не означава, че алгоритъмът има намерение, идеология или съзнание. Означава, че системата може да изпълнява функции на селекция и персонализация, които при неблагоприятно съдържание създават условия за постепенно радикализиращо въздействие.

Предложената концепция за поведенчески дигитален двойник на уязвимостта поставя фокуса

именно върху тази промяна. Тя не описва „виртуално копие“ на детето и не претендира да прогнозира бъдещо престъпно поведение. BVT е начин да се назове натрупаната информационна асиметрия между детето и дигиталната система: едната страна се учи от поведението в реално време, а другата често не знае какво точно е научено и защо следващото съдържание изглежда толкова „подходящо“.

От гледна точка на националната сигурност най-опасно би било да чакаме процесът да стане видим едва когато се появят намерение, организация или насилие. Съвременната превенция трябва да разпознава по-ранния момент, когато дигиталната среда започва да затваря хоризонта на детето, да повтаря една и съща емоционална рамка и да превръща крайното съдържание в нормална част от ежедневието. Това изисква по-добра технологична регулация, по-висока отговорност на платформите, професионална подготовка на институциите и образование, което развива реален дигитален рефлекс.

Същевременно границата трябва да остане ясна: превенцията не бива да се превръща в наблюдение на детето като потенциален извършител. Един модел за защита има стойност само ако защитава едновременно сигурността, личното пространство, свободата на мисълта и правото на развитие. Затова BVT-R следва да бъде използван като рамка за изследване на средата и механизмите на въздействие, а не като инструмент за прогнозно криминализиране на личността.

Тук започва следващата фаза на изследването. Необходимо е моделът да бъде проверен емпирично: кои поведенчески сигнали действително предхождат ескалацията, кои са фалшиви индикатори, как се различават социалните мрежи от gaming платформите и AI companions, и кои интервенции прекъсват процеса без да нарушават правата на детето. Следващият въпрос вече не е само „кой говори на детето?“. Той е по-труден и по-важен: „коя система се учи от него, какво научава и кой носи отговорност за това, което следва?“. Отговорът на този въпрос ще определи дали превенцията ще остане една стъпка след риска или ще започне да го изпреварва.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. Закон за противодействие на тероризма. Обн., ДВ, бр. 103 от 27 декември 2016 г., с последващи изменения и допълнения

2. Министерски съвет на Република България. Стратегия за противодействие на радикализацията и тероризма (2026-2030 г.). Приета с Решение № 316 на Министерския съвет от 23 април 2026 г.
3. Европейски парламент и Съвет на Европейския съюз. Регламент (ЕС) 2021/784 от 29 април 2021 г. относно справянето с разпространението на терористично съдържание онлайн. Официален вестник на Европейския съюз, L 172, 17 май 2021 г., с. 79-109.
4. Европейски парламент и Съвет на Европейския съюз. Регламент (ЕС) 2022/2065 от 19 октомври 2022 г. относно единния пазар на цифрови услуги (Digital Services Act). Официален вестник на Европейския съюз, L 277, 27 октомври 2022 г., с. 1-102.
5. Европейски парламент и Съвет на Европейския съюз. Регламент (ЕС) 2024/1689 от 13 юни 2024 г. за установяване на хармонизирани правила относно изкуствения интелект (AI Act). Официален вестник на Европейския съюз, 2024.
6. European Commission. Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065. C/2025/5519, Official Journal of the European Union, 10 October 2025.
7. Council of Europe. Recommendation CM/Rec(2026)6 of the Committee of Ministers to member States on countering terrorism, violent extremism and the underlying radicalisation process on the internet. Strasbourg, 8 April 2026.
8. Europol. European Union Terrorism Situation and Trend Report 2026 (EU TE-SAT). Luxembourg: Publications Office of the European Union, 2026. ISBN 978-92-9414-099-9; DOI: 10.2813/5264545.
9. Europol. European Union Terrorism Situation and Trend Report 2025 (EU TE-SAT). The Hague/Luxembourg: European Union Agency for Law Enforcement Cooperation, 2025.
10. Europol. "Europol coordinates operation against terrorist content online targeting minors - Over 2 000 links were referred during the action day." Press release, 3 June 2025.
11. Europol. "Europol-led action against nihilistic violent extremist network 'The Com' - Referral Action Days disrupt online ecosystem and leads to the referral of 4 340 URLs." Press release, 24 July 2026.
12. Dukić, S.; Vela, N.; Venkataramakrishnan, S.; von Bredow, C. Radicalisation in Closed Loops: Risks and Intervention Opportunities with AI Chatbots and Companions. London: Institute for Strategic Dialogue, 2026.
13. Yeo, K. Y. "When AI Agents Recruit: The Future of Extremist Radicalisation Online." Counter Terrorist Trends and Analyses, Vol. 18, No. 4, July 2026, pp. 26-31.
14. UNICEF. When AI Becomes a Friend: Child Rights Risks, Harms, and Regulatory Responses to AI Chatbots and Companions. Policy Brief. New York: United Nations Children's Fund, June 2026.
15. eSafety Commissioner. Talking to Machines: Children's Experiences with AI Assistants and Companions. Canberra: Australian Government, 2026.