КИБЕРПРЕСТЪПЛЕНИЯ И ПРАНЕ НА ПАРИ. ПРОБЛЕМИ НА НОРМАТИВНАТА РЕГЛАМЕНТАЦИЯ

Йовита Григорова
Заместник Административен ръководител
Заместник Апелативен прокурор при Апелативна прокуратура, Бургас

CYBERCRIME AND MONEY LAUNDERING. PROBLEMS OF NORMATIVE REGULATION

Jovita Grigorova
Appellate prosecutor’s office Burgas

Резюме: *Настоящият доклад разглежда проблемите на съдебната практика, които се поставят пред правоприлагащите органи, породени от динамиката на наказателните производства с предмет престъпления против реда на управление и конкретно тези, за противозаконно преминаване на държавните граници на Република България, съотнесени със съдебната практика по наказателните дела против личността и в частност тези с предмет трафик на хора. Аргументира се необходимостта от еднообразна съдебна практика.*

Ключови думи: *съдебна практика, трафик на хора, противозаконно преминаване на държавните граници*.

Abstrsct: *This report examines the problems of judicial practice, which law enforcement authorities face, caused by the dynamics of criminal proceedings with the subject of crimes against public order and specifically those for illegal crossing of the national borders of the Republic of Bulgaria, correlated with the judicial practice in criminal cases against a person’s dignity and in particular those with the subject of human trafficking. The need for uniform judicial practice is argued.*

Key words: *judicial practice, human trafficking, illegal crossing of national borders*.

Пристъпвайки към разглеждане на темата за киберсигурността, борбата с киберпрестъпността и прането на пари, следва да се отбележи, че тази тема все повече се налага като основополагаща, с цел осигуряване на възможността за законосъобразното протичане на множество социални отношения, включително и по отношение на националната сигурност. Тази актуалност се определя с оглед възходящата динамика в развитието на обществото ни и цялостната му глобализация. Ето защо, разискването на въпросите за правилното и безпроблемно функциониране и прецизиране на нормативния подход за справянето на този проблем, е ключът за оптимизиране на работата не само на законодателната, изпълнителната и съдебна власти, но и на ежедневните социални контакти в гражданския и стопански оборот. Изработването на стабилна рамка от закони, разпоредби и оперативни мерки гарантира, че националните органи могат да предприемат ефективни действия за откриване и

прекъсване на финансовите потоци, които подхранват престъпността и наказват отговорните за тази незаконна дейност.

Анализът на актуалната национална нормативна регламентация на понятието „пране на пари“, закрепено законово в Глава VII от Наказателния кодекс на Р.България /НК/ и компютърните престъпления /по отношение на понятието киберпрестъпленията – няма законово определение в НК на Р.България/ по реда на Глава IXа от НК, несъмнено следва да посочи, че първоначалната национална правна рамка за Република България е в логична връзка с Дял VII от Договора за функционирането на Европейския съюз (ДФЕС), съгласно който: със създаването на единния пазар е създадена обща правна рамка в целия ЕС с цел ефективно предотвратяване на изпирането на пари. Въведено е изискване за движението на финансовите потоци, които следва да се регулират, за да се гарантира възможността за идентифициране на сделките. От друга страна е обособена правна регулация за финансовите оператори и се определят нефинансовите такива, които следва да идентифицират своите клиенти (включително действителните собственици на дружества) с необходимост за проследяване на сделките и за докладване на звената за финансово разузнаване при съмнения за пране на пари и Дял V Договора за функционирането на Европейския съюз (ДФЕС), касаещ полицейско и съдебно сътрудничество по наказателноправни въпроси с акцент върху идентифицирането на престъпленията и укрепването на институционалната взаимопомощ.

Правилата на ЕС относно финансовите престъпления се основават и на международните стандарти, приети от Специалната група за финансови действия FATF (The Financial Action Task Force). В частност това е:

- Резолюция на Европейския парламент от 3 октомври 2017 г. относно борбата с киберпрестъпността (2017/2068(INI)) (2018/C 346/04)
- Директива (ЕС) 2018/843 – петата директива на ЕС за борба с изпирането на пари, с която се изменя четвъртата директива относно борбата с изпирането на пари (Директива (ЕС) 2015/849). Същата изтъква за цел борбата с изпирането на пари и с финансирането на тероризма чрез предотвратяване на злоупотребата на финансовия пазар за тези цели.
- Директива (ЕС) 2018/1673 с фокус върху криминализиране на изпирането на пари в случаите, когато изпирането на пари се извършва умишлено и със знанието, че имуществото е придобито от престъпна дейност. В същата се определят престъпленията и санкциите в областта на изпирането на пари и се разрешава на държавите членки да криминализират изпирането на пари, когато нарушителят е имал съмнения или е трябвало да знае, че имуществото е придобито от престъпна дейност.

През 2020 г. Европейската комисия прие план за действие на ЕС за предотвратяване на изпирането на пари и финансирането на тероризма, който включва мерките за по-добро прилагане, надзор и координиране на съответните правила на ЕС. Формулират се и методите за идентифициране на високорисковите държави извън ЕС, чиито слабости в техните регулаторни режими за борба с изпирането на пари представляват съществени заплахи за финансовата система на ЕС. Акцент е поставен върху една от безспорно най-актуалните и динамично развиващите се форми на предикатна дейност при прането на пари, а именно компютърните престъпленията.

Във връзка с тази общо-европейска правна рамка, през м.I.2020 г. Р.България обяви завършването на първата си Национална оценка на риска от изпиране на пари и финансиране на тероризъм, което доведе до постоянно действаща междуведомст-

вена работна група по см. на чл.96 от Закона за мерките за изпиране на пари и на формулиране на Доклад за национална оценка за 2019 г. с анализ на външните и вътрешни рискове от изпиране на пари и финансиране на тероризъм, пред които е изправена Р.България. Предвид необходимостта от комплексен професионален подход при изготвяне на тази национална оценка в цитирания екип са представени следните компетентни ведомства:

- Държавна агенция „Национална сигурност“, чрез специализираната административна дирекция „Финансово разузнаване“;
- Министерство на вътрешните работи;
- Прокуратурата на Р.България;
- Българска народна банка;
- Комисията по финансов надзор;
- Комисията за противодействие на корупцията и за отнемане на незаконно придобито имущество;
- Национална агенция по приходите;
- Агенция „Митници“;
- Агенция по вписванията;
- Министерство на правосъдието;
- Министерство на финансите.

Последвалата актуализация на Националната оценка на риска от изпиране на пари и финансиране на тероризъм през м.II.2023 г. откроява в един от секторните анализи компютърните престъпленията, като рисково събитие за изпиране на пари. В България бяха приети множество законодателни промени, които засилват контрола върху бизнеса и финансовите институции, както и наказанията за пране на пари от юридически лица.

Тук е мястото да се посочи, че законодателният подход на използваната лексикалност при формулиране на съставите на престъпленията по Глава VII от Наказателния кодекс от обективна страна, е последователен и намира своето логично нормативно развитие в специалните закони. При систематичното тълкуване на въведените термини бихме могли да намерим опора в чл.2 от Закона за мерките срещу изпирането на пари (изм., Д.В. бр.32 от 26.04.2022 г., в сила от 28.07.2022 г.), който въвежда легалното определение на понятието „изпиране на пари“. Според законодателя, налице е изпиране на пари, когато е извършено умишлено, и е осъществено чрез:

1. (изм. – ДВ, бр. 42 от 2019 г., в сила от 28.05.2019 г.) преобразуването или прехвърлянето на имущество, със знанието, че това имущество е придобито от престъпление или от акт на участие в престъпление, за да бъде укрит или прикрит незаконният произход на имуществото или за да се подпомогне лице, което участва в извършването на такова действие с цел да се избегнат правните последици от деянието на това лице;

2. (изм. – ДВ, бр. 42 от 2019 г., в сила от 28.05.2019 г.) укриването или прикриването на естеството, източника, местонахождението, разположението, движението, правата по отношение на или собствеността върху имущество, със знанието, че това имущество е придобито от престъпление или от акт на участие в престъпление;

3. (изм. – ДВ, бр. 42 от 2019 г., в сила от 28.05.2019 г.) придобиването, владението, държането или използването на имущество със знание към момента на получаването, че е придобито от престъпление или от акт на участие в престъпление;

4. участието в което и да е от действията по т. 1 – 3, сдружаването с цел извършване на такова действие, опитът за извършване на такова действие, както и подпомагането, подбуждането, улесняването или даването на съвети при извършването на такова действие или неговото прикриване.

Цитираната норма би могла да се разглежда в светлината на правна бланкетност, дотолкова доколкото Законът за мерките срещу изпирането на пари е специален по отношение на нормите, визирани в Глава VII от Наказателния кодекс „Престъпления против финансовата, данъчната и осигурителната системи“ и липсва конкретна дефиниция на понятието „пране на пари“ в Общата част на Наказателния кодекс. Налице е и по-голяма пълнота в изпълнителните деяния, което обективно се дължи на факта, че Законът за мерките срещу изпирането на пари е значително по-нов като редакция /с последно изменение от изм., бр.32 от 26.04.2022 г., в сила от 28.07.2022 г./ в сравнение с първоначалната криминализация на прането на пари в Наказателния кодекс /с последно изменение от изм., бр.75 от 2006 г./. Налице е не само препращане, но и нормативно синхронизиране на Закона за мерките срещу изпирането на пари с Директива (ЕС) 2015/849 за предотвратяване използването на финансовата система за целите на изпирането на пари и финансирането на тероризма, за изменение на Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета. В цитирания специален закон се държи сметка за това, че добрите примери в борбата с прането на пари включват единодействие на правоприлагащите органи, по отношение на работата с различни цифрови инструменти и технологии, за да подпомогнат ежедневната си работа за откриване и прекъсване на незаконни финансови потоци, за смекчаване на рисковете от престъпления – в частност в сферата на киберсигурноста и споделяне на информация в публичния сектор и с частния сектор по сигурен начин. Ето защо, освен мерките за превенция на използването на финансовата система за целите на изпирането на пари, са уточнени и задължените субекти по тях.

За разлика от наличното легално определение на понятието „изпиране на пари“, в българското законодателство липсва легално такова на понятието „киберпрестъпност“. Това налага, съобразно принципа на систематичния анализ, да се обърнем към Акта за киберпрестъпността на Съвета на Европа, според който това са „престъпления, в които компютърните системи или компютърните мрежи са обект на нарушение и които включват компютърни инструменти като средство, обект или място на престъпна дейност“.

Нещо повече, при преценката за степента на обществена опасност на този вид деяния, Европейският парламент в Резолюция от 3 октомври 2017 г. относно борбата с киберпрестъпността (2017/2068(INI)) (2018/C 346/04), се сочи че киберпрестъпността нанася все повече значителни социални и икономически щети, като засяга основните права на физическите лица, създава заплахи за принципите на правовата държава в киберпространството и застрашава стабилността на демократичните общества, като представлява нарастващ проблем в държавите членки на ЕС, а регистрираните случаи на киберпрестъпност в някои държави от ЕС надхвърлят случаите на традиционна престъпност и по обем тя обхваща и други области на престъпност. Тази оценка недвусмислено сочи на актуалността на този вид деяния, но и на нарастващия им интензитет, сложност, изключителна времева динамика и транснационалност.

Възходящият технологичен напредък през последните години позволява на множество субекти в публичната и частна дейност да съберат големи количества

структурирани и неструктурирани данни в най-разнообразен аспект, в това число такива касаещи лични данни, данни за финансови активи или пасиви и друга чувствителна информация, включително и такава, касаеща информационна система или компютърна мрежа, която е част от критичната инфраструктура на държавата. С последните изменения на Наказателния кодекс на Р.България (Д.В. бр.№53/ 08.07.2022 г.), законодателят въведе горното понятие в текста на чл.319г ал.IV от НК, като изтъкна високата степен на обществена опасност на това престъпление чрез структурирането му, като тежко умишлено престъпление в частта на предвиденото наказание лишаване от свобода в размер на от пет до дванадесет години.

Именно в цитираното по-горе изменение на Наказателния кодекс, се наблюдава устойчиво превантивната функция на закона, изразяваща се в законодателния подход на увеличаване на наказанията. В дадения случай това касае всички състави от Глава IXа от Наказателния кодекс „Компютърни престъпления“. Нещо повече, в последната им редакция, без изключение, тези състави придобиват характеристиката на тежки умишлени престъпления по смисъла на чл.93 т.7 от Наказателния кодекс. Това касае както формалните престъпления, така и тези, за които законодателят е предвидил настъпването на „тежки последици“ (чл.319а ал.V от Наказателния кодекс; чл.319б ал.II от Наказателния кодекс), „имотна облага“ (чл.319б ал.III от Наказателния кодекс), „значителни вреди“ (чл.319г ал.III от Наказателния кодекс) или извършени с „користна цел“ (чл.319д ал.III от Наказателния кодекс).

Независимо от непоследователния законодателен подход по използване на разнообразна лексикалност при формулиране на съставите на резултатните престъпления по Глава IXа от Наказателния кодекс от обективна страна, именно в тях следва основно да се дири и предикатността, като логична връзка с деянията по см. на чл.253 – чл.253б от Наказателния кодекс, нормативно уреждащи прането на пари. При систематичното тълкуване на въведените термини бихме могли да намерим опора и в & 3 от Допълнителните разпоредби на Закона за киберсигурността, който въвежда легалното определение на понятието „значително увреждащо въздействие“. В този случай, според законодателя, се вземат предвид следните показатели: а) брой ползватели, разчитащи на услугите, предоставяни от субекта; б) зависимост на други сектори – от посочените в приложение № 1, от услугата, предоставяна от субекта; в) въздействието, което инцидентите биха могли да имат от гледна точка на мащаб и продължителност върху стопанските и обществените дейности или върху обществената безопасност; г) пазарният дял на субекта; д) географският обхват на областта, която би била засегната от даден инцидент; е) значението на субекта за поддържането на достатъчно ниво на услугата, като се взема предвид наличието на други средства за предоставянето на тази услуга. Когато е целесъобразно, се вземат предвид и характерните за сектора показатели, за да се определи дали даден инцидент би имал значително увреждащо въздействие. Цитираната норма би могла да се разглежда в светлината на правна бланкетност, дотолкова доколкото Законът за киберсигурността е специален по отношение на нормите, визирани в Глава IXа от Наказателния кодекс „Компютърни престъпления“ и липсва конкретна дефиниция на тези квалифициращи деянията, обстоятелства.

Тук е мястото да се посочи, че в санкционната част на текстовете по Глава VII от Наказателния кодекс „Престъпления против финансовата, данъчната и осигурителната системи“, в която са и текстовете, регулиращи прането на пари, законодателят е предприел подобно отношение, обособявайки отделните изпълнителни деяния от състава на чл.253 от Наказателния кодекс отново като тежки умишлени та-

кива. Налице е следователно поредно акцентиране на възгледа на националния ни законодател върху приетата висока степен на обществена опасност и на това престъпление чрез структурирането му, като тежко умишлено престъпление в частта на предвиденото наказание лишаване от свобода.

В обобщение следва да се посочи, че осветляването на горепосочените нормативни проблеми, е основата за намиране на работещо решение за по-доброто разбиране на ефективни модели в борбата с компютърните престъпления и свързаната с тях потенциална възможност за пране на пари. При изключително добре развитият IT сектор в страната ни, е необходимо по-добро взаимодействие с цел намиране на решения за потенциален растеж на бизнеса, публичните институции и като цяло гражданското общество. Обединяването на данни и съвместните анализи могат да помогнат на институциите да разберат, оценят и намалят рисковете от пране на пари. Това ще направи идентифицирането на тези дейности по-лесно, динамично, ефективно и ефикасно. Резултатът ще бъде намаляване на броя на фалшиво положителните резултати и възможност частният сектор да се съобрази със законовите изисквания по-навреме и по по-малко натоварващ начин. Безусловен резултат ще е и предотвратяването от възползване на отделни субекти от пропуските в информацията, тъй като същите се свързват с множество местни и международни институции, всяка от които има ограничен и частичен поглед върху виртуалната информация, при съблюдаване на изискванията за необходима защита на личните и основните права на участващите страни.

Използвана литература:

1. Резолюция на Европейския парламент от 3 октомври 2017 г. относно борбата с киберпрестъпността (2017/2068(INI)) (2018/C 346/04)
2. Директива (ЕС) 2018/843 – петата директива на ЕС за борба с изпирането на пари, с която се изменя четвъртата директива относно борбата с изпирането на пари (Директива (ЕС) 2015/849).
3. Директива (ЕС) 2018/1673.
4. Национална оценка на риска от изпиране на пари и финансиране на тероризъм за 2020 г. https//dans.bg.
5. Закон за мерките срещу изпирането на пари (Обн., ДВ, бр. 27 от 27.03.2018 г., изм., бр. 94 от 13.11.2018 г., в сила от 1.10.2018 г., изм. и доп., бр. 17 от 26.02.2019 г., изм., бр. 34 от 23.04.2019 г., бр. 37 от 7.05.2019 г., изм. и доп., бр. 42 от 28.05.2019 г., в сила от 28.05.2019 г., бр. 94 от 29.11.2019 г., доп., бр. 18 от 28.02.2020 г., в сила от 28.02.2020 г., изм. и доп., бр. 69 от 4.08.2020 г., изм., бр. 7 от 26.01.2021 г., доп., бр. 17 от 26.02.2021 г., изм. и доп., бр. 21 от 12.03.2021 г., бр. 25 от 29.03.2022 г., в сила от 8.07.2022 г., изм., бр. 32 от 26.04.2022 г., в сила от 28.07.2022 г.);
6. Директива (ЕС) 2015/849 за предотвратяване използването на финансовата система за целите на изпирането на пари и финансирането на тероризма, за изменение на Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета;
7. Закон за киберсигурност (обн., ДВ, бр. 94 от 13.11.2018 г., изм., бр. 69 от 4.08.2020 г., изм. и доп., бр. 85 от 2.10.2020 г., в сила от 2.10.2020 г., бр. 15 от 22.02.2022 г., в сила от 22.02.2022 г., изм., бр. 25 от 29.03.2022 г., в сила от 29.03.2022 г.).

8. Наказателен кодекс на Р.България (обн., ДВ, бр. 26 от 2.04.1968 г., в сила от 1.05.1968 г., попр., бр. 29 от 12.04.1968 г., изм., бр. 92 от 28.11.1969 г., изм. и доп., бр. 26 от 30.03.1973 г., доп., бр. 27 от 3.04.1973 г., изм., бр. 89 от 15.11.1974 г., в сила от 1.03.1975 г., изм. и доп., бр. 95 от 12.12.1975 г., изм., бр. 3 от 11.01.1977 г., доп., бр. 54 от 11.07.1978 г., бр. 89 от 9.11.1979 г., изм. и доп., бр. 28 от 9.04.1982 г., в сила от 1.07.1982 г., попр., бр. 31 от 20.04.1982 г., доп., бр. 44 от 5.06.1984 г., изм. и доп., бр. 41 от 28.05.1985 г., доп., бр. 79 от 11.10.1985 г., попр., бр. 80 от 15.10.1985 г., изм. и доп., бр. 89 от 18.11.1986 г., попр., бр. 90 от 21.11.1986 г., изм., бр. 37 от 16.05.1989 г., в сила от 16.05.1989 г., бр. 91 от 24.11.1989 г., в сила от 24.11.1989 г., бр. 99 от 22.12.1989 г., в сила от 22.12.1989 г., доп., бр. 10 от 2.02.1990 г., изм., бр. 31 от 17.04.1990 г., изм. и доп., бр. 81 от 9.10.1990 г., в сила от 9.10.1990 г., бр. 1 от 4.01.1991 г., бр. 86 от 18.10.1991 г., попр., бр. 90 от 1.11.1991 г., изм., бр. 105 от 19.12.1991 г., доп., бр. 54 от 3.07.1992 г., в сила от 3.07.1992 г., изм. и доп., бр. 10 от 5.02.1993 г., бр. 50 от 1.06.1995 г.; Решение № 19 от 12.10.1995 г. на Конституционния съд на РБ – бр. 97 от 3.11.1995 г.; доп., бр. 102 от 21.11.1995 г., в сила от 21.01.1996 г., изм. и доп., бр. 107 от 17.12.1996 г., бр. 62 от 5.08.1997 г., изм., бр. 85 от 26.09.1997 г.; Решение № 19 от 21.11.1997 г. на Конституционния съд на РБ – бр. 120 от 16.12.1997 г.; доп., бр. 83 от 21.07.1998 г., изм. и доп., бр. 85 от 24.07.1998 г., доп., бр. 132 от 10.11.1998 г., в сила от 1.01.1999 г., изм., бр. 133 от 11.11.1998 г., изм. и доп., бр. 153 от 23.12.1998 г., бр. 7 от 26.01.1999 г., изм., бр. 51 от 4.06.1999 г., бр. 81 от 14.09.1999 г., в сила от 15.12.1999 г., изм. и доп., бр. 21 от 17.03.2000 г., бр. 51 от 23.06.2000 г.; Решение № 14 от 23.11.2000 г. на Конституционния съд на РБ – бр. 98 от 1.12.2000 г.; доп., бр. 41 от 24.04.2001 г., изм., бр. 101 от 23.11.2001 г., бр. 45 от 30.04.2002 г., изм. и доп., бр. 92 от 27.09.2002 г., бр. 26 от 30.03.2004 г., бр. 103 от 23.11.2004 г., в сила от 1.01.2005 г., бр. 24 от 22.03.2005 г., бр. 43 от 20.05.2005 г., в сила от 1.09.2005 г., изм., бр. 76 от 20.09.2005 г., в сила от 1.01.2007 г., изм. и доп., бр. 86 от 28.10.2005 г., в сила от 29.04.2006 г., бр. 88 от 4.11.2005 г., изм., бр. 59 от 21.07.2006 г., в сила от 1.01.2007 г., изм. и доп., бр. 75 от 12.09.2006 г., в сила от 13.10.2006 г., бр. 102 от 19.12.2006 г., бр. 38 от 11.05.2007 г., бр. 57 от 13.07.2007 г., в сила от 13.07.2007 г., изм., бр. 64 от 7.08.2007 г., доп., бр. 85 от 23.10.2007 г., в сила от 23.10.2007 г., изм., бр. 89 от 6.11.2007 г., доп., бр. 94 от 16.11.2007 г., изм. и доп., бр. 19 от 22.02.2008 г., изм., бр. 67 от 29.07.2008 г., бр. 102 от 28.11.2008 г., бр. 12 от 13.02.2009 г., в сила от 1.01.2010 г. (*) - изм., бр. 32 от 28.04.2009 г., доп., бр. 23 от 27.03.2009 г., в сила от 1.11.2009 г., изм. и доп., бр. 27 от 10.04.2009 г., доп., бр. 47 от 23.06.2009 г., в сила от 1.10.2009 г., изм., бр. 80 от 9.10.2009 г., бр. 93 от 24.11.2009 г., в сила от 25.12.2009 г., бр. 102 от 22.12.2009 г., в сила от 22.12.2009 г., изм. и доп., бр. 26 от 6.04.2010 г., доп., бр. 32 от 27.04.2010 г., в сила от 28.05.2010 г., изм. и доп., бр. 33 от 26.04.2011 г., в сила от 27.05.2011 г., бр. 60 от 5.08.2011 г., доп., бр. 19 от 6.03.2012 г., изм. и доп., бр. 20 от 9.03.2012 г., в сила от 10.06.2012 г., бр. 60 от 7.08.2012 г., в сила от 8.09.2012 г., изм., бр. 17 от 21.02.2013 г., доп., бр. 61 от 9.07.2013 г., изм. и доп., бр. 84 от 27.09.2013 г., бр. 19 от 5.03.2014 г., в сила от 5.03.2014 г., изм., бр. 53 от 27.06.2014 г., доп., бр. 107 от 24.12.2014 г., в сила от 1.01.2015 г., изм., бр. 14 от 20.02.2015 г., изм. и доп., бр. 24 от 31.03.2015 г., в сила от 31.03.2015 г., доп., бр. 41 от 5.06.2015 г., в сила от 6.07.2015 г., изм. и доп., бр. 74 от 26.09.2015 г., изм., бр. 79 от 13.10.2015 г., в сила от 1.11.2015 г., доп., бр. 102 от 29.12.2015 г.,

в сила от 1.01.2016 г., изм., бр. 32 от 22.04.2016 г., доп., бр. 47 от 21.06.2016 г.; Решение № 12 от 13.10.2016 г. на Конституционния съд на РБ - бр. 83 от 21.10.2016 г.; изм. и доп., бр. 95 от 29.11.2016 г., изм., бр. 13 от 7.02.2017 г., в сила от 7.02.2017 г., доп., бр. 54 от 5.07.2017 г., изм., бр. 85 от 24.10.2017 г., изм. и доп., бр. 101 от 19.12.2017 г., изм., бр. 55 от 3.07.2018 г., доп., бр. 1 от 3.01.2019 г., изм. и доп., бр. 7 от 22.01.2019 г., бр. 16 от 22.02.2019 г., бр. 83 от 22.10.2019 г., изм., бр. 13 от 14.02.2020 г., в сила от 14.02.2020 г., изм. и доп., бр. 23 от 14.03.2020 г., бр. 28 от 24.03.2020 г., в сила от 24.03.2020 г., доп., бр. 88 от 13.10.2020 г., изм. и доп., бр. 103 от 4.12.2020 г., доп., бр. 108 от 22.12.2020 г., изм., бр. 9 от 2.02.2021 г., в сила от 6.02.2021 г.; Решение № 12 от 30.09.2021 г. на Конституционния съд на РБ - бр. 84 от 8.10.2021 г.; изм. и доп., бр. 53 от 8.07.2022 г.; изм. с Решение № 13 от 27.09.2022 г. на Конституционния съд на РБ – бр. 79 от 4.10.2022 г.; Решение № 1 от 24.01.2023 г. на Конституционния съд на РБ – бр. 10 от 31.01.2023 г.);

9. Резолюция на Европейския парламент от 3 октомври 2017 г. относно борбата с киберпрестъпността (2017/2068(INI)) (2018/C 346/04);
10. Digital AML/CFT Strategy for Law Enforcement Paris, 8 June 2022 – report of FATF;
11. International standarts on combating money laundering and the financing of terrorism & proliferation – the FATF recommendation.