

ДИГИТАЛИЗАЦИЯТА И ПРЕСТЪПЛЕНИЯТА ПРОТИВ НЕПРИКОСНОВЕНОСТТА НА КОРЕСПОНДЕНЦИЯТА

*Гл. ас. д-р Мария Михайлова
Институт за държавата и правото
при Българска академия на науките*

DIGITALIZATION AND CRIMES AGAINST THE PROPERTY OF CORRESPONDENCE

*Chief Assist. Prof. Mariya Mihaylova, PhD
Institute for Legal Studies – Bulgarian Academy of Sciences*

Резюме: Засилените темпове на дигитализация на съвременното общество поставиха въпроса за съответствието на наказателноправната защита с особеностите на новите форми на общуване.

Ключови думи: *дигитализация, престъпления против неприкосновеността на кореспонденцията*

Abstract: The intensified pace of digitalization of modern society has raised the question of the conformity of criminal law protection to the peculiarities of the new forms of communication.

Key words: *digitalization, crimes against the property of correspondence*

Doi: <https://doi.org/10.36997/LBCS2021.393>

Въведение

Неприкосновеността на кореспонденцията е еманация на идеята за личната неприкосновеност. Усилените темпове на дигитализация на съвременното общество поставиха с особена острота въпроса за съответствието на най-висшата правна защита – наказателноправната, на особеностите на новите форми на общуване.

Изложение

Престъпленията против неприкосновеността на кореспонденцията се регламентирани в раздел V „Нарушаване на неприкосновеността на кореспонденцията” на Глава III от ОсЧ на НК. В самото на-

именование на раздела терминът „кореспонденция” е употребен като сборно понятие, макар отделните престъпни състави да третират определени конкретни форми на кореспонденцията.¹ Това налага да се изясни наказателноправното значение на това понятие. Най-общо кореспонденцията може да бъде определена като средство за обмен на информация между хора от разстояние. Тя представлява както самият носител на информация (писма, пощенски пратки, телефонни обаждания, телекс, телеграф, електронни съобщения или други), така и самото действие по обмена ѝ.

Кореспонденцията има четири основни белега: 1) съдържа информация/данни; 2) тази информация/данни са отразени на материален или електронен носител; 3) има две страни по кореспондентското отношение – изпращач/и и получател/и, които са конкретни и индивидуализирани; 4) обменът се осъществява по начин, възпрепятстващ достъпа на други лица, които не са страни по кореспондентското отношение, до съдържанието на разменяната информация.

Българският НК е криминализирал следните посегателства срещу неприкосновеността на кореспонденцията:

1) Наказание ЛОС до 1 година и глоба от 100 до 300 лева е предвидено за лице, което противозаконно (чл. 171, ал. 1 от НК):

¹ В чл. 38, ал. 1 от КРБ е провъзгласено, че свободата и тайната на кореспонденцията и на другите съобщения са неприкосновени, като начинът, по който е формулирана разпоредбата, показва, че кореспонденцията е вид съобщение. Съгласно § 1, т. 5 от ДР на ЗПУ кореспондентската пратка (писмо и/или пощенска карта) е пощенска пратка, която съдържа писмено съобщение върху какъвто и да е физически носител, което трябва да бъде пренесено и доставено на адреса, посочен от подателя върху пратката, с уточнението, че печатните произведения не са кореспондентски пратки. Тази дефиниция обслужва само изясняването на обхвата на понятието за пощенската пратка, но не дава точно определение за понятието „кореспонденция“. Същевременно в посочения нормативен акт неколккратно е закрепено задължението за опазване на тайната на кореспонденцията, а в компетентността на КРС е предвидено и издаването на Мерки за опазване на тайната на кореспонденцията. В чл. 5 от Мерките е предвидено, че тайната на кореспонденцията обхваща вида, съдържанието на пощенската пратка и всички данни, свързани с предоставяне на услугата, а в § 1, т. 1 от ДР се съдържа легална дефиниция на понятието „тайна на кореспонденцията“, определена като възможността съдържащите се в пощенските пратки информация и/или предмети да могат да останат известни само на подателя и на получателя до момента, в който поне един от тях реши друго. Същевременно в т. 2 е предвидено, че „нарушаване тайна на кореспонденцията“ е налице при нарушаване физическата цялост на пощенските пратки, извличане на информация и/или предмети и/или предаването им на трети лица.

- отвори, подправи, скрие или унищожи чуждо писмо, телеграма, запечатани книжа, пакет или други подобни;
- вземе чуждо, макар и отворено, писмо или телеграма с цел да узнае тяхното съдържание или пък със същата цел предаде другиму чуждо писмо или телеграма;
- узнае неадресирано до него съобщение, изпратено по електронен път, или отклони от адресата му такова съобщение.

2) Уреден е квалифициран състав с оглед на специалното качество на престъпния деец (чл. 171, ал. 2 от НК) – ако деянието е извършено от длъжностно лице, което се е възползвало от служебното си положение, наказанието е ЛОС до 2 години, като съдът може да постанови и лишаване от право по чл. 37, ал. 1 т. 6 от НК.

3) Който чрез използване на специални технически средства противозаконно осъществи достъп до или узнае неадресирано до него съобщение, предадено по телефон, телеграф, чрез компютърна мрежа или по друго далекосъобщително средство, се наказва с ЛОС до 2 години (чл. 171, ал. 3 от НК).

4) Наказанието по ал. 3 се налага и когато предмет на деянието са компютърни данни, изпращани в рамките на една или между повече информационни системи, включително електромагнитни емисии от информационна система (чл. 171, ал. 4 от НК).

5) Ако деянието по чл. 171, ал. 3 и ал. 4 от НК е извършено с користна цел или са причинени значителни вреди, наказанието е ЛОС до три години и глоба до пет хиляди лева (квалифициран състав).

6) Чл. 171а от НК криминализира противозаконното придобиване, съхраняване, разкриване или разпространение на данни, каквито се събират, обработват, съхраняват или използват съгласно ЗЕС. Предвиденото наказание е ЛОС до 3 години или пробация.

7) Квалифицираният състав на ал. 2 на чл. 171а от НК предвижда по-тежко наказание ЛОС от 1 година до 6 години, ако деянието по ал. 1 е извършено с користна цел.

Нормата на чл. 171, ал. 1, т. 3 от НК е нова – деянието е криминализирано през 2002 г. като естествен отговор на необходимостта от защита на развиващите се нови кореспондентски способности за обмен на информация, които не могат да се класифицират към уредените до този момент в наказателноправната норма писмени материални носители на информация в кореспондентското отношение. По отношение на писмените материални носители на информация защитата е изтег-

лена на по-преден етап – криминализирана е предхождащата узнаването на съобщението деятелност – отварянето на пратката, вземането на самия материален носител. При електронните съобщения обратно – криминализирано е самото узнаване на пренасяната в съобщението информация, а не отварянето на електронното съобщение или пък осъществяването на достъп до него. Що се отнася до електронното съобщение, вземане на съобщението като действие по установяване на фактическа власт върху него не е възможно предвид характеристиките му, което може да не е материализирано на конкретен носител, а да се намира и респективно съхранява в информационна система.

Предвид разновидностите на самите информационни системи би могло съобщението изобщо да не подлежи на отваряне. Например в една информационна система е възможно съобщенията да се изписват автоматично с пълния си текст на монитора на компютъра, без да е необходимо това съобщение да се отваря или да се извършват каквито и да било допълнителни технически операции, за да се достигне до съдържанието му. Ето защо разпоредбата на чл. 171, ал. 1, т. 3 от НК е подходяща да обхване всички възможни форми на неправомерно цяло узнаване на съдържанието на едно електронно съобщение.

По отношение на състава по т. 3 интерес представлява едно съдебно решение по конкретен казус.² През първата половина на 2012 г. у обвиняемия (*който бил кмет на община Твърдица*) възникнали съмнения в качеството и естеството на работа на някои от служителите му. За да потвърди или отхвърли съмненията си, той разпоредил устно на системния администратор да инсталира програма на компютрите на множество служители, чрез която искал да разбира какво вършат в работно време, т.е. дали се занимават с несвойствени за длъжностите им дейности. Системният администратор монтирал програмния продукт „Чайлд Дефендър“, изтеглен безплатно от интернет и предназначен за родителски контрол върху деца при достъпа им до компютри. Подсъдимият поискал системният администратор да му предостави достъп до информацията, която била налична в компютъра на пострадалата и администраторът предоставил исканата информация, която съставлявала разговори (разменени електронни съобщения) по програмата „Скайп“ между нея и нейни познати.

² Решение от 15.04.2015 г. на РС – Сливен по н.а.х.д. № 360/2015 г.

Обвиняемият прочел съдържанието на кореспонденцията. По делото е изготвена съдебно-техническа експертиза, от заключението на която е видно, че инсталираната програма „Чайлд Дефендър“ е за родителски контрол с интернет филтър, създадена за защита на децата във виртуалното пространство. Програмата създава възможност за запис на дейностите на детето (или на потребителя), като се проследяват посещаваните сайтове, запис на стартирани програми, както и създаване на снимки на работния плот на всеки 15 минути. Програмата може да бъде настроена така, че потребителят да не знае за съществуването ѝ, т. е. да е в режим „невидим“. От въпросния външен диск (*намерен в бюрото на подсъдимия*) са били свалени множество файлове, достъпни директно от компютъра му, записани от устройствата, ползвани от пострадалата. Технически не е възможно установяването на това в кой момент след записването на всяко съобщение от 04.07.2012 г. до 18.02.2014 г. обвиняемият е узнавал съдържанието му. Предвид на изложеното *de lege ferenda* следва да се предложи криминализирането наред с узнаването на неадресирано до дееца съобщение, изпратено по електронен път, също така и осъществяването на достъп или отварянето на такова съобщение.

Всички престъпления по чл. 171, ал. 1 от НК се преследват *по тъжба на пострадалия*, като законодателят е отчел спецификата на личните отношения.³ При сегашния интензитет на развитие на средствата за комуникация част от тези престъпления следва да се преследват по общия ред, тъй като информацията и свободното движение на информацията между лица, физически отдалечени едно от друго, се превръщат в основен движещ фактор както на икономиките на различните страни, така и на личните отношения. При условията на глобализация и превръщането на информацията в един от най-ценните ресурси наказателноправната защита трябва да е по-интензивна и целенасочена. Не на последно място в тази връзка следва да се отчете, че едно юридическо лице не би могло да бъде частен тъжител⁴, а всъщност именно то може да бъде жертва на подобно

³ Митов, Г. Срок за подаване на тъжба на пострадалия по наказателни дела от частен характер. // Научни четения в памет на Венелин Ганев и Никола Долапчиев, София: Св. Климент Охридски, ISBN 978-954-07-4260-1, с. 180.

⁴ Относно процесуалните възможности на едно юридическо лице за участие в наказателния процес виж по-подробно: Салкова, Ек. (2008). Фигурата на ошетеното юридическо лице в наказателното производство. // Правна мисъл, №4.

престъпление⁵ – напр. кореспонденцията е адресирана не към представляващия търговското дружество, а към самото дружество или пък е изпратена на електронен имейл на самото търговско дружество. В този случай съответното юридическо лице⁶ не би могло да предяви частна тъжба спрямо извършителя на престъплението, тъй като не би имало качеството на пострадало лице.

Интерес за това изложение представлява и квалифицираният състав по ал. 3 на чл. 171 от НК, като там квалифициращото обстоятелство е с оглед на средството, чрез което деецът е узнал неадресираното до него съобщение – чрез използване на специални технически средства. Първата форма на изпълнителното деяние е *противозаконното осъществяване на достъп до съобщение, предадено чрез далекосъобщително средство*. Тази форма на изпълнително деяние е въведена с промяната на НК, извършена със ЗИД на НК от 2017 г. Тя е продиктувана от изпълнението на ангажиментите на държавата ни по транспонирането на Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 г. относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета. Съгласно чл. 3 от нея държавите членки предприемат необходимите мерки, за да гарантират, че когато е извършен умишлено, неправомерният достъп до цялата информационна система или до части от нея е наказуем като престъпление, когато е извършен чрез нарушаване на мярка за сигурност, поне в случаите, които не се считат за маловажни. Важно тук е да се отбележи, че нормата има за цел да охрани самото съобщение, т.е. самата информация, която се предава чрез изрично изброените в нормата далекосъобщителни средства, но не и достъпът до информационната система, както повелява директивата. Защитата на самата информационна система чрез

⁵ По-подробно относно процесуалната правоспособност на частния тъжител – вж. Ройчев, Ян. (2017). Частното обвинение в българския наказателен процес. София: Сиела, ISBN 978-954-28-2453-4. Посочените проблеми във връзка с невъзможността самото оштетено юридическо лице да бъде частен тъжител от своя страна ясно извеждат проблема за необходимостта от преосмисляне на конструкцията за пострадалото лице по българското наказателно-процесуално право. В тази връзка Митов, Г. (2017). Наказателните дела от частен характер, София: Сиби, ISBN 978-619-226-045-3, с. 108 посочва, че „моралното удовлетворение” на физическите лица при осъждането на дееца при юридическото лице е заменено с имущественото обезщетение на причинените с деянието вреди, които се разглеждат в гражданския процес.“

⁶ Пак там.

запретяването под страх от наказание на противозаконния достъп до нея е дадена в следващата ал. 4, която също е създадена с измененията на НК през 2017 г.

Законодателят, при извършената промяна на специалната регулираща материя в областта на далекосъобщенията, не е извършил преоценка и на дадената ѝ с разпоредбата на чл. 171, ал. 3 от НК наказателноправна защита. Последното за пореден път показва, че наказателноправната регламентация не е изолирана, а трябва да се базира и да надгражда създадената с други нормативни актове регламентация на обществените отношения, да се развива заедно с нея и да бъде адекватна на измененията в нея. В противен случай наказателноправната норма не би могла да осъществи своето основно социално предназначение – да създаде най-високата степен на защита на обществено значимите ценности.

При действието на нормата на чл. 171 от НК до редакцията ѝ през 2002 г. предмет на наказателноправната защита е съдържанието на информацията, която се предава чрез технически средства, които по своята същност наистина са само далекосъобщителни – телефон, телеграф или други такива. През 2002 г. в обхвата на защитата е добавено и съобщението, което се предава чрез компютърна мрежа. Легалната дефиниция на понятието „компютърна мрежа” е дадена доста по-късно през 2007 г., като съгласно чл. 93, т. 25 от НК „компютърна мрежа” е съвкупност от свързани помежду си компютърни системи или съоръжения, която дава възможност за обмен на компютърни данни, т.е. касае се отново до средство за обмен на данни, в това число и информация, от разстояние посредством вид далекосъобщително средство. Съгласно настоящата редакция на понятието, дадена при изменението на НК от 2017 г., „компютърната мрежа” е съвкупност от свързани помежду си информационни системи или съоръжения, която дава възможност за обмен на компютърни данни, т.е. обхватът е разширен, като вместо за компютърни мрежи вече става въпрос за по-широкото понятие – информационни системи.

С изменението през 2017 г. обхватът на наказателноправната защита по чл. 171, ал. 3 от НК е значително разширен: от една страна се криминализира още едно изпълнително деяние – осъществяването на достъп до съобщение, а от друга страна се разширява обхватът на понятието „компютърна мрежа”, в което се включва не само компютърната система, но и всяка друга информационна система за обмен

на компютърни данни.

Чл. 171, ал. 4 от НК е нов състав, който е създаден също с цел синхронизиране на националното ни наказателно право с Директива 2013/40/ЕС. Престъплението е криминализирано в края на 2017 г. и предвижда същото наказание, както по ал. 3, т.е. ЛОС до 2 години, и когато предмет на деянието по ал. 3 са компютърни данни, изпращани в рамките на една или между повече информационни системи, включително електромагнитни емисии от информационна система.

С посоченото законодателно изменение в НК е дадена легална дефиниция на понятието „информационна система”, която е в унисон с въведеното с Директивата определение. Съгласно чл. 93, т. 21 от НК „информационна система” е всяко отделно устройство или съвкупност от взаимосвързани или сходни устройства, което в изпълнение на определена програма осигурява или един от елементите на което осигурява автоматична обработка на данни, както и компютърните данни, съхранявани, обработвани, извличани или предавани от такова устройство или група от устройства с цел оперирането с тези данни и използването, защитата и поддръжката им, а съгласно т. 22 „компютърни данни” е всяко представяне на факти, информация или понятия във форма, поддаваща се на обработка в информационни системи, включително програма, която е в състояние да направи така, че дадена информационна система да изпълни определена функция.

От посоченото понятие за информационна система могат да бъдат изведени следните нейни основни характеристики:

1) Устройство – информационната система всякога представлява едно техническо устройство, резултат на научно-техническия прогрес. Като една информационна система могат да се разглеждат и система от технически устройства, но за да имат характера на единна информационна система, те следва да бъдат взаимосвързани или пък да бъдат сходни.

2) Съоръженост с определена програма – за да бъде едно техническо устройство информационна система, то трябва да е съоръжено с определена програма.

3) Да извършва автоматична обработка на данни – тази програма трябва да притежава такива характеристики, че посредством нея устройството (в цялост или един елемент от него) да осигурява автоматична обработка на данни. Тя представлява система от операции, при които се регистрират, систематизират и анализират данните въз

основа на предварително зададени критерии, при което въпросните операции не се контролират и управляват от човешка дейност, а се извършват по предварително зададен компютърен алгоритъм.

4) Като част от информационната система се третират и компютърните данни, които са съхранявани, обработвани, извличани или предавани от такова устройство с цел оперирането с тези данни и използването, защитата и поддръжката им.

Въз основа на изведените белези може да се обобщи, че информационната система представлява съвкупността от хардуера (техническото устройство), софтуера (програмата, позволяваща автоматичната обработка на данни) и самите компютърни данни, налични в системата.

През 2010 г. законодателят криминализира в чл. 171а от НК противозаконното придобиване, съхраняване, разкритие или разпространение на данни, които се събират, обработват, съхраняват или използват съгласно ЗЕС.

При анализа на съставите на престъпленията по Раздел V от Глава III от ОсЧ на НК прави впечатление липсата на унификация на използваната терминология. Например не може ясно да бъде направено разграничението между престъплението узнаване на неадресирано до дееца *съобщение, изпратено по електронен път* (чл. 171, ал. 1, т. 3 от НК) и съставът на чл. 171, ал. 3 от НК – противозаконно узнаване чрез използването на специални технически средства на неадресирано до дееца *съобщение, предадено по телефон, телеграф, чрез компютърна мрежа или по друго далекосъобщително средство*. Съвсем основателно възниква въпросът за разликата между понятията „съобщение, изпратено по електронен път“, и „съобщение, изпратено чрез компютърна мрежа или друго далекосъобщително средство“. Законодателят не е провел ясно разграничение на тази плоскост. Действително чл. 93, т. 25 от НК дава легална дефиниция на понятието „компютърна мрежа“, т. 21 пък дефинира понятието „информационна система“, а т. 22 дефинира понятието „компютърни данни“. Същевременно НК няколко пъти в ОсЧ използва понятието съобщение, изпратено по електронен път, но в чл. 93 от НК не дава дефиниция на това понятие.

По отношение на наказателноправната защита на неприкосновеността на кореспонденцията е необходимо да бъде извършена ревизия на съществуващите състави, като ясно се разграничат отделните

престъпления както по отношение на типа на кореспонденцията и на съобщителното средство, чрез което се предава тя, така и по отношение на изпълнителните деяния, с които се нарушава тяхната неприкосновеност. Извършваните законодателни промени не са създали необходимата яснота при тълкуването на правните норми, включително относно тяхното систематично място, нито пък създават нужната степен на разграничение между отделните престъпления.

Развитието на наказателната политика на държавата по защита на неприкосновеността на кореспонденцията може да бъде проследено след анализ на измененията в Раздел V на Глава III от ОсЧ на НК. Той показва динамиката на наказателноправната защита на неприкосновеността на кореспонденцията, която следва и се опитва да навакса темповете на растеж в технологичното развитие и на дигитализацията. Ясно се открояват етапите, през които преминава наказателноправната политика за защита на неприкосновеността на кореспонденцията.

Първоначално предмет на наказателноправната защита са само писмените материални носители на информация – писма, телеграми, запечатани книжа, пакети и други подобни, като и информацията, предавана чрез тях, а от друга страна – предмет на защитата е информацията, предавана чрез далекосъобщителните средства – телефон, телекс и друго далекосъобщително средство.

С развитието на средствата за предаване на информация предмет на защитата при редакцията на НК през 2002 г. става и съобщението, предавано по електронен път (чл. 171, ал. 1, т. 3 от НК), както и съобщението, предадено чрез компютърна мрежа (чл. 171, ал. 3 от НК). През 2007 г. е предвиден квалифициран състав на престъплението по чл. 171, ал. 3 от НК – когато е извършено с користна цел или са причинени значителни вреди.

През 2010 г. наказателноправната защита отново се разширява с новосъздадения чл. 171а, ал. 1 от НК и вече са разпростира и върху трафичните данни по ЗЕС. А при редакцията на същата норма през 2015 г. обхватът отново се разширява и вече предметът на престъплението са всички данни – съобщението, трафичните данни, данните за изпращача и получателя и други данни съгласно ЗЕС. Криминализирано е и противозаконното съхранение на такива данни.

През 2017 г. обхватът на защитата отново е разширен, като е предвидено наказание и за противозаконното осъществяване на дос-

търп (а не само узнаването) на съобщение, предадено по телефон, телеграф, чрез компютърна мрежа или друго далекосъобщително средство. Разширява се и обхватът на понятието „компютърна“ мрежа, което включва не само компютърните, но и всички информационни системи за пренос на данни. А също така се криминализира и противозаконният достъп и узнаването на компютърни данни, изпращани в рамките на една или повече информационни системи.

Криминализацията на посегателствата срещу кореспонденцията се разпростира не само върху съобщението в съдържателен аспект и върху материалните му носители, но и върху всички други данни, разпространявани или налични при едно кореспондентско отношение, като това произтича от самия характер на кореспондентското отношение, който се променя. Това от своя страна предизвиква и необходимостта от разширяване на съставите на престъпленията и на техните изпълнителни деяния.

Както се посочва в Директива 2013/40/ЕС, информационните системи са ключов елемент от социалното и икономическото ни развитие и осигуряването на подходящи равнища на защитата им са от съществено значение за нормалното функциониране на обществата ни.⁷ Това извежда на преден план с още по-голяма острота необходимостта да се извърши цялостна ревизия на уредбата на престъпленията по Раздел V на Глава III от ОсЧ на НК, като се извърши тяхната преоценка, прецизиране и систематизация, каквато в момента липсва. Анализът на развитието на промените показва липсата на единна ясна политика на държавата за защита на това обществено благо, извършваните промени са спорадични, породени от необходимостта да се изпълни ангажимент на държавата по международното право или произтичащ от правото на ЕС. Липсва обаче единна концепция за това как трябва да се противодейства на нарушенията на неприкосновеността на кореспонденцията, които са с висока степен на обществена опасност. Липсва и ясно развита система на административно санкциониране на нарушенията на неприкосновеността на кореспонденцията с по-ниска степен на обществена опасност. Това поставя държавата и обществото ни пред сериозно предизвикателство относно намирането на правилната формула на съотношението между не-

⁷ Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 година относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета.

обходимостта от защита на личния и на публичния интерес. Поставя се и въпросът за необходимата мяра на наказателноправна защита на посегателствата по чл. 171, ал. 1 от НК, което престъпление се преследва по тѣжба на пострадалото лице, когато противоправното въздействие е насочено спрямо кореспонденцията на юридическо лице.

При използване на математическия модел за изчисляване на ОТНР е видно, че по отношение на престъпления против неприкосновеността на кореспонденцията ОТНР е по-ниска спрямо останалите престъпления по Глава III от ОсЧ на НК – ОТНР за престъпленията против неприкосновеността на кореспонденцията е 2,89 спрямо ОТНР за престъпленията против равенството – 6,58, и против политическите права на гражданите – 6,28. Този въпрос трябва да бъде обсъден в контекста на значимостта и актуалността на защитената обществена ценност в процеса на дигитализиращото се с много бързи темпове общество и в контекста на извършените значителни законодателни промени на наказателноправната уредба на тези престъпления през последните години.

Полицейската статистика показва изключително ниски нива на регистрирана престъпност против неприкосновеността на кореспонденцията в България (по 2 престъпни посегателства на година) и относително стабилен тренд. Увеличение се забелязва само през 2008 (4 регистрирани престъпления), 2011 (5) и 2012 г. (8), като същевременно тези пикове не могат да бъдат свързани с предприетите значителни промени в уредбата на престъпленията против неприкосновеността на кореспонденцията през 2010, 2015 и 2017 г., които са свързани с разширяване на обхвата на наказателноправната защита чрез криминализирането на нови престъпни състави и допълването на вече съществуващите. Тези законодателни промени не водят нито до ръст на регистрираната престъпност от този вид, нито до някакво раздвижване на съдебната практика.

От направения анализ може се изведе заключението за липсата на систематика в Раздел V и ясно разграничение между отделните престъпни състави, както и за липсата на цялостна визия на държавата за обхвата на предоставяната наказателноправна защита. Тези изводи, направени въз основа на анализа на историческото развитие на предоставяната наказателноправна защита и съпоставянето на действащата уредба по различните състави на престъпления против неприкосновеността на кореспонденцията, се подкрепят и от статис-

тическият анализ на динамиката на регистрираната престъпност, който не показва никакво повлияване на състоянието на този вид престъпност от промените в наказателноправната уредба.

Причините за ниския брой на регистрираните престъпления против неприкосновеността на кореспонденцията са свързани също така с някои особености на народопсихологията на нашето общество. Гражданите не винаги осмислят, че дадено поведение, с което се нарушава неприкосновеността на кореспонденцията им, е престъпно, т.е. неприкосновеността на кореспонденцията все още не е толкова чувствителна категория както другите основни права и свободи. Чувствителността на населението към този проблем започва да се увеличава в контекста на дигитализацията, като гражданите основно се насочват към използването на предоставяните от различните социални мрежи или оператори мерки за сигурност и ограничаване на достъпа на трети лица до тяхната кореспонденция, т.е. използват системни мерки, но рядко се обръщат към правораздавателните органи да търсят защита, в това число наказателноправна.

Емпиричните изследвания, проведени във връзка с настоящата разработка, показват засилване на чувствителността на гражданите към защита на тяхната кореспонденция. Темата буди интерес и предизвиква засилени дискусии сред малки групи от разнородни според социалния и възрастовия им статус респонденти. В хода на изследването обаче се установява липса на базови познания относно това основно човешко гражданско право, която е съпроводена и с липса на достатъчна информираност относно начините за преследване на извършителите на това престъпление.

Причините са основно стереотипите и предразсъдъците в малките населени места от типа „какво ще кажат хората?“, необходимостта от финансови средства за наемане на професионална защита за изготвянето на частната тъжба и за процесуалното представителство, ба-

вността на съдебната система⁸, тъй като провеждането на множество съдебни заседания създават съществени затруднения в ежеднезната организация на живота на хората.

От значение е и обстоятелството, че много често тези престъпления засягат юридическите лица, а същите не са правосубектни да подават тѣжби. От друга страна, когато става въпрос за бизнес, често огласяването на определен пробив в сигурността на кореспонденцията на търговеца би довело до значително по-големи вредни последици за него от самото извършено конкретно посегателство спрямо кореспонденцията му. Ето защо често реакциите на юридическите лица при посегателства против кореспонденцията им са свързани основно с предприемането на мерки за запазване в тайна на това обстоятелство и незабавни мерки за елиминиране на пропуска в сигурността на системите им, който е довел до нарушаването на неприкосновеността на кореспонденцията им. Това предполага запазването на дял за престъпленията против кореспонденцията в скритата престъпност.

Заклучение

Обстоятелството, че въпреки криминализирането на нови престъпления, които привеждат наказателноправната ни уредба в унисон с изискванията на общностното право, не се забелязва никаква динамика на регистрираната престъпност при наличието на емпирични данни за наличието на такава, води на извода за неуспех на наказателната политика на държавата по превенция на престъпленията против неприкосновеността на кореспонденцията. Държавата не следва да се дезинтересира от този вид престъпления, а да провежда целенасо-

⁸ Маринова, Г. (2016). Диференциация на наказателната процедура – традиции и перспективи. // Наказателно законодателство – традиции и перспективи, София: Климент Охридски, ISBN 978-954-07-4170-3, с. 379, посочва: „Нещата опират и до друг фундаментален проблем на наказателното право и на наказанието в частност – неговата неизбежност и бързината, с която се налага. Още през XVIII в. Чезаре Бекария стига до извода, че „онова, което преди всичко трябва да застрашава престъпниците, то не е жестокостта, но неизбежността на наказанието. (...) Увереността, че ще настъпи известно наказание, ако и да е то леко, винаги ще произведе много по-силно впечатление, отколкото страхът от едно много строго наказание, но което не изключва възможността за избягване на наказанието.“ Същият автор обръща специално внимание и на бързината, с която се налага наказанието, като подчертава, че „колкото е по-близко и колкото по-бързо се налага наказанието за едно извършено престъпление, толкова е то по-справедливо, толкова е по-полезно.“

чена превантивна политика за повишаване на разпознаваемостта им от гражданите и от правоприлагащите органи и създаване на нагласи за тяхното наказателноправно преследване.

Използвана литература

1. Маринова, Г. (2016). Диференциация на наказателната процедура – традиции и перспективи. Наказателно законодателство – традиции и перспективи, ISBN 978-954-07-4170-3.

(Marinova, G. (2016) Deferenciacia na nakazatelnata procedura – tradicii i perspektivi. Nakazatelno zakonodatelstvo - tradicii i perspektivi, ISBN 978-954-07-4170-3)

2. Митов, Г. (2017). Наказателните дела от частен характер. София: Сиби, ISBN 978-619-226-045-3.

(Mitov, G. (2017). Nakazatelnite dela ot chasten haracter. Sofiya: Sibi, ISBN 978-619-226-045-3)

3. Митов, Г. (2017). Срок за подаване на тѣжба на пострадалия по наказателни дела от частен характер. Научни четения в памет на Венелин Ганев и Никола Долапчиев, ISBN 978-954-07-4260-1.

(Mitov, G. (2017). Srok za podavane na tajba na postradalia po nakazatelni dela ot chasten hacter. Nauchi chetenia v pamet na Venelin Ganev I Nikola Dolapchiev, ISBN 978-954-07-4260-1)

4. Ройчев, Ян. (2017). Частното обвинение в българския наказателен процес. София: Сиела, ISBN 978-954-28-2453-4.

(Roychev, Yan. (2017). Chastното obvinenie v balgarskia nakazatelen kodeks. Sofiya: Siela, ISBN 978-954-28-2453-4)

5. Салкова, Ек. (2008). Фигурата на ошетеното юридическо лице в наказателното производство.// Правна мисъл, №4.

(Salkova, Ek. (2008). Figurata na oshtetenoto uridichesko lice v nakazatelnoto proizvodstvo. Pravna misal, № 4)

За контакти: гл. ас. д-р Мария Михайлова
ИДП при БАН
m.petrova_law@abv.bg