НАЦИОНАЛНА СИГУРНОСТ
NATIONAL SECURITY

ПРАВНА ЗАЩИТА НА ЛИЧНОТО ПРОСТРАНСТВО – ОСОБЕНОСТИ И ПРОБЛЕМИ

Ана Андонова
Районна прокуратура – Кюстендил

Александър Кирков
Университет по библиотекознание и информационни технологии

Резюме: *Живеем в дигитална ера, в която всяка споделена информация онлайн е допустимо да се разпространи до невиждани размери, дори и след като сме я изтрили от собствения си профил. Достатъчна ли е защитата на личното ни пространство? Какво представлява „лично пространство“, как се обработват личните данни и как се записват в регистри, ами ролята на Комисията за защита на личните данни в качеството ѝ на регулаторен орган?*

За нарушаване на личното пространство се носи наказателна и административно-наказателна отговорност, а самите нарушения се проявяват от разпространение на класифицирана информация, кражба на лични данни (т.нар. „фишинг“) до интернет изнудване в социалните медии.

Ключови думи: *лично пространство, интернет бисквитки, онлайн тормоз, обработка на лични данни, регистър на личните данни, нарушения и престъпления, юридическа закрила, Комисия за защита на личните данни в България*

ВЪВЕДЕНИЕ

Живеем в интернет общество, в което от изключителна важност е публичността. Публикуваме важни подробности от нашия личен живот във Фейсбук, разплащаме се онлайн, а често пъти пишем и лични данни – номер на банкова сметка или ЕГН. И сред цялата тази публичност защитата на личното пространство следва да е приоритет.

В настоящото изследване е направен опит за систематизиране на видовете нарушения на личното пространство, обособена е и правна рамка на национално и наднационално, международно равнище, изведен е ползваният понятиен апарат.

ЛИЧНО ПРОСТРАНСТВО И ИНТЕРНЕТ

Живеем в дигитална ера, в която всяка една споделена информация във Фейсбук, Туитър, Инстаграм е напълно възможно и допустимо да се разпространи до невиждани размери, дори и след като сме я изтрили от собствения си профил. Публичното оклеветяване

в някоя от социалните платформи е предпоставка за търсене на наказателна отговорност по дела от частен характер. Не са редки и случаите, в които споделени мнения по отношение на определено лице спрямо фирма – работодател, могат да доведат и до неговата последваща оставка. В социалните мрежи популярност придобиват т.нар. „затворени групи“ – има ограничения от модератори, като всеки пост преминава през корекция и проверка дали въпросната публикация не противоречи на правилата, предварително зададени в групата. За членовете на тези групи обикновено се изисква специална покана, а самите публикации не могат да бъдат разглеждани от хора извън групата. И все пак това достатъчна защита ли е на личното ни пространство, или не?

Чрез съгласяването с т.нар. „бисквитки“ за влизането във всеки един сайт ние предоставяме достъп до важна информация какво харесваме онлайн, какви интереси имаме, с какъв здравен статус сме. А в случай на появата на лични компрометиращи снимки, разпространявани до неограничен брой чужди потребители, как бихме могли да се защитим?

ЛИЧНО ПРОСТРАНСТВО И ЛИЧНИ ДАННИ

Под **„лично пространство“** следва да се разбира общочовешката възможност на всеки индивид да има собствени чувства и мисли, свобода на действията и свобода на изразяването. Личното информационно пространство е регламентираното право на физическото лице да има собствени тайни.

Икономическата и социалната интеграция и увеличаващите се търговски връзки водят до интензивно движение на трансгранични данни. Нараства комуникацията както между отделни физически лица, така и между физически лица и юридически лица в рамките на ЕС.[1] Защитата на отделните индивиди във връзка с обработването на лични данни е основноправо, признато от Хартата на основните права на ЕС.

Под **„лични данни“** следва да се разбира „всяка една информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде субект на данни“[2]. Тази идентификация се постига посредством име, ЕГН, ЛНЧ, данни за местонахождение, здравен статус, особености на „физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социалната идентичност“. Личните данни се съхраняват в различни операционни системи от лица, спазващи всички мерки за конфиденциалност, често пъти наличната информация е засекретена. Най-големите оператори на лични данни са различните държавни ведомства. Структурите на МВР събират, обработват и съхраняват лични данни във връзка с издаването на български документи за самоличност, като при издаването на международни паспорти се събират и биометрични данни. Националният осигурителен институт събира данни във връзка с периодичните годишни преброявания на населението. Също така големите куриерски фирми „Еконт“ и „Speedy“, с клонове в цялата страна, събират данни за адреси, а Български пощи – лични данни за получателите на пенсии. Всички лечебни заведения, предлагащи здравни услуги, хотели и места за настаняване също оперират с лични данни т.н. В частните фирми, в отдел „Човешки ресурси“ се съхраняват кадровите досиета на техните служители. На сайта на Комисията за защита на личните данни е публикуван списък на видовете операции по обработка на лични данни, за които се изисква извършване на оценка за въздействие върху защитата на данните съгласно чл. 35, параграф 4 от Регламент (ЕС) 2016/679.

Регистър с лични данни съгласно параграф 1, т. 8 от Закона за защита на личните данни означава: всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран, функционален или съобразно база от данни.

Как се обработват личните ни данни? Това е „всяка една операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или по друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване“. Във всеки един момент тези лични данни могат по един или друг начин да попаднат в онлайн пространството – злонамерено или по погрешка. Как можем да се защитим?

Видове нарушения и престъпления, свързани с нарушаване закрилата на личното пространство:

- Административни производства пред административен съд и Върховния административен съд по смисъла на Закона за защита на личните данни – издаване на професионална тайна или изтичане на секретна информация в интернет пространството. Типичен пример е всеизвестният казус с изтичането на данните от системата на Националната агенция по приходите на над 2 млн. българи в интернет.
- Изнудването по смисъла на чл. 214 от НК, включващо в своя състав елемента на принуда, съставлява психологическа заплаха и тормоз, при които определено лице се принуждава да извърши или да претърпи нещо против волята си, като в противен случай за него ще бъде разгласена опозоряваща лична информация в интернет медиите или компрометиращи снимки. При упражняване на принудата деецът сам решава кой от двата неприемливи за него крайни резултата да изтърпи – да извършинещо против волята си или да бъде публично опозорен.
- Кражба на лични данни (фишинг) – придобити отнапред чужди лични данни се ползват за извършване на финансови схеми и злоупотреби, като например теглене отбанкови сметки или придобиване на кредит от името на трето лице. Подобен вид компютърна измама най-често се осъществява чрез получаване на информация за номера на банкови карти и личните данни на самите картодържатели.

ПРАВНА ЗАЩИТА НА ЛИЧНОТО ПРОСТРАНСТВО – ЗАЩИТА НА НАЦИОНАЛНО И МЕЖДУНАРОДНО НИВО

Вече знаем, че едни от най-големите оператори на бази данни са държавните учреждения. Лицата, компетентни да събират и съхраняват лични данни, преминават през изпит, с който удостоверяват, че са запознати с правилата по смисъла на Закона за защита на класифицираната информация. Рискът при обработката на личните данни може да доведе до значителни материални и нематериални вреди.

Защитата на национално ниво е правно регламентирана в Закона за защита на личните данни.[3] Важно е да се отбележи, че от 25 май 2018 г. се прилага Регламент (ЕС) 2016/679 на Европейския парламент относно защитата на физическите лица във връзка с обработването на личните данни. Той се прилага във всички държави – членки на ЕС, и засяга и държави, които не са членки на ЕС, но обработват лични данни на лица, граждани на ЕС. Според този

регламент, приет и в Република България директно, без транспониране, личните данни на физическите лица могат да бъдат свързани с онлайн идентификатори, предоставени от техните устройства, приложения, инструменти и протоколи, IP адреси или бисквитки, като чрез ползването им се оставят следи върху сървърите на компютрите, съдържащи база данни за профилите на физическите лица и тяхното идентифициране. Администраторът (обработващият лични данни) следва да предприеме всички необходими технически и организационни мерки, за да защити данните от случайно или незаконно унищожаване или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване, като в някои случаи той се консултира с надзорния орган преди обработката на данните.

В международен план в Кодекса на ЕС за правата в онлайн среда изрично е записано, че физическите лица, предоставяйки своите данни, следва да бъдат уведомявани, в случай че „личните им данни, съхранявани от техния доставчик на интернет услуги, са били изложени на риск, например изгубени или откраднати, и е вероятно неприкосновеността наличния им живот да бъде повлияна отрицателно; да не им се изпращат нежелани търговски съобщения, известни като СПАМ, освен ако те са дали изричното си съгласие за това“[4].

Регламент (ЕС) 2016/679 на ЕС и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и свободното движение на такива данни потвърждава с по-голям интензитет въведеното по-рано „право да бъдеш забравен“, т.е. да бъдат изтрити личните данни на едно лице от дадена система, в случай че вече няма основание те да се съхраняват и при изрично желание от страна на лицето, собственик на личните данни. Също така гражданите имат правото да пренасят личните си данни от една фирма оператор на данни в друга, като така се изгражда доверие в информационната среда.

ПРОИЗВОДСТВО ПРЕД КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

При нарушаване на правата на всяко едно лице по смисъла на Регламент (ЕС) 2016/679 и ЗЗЛД субектът на данни (въпросното физическо лице, носител на данните) има право да сезира комисията в срок от шест месеца след узнаване на нарушението до най-късно две години от извършването му, като срокът е преклузивен и след изтичането му правото на засегнатото лице да търси юридическа закрила се губи. Самата жалба може да се подаде по електронен път по реда на Закона за електронния документ и електронните удостоверителни услуги. Възможно е да се подаде и от пълномощник. Не се разглеждат анонимни или неподписани жалби.

Комисията се произнася с решение, като може да приложи някоя от мерките, посочени в регламента, или да наложи административно наказание. Комисията може да откаже и да образува производство, като отказът ѝ се обжалва в 14-дневен срок по реда на Административно-процесуалния кодекс. При евентуално налагане на глоба или имуществена санкция същата следва да бъде ефективна, пропорционална и възпираща.[5] Обжалването на тези санкции е регулирано в Данъчно-осигурителния процесуален кодекс, а събраните суми влизат в държавния бюджет.

ВЪЗНИКВАЩИ ПРОБЛЕМИ ВЪВ ВРЪЗКА С ОПАЗВАНЕТО НА ЛИЧНОТО ПРОСТРАНСТВО

Напоследък във фейсбук пространството възникват още две възможности – да се публикува анонимно в някоя група или да се заключи личният фейсбук профил (втората възможност засега не се предлага на територията на Република България). Когато ние, като граждани и физически лица, подаваме заявление за сключване на договор с някой от мобилните оператори или изтегляме потребителски заем от банка, задължително ни снимат личната карта. Каква е вероятността данните от тази лична карта да попаднат в имотни измамници или недобросъвестни хора? С въвеждането на GDPR регламент постепенно започват да се попълват и декларации за съгласие за обработка на доброволно дадените лични данни. Но в крайна сметка тези данни доброволно ли са дадени или даването им е единствената възможност за сключване на договор с А1 например или получаване на банков кредит? Днес, повече от последните 20 години, се ползват електронни технологии за пренос на данни. Как можем да разчитаме, че записвайки номер на банковата си карта, пазарувайки от интернет сайт отвъд Тихия океан, от другата страна се намира реална фирма, предлагаща стока онлайн, а не интернет измамник, източващ пари от чужди карти.

Възможните решения са свързани с криптиране на информацията и комуникацията между потребители от край до край (Viber) или пък редуциране на идентифициращите данни, които предоставяме онлайн.

Неприкосновеността на личното пространство в дигиталния век, в който живеем, е предизвикателство за всеки онлайн потребител, а редица законови и подзаконови нормативни актове на национално и международно ниво гарантират, че личното пространство трябва да си остане само и единствено лично.

ЗАКЛЮЧЕНИЕ

„Теч на лични данни“ е едно от „модерните“ престъпления в интернет пространството, заедно с кражба на идентичност и фишинг измамите. Профилът на лицата, осъществяващи подобни противозаконни действия, кореспондира на млад човек, обикновено от мъжки пол, с добри компютърни познания. Често се цели и имуществена облага от кражбата на данни – например обещанието за непубликуване на клип с порнографско съдържание на заснетите участници срещу заплащане от тяхна страна. Самото публикуване на личните данни може да доведе и до сериозен психологически тормоз спрямо техния собственик. С оглед негативните изводи следва да се промени законодателната рамка с тенденция към увеличаване размера на наказанията на лица, злоупотребяващи с чужди лични данни, така България ще се превърне в модерна държава, чието законодателство е конкурентно на западноевропейското такова.

БЕЛЕЖКИ

[1]По-подробно вж. Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защита на данните).

[2]Сайт на фондация „LIBRe“ – интернет, адрес: libreresearchgroup.org/.

[3]ЗЗЛД – обн. ДВ, бр. 1/2022 г., изм. и доп. ДВ, бр.11/2023 г., в сила от 04.05.2023 г.

[4]Кодекс на ЕС за правата в онлайн среда.

[5]По-подробно вж. Регламент (ЕС) 2016/679.

LEGAL PROTECTION OF PERSONAL SPACE – FEATURES AND PROBLEMS

Abstract: *We live in a digital age where any information shared online is allowed to spread to unprecedented proportions, even after we have deleted it from our own profile. Is the protection of our personal space enough? What is 'personal space', how is personal data processed and recorded, and what is the role of the Data Protection Commission as a regulator?*
Violation of personal space carries criminal and administrative-penal liability, and the violations themselves manifest themselves from distribution of classified information, theft of personal data (the so-called "phishing") to Internet blackmail on social media.
Keywords: *Personal space, internet cookies, online harassment, processing of personal data, personal data register, violation and crime legal protection, Commission for protection of personal data*

Prosecutor Ana Andonova, PhD
Kyustendil district prosecutor office
E-mail: ana_vasileva@mail.bg

Assist. Prof. Aleksandar Kirkov, PhD
University of Library Studies and Information Technologies
E-mail: a.kirkov@unibit.bg