INFORMATION PROTECTION SYSTEM IN THE REPUBLIC OF BULGARIA - LEGAL ACTS AND INSTITUTIONS

VALENTINA S. HOROZOVA

ABSTRACT: *The article presents the modern system for information protection in the Republic of Bulgaria. The three types of legally defined information are presented. A review of the relevant legal acts in the study area has been made. Special attention is paid to the specifics of the modern security environment and the challenges it brings. Based on this, proposals have been made for guidelines for the development and improvement of the information protection system, the main direction being the prevention of unauthorized access.*

KEYWORDS: *classified information, personal data, public information, protection, system.*

DOI: https://doi.org/10.46687/MT22VSH

СИСТЕМА ЗА ЗАЩИТА НА ИНФОРМАЦИЯТА В РЕПУБЛИКА БЪЛГАРИЯ – ПРАВНИ АКТОВЕ И ИНСТИТУЦИИ

ВАЛЕНТИНА С. ХОРОЗОВА

АБСТРАКТ: *В статията е представена съвременната система за защита на информацията в Република България. Разгледани са трите вида правнодефинирана информация. Направен е преглед на релевантите правни актове в изследваната област. Специално внимание е отделено на спецификата на съвременната среда за сигурност и предизвикателствата, които тя носи със себе си. Въз основа на това са направени предложения за насоки на развитие и усъвършенстване на системата за защита на информацията, като основната насока е предотвратяване на неоторизиран достъп.*

1 Въведение

От дълбока древност информацията винаги е представлявала ценен ресурс. Особено тази, която е свързана с нашата мисия, визия, цел или интерес, който защитаваме. Това е такава информация, която може да предопредели изхода от битка на бойното поле, да наклони везните в оспорван дебат, да осигури предимство в конкуренцията, да гарантира преднина при преговори, да спаси човешки живот, да предотврати военен конфликт или да предизвика такъв и т.н. Нуждата от подобен род специфична и в същото време значима информация може да се приеме като предпоставка за зараждането и развитието на една от най-древните професии на всички времена – разузнаването. Всяка епоха се характеризира със свои специфични методи и средства на разузнавателната дейност. Всичко това постепенно извежда на преден план необходимостта от изграждане на адекватна за времето си система за защита на същата тази информация. Актуалността на темата рязко се повиши след избухване на конфликта в Украйна. Свидетели сме на безпрецедентна хибридна война, масова дезинформация и кражба на информация. Особена роля и място в целия процес заемат Интернет и социалните мрежи. Всичко това за пореден път доказва и извежда на преден план значението на защитата на информацията както в корпоративен, така и в национален аспект. [1, 2, 3]

Съвременната система за защита на информацията в Република България е създадена

нормативно в началото на 2000 година**.** Процесът е свързан с присъединяването на Република България към НАТО и ЕС.[1]

Като условие за бъдещето членство е стояла необходимостта от регламентиране на:

- основните видове правно дефинирана информация в Република България;
- начина на обмена на специфичните видове правно дефинирана информация със страните - членки на НАТО и ЕС;
- начина на защита на видовете правно дефинирана информация в Република България;
- начина за получаване на достъп до видовете правно дефинирана информация;
- конкретните и специфични методи и средства за защита на различните видове правно дефинирана информация;
- административните и наказателни отговорности при неспазване на нормативните разпоредби;
- институциите и служителите, които ще отговарят за спазване на вече споменатите изисквания;
- специфичните задължение на служителите, които при изпълнение на служебните си задължения ще работят с някои или с всички от посочените видове информация в Република България и други. [4, 5, 7]

Без съмнение, регламентацията на защитата на информацията заема ключово място в цялостния процес по управление и гарантиране на сигурността в национален и в международен план. Информационната революция(известна още като Трета индустриална революция) предизвика безпрецедентни промени в сферата на информацията, а оттам се ражда и необходимостта от създаване на адекватни механизми и контроли за защита на стратегическата и важна информация. В отговор, както в ЕС и НАТО, така и в България се приемат редица документи и нормативни актове в сферата на защита на информацията. Сред тях са:

Закон за защита на класифицираната информация, приет през 2002 година, (последно изменение ДВ. бр.80 от 24 Септември 2021г.). С него се въвежда термина класифицирана информация (КИ). Разграничават се основните видове КИ - държавна, служебна тайна и чуждестранна класифицирана информация. ЗЗКИ налага обща политика, общи правила, стандарти, процедура и защита при работата с трите вида КИ. По този начин се полагат основите на съвременната система за защита на класифицирана информация в Република България. Дефинират се още и:

- основните правила, свързани с класифицирането;
- условията за получаване на право на достъп;
- условията за работата с КИ;
- особеностите при нейната защита;
- особености при транспортирането на КИ;
- специфика при обучението за работа и защита на КИ;
- определяне на административната и наказателна отговорност;
- условия за унищожаване на КИ и т.н

Изпълнението на посочените правила е подчинено на единствената цел на закона – защита на КИ от нерегламентиран достъп и на стриктното спазване на принципа

[1] Някои основни предизвикателства към този момент са очертани от Иванов, Владко.България в съвременните съюзи на Европа, С., 2011 г., Академия на МВР, стр. 280-291.,ISBN 978-954-348-065-4

необходимост да се знае. Това са основните корективи, които насочват служителите как да работят и защитават КИ при изпълнението на служебните си задължения и/или при конкретното възложена задача. [16, 17]

Защитата на класифицираната информация е съществен елемент от националната сигурност. Неслучайно и първото легално определение за национална сигурност в Република България е въведено с приемането на ЗЗКИ.

Закон за защита на личните данни, приет през 2002 година (последно изменение *ДВ. бр. 93 от 26 Ноември 2019 г.).* Този закон поставя основите на подробно регламентиране на обществените отношения в областта на обработката и защитата на личната информация на гражданите. С него се определят правилата за защита на личните данни. Оформен е кръгът от данни, които са дефинирани като лични, от което следва, че същите ще подлежат на специална защита. На следващо място са предвидени мерките, които трябва да се спазват при тяхната обработка, съхранение и унищожаване. Целта на Закона за защита на личните данни е да се гарантират основните човешки права на неприкосновеност на личността и личния живот посредством защитата на физическите лица при неправомерно обработване на свързаните с тях лични данни. Правото на лична неприкосновеност е прогласено сред списъка на основните човешки права още в Международния пакт за граждански и политически права (1966, чл. 17), както и в Европейската конвенция за защита на правата на човека и основните свободи (1951, чл. 8), по които България е страна. Това право намира още защита и в Хартата на основните права в Европейския съюз. [11, 12, 15]

Защитата на личните данни е задача с изключителен приоритет. Нейната сложност произтича не само от демократичните изисквания към всяко съвременно общество, към изискванията за демократично управление от страна на държавата, но и от наличието на вече разгърнато национално и европейско законодателство, от практическата необходимост на хора, организации, общество, медии и държава ежеминутно да обработват, съхраняват, използват и предоставят ЛД на лица. [8, 9, 10]

Обхватът на правото на неприкосновеност на личността в контекста на защитата на личните данни включва няколко подкатегории:

– физическа неприкосновеност – защитата на личността във физически план срещу вмешателски процедури от рода на тестове за медикаменти, експерименти и др.;

– неприкосновеност на комуникацията – сигурност и неприкосновеност на пощата, телефоните[2], включително електронната поща и другите форми на комуникация;

– неприкосновеност на личната територия – поставянето на ограничения за нахлуване в домашна и друга среда;

– неприкосновеност на личната информация – определянето на правила, управляващи събирането и предоставянето на лични данни, като кредитна информация, медицински експертизи и др.[3]

Бихме могли да отбележим четири различни модела за защита на личните данни:

- изчерпателно законодателство;
- секторно законодателство;
- саморегулация и

[2] Савов, И., Възможности за определяне на местоположението на човек по номера на мобилното устройство, Годишник на Шуменския университет „Епископ Константин Преславски“ Университетско издателство „Епископ Константин Преславски“, ISSN 1311-834X, Шумен, 2020 г., стр.247-257 стр.

[3] Великов, И., Политиката по защита на личните данни в контекста на присъединяването на Република България към Шенген, Фондация НМС, Научни трудове том Първи, 2012 г., ISSN 1314-9105, стр.143-164

- технологични защити.

В зависимост от тяхното приложение, тези модели биха могли да се допълват или да си противоречат, като в много страни няколко от тях се използват заедно. В държавите, които гарантират най-добре правото на защита на личните данни, всички тези модели работят едновременно и се допълват.[4]

Закон за достъп до обществена информация, приет през 2000 година (последно изменение ДВ. бр.15 от 22 Февруари 2022г). В закона са дефинирани видовете обществена информация, законовите процедури за достъп до нея и случаите, при които достъпа може да бъде отказан. Уреден е и въпроса свързан с правото на достъп до обществена информация, както и с повторното й използване от обществения сектор.

Този закон има ключово значение по отношение на възможността и правото на гражданите на Република България да бъдат информирани своевременно от органите за всяка информация, събрана или станала им известна при осъществяване на тяхната дейност, чрез която може да се предотврати заплаха за живота, здравето и безопасността им, както и на тяхното имущество. [5]

Следваща важна част от закона е насочена към насърчаване и толериране на прозрачността относно дейността на администрацията. [20, 23]

Общ Регламент за защита на личните данни, приет през 2016 година. Европейският регламент надгражда и актуализира вече съществуващата нормативна база в областта на защитата на личните данни. Целта му е да въведе единен подход за защита на личните данни в Европейския съюз и на европейските граждани по целия свят.

Тези нормативни актове фактически са основата на правната регламентация на дефинираните видове информация в Република България - класифицирана информация, лични данни и обществена информация. Те служат за отправна точка при събирането, обработването, пренасянето, съхранението и унищожението на вече споменатите видове информация.

Последиците от приемането на гореспоменатите стратегически документи и нормативни актове в областта на защитата на информацията практически водят до поредица от институционални реформи. Това доведе до създаване на:

- Държавна комисия по сигурност на информацията, създадена през 2002 година.
- Комисия за защита на личните данни, създадена с решение на Народното събрание от 23 май 2002 година. [21, 22]

Успоредно с това, съвременният динамичен свят създаде нови форми на комуникация, социално-технологични проблеми и заплахи. Навлизането на интернет технологиите във всички сфери на обществения живот предизвикват достигането на огромен поток информация от всички точки на света до всички потребители на глобалната мрежа. Грета Дерменджиева[6] отбелязва, че новоформираното глобално информационно общество се отличава с т.нар. дигитализация на информацията, чрез която става възможно и пренасяне на сложни съчетания на различни видове данни - текст, звук, статични и динамични изображения (мултимедия). На следващо място се забелязва експоненциално нарастване на данни и тяхното разпространение; достъп до информация във всяка точка от света; безжични услуги с глобално покритие; интелигентни мрежи с интерактивни услуги;

[4] Великов, И., Киряков, З., Основи на защитата на информацията, EHSEM Publishing (Издателство ЕВУИМ), Пловдив, 2016 г., стр. 162 и следващи, ISBN 978-954-2959-26-7

[5] Закон за достъп до обществената информация

[6] Дерменджиева, Г. Увод в компютърно-опосредстваната комуникация. Университетско издателство „Св. Климент Охридски“, София, 2001 г

информационни услуги като нови форми на дейност.[7] Традиционните средства за масова информация отстъпиха място на социалните мрежи, които не само станаха източник на информация, но и източник на директно споделяне и направляване на общественото мнение. Т.е. гражданите от потребители на информация се превърнаха в създатели на информация и субекти на социално-политическо въздействие. Логична последица от всички тези промени са сериозни социални изменения и ефекти и то в глобален аспект. Скот Лаш отстоява тезата, че съвременната социална класа и социалното неравенство вече зависят от достъпа до информация, а не от начина на производство.[8]

Всички тези революционни изменения създадоха предпоставки за формирането на нови рискове и заплахи, свързани със защитата на лични данни и лична информация на всеки потребител на интернет и социалните медии и мрежи. Това от своя страна води до необходимостта от нови форми на защита, нова правна регламентация и нови правила за работя с лични данни и лична информация. [18, 19]

Глобалните проблеми се прехвърлиха и при нас. Системата за защита на информацията в Република България е изправена пред сериозно предизвикателство - гарантиране на защитата на информацията от неоторизиран достъп. Един от проблемите е дисбалансът в сферата на сигурността както в национален, така и в международен план. Засилват се асиметричните рискове, които се превръщат в иманентна характеристика на съвременната среда за сигурност, която се отличава с:

- нова и постоянно променяща се роля и ценност на информацията;
- фалшиви новини;
- дезинформация;
- манипулация на обществено мнение;
- наслагване и/или провокиране на определена нагласа, а оттам и поведение;
- разпространение на пропагандна информация и/или клипове с подривна цел;
- увеличаване на фалшивите профили – в резултат създаване на цели общества от фалшиви (кухи) профили;
- променена роля и значение на социалните мрежи - от средство за комуникация до глобализационен фактор върху сигурността;
- промяна в характера на социалните взаимодействия;
- ескалиране на опитите за придобиване на информация;
- дестабилизация на информационните системи с всички възможни методи;
- хибридни атаки и войни;
- киберрискове и заплахи;
- киберпрестъпност;
- епоха на кибервойни и други.

Всяка от посочените характеристики на средата за сигурност създава предпоставки за оформяне на облика на невидимия заплаха. Този, който се крие зад фалшива самоличност, зад фалшиви общности, зад възможността за отдалечен достъп и анонимно споделяне и разпространение на информация и/или дезинформация, зад възможността за анонимно провокиране и ескалиране на дестабилизиращи процеси във виртуалното пространство, които много лесно от чисто виртуални могат да прераснат в реални сблъсъци, протести, конфликти и т.н. Всичко това създава предпоставки за оформяне на непознати предизвикателства пред защитата на информацията и пред възможността да се отсее вярната от лъжливата такава. [24, 25]

[7] Дерменджиева, Г. Цит. съч.
[8] Лаш, С. Критика на информацията. София, ИК „Кота“, 2004 г

Препоръчително е да се изясни вида и обхвата на информацията, която може да бъде защитавана, макар и временно и при необходимите гаранции. От самото естество на ограничаването на правото на информация като изключение от един принцип, се извежда правилото, че това ограничение може да се налага само с акт, който се основава на преценка на конкретните факти за всеки отделен случай.[9]

2 Заключение

Съгласно Конституцията, Решение № 7/1996г. на Конституционния съд и международните договори за правата на човека, свободата на всеки да търси, получава и разпространява информация е в **основата на демократичния процес.** Тази свобода може да бъде ограничавана само в точно определени случаи при съответните гаранции. На дневен ред пред институциите стои въпроса за актуализация на професионалната квалификация и развиване на професионалните знания, умения и компетенции в областта на защитата на информацията в съответствие с настъпилите промени в европейското и национално законодателство и новите рискове и заплахи, които водят със себе си Интернет и социалните мрежи и медии. Войната в Украйна е приоритет – Европа ще тряба да свиква с предизвикателсвата на изтока. [6, 13, 14]

ЛИТЕРАТУРА:

[1] Международния пакт за граждански и политически права, обн. бр. 43 от 28.05.1976 г.

[2] Европейската конвенция за защита на правата на човека и основните свободи, Рим, 04.09. 1950 г.

[3] Хартата на основните права в Европейския съюз

[4] Общ Регламент за защита на личните данни, приет през 2016 година.

[5] Конституция на Република България, последно изм. и доп. ДВ. бр.100 от 18 Декември 2015г.

[6] Решение № 7/1996г. на Конституционния съд

[7] Закон за защита на класифицираната информация, приет през 2002 година, последно изменение ДВ. бр.80 от 24 Септември 2021 г.

[8] Закон за защита на личните данни, приет през 2002 година, последно изменение ДВ. бр.93 от 26 Ноември 2019 г.

[9] Закон за достъп до обществена информация, приет през 2000 година, последно изменение ДВ. бр.15 от 22 Февруари 2022 г.

[10] Закон за достъп до обществена информация, приет през 2000 година, последно изменение ДВ. бр.15 от 22 Февруари 2022 г

[11] Великов, И., Киряков, З., Основи на защитата на информацията, EHSEM Publishing (Издателство ЕВУИМ), Пловдив, 2016 г., стр. 162 и следващи, ISBN 978-954-2959-26-7

[12] https://www.aip-bg.org/documents/zzki_predlozenia_AIP.htm - посетен на 28.06.2022 г

[13] Великов, И., Политиката по защита на личните данни в контекста на присъединяването на Република България към Шенген, Фондация НМС, Научни трудове том Първи, 2012 г., ISSN 1314-9105, стр.143-164

[14] Дерменджиева, Г. Увод в компютърно-опосредстваната комуникация. Университетско издателство „Св. Климент Охридски“, София, 2001 г

[9] https://www.aip-bg.org/documents/zzki_predlozenia_AIP.htm - посетен на 28.06.2022 г

[15] Иванов, Владко. България в съвременните съюзи на Европа, С., 2011 г., Академия на МВР, стр. 280-291.,ISBN 978-954-348-065-4

[16] Лаш, С. Критика на информацията. София, ИК „Кота“, 2004 г

[17] Савов, И., Възможности за определяне на местоположението на човек по номера на мобилното устройство, Годишник на Шуменския университет „Епископ Константин Преславски“ Университетско издателство „Епископ Константин Преславски“, ISSN 1311-834X, Шумен, 2020 г., стр.247-257 стр.

[18] Методиева, Ц. Парашкеванова, Г., Махмуд, А. "Заплахи в интернет. Фишинг и финансово муле.", международна научна конференция „Киберсигурността в информационното общество“, НВУ „Васил Левски“ факултет „Артилерия, ПВО и КИС“ - гр. Шумен, 20-21 Април 2017г., ISBN 978-954-9681-82-6, с. 157- 160

[19] Николова, М., Стоянова, Т., Железов, С., Янакиева, В., Изграждане на виртуален модел на защитена инфраструктура. MATTEX 2020, Сборник научни трудове, том 1, Университетско издателство „Епископ Константин Преславски“, 2020, стр. 87 - 103, ISSN: 1314-3921

[20] Христов, Х., Характеристика на съвременните видове шпионски информационни програми. Политика и сигурност, Год. III, бр.1, 2019г. Издателски комплекс ВУСИ – Пловдив, 2019, ISSN 2535- 0358, с. 30-37

[21] Митевска-Енчева, М, Христов. Х, Боянов, П. Доклад на тема: „ Характеристика на сканиращите мрежови кибератаки“. В: Сборник трудове на XV национална научна конференция с международно участие „Обществото на знанието и хуманизмът на XX1 век”, Панел „ИНФОРМАЦИОННО ОБЩЕСТВО И СИГУРНОСТ“ Университет по библиотекознание и информационни технологии, София, 2017; ISSN 1314-7099, Издателство "ЗА БУКВИТЕ – О ПИСМЕНЕХЬ".

[22] Митевска-Енчева, М, Христов. Х, Боянов, П. Доклад на тема: „Характеристика на кибератаката за получаване на информационни отпечатъци и прилагане на разузнавателни техники“. В: Сборник трудове на XV национална научна конференция с международно участие „Обществото на знанието и хуманизмът на XX1 век”, Панел „ИНФОРМАЦИОННО ОБЩЕСТВО И СИГУРНОСТ“ Университет по библиотекознание и информационни технологии, София, 2017; ISSN 1314-7099, Издателство "ЗА БУКВИТЕ – О ПИСМЕНЕХЬ".

[23] Христов, Х., Организация и управление на оперативното противодействие на нерегламентиран достъп до чувствителна информация в социалната организация, Сборник научни трудове от научна конференция „Защита на информацията –състояние и перспективи”, проведена в НВУ „В. Левски” – Факултет „Артилерия, ПВО и КИС” на 07-08.06.2012 г., ISBN 978-954-9681-49-9

[24] Boyanov, P., Hristov, H., Security and vulnerability of the modern information systems in the government agencies, private organizations and academic institutions, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 42, February 2018

[25] Boyanov, P., Stoyanov St., Hristov, Hr., Fetfov, O., Trifonov, T., Routing information security in the local area network of academic departments using an enhanced distance vector routing protocol - EIGRP, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 11, 2017