УДК 004

Н.З. Арабаджийский
рук. секции «Публичной администрации»
в Департаменте «Администрация и управление»,
Новый болгарский университет,
доктор экономики, профессор
(г. София, Республика Болгария)

Prof. Nikolay Arabadzhiyski, Ph.D. in Economics
Head of the Public Administration section of the
Department of Administration and Management of
New Bulgarian University, Republic of Bulgaria

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ КЛАССИФИЦИРОВАННОЙ ИНФОРМАЦИИ И ЛИЧНЫХ ДАННЫХ В РЕСПУБЛИКЕ БОЛГАРИЯ

ORGANIZATIONAL LEGAL ASPECTS FOR THE PROTECTION OF CLASSIFIED INFORMATION AND PERSONAL DATA IN THE REPUBLIC OF BULGARIA

Аннотация. Целью разработки является представление организационно-правовых аспектов создания и функционирования систем защиты классифицированной информации (информации, представляющей государственную или служебную тайну, а также иностранной секретной информации) и личных данных физических лиц в Республике Болгарии в период с 2002 по 2018 г. На основе анализа нормативных актов национальнооого законодательства, директив и регламентов Европейского союза предпринимается попытка защитить основной тезис о том, что системы, включая поддерживающие их государственные органы и администрацию, постоянно совершенствуются, являются надежными и эффективно защищают секретную информацию и права отдельных лиц при обработке их персональных данных.

Ключевые слова: секретная информация, персональные данные, защита, государственные органы, администрация

Annotation. The aim of the thesis is to present the organizational and legal aspects of the establishment and functioning of the systems for protection of classified information (information representing state or official secret as well as foreign classified information) and personal data of individuals in the

Republic of Bulgaria, in the period from 2002 to 2018. Following analyzes of normative acts in the national legislation, directives and regulations of the European Union, it is attempted to protect the basic thesis that ystem, including state bodies and governments who assist them permanently improve, and reliable are effectively protect classified information and the rights of individuals in the processing of their personal data.

Keywords: classified information, personal data, protection, state authorities, administration

1. Организационно-правовые аспекты защиты классифицированной информации

В 2002 году в Республике Болгарии принят *Закон о защите классифицированной информации /ЗЗКИ/*.[1] *Закон* упорядочивает общественные отношения, связанные с созданием, обработкой и хранением *классифицированной информации*, а также и условия и порядок предоставления доступа к ней. *Закон* применяется и в отношении иностранной классифицированной информации, предоставляемой другим государством или международной организацией, если вступивший в силу международный договор, по которому Республика Болгария является стороной, не предусматривает иное. Цель *закон - защита классифицированной информации* от нерегламентированного доступа посредством ее сохранения и предохранения.

В законодательном аспекте понятие «*классифицированная информация*» - это «*информация, представляющая собой государственную или служебную тайну, а также и иностранная классифицированная информация*». В этом смысле законодатель воспринимает не каждую систематически выложенную в отдельных разрядах и классах информацию, а только ту, представляющую собой «*государственную тайна»* или «*служебную тайна».* Это налагает дополнительное определение законодателем этих двух понятий.

В *ЗЗКИ* установлено, что «*государственная тайна - это информация, определенная в перечне по Приложению №1 к закону, нерегламентированный доступ к которой создал бы опасность или ущемил бы интересы Республики Болгарии, связанные с национальной безопасностью, обороной, внешней политикой или защитой конституционно установленного порядка*». Перечень по Приложению №1 к *ЗЗКИ* категорий информации, подлежащих классификации, *а также и государственная тайна*, устанавливает *три категории информации*: 1) информация, связанная с обороной страны; 2) информация, связанная с внешней политикой и внутренней безопасностью страны, и 3) информация, связанная с экономической безопасностью страны.

В законодательном аспекте понятие «*служебная тайна»* определено как «*информация, связанная или хранимая государственными органами или органами местного самоуправления, которая не является государственной тайной, нерегламентированный доступ к которой сказался бы неблагоприятно на интересы государства или ущемил бы другой правозащитный интерес*». Информация, подлежащая *классификации, как «служебная тайна»*, определяется *законом.* Руководители соответствующих организационных единиц в рамках *закона* объявляют *Перечень категорий информации, подлежащей классификации, как служебная тайна* относительно сферы деятельности организационной единицы. Порядок и способ объявления Перечня определяются в *Правилах применения ЗЗКИ.*[2]

Уровни классификации о безопасности информации и их гриф безопасности следующие: «*строго секретно»* - хранится 30 лет; «*секретно»* - хранится 15 лет; «*доверительно»* - хранится 5 лет и *на «служебное пользование»* - хранится 6 месяцев. В целях обеспечения дополнительной защиты, когда это необходимо из-за характера информации или когда это предусмотрено в международных договорах, по которым Республика Болгария является стороной, Государственная комиссия по безопасности информации /ДКСИ/ по предложению министра внутренних дел, министра обороны или директоров служб безопасности может определить на основании решения дополнительные маркировки материалов и документов *более высокого уровня классификации*, чем «*строго секретно»*. Решением Государственной комиссии по безопасности /ДКСИ/, когда национальные интересы требуют этого, *сроки* можно продлить, но не более, чем на первоначально определенные. По истечении сроков уровень классификации удаляется, и доступ к данной информации осуществляется в порядке *Закона о доступе к общественной информации*.[3]

Уравнение уровней классификации безопасности получаемой иностранной классифицированной информации или предоставляемой Республикой Болгарией другому государству или международной организации такой информации во исполнение вступившего в силу международного договора для Республики Болгарии и соответствующего государства или международной организации осуществляется в соответствие с положениями подписанного *договора.*

Национальная система защиты классифицированной информация в Республике Болгарии - это комплекс компетентных *государственных органов* и *мер* на осуществление специфических информационных, аналитических и контрольных видов деятельности. Данные виды деятельности дают возможность объединения информации организационными единицами способом, позволяющим сделать оценку и

дать прогноз о качестве *защиты классифицированной информации* на территории страны и за границей.

Органы по защите классифицированной информации следующие:

❖ **Государственная комиссия по безопасности информации /ДКСИ/** - она является *коллегиальным государственным органом*, который осуществляет политику Республики Болгарии о *защите классифицированной информации*. Комиссия - первостепенный распорядитель бюджетных средств и ей способствует администрация - *общая* и *специализированная*, и она структурирована в *дирекции.* Деятельность ДКСИ, а также структура, организация работы и численность ее администрации определяются *Устройственными правилами*, принятыми Советом министров.[4] Состав Комиссии – из *пяти членов*, в т.ч. председатель и *заместитель председателя.* Состав определяется решением Совета министров по предложению министра-председателя, причем члены назначаются им на срок 5 лет.

❖ **Службы безопасности** - в Республике Болгарии это следующие службы: Государственное агентство "Разведка", Национальная служба охраны, Государственное агентство "Национальная безопасность", Главная дирекция "Борьба с организованной преступностью" и дирекция "Внутренняя безопасность " Министерства внутренних дел /МВД/, служба "Военная информация" Министерства обороны /МО/, Государственное агентство "Технические операции" и органы по части 2 ст. 16 *Закона о противодействии коррупции и о изъятии незаконно приобретенного имущества* (прим. авт. – такими являются директоры территориальных дирекций Комиссии и инспекторы к ним).[5]

❖ **Службы общественного порядка** – в Республике Болгарии это следующие службы: Главная дирекция "Национальная полиция" МВД, Главная дирекция "Пограничная полиция" МВД, Главная дирекция "Пожарная безопасность и защита населения" МВД, областные дирекции МВД – 28, и служба "Военная полиция" при министре обороны.

Как таковые *органы* законодательно установлены и:

❖ **Организационные единицы –** такими являются все публичные органы, а также и физические и юридические лица, где создается, обрабатывается, хранится или предоставляется классифицированная информация.

❖ **Сотрудники по безопасности информации** – такими являются физические лица, назначенные руководителем организационной единицы для осуществления деятельности по *защите классифицированной информации* в данной единице.

❖ А**дминистративные звенья по безопасности информации –** сотрудники этих звеньев способствуют деятельности сотрудников по безопасности информации.

Законодательно *защита классифицированной информации* подразделяется на следующие *шесть видов:*

- Физическая безопасность классифицированной информации – представляет собой систему *мер, способов и средств* физической безопасности, причем условия и порядок их использования определены *Распоряжением,* принятым Советом Министров.[6]
- Документальная безопасность – представляет собой систему *мерк, способов и средств* документальной безопасности, причем условия и порядок их использования определены в *Правилах применения ЗЗКИ*.
- Персональная безопасность – *принципы и меры* персональной безопасности включают *принцип "необходимо знать", процедуру по изучению лиц* и *выдачу разрешения на доступ, проведение обучения для лиц,* причем условия осуществления контроля в этой области регламентированы в *ЗЗКИ* и *Правилах применения ЗЗКИ*.
- Криптографическая безопасность - условия и порядок использования, производство и введение *криптографических методов и средств защиты классифицированной информации* определяются *Распоряжением*, принятым Советом Министров по предложению министра внутренних дел.[7]
- Безопасность автоматизированных информационных систем или сетей - обязательные общие условия их безопасности определены в *Распоряжении,* принятом Советом Министров по предложению министра внутренних дел.[8]
- Индустриальная безопасность - общие требования к гарантированию индустриальной безопасности определяются *ЗЗКИ* в *Распоряжении,* принятом Советом министров.[9]

В период с 2002 года по 2018 год *ЗЗКИ* изменяли и дополняли 42 раза. Вносили от 2 до 3 изменений каждый год. Они прямо касаются и вторичное законодательство по применению *закона*. Результаты проведенного правового и сравнительного правого анализа исследованных нормативных актов показывают, что преобладающее большинство изменений продиктованы динамикой изменения в подчиненности, структуре и компетенциях многочисленных ***служб безопасности*** и ***служб общественного порядка*** в Республике Болгарии.

Можно сделать ***обобщенный вывод***, что вследствие внесенных изменений, Национальная система защиты классифицированной информации в Республике Болгарии непрерывно усовершенствуется,

причем в современных условиях она является надежной и эффективной. Вывод подтверждает частично заявленный основной тезис.

2. Организационно-правовые аспекты защиты личных данных

В 2002 году в Республике Болгарии принят *Закон о защите личных данных /ЗЗЛД/.*[10] В нем дана следующая дефиниция понятия «личные данные»: «*информация о физическом лице, которая раскрывает его физическую, психологическую, умственную, семейную, экономическую, культурную или общественную идентичность*». В соответствие с *ЗЗЛД личными данными* являются и: «*данные о физических лицах, связанные с их участием в гражданских обществах или в органах управления, контроля и надзора юридических лиц, а также и при исполнении функций государственных органов*».

Изменениями *ЗЗЛД* в 2006 году регламентируется, что «*личными данными*» является: «*любая информация, относящаяся к физическому лицу, которое идентифицировано или может быть идентифицировано прямо или косвенно посредством идентификационного номера или посредством одного или более специфических признаков*».

ЗЗЛД упорядочивает защиту прав физических лиц при обработке их *личных данных*. Цель *закона* - гарантировать неприкосновенность личности и личной жизни посредством обеспечения защиты физических лиц при неправомерной обработке связанных с ними *личных данных* в процессе свободного движения данных. В *специальных законах* упорядочивается обработка и доступ к *личным данным* в целях обороны, национальной безопасности и общественного порядка, а также и функционирования *органов* исполнительной и судебной власти при применении *уголовного права.*

В 2002 году 39-ое Народное собрание Республики Болгарии ратифицировало законом *Конвенцию №108 Совета Европы от 28.01.1981 г. о защите физических лиц при автоматизированной обработке персональных данных*.[11] Цель *Конвенции* - гарантировать на территории каждой страны относительно каждого физического лица, независимо от его национальности и места пребывания, соблюдение его прав и основных свобод, и конкретнее его права на личную жизнь в отношение автоматизированной обработки *личных данных*, относящихся к нему. В *Конвенции* понятие «*личные данные*» определяется, как: «*любая информация относительно определенного или определяемого физического лица*». Такое лицо называется еще «*заинтересованным лицом*». *Определенное физическое лицо* понимается, как лицо, которое категорически и ясно идентифицировано. *Определяемое физическое лицо* – это то, что идентифицируется на базе известных или установленных признаков.

Совет Европы воспринял в *Конвенции* три основные принципа:

- *качество данных* – *личные данные*, подвергнутые автоматизированной обработке, должны быть получены и должны обрабатываться добросовестно и законосообразно. Они хранятся на точно определенные и правомерные цели и не должны быть использованы способом, не совместимым с данными целями. *Личные данные* должны быть соответствующими, релевантными и не превышающими меру, с учетом целей, в которых они собраны. Они должны быть точными и, при необходимости, должны быть актуализованы. *Личные данные* должны быть сохранены в виде, позволяющем идентификацию заинтересованных лиц на период не дольше необходимого для той цели, в которой они сохранены. *Личные данные*, которые раскрывают расовое происхождение, политические взгляды, религиозные или другие убеждения, а также и личные данные относительно здоровья или сексуальной жизни нельзя обрабатывать автоматизировано, кроме как если внутреннее право гарантирует подходящую защиту. Это же распространяется и на личные данные, связанные с осудительными приговорами;
- *безопасность данных* – для защиты *личных данных* необходимо принять подходящие меры безопасности. Данные должны быть сохранены в автоматизированных реестрах, обеспеченных от случайного или непозволенного уничтожения или случайной погибели. Необходимо обеспечить защиту от недозволенного доступа, изменения или распространения *личных данных;*
- *дополнительные гарантии для заинтересованного лица* – каждому лицу необходимо дать возможность установить существование автоматизированного реестра *личных данных*, его основные цели, а также и самоличность и обычное место жительства или основное место деятельности администратора реестра. Любое лицо должно иметь возможность получать через разумные интервалы и без слишком длительного замедления или расходов, подтверждение о наличии или отсутствии *личных данных* о нем, сохраненных в автоматизированных реестрах данных, а также эти *данные* должны сообщаться ему в доступной форме. Лицо должно иметь возможность получать в зависимости от случая исправлять или удалять такие *данные*, если они были обработаны в нарушение распоряжений внутреннего права, чем вводится основной принцип качества *данных*. Лицо может получить компенсацию в случае, если заявление об информации или, соответственно, о сообщении, исправлении или удалении *данных* о нем не будет утверждено.

Во всех случаях *личные данные обрабатываются* и обязательно поддерживаются в *реестрах*, а именно: *документальных, картотечных* или *автоматизированных информационных фондах*, структурированных

по нескольким специфическим критериям, подходящим для облегчения их обработки, состоящих из одного или нескольких элементов в одном или нескольких физических мест.

Каждое физическое лицо имеет право доступа к относящимся к нему *личным данным*. В случаях, когда при осуществлении права доступа физического лица могут быть раскрыты *личные данные* и о третьем лице, *администратор личных данных* обязан предоставить соответствующему физическому лицу доступ к их части, относящейся только к нему. Осуществление права доступа к *личным данным* не может быть направлено против прав и доброго имени другого физического лица, а также и против национальной безопасности, общественного порядка, народного здоровья и морали. Право доступа осуществляется на основании *письменного заявления* к *администратору личных данных*. *Заявление* можно отправить и электронно.

Администратор личных данных принимает решение о предоставлении *полного* или *частичного доступа* заявителю или мотивирует отказ в предоставлении доступа. Доступ отказывается, когда *данные* не существуют или их нельзя предоставлять на определенном правовом основании. В отказе обязательно указать *орган*, где можно *обжаловать решение администратора* и срок его *обжалования. Администратор* обязан письменно уведомить заявителя о своем решении. Уведомление – личное, под подпись, или по почте с обратной распиской.

Форма предоставления доступ к личным данным может быть следующая: *устная справка, письменная справка* и *просмотр данных соответствующим физическим лицом или специально уполномоченным им другим лицом*. При нарушении его прав по *ЗЗЛД* каждое физическое лицо может *обжаловать* действия и акты *администратора* в судебном порядке в соответствующем районном административном суде или в Верховном административном суде по общим правилам подсудности. В производстве *физическое лицо* может потребовать *возмещения* за понесенный им ущерб, вследствие неправомерной обработки *личных данных* со стороны *администратора.*

Независимый государственный орган, который осуществляет защиту лиц при обработке их *личных данных* и при осуществлении доступа с этим *данным*, а также и контроль над соблюдением *ЗЗЛД* в Республике Болгарии - **Комиссия по защите личных данных**. Деятельность Комиссии и ее администрации регламентируется *Правилами*, выданными ее председателем.[12] Комиссия состоит из *председателя* и *четырех членов*. Их выбирает Народное собрание по предложению Совета министров. Их мандат - 5 лет, причем членов можно переизбрать на еще один мандат. Комиссия определяет в

распоряжении минимальные необходимые технические и организационные меры, а также и допустимый вид защиты.[13] Она может запретить хранение *личных данных*, если *администратор* не обеспечил достаточную защиту обработанных *данных* как *анонимные данные*. Комиссия - *наблюдающий орган* относительно безопасности данных, которые хранят предприятия, предоставляющие общественные электронные сети сообщения и/или услуги в соответствие с *Законом о электронных сообщениях*[14] и *Законом о электронной идентификации*.[15] Она осуществляет методическое руководство и контроль за деятельностью, связанной с гражданской регистрацией в порядке *Закона о гражданской регистрации*.[16]

Комиссия по защите личных данных следит за применением *директив*, *регламентов* и *решений* Европейского парламента и Европейской комиссии в области защиты личных данных. Это следующие:

- *Директива 95/46/ЕО О защите физических лиц применительно к обработке персональных данных и о свободном движении таких данных (*действует до вступления в силу *Регламента (ЕС) 2016/679 - общее регулирование защиты данных* - **GDPR***);*
- *Рамочное решение 2008/977/ПВД Совета о защите персональных данных, обработанных в рамках полицейского и судебного сотрудничества по уголовным делам (*действует до вступления в силу *Директивы (ЕС) 2016/680 о защите физических лиц применительно к обработке персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования уголовных преступлений или исполнения уголовных наказаний);*
- *Директива (ЕС) 2016/681 Европейского парламента и Совета Европейского Союза от 27 апреля 2016 года об использовании данных системы бронирования (PNR) для предотвращения, выявления, расследования и уголовного преследования преступлений террористической направленности и тяжких преступлений***;**
- *Регламент (ЕС) 211/2011 Европейского парламента и Совета ЕС о гражданских инициативах;*
- *Регламент 611/2013 Европейской комиссия о мерах, применимых к сообщению о нарушениях безопасности личных данных, согласно Директиве 2002/58/ об уважении права на частную жизнь, о конфиденциальности и электронных средствах связи*.[17]

Новый **GDPR (General Data Protection Regulation) -** *Регламент (ЕС) 2016/679 Европейского парламента и Совета Европейского Союза о защите физических лиц применительно к обработке персональных данных и о свободном движении таких данных* – должен применяться прямо во всех 28 государствах-членах Европейского союза от 25 мая 2018

г. Штрафы, предусмотренные Регламентом за его неприменение, составляют до 20 млн. евро или 4% от годового оборота бизнес организаций в каждом государстве. В Республике Болгарии число бизнес организаций приблизительно 50 000. Регламент требует назначить сотрудников в каждой из этих организаций, которые должны пройти обучение защите личных данных в них. Большинство Европейских национальных регуляторов по защите личных данных заявили, что не имеют возможности обеспечить применение регламента, считая с этого дня.

В период с 2002 года по 2018 год *ЗЗЛД* изменяли и дополняли 19 раз. Результаты проведенного правового и сравнительного правового анализа показывают, что преобладающие изменения в *законе* продиктованы необходимостью гармонизировать внутреннее законодательство с европейскими *директивами*, *регламентами* и *решениями* о защите личных данных. Их применение требует принятия соответствующих организационно-правовых видов деятельности национальными властями, но они не достаточно финансово обеспечены.

Можно сделать ***обобщенный вывод***, что построенная Национальная система защиты личных данных в Республике Болгарии не достаточно эффективная и надежная. Вывод не подтверждает частично заявленный основной тезис. Рекомендательно, чтобы усилия депутатов в Европейском парламенте и Народном собрании Республики Болгарии направить на новые законодательные инициативы, ведущие к преодолению проблемы с защитой личных данных, которая будет адекватна и соображена с мировыми тенденциями в данной области.

Литература:

1. Закон о защите классифицированной информации, обн.ДВ. №45/2002 г. с посл. изм. и доп. ДВ. №17/2018 г.
2. Правила применения Закона о защите классифицированной информации, обн. ДВ.№115/2002 г., с посл. изм. и доп. ДВ.№68/2017 г.
3. Закон о доступе к общественной информации, обн. ДВ.№55/2000 г., с посл. изм. и доп.85/2017 г.
4. Устройственные правила Государственной комиссии по безопасности информации и на ее администрации, обн.ДВ.бр.19/2017 г.
5. Закон о противодействии коррупции и об изъятии незаконно приобретенного имущества, обн. ДВ.№
6. Распоряжение о системе мер, способов и средств физической безопасности классифицированной информации и об условиях и порядке их использования – обн.ДВ.№22/2003 г.

7. Распоряжение о криптографической безопасности классифицированной информации – обн.ДВ.№102/2003 г. с посл. изм. и доп. ДВ №35/2016 г.

8. Распоряжение об обязательных общих условиях безопасности автоматизированных информационных систем или сетей, в которых создается, обрабатывается, хранится и переносится классифицированная информация – обн. ДВ.№46/2003 г. с посл. изм. и доп. ДВ №35/2016 г.

9. Распоряжение об общих требованиях к гарантированию индустриальной безопасности – обн.ДВ.№22/2003г. с посл. изм. и доп.104/2007 г.

10. Закон о защите личных данных, обн.ДВ.№1/2002 г., с посл. изм. и доп. ДВ.№7/ 2018 г.

11. Конвенция №108 Совета Европы от 28.01.1981 г. о защите физических лиц при автоматизированной обработке персональных данных, обн.ДВ.бр.26/2003 г.

12. Правила о деятельности Комиссии по защите личных данных и ее администрации – выданы председателем Комиссии по защите личных данных – обн.ДВ.№11/2009 г. , с посл. изм. и доп.ДВ.№10/2016 г.

13. Распоряжение №1 от 30 января 2013 г. о минимальном уровне технических и организационных мер и о допустимом виде защиты личных данных – выдано Комиссией по защите личных данных, обн.ДВ.№14/2013 г.

14. Закон о электронных сообщениях, обн.ДВ.№41/200г., с посл. изм. и доп.28/2018 г.

15. Закон о электронной идентификации, обн.ДВ.№38/2016 г., с посл. изм. и доп.ДВ.№14/2018 г.

16. Закон о гражданской регистрации, обн.ДВ.№67/1999 г., с посл. изм. и доп.ДВ.№91/2017 г.

17. Прим.авт. – Директивы, регламенты и решения ЕС опубликованы на интернет странице Комиссии по защите личных данных Республики Болгарии - https://www.cpdp.bg/