СТАНОВИЩЕ

от проф. д.н. Георги Георгиев Димитров

Университет по библиотекознание и информационни технологии

Член на научното жури

на докторска дисертация на

Маргарита Евгениева Ойсолова

Професионално направление: 3.6. Право

Научна специалност: Международно право и международни отношения

Научен ръководител: проф. д-р Ирена Илиева

ТЕМА: „РЕГЛАМЕНТАЦИЯ НА КИБЕРСИГУРНОСТТА В ЕВРОПЕЙСКИЯ СЪЮЗ – ПРОБЛЕМИ И ПЕРСПЕКТИВИ“

1. Актуалност и значимост на темата

Представеният дисертационен труд е посветен на изключително актуална тема – правната регламентация на киберсигурността в Европейския съюз. В ерата на дигитализацията мрежовата и информационната сигурност имат ключово значение за функционирането на обществото, икономиката и държавните институции. Все по-голяма част от ежедневните дейности, публичните услуги и бизнес процесите разчитат на информационни и комуникационни технологии. Увеличаващият се брой кибератаки и киберзаплахи в глобален мащаб налага предприемането на адекватни мерки на наднационално ниво за защита на критичните мрежи, системи и данни на наднационално ниво.

Темата е не само навременна, но и с голяма научна и практическа значимост. В Европейския съюз бяха приети няколко стратегически акта в областта на киберсигурността – от първия всеобхватен акт като Директивата за мрежова и информационна сигурност (МИС1 от 2016 г.), до най-новите инициативи като нейното актуализиране с Директива (ЕС) 2022/2555 (МИС2), Регламента за киберсигурността (Регламент (ЕС) 2019/881) и др. Изследването на тази еволюция е от важно значение за правната наука и за практиката, тъй като позволява да се оценят постигнатите резултати, съществуващите пропуски и предизвикателствата, както и да се формулират препоръки за усъвършенстване на нормативната уредба.

Дисертантката ясно е формулирала тезата, че макар ЕС да е направил значителни крачки в законодателството по киберсигурност (чрез стратегии, регламенти и директиви), все още съществуват празноти и необходимост от допълнения и актуализации, продиктувани от появата на нови заплахи в киберпространството. Това схващане подчертава актуалността на изследването – киберсигурността е динамична област, в която правната рамка трябва непрекъснато да догонва техническия прогрес и нововъзникващите рискове. Темата представлява новост и ценен принос за българската правна доктрина, тъй като досега липсва цялостно академично изследване на вторичното право на ЕС относно киберсигурността в такава широта и дълбочина. Доколкото киберсигурността е интердисциплинарна сфера, разглеждането ѝ през призмата на правото на ЕС е особено важно и полезно за въвеждане на общи стандарти и споделени ценности в дигиталната среда.

Може да се заключи, че изборът на тема е обоснован и навременен. Трудът адресира реални нужди – за изясняване на сложната мозайка от нормативни актове на ЕС в областта на киберсигурността и за подпомагане на юристи и експерти в разбирането и прилагането им на практика. Актуалността личи и от включените в изследването най-нови нормативни изменения от края на 2022 г., което показва стремеж дисертацията да обхване най-съвременните развития в областта. Темата притежава и значимост с оглед перспективността – изводите и препоръките на автора биха могли да подкрепят по-нататъшното развитие на европейската политика по киберсигурност, както и националните усилия по транспониране и прилагане на тези политики.

2. Кратка аналитична характеристика на дисертационния труд

Дисертационният труд на Маргарита Ойсолова е с обем от 246 страници, от които 200 страници основен текст и 46 страници приложения и използвана литература. Структурно дисертацията е издържана в класически вид – съдържа увод, три глави, заключение, списък на използваните източници и приложения. В основния текст са използвани над 100 източника, включително нормативни актове на ЕС, официални документи, стратегии, научни публикации и интернет ресурси. Цитираните източници са актуални и обхващат както правни актове, така и съвременни изследвания по разглежданата проблематика, което свидетелства за задълбочеността на проучването и познаването на състоянието на тематиката от страна на докторантката.

Уводът на дисертацията ясно очертава обекта, предмета, целите и задачите на изследването. Аргументирана е необходимостта от цялостен преглед на законодателството на ЕС в сферата на киберсигурността с цел идентифициране на проблемите и пропуските в него. Формулирана е основната изследователска теза и са представени използваните методи на изследване – юридически телеологичен подход, допълнен от критичен анализ на съвременните научни разработки по темата, интервюта с експерти, исторически, формално-логически методи (синтез, дедукция) и др. Докторантката е определила и границите на изследването (главно периодът след 2000 г.), което е уместно предвид бурното развитие на киберотношенията именно през последните две десетилетия. В увода прави впечатление и засегнатият интердисциплинарен контекст – разглежда се връзката между правните измерения на киберсигурността и етичните аспекти (киберетика) и се подчертава значението на споделените стандарти и ценности в глобализираното киберпространство. Уводната част е написана на добър академичен стил, въвежда читателя в темата и подготвя почвата за последващия анализ.

Първа глава е озаглавена „Стратегически документи“ и съдържа пет раздела. В нея са разгледани четири основни стратегически документа на Европейския съюз в областта на киберсигурността. Дисертантката започва с анализ на първата Стратегия на ЕС за киберсигурност

от 2013 г., която очертава визията на Съюза за свободно и сигурно киберпространство и въвежда пет стратегически приоритета за повишаване нивото на киберсигурност. Разгледано е следващото развитие – актуализираната Стратегия на ЕС за киберсигурност от 2020 г., в която се отбелязва значителна промяна към по-интегриран подход и са предложени конкретни мерки в отговор на новопоявилите се заплахи. Докторантката прави сравнение между стратегия 2013 и 2020, изтъквайки приемствеността и разликите (например засиления фокус върху икономическите и военни аспекти на заплахите в стратегия 2020). Освен това, в главата са анализирани Стратегията за Единен цифров пазар (2015 г.) и нейната актуализация през 2025 г., като се акцентира върху централната роля на киберсигурността за изграждане на доверие сред гражданите и бизнеса в цифровите услуги. Отбелязано е, че в версията от 2025 г. липсват специални текстове за киберсигурност, което е интересен извод относно приоритетите към момента. Друг стратегически документ, разгледан от авторката, е Стратегията на ЕС за Съюза на сигурността (2020 г.), където се подчертава необходимостта от действия както във физическата, така и в дигиталната сфера срещу заплахи като тероризъм и кибератаки. Докторантката умело свързва тези стратегически визии с темата на дисертацията, извеждайки общия извод, че на най-високо ниво ЕС осъзнава критичността на киберсигурността и планира мерки за укрепването ѝ. В края на главата са синтезирани резултатите от анализа на стратегиите – идентифицирани са ключовите приоритети и пропуски, например нуждата от общи минимални изисквания за киберсигурност на национално ниво и подобрена координация при трансгранични инциденти. Първа глава е структурирана логично, показва познаване на политическия контекст и има принос чрез систематизирането на стратегическите основи, върху които стъпва законодателството.

Втора глава е озаглавена „Регламенти в областта на киберсигурността“ и обхваща осем раздела. В тази част дисертантката разглежда подробно основните регламенти (регламентни актове) на ЕС, имащи отношение към киберсигурността. Започнато е с нормативната уредба на електронната идентификация и удостоверителните услуги – анализиран е Регламент (ЕС) № 910/2014 (eIDAS), който създава рамка за сигурни електронни транзакции и доверени услуги в рамките на ЕС. Авторката изтъква значението на eIDAS за повишаване на доверието в цифровите взаимодействия, включително за граждани, бизнес и публични органи. След това е разгледана връзката между защитата на личните данни и киберсигурността. Докторантката прави анализ на Общия регламент относно защитата на данните – GDPR (Регламент (ЕС) 2016/679), подчертавайки неговата роля за уеднаквяване на стандартите за сигурност при обработване на лични данни в цифрова среда . Разгледан е и специалният Регламент (ЕС) 2018/1725, който урежда защитата на данните при институциите на ЕС – правилно е отчетена тясната връзка между киберсигурността и защитата на личната информация. Докторантката прави изключително значим анализ на Регламент (ЕС) 2017/2394 относно сътрудничеството между националните органи за защита на потребителите, „Акта за киберсигурността“ (Регламент (ЕС) 2019/881), Регламент (ЕС) 2022/2554 (DORA) относно цифровата оперативна устойчивост във финансовия сектор – един съвсем скорошен акт (приет в края на 2022 г.), който авторката правилно е оценила като релевантен – финансовите услуги са силно дигитализирани, а DORA цели да повиши тяхната киберустойчивост.

Трета глава носи заглавието „Директиви в областта на киберсигурността“ и е структурирана в девет раздела. Това е най-обемната част на труда, като в нея са анализирани единадесет директиви на ЕС, свързани с различни аспекти на киберсигурността. Докторантката започва с Директива 2002/58/ЕО (Директива за електронната неприкосновеност, изменена с Директива 2009/136/ЕО), която урежда защитата на личните данни и неприкосновеността на комуникациите в сектора на електронните съобщения. Авторката дава синтезиран преглед на съдържанието на измененията от 2009 г., които засилват правата на потребителите и изискванията към операторите (напр. въвеждането на изискване за съгласие при „бисквитки“, уведомяване при нарушения на сигурността и др.). Посочени са основните цели – по-добра защита на личния живот онлайн и укрепване на доверието в цифровите услуги. Дисертантката идентифицира проблеми и слабости в тази директива

(напр. предизвикателства пред прилагането ѝ във връзка с бързото технологично развитие), което демонстрира критичен подход. Впоследствие са анализирани последователно Директива 2013/40/ЕС относно атаки срещу информационни системи (киберпрестъпления), Директива 2007/64/ЕО (PSD) относно платежните услуги, както и на Директива (ЕС) 2015/1535 (процедура за предоставяне на информация в сферата на техническите стандарти за услугите на информационното общество), Директива (ЕС) 2016/680 (т.нар. Директива за защита на данните при полицейско и съдебно сътрудничество) и Директива (ЕС) 2016/2102 за достъпността на уебсайтовете и мобилните приложения на публичния сектор.

Кулминацията на трета глава е посветена на най-важните директиви пряко в областта на киберсигурността - Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета (т.нар. Директива за сигурността на мрежите и информацията, или NIS1). Същата е подробно разгледана. Дисертантката обяснява, че това е първият цялостен европейски законодателен акт, целящ постигане на високо общо ниво на мрежова и информационна сигурност в Съюза. Изведени са основните изисквания на директивата – всяка държава членка да определи национални компетентни органи по киберсигурност, да изгради екипи за реагиране при компютърни инциденти (CERT/CSIRT), да приеме национална стратегия за киберсигурност, както и да идентифицира оператори на съществени услуги и доставчици на цифрови услуги, които да спазват мерки за сигурност и уведомяване при инциденти. Авторката отбелязва, че в резултат от приемането на NIS1 в ЕС е постигнато повишение на общото ниво на киберсигурност, но са останали и пропуски, което е наложило последващи действия.

На второ място, дисертацията анализира Директива (ЕС) 2022/2555 (NIS2) – актуализирания вариант на директивата за мрежова и информационна сигурност, приет през декември 2022 г. като заместител на NIS1. Докторантката прави съпоставка между NIS1 и NIS2, посочвайки как NIS2 надгражда предшественика си: разширява обхвата, като добавя нови сектори и видове уязвими субекти; въвежда по-строги изисквания за управление на рисковете и отчетност; засилва координацията и обмена на информация между държавите членки; предвижда по-сериозни санкции при неспазване. Правилно е изтъкнато, че NIS2 е част от отговора на ЕС на нарастващата цифровизация и еволюиращите киберзаплахи. В труда се подчертава, че NIS2 цели да отстрани констатираните слабости в NIS1 и да повиши още повече нивото на киберсигурност в Съюза в идните години.

Наред с NIS2, в дисертацията е разгледана и Директива (ЕС) 2022/2557 за устойчивостта на критичните субекти (CER) . Макар CER да е фокусирана повече върху физическата устойчивост на критичната инфраструктура, авторката правилно я вписва в общата стратегия за цифрова сигурност, отбелязвайки че тя допълва NIS2 и отразява необходимостта от повишена защита срещу новите комплексни заплахи, пред които са изправени ключовите сектори в контекста на цифровизацията.

Характерно за третата глава е, че за всяка от анализираните директиви авторката представя и информация за нейното транспониране в българското законодателство. Това придава допълнителна практическа стойност на изследването. Например, споменато е че Директива 2016/1148 (NIS1) е транспонирана в българското право чрез Закона за киберсигурност от 2018 г., и са обсъдени основните положения на този закон. По подобен начин са отбелязани националните мерки по останалите директиви – дали и как са имплементирани в българските нормативни актове. Този подход показва умение за свързване на наднационалната рамка с националния контекст, което е особено ценно за оценка на ефективността и приложимостта на европейските политики у нас.

Обобщено, третата глава предоставя цялостен преглед на директивната основа на европейската киберсигурност. Дисертантката систематично е изложила съдържанието на всеки акт,

идентифицирала е неговите цели, обхват, принос и недостатъци, както и взаимодействието му с останалите. В края на главата логично следва Заключение, в което авторката синтезира изведените в предходните части изводи и потвърждава тезата на изследването. Констатирано е, че ЕС е постигнал напредък чрез разнообразни законодателни мерки, но правната рамка трябва да се развива динамично с оглед появата на нови технологии и заплахи. Дисертантката особено акцентира върху необходимостта от по-честа актуализация на нормативните актове и проактивно идентифициране на нововъзникващи рискове (например квантовите компютри като бъдещо предизвикателство за киберсигурността). Формулирани са обобщени препоръки *de lege ferenda* – за актуализиране на правната рамка спрямо новите технологии, за намаляване на фрагментираното прилагане в различните държави членки, за засилване на координацията и обмена на добри практики и др. Заключението е аргументирано, показва, че поставената цел е постигната, и ясно посочва оригиналния принос на труда: първо по рода си у нас цялостно изследване на европейското киберзаконодателство, разкриване на неговите тенденции, проблеми и възможности за развитие.

Като цяло, дисертационният труд прави много добро впечатление със своята структура, прецизност и изчерпателност. Докторантката демонстрира отлична осведоменост по тематиката, борави уверено с понятийния апарат на киберсигурността и правото на ЕС, умее да анализира и синтезира информацията от множество източници. Текстът е написан в академичен стил, аргументацията е последователна, а изводите – убедително обосновани. Налице е умело съчетаване на описателния преглед на нормативната уредба с критичен анализ на нейните недостатъци и ефективност. По този начин дисертантката постига поставената цел и доказва тезата си, че съществуващата европейска правна рамка за киберсигурност, макар и напреднала, се нуждае от допълнително усъвършенстване, за да отговори адекватно на бързопроменящата се среда.

3. Оценка на научните и научно-приложните приноси

Приносите на дисертационния труд на Маргарита Ойсолова могат да се систематизират в две основни направления: научни (теоретични) приноси и научно-приложни (практически) приноси.

Научни приноси

На първо място, трудът представлява първото по рода си в българската специализирана литература цялостно изследване на вторичното право на ЕС в областта на киберсигурността. Дисертантката е извършила впечатляващо по обхват проучване, включващо анализ на 6 стратегически документа, 8 регламента и 11 директиви на ЕС, свързани с киберсигурността. Съдържанието на всички тези актове е предадено в синтезиран вид, което улеснява разбирането им дори от читатели извън юридическата общност (напр. ИТ специалисти, които трябва да прилагат тези изисквания). Такъв широк обхват и синтез е значим научен принос сам по себе си, тъй като събира на едно място разпилената иначе нормативна уредба, осигурявайки „голямата картина“ на европейската политика за киберсигурност.

На второ място, авторката е направила оригинален сравнителен анализ на ключови документи: например сравнението между двете стратегии на ЕС за киберсигурност (2013 и 2020) и извеждането на тенденциите и промените в политическия подход; сравнението между Директива NIS1 и Директива NIS2 и идентифицирането на конкретните подобрения и разширения в новата директива. Тези сравнения допринасят към научното познание, тъй като осветляват еволюцията на концепциите и приоритетите в рамките на ЕС.

На трето място, дисертантката е идентифицирала основните проблеми и слабости във всеки от разгледаните нормативни актове и политики. Това не е просто описателно изброяване, а е обосновано чрез анализ на практиката – посочено е доколко отделните държави членки са успели да приложат изискванията, къде са срещнати трудности, какви изменения са наложени на ниво ЕС вследствие на установени слабости. Така трудът има ясна критична насоченост и излиза извън рамките на компилация от текстове – авторката формира самостоятелни изводи относно ефективността на съществуващата уредба.

На четвърто място, предложени са конкретни идеи *de lege ferenda* за подобрение на европейската нормативна уредба по киберсигурност. Докторантката формулира редица препоръки, базирани на констатациите от анализа: необходимост от по-гъвкав механизъм за периодично актуализиране на законодателството с оглед на появяващи се нови технологии (напр. блокчейн, квантови компютри) ; унифициране и изчистване на понятията и изискванията, за да се избегне нееднаквото прилагане в държавите членки; засилване на трансграничните координационни механизми при киберинциденти; интегриране на киберетични стандарти и повишаване на осведомеността. Тези препоръки показват способност за прогностично мислене и принос в теоретичен план – предлагат се насоки за развитие на правото, които могат да бъдат основа за бъдещи научни обсъждания и законодателни инициативи.

Не на последно място, трябва да се отбележи интердисциплинарният принос на труда. Дисертантката съчетава правния анализ с познания от сферата на информационната сигурност и етиката. Включването на концепцията за „киберетика“ и обсъждането на етичните и правните измерения на киберсигурността в стратегическата рамка на ЕС демонстрира новаторски подход към темата, поставяйки я в по-широк ценностен контекст. Това допринася към научните дебати за необходимостта от съчетаване на технологичните решения с етични и правни принципи.

Научно-приложни приноси

Трудът на Маргарита Ойсолова има и ясно изразено приложно значение.

На първо място, систематизацията на европейското законодателство по киберсигурност в един труд е практическо улеснение за различни целеви групи – юристи, които работят или предстои да работят по въпросите на киберсигурността, могат да ползват дисертацията като справочник за релевантните актове и техните основни положения; технически експерти по информационна сигурност биха намерили в нея разбираемо представяне на правните им задължения и рамки; публични органи и политици – консолидиран източник при формиране на политики и законопроекти в областта. Самата авторка изрично отбелязва, че стремежът ѝ е трудът да бъде полезен и разбираем не само за юристи, но и за „неюристи, технически лица“ и дори за обикновени потребители на Интернет, които са засегнати от въпросите на киберсигурността. В този смисъл дисертацията изпълнява образователна и практическа функция.

На следващо място, анализът на транспонирането на директивите в националното законодателство е ценен практически принос. По този начин трудът служи като „мост“ между европейското и българското право – показва къде България стои в прилагането на изискванията, кои директиви вече са имплементирани (например чрез Закона за киберсигурност, Закона за електронното управление, изменения в секторни закони и др.), и дали има изоставане или трудности. Това е полезно за националните институции, натоварени с въвеждането на тези политики, и може да послужи за идентифициране на области, които изискват допълнителни усилия или изменения у нас. Например, ако дадена директива (като NIS2) все още е в процес на

транспониране, анализът на Ойсолова може да ориентира законодателя за ключовите моменти, на които да обърне внимание.

Практически принос са и предложенията *de lege ferenda*, които имат конкретна насоченост. Те биха могли да се използват от европейските институции при бъдещи ревизии на нормативната уредба или при изготвяне на нови стратегии. Предложенията на докторантката, като включване на квантовата сигурност в политиките, по-чести прегледи на законодателството, експертни панели по дигитализация и др. , са реалистични и изпълними мерки. Макар и формулирани общо, те предоставят конструктивни насоки, които показват къде са слабите места и как биха могли да се адресират. Това е ценен принос за практиката, защото превежда научните изводи в потенциални действия.

Като *цялостна оценка* може да се каже, че приносите на дисертацията са значими както за развитието на научната теория в разглежданата област, така и с непосредствена практическа приложимост. Трудът обогатява доктрината с нови обобщения, класификации и идеи, а същевременно е в състояние да подпомогне практическия процес на законотворчество и прилагане на правото в сферата на киберсигурността.

4. Оценка на публикациите по темата на дисертационния труд

Докторантката Маргарита Ойсолова е представила три научни публикации, които отразяват основните изследователски тези и резултати от дисертацията. Всички публикации са тематично свързани с дисертационния труд и представляват части от изследваната проблематика, което показва последователност и ангажираност на авторката с темата през целия период на обучение.

Първата публикация е научен доклад на тема „Транспониране на Директива (ЕС) 2016/1148 в българското законодателство“, включен в сборника с доклади от XI национална конференция на докторантите в областта на правните науки (2021 г.). В този труд докторантката разглежда процеса по въвеждане на изискванията на Директивата NIS1 (2016/1148) в националното право, анализирайки Закона за киберсигурност и свързаните подзаконови актове. Публикацията отразява части от третата глава на дисертацията, където се разглеждат директивите и тяхното приложение в България. В нея Ойсолова достига до изводи за степента на съответствие на българското законодателство с европейските стандарти, посочва предизвикателствата (например координацията между националните компетентни органи, обхвата на определяне на оператори на съществени услуги и др.) и така пряко допринася за доказването на тезата, че макар България да е транспонирала NIS1, продължаващото развитие (впоследствие NIS2) изисква допълнителни усилия.

Втората публикация е доклад „Акт за киберсигурността“, представен на XII национална конференция на докторантите в областта на правните науки (2022 г.). Този доклад обхваща анализа на Регламент (ЕС) 2019/881, посветен на ENISA и сертификацията по киберсигурност – същият този акт е детайлно разгледан и във втора глава на дисертацията. В публикацията докторантката е изложила основните цели и положения на „Акта за киберсигурността“, вероятно разглеждайки и първите стъпки по прилагането му (тъй като през 2022 г. вече са били установени първи европейски схеми за сертифициране). Този доклад е ценен, защото демонстрира, че авторката е в течение с новостите и участва в научния дискурс по тях още преди финализиране на дисертацията. Материалът подкрепя тезата на дисертацията, тъй като анализира един от ключовите нови инструменти на ЕС за повишаване на киберсигурността – сертифицирането – и оценява неговото значение и предизвикателства.

Третата публикация е „Съпоставка между директивите 2016/1148 и 2022/2555 на Европейския парламент и на Съвета“, която към момента на подаване на документите е посочена като „под печат“ (предстояща за публикуване, 2024 г.). В нея Ойсолова прави директно сравнение между старата и новата директива за мрежова и информационна сигурност (NIS1 и NIS2), обобщавайки в синтезиран вид сходствата и разликите. Тази статия отразява много ясно научния принос на дисертацията – именно съпоставката на двата режима и изводите за необходимостта от промени. Очаква се в публикацията авторката да е изтъкнала, че след приемането на NIS1 е постигнат напредък, но са откроени пропуски (ограничен обхват, недостатъчни санкции, липса на единни изисквания за сигурност и др.), които NIS2 адресира чрез разширяване на приложното поле, по-строги мерки и по-засилен надзор . Този труд практически извежда на преден план една от главните тези на дисертацията – развитието на европейското законодателство продължава еволюционно, като новите актове надграждат предходните за постигане на по-високо ниво на киберустойчивост.

И трите публикации свидетелстват, че докторантката активно е работила и обсъждала своята тема в научни форуми, получавайки, вероятно, обратна връзка и възможност да доусъвършенства изследването си. Те също така показват, че основните части на дисертацията (анализ на директивите, анализ на регламентите) са били подложени на „пилотно“ представяне и критика, което дава допълнителна достоверност на резултатите. Публикациите напълно кореспондират с темата на дисертацията, отразяват основните ѝ приноси и са в съавторство единствено с докторантката, което означава, че тя самостоятелно е разработила и представила тези резултати. Това отговаря на изискванията към докторантите за минимум публикации по темата и уверено мога да кажа, че представените трудове покриват и дори надграждат необходимия минимум.

5. Оценка на автореферата

Авторефератът на дисертационния труд е изготвен прецизно и в съответствие с утвърдените изисквания за такъв вид академичен документ. Структурата на автореферата е ясна – съдържа обща характеристика на дисертацията, вкл. цел, предмет, задачи, теза, методология и очаквани резултати; следва описание на обема и структурата на самия труд; представени са накратко съдържанието на всяка глава и заключението; накрая са изброени приносите на изследването и списъкът на публикациите по темата.

С оглед на изложеното, считам, че авторефератът напълно отговаря на изискванията за академичен автореферат, съпровождащ докторска дисертация. Той е структуриран правилно, написан е в стегнат и ясен стил, дава цялостна представа за съдържанието и приносите на труда, без да се впуска в излишни детайли. Авторефератът успешно изпълнява ролята си да презентира накратко изследването и постиженията на докторантката, и по тази причина му давам положителна оценка.

6. Забележки и препоръки

Дисертационният труд на Маргарита Ойсолова притежава безспорни достойнства – актуална тема, широк обхват, дълбочина на анализа и ясно формулирани резултати. Въпреки това, в духа на академичната критичност и с цел бъдещо надграждане на изследването (например при публикуване като монография), си позволявам да направя следните забележки и конструктивни препоръки:

1. *Относно обхвата на изследването.* Докторантката е включила много широк кръг от нормативни актове – практически всички важни стратегии, регламенти и директиви, имащи дори косвено отношение към киберсигурността. Този всеобхватен подход е похвален, но крие риск анализът на места да остане не толкова задълбочен. На някои места в труда описателното представяне доминира над критичния анализ поради огромния материал за обхващане. Препоръката ми е при евентуално публикуване докторантката да обмисли фокусиране върху по-тесен кръг ключови актове или групиране по тематични направления (например отделно разглеждане на рамката за защита на данните, отделно – на рамката за критични инфраструктури, отделно – на наказателноправните аспекти и т.н.). Това би позволило още по-задълбочено изследване на вътрешните връзки и противоречия, без да се жертва пълнотата.
2. *Отграничаване на понятието „киберсигурност".* В труда понятието „киберсигурност" е използвано в широк контекст, включващ множество съпътстващи области (достъпност, електронни удостоверителни услуги, защита на потребителите, платежни услуги и пр.). Това отразява реалността, че киберсигурността прониква навсякъде, но би било добре по-ясно да се очертае обхватът на термина. Например, читателят може да се запита защо Директивата за платежните услуги или тази за техническите стандарти са разгледани тук – обяснението е налице, но е имплицитно. Препоръчително е авторката изрично да дефинира или дискутира понятието „киберсигурност" в началото на труда и да обоснове критериите, по които решава кои актове са „в областта на киберсигурността". Това би предотвратило евентуално объркване и би подсилило методологичната рамка на изследването.
3. *Баланс между нормативен и доктринален анализ.* Дисертацията е силна в юридическия (нормативния) анализ – детайлно е проучено съдържанието на актовете и какво е направено на практика. На моменти обаче се усеща липса на по-задълбочено обсъждане на доктриналните източници и научни възгледи по темата. Например, би било полезно да се цитира мнението на автори относно ефективността на NIS1 или критики от научната общност към GDPR в контекста на киберсигурността. Препоръката ми е в доразвита версия на труда докторантката да интегрира повече сравнителен анализ с мненията на утвърдени европейски експерти и научни работници (напр. оценки от ENISA доклади, академични статии за NIS2, анализи на прилагането на Акта за киберсигурността и др.). Това би придало още по-висока научна стойност и би показало диалог с наличната литература, освен с нормативните текстове.
4. *Анализ на глобалния контекст.* Фокусът на дисертацията е върху правото на ЕС, което е оправдано предвид темата и научната специалност. Все пак, киберсигурността е глобален проблем и би било интересно да се отчетат международните усилия и стандарти, които влияят или кореспондират с правото на ЕС. Например, Будапещенската конвенция на Съвета на Европа за киберпрестъпността, рамките на НАТО за киберотбрана, стандартите на ISO/IEC за информационна сигурност, насоките на ООН в цифровата сфера и др. Препоръчително е в увода или заключението, макар и телеграфно, да се направи връзка между европейската уредба и по-широкия международен контекст – това би подчертало цялостно разбирането, че усилията на ЕС са част от глобалната картина и че съществува взаимодействие между различните нива на правна регулация на киберсигурността.
5. *Конкретизация на някои препоръки de lege ferenda!* В заключителната част докторантката дава ценни препоръки за бъдещи действия. Някои от тях обаче са формулирани сравнително общо (напр. „ограничаване на нееднаквото прилагане" или „периодични прегледи на законодателството"). Бих препоръчал в публикация или доклад, основаващ се на дисертацията, тези идеи да се развият по-конкретно – например, да се предложи механизъм за мониторинг на прилагането на директивите във всички държави членки (може би чрез специална агенция или разширяване мандата на съществуваща структура); или идея за приемане на „кодекс" за киберсигурност на ниво ЕС, който да обедини основните принципи, вместо фрагментирано регулиране. Също, препоръката за квантовите компютри е много

актуална – би могла да се подкрепи с конкретика, като призив ЕС да финансира изследвания в областта на пост-квантовата криптография и да приеме законодателна инициатива по темата. Така препоръките биха придобили по-голяма тежест и приложимост.

Направените забележки по-горе в никакъв случай не омаловажават качествата и достойнствата на дисертационния труд. Те са насочени единствено като препоръки за неговото усъвършенстване, ако докторантката реши да го доразвие и публикува като академично издание или серия от статии. В цялост трудът е на високо ниво и забележките по-скоро целят да стимулират бъдещи изследвания на авторката в тази толкова динамична област.

7. Заключение

Дисертационният труд на Маргарита Евгениева Ойсолова отговаря на всички изисквания за съдържание и качество, предявявани към докторски дисертации. Темата е актуална и значима, разработката има ясно формулирана теза, която е логически издържана и последователно доказана чрез анализа. Докторантката демонстрира задълбочено познаване на изследваната област, владеене на понятийния апарат на киберсигурността и европейското право, както и умение да прилага подходящи методи на научно изследване (анализ, синтез, сравнителен подход, исторически и др.). Изводите в труда са обосновани и убедителни, не оставят съмнение относно валидността на научните твърдения.

Особено впечатление прави междудисциплинарният подход на авторката – съчетание на правна рамка с технически и етични аспекти – което обогатява анализа и го прави релевантен за по-широка аудитория. Научните и научно-приложните приноси на дисертацията са безспорни: за първи път у нас е картографирано изцяло европейското законодателство по киберсигурност; идентифицирани са празноти и са предложени решения; резултатите могат да послужат пряко на практиката (законотворческа и правоприлагаща).

Считам, че представеният труд напълно покрива критериите за оригиналност и значимост. Дисертацията демонстрира творчески заложби на докторантката да обобщава и анализира комплексна материя, както и да генерира идеи за нейното развитие.

Въз основа на всичко изложено давам своята положителна оценка на дисертационния труд. Убедена съм, че Маргарита Ойсолова заслужава да ѝ бъде присъдена образователната и научна степен „доктор“ по професионално направление 3.6. Право (научна специалност „Международно право и международни отношения“). Препоръчвам на уважаемото научно жури да гласува за присъждане на исканата степен.

07.10.2025 г.
гр. София

Проф. д.н. Георги Г. Димитров
(Електронно подписано)

OPINION

by Prof. Dr. Georgi Georgiev Dimitrov

University of Library Studies and Information Technologies

Member of the scientific jury

of the doctoral dissertation of

Margarita Evgenieva Oysolova

Professional field: 3.6. Law

Scientific specialty: International Law and International Relations

Scientific supervisor: Prof. Dr. Irena Ilieva

TOPIC: "CYBERSECURITY REGULATION IN THE EUROPEAN UNION - PROBLEMS AND PROSPECTS"

1. Relevance and importance of the topic

The presented dissertation is dedicated to an extremely actual topic – the legal regulation of cybersecurity in the European Union. In the era of digitalization, network and information security are of key importance for the functioning of society, the economy and state institutions. An increasing part of daily activities, public services and business processes rely on information and communication technologies. The increasing number of cyberattacks and cyberthreats on a global scale necessitates the adoption of adequate measures at the supranational level to protect critical networks, systems and data at the supranational level.

The topic is not only timely relevant, but also of great scientific and practical importance. The European Union has adopted several strategic acts in the field of cybersecurity – from the first comprehensive act such as the Network and Information Security Directive (NIS1 of 2016), to the latest initiatives such as its update with Directive (EU) 2022/2555 (NIS2), the Cybersecurity Regulation (Regulation (EU) 2019/881), etc. The study of this evolution is of great importance for legal science and practice, as it allows to assess the results achieved, the existing gaps and challenges, as well as to formulate recommendations for improving the regulatory framework.

The dissertation clearly formulated the thesis that although the EU has made significant strides in cybersecurity legislation (through strategies, regulations and directives), there are still gaps and a need for additions and updates, dictated by the emergence of new threats in cyberspace. This understanding emphasizes the relevance of the study – cybersecurity is a dynamic area in which the legal framework must constantly catch up with technical progress and emerging risks. The topic represents a novelty and a valuable contribution to Bulgarian legal doctrine, as there has been no comprehensive academic study of EU secondary law on cybersecurity in such breadth and depth. Since cybersecurity is an interdisciplinary field, examining it through the prism of EU law is particularly important and useful for introducing common standards and shared values in the digital environment.

It can be concluded that the choice of topic is justified and timely elaborated. The work addresses real needs – to clarify the complex mosaic of EU regulatory acts in the field of cybersecurity and to assist lawyers and experts in understanding and applying them in practice. The relevance is also evident from the latest regulatory amendments from the end of 2022 included in the study, which shows the dissertation's desire to cover the latest developments in the field. The topic is also significant in terms of its prospects – the author's conclusions and recommendations could support the further development of European cybersecurity policy, as well as national efforts to transpose and implement these policies.

2. Brief analytical description of the dissertation work

Margarita Oysolova's dissertation has a volume of 270 pages, of which 252 pages are the main text and 46 pages are appendices and used literature. Structurally, the dissertation is in a classic form - it contains an introduction, three chapters, a conclusion, a list of sources used and appendices. The main text uses over 100 sources, including EU regulatory acts, official documents, strategies, scientific publications and Internet resources. The cited sources are up-to-date and cover both legal acts and contemporary research on the issue under consideration, which testifies to the depth of the research and knowledge of the state of the subject by the doctoral student.

The introduction of the dissertation clearly outlines the object, subject, goals and objectives of the study. The need for a comprehensive review of EU legislation in the field of cybersecurity is argued in order to identify the problems and gaps in it. The main research thesis is formulated and the research methods used are presented - a legal teleological approach, supplemented by a critical analysis of modern scientific developments on the topic, interviews with experts, historical, formal-logical methods (synthesis, deduction), etc. The doctoral student has also defined the boundaries of the study (mainly the period after 2000), which is appropriate given the rapid development of cyber relations in the last two decades. The interdisciplinary context involved is also impressive in the introduction - the relationship between the legal dimensions of cybersecurity and ethical aspects (cyberethics) is examined and the importance of shared standards and values in globalized cyberspace is emphasized. The introductory part is written in a good academic style, introduces the reader to the topic and prepares the ground for the subsequent analysis.

Chapter One is entitled “Strategic Documents” and contains five sections. It examines four main strategic documents of the European Union in the field of cybersecurity. The doctoral candidate begins with an analysis of the first EU Cybersecurity Strategy from 2013, which outlines the Union’s vision for a free and secure cyberspace and introduces five strategic priorities for increasing the level of cybersecurity. The next development is examined – the updated EU Cybersecurity Strategy from 2020, which notes a significant shift towards a more integrated approach and proposes specific measures in response to newly emerging threats. The doctoral candidate makes a comparison between the 2013 and 2020 strategies, highlighting the continuity and differences (e.g. the increased focus on the economic and military aspects of threats in the 2020 strategy). In addition, the chapter analyses the Digital Single Market Strategy (2015) and its update in 2025, focusing on the central role of cybersecurity in building trust among citizens and

businesses in digital services. It is noted that the 2025 version lacks specific texts on cybersecurity, which is an interesting conclusion about the priorities at the moment. Another strategic document reviewed by the author is the EU Security Union Strategy (2020), which emphasizes the need for action in both the physical and digital spheres against threats such as terrorism and cyberattacks. The doctoral candidate skillfully connects these strategic visions with the topic of the dissertation, drawing the general conclusion that at the highest level the EU is aware of the criticality of cybersecurity and is planning measures to strengthen it. The end of the chapter synthesizes the results of the analysis of the strategies – identifying key priorities and gaps, such as the need for common minimum requirements for cybersecurity at national level and improved coordination in cross-border incidents. The first chapter is structured logically, demonstrates knowledge of the political context and contributes by systematizing the strategic foundations on which the legislation is based.

Chapter Two is entitled "Cybersecurity Regulations" and covers eight sections. In this part, the doctoral candidate examines in detail the main EU regulations (regulatory acts) relevant to cybersecurity. It began with the regulatory framework for electronic identification and authentication services - Regulation (EU) No 910/2014 (eIDAS) was analyzed, which creates a framework for secure electronic transactions and trusted services within the EU. The author highlights the importance of eIDAS for increasing trust in digital interactions, including for citizens, businesses and public authorities. Then, the relationship between personal data protection and cybersecurity is examined. The doctoral candidate analyzes the General Data Protection Regulation - GDPR (Regulation (EU) 2016/679), emphasizing its role in unifying security standards for the processing of personal data in a digital environment. The special Regulation (EU) 2018/1725, which regulates data protection in the EU institutions, is also examined – the close connection between cybersecurity and the protection of personal information is correctly taken into account. The doctoral student makes an extremely significant analysis of Regulation (EU) 2017/2394 on cooperation between national consumer protection authorities, the "Cybersecurity Act" (Regulation (EU) 2019/881), Regulation (EU) 2022/2554 (DORA) on digital operational resilience in the financial sector – a very recent act (adopted at the end of 2022), which the author correctly assessed as relevant – financial services are highly digitalized, and DORA aims to increase their cyber resilience.

Chapter Three is entitled “Cybersecurity Directives” and is structured in nine sections. This is the most voluminous part of the work, analyzing eleven EU directives related to various aspects of cybersecurity. The doctoral student begins with Directive 2002/58/EC (ePrivacy Directive, amended by Directive 2009/136/EC), which regulates the protection of personal data and the privacy of communications in the electronic communications sector. The author provides a synthesized overview of the content of the 2009 amendments, which strengthen users’ rights and requirements for operators (e.g. the introduction of a consent requirement for cookies, notification of security breaches, etc.). The main objectives are stated – better protection of online privacy and strengthening trust in digital services. The doctoral student identifies problems and weaknesses in this directive (e.g. challenges to its implementation in connection with rapid technological development), which demonstrates a critical approach. Subsequently, Directive 2013/40/EU on attacks against information systems (cybercrime), Directive 2007/64/EC (PSD) on payment services, as well as Directive (EU) 2015/1535 (procedure for the provision of information in the field of technical standards for information society services), Directive (EU) 2016/680 (the so-called Data Protection Directive in the field of police and judicial cooperation) and Directive (EU) 2016/2102 on the accessibility of public sector websites and mobile applications were analyzed in sequence.

The culmination of the third chapter is dedicated to the most important directives directly in the field of cybersecurity - Directive (EU) 2016/1148 of the European Parliament and of the Council (the so-called Network and Information Security Directive, or NIS1). It is examined in detail. The dissertation explains that this is the first comprehensive European legislative act aimed at achieving a high common level of network and information security in the Union. The main requirements of the directive are outlined - each Member State must designate national competent authorities for cybersecurity, establish computer

incident response teams (CERT/CSIRT), adopt a national cybersecurity strategy, and identify operators of essential services and digital service providers that must comply with security and incident notification measures. The author notes that as a result of the adoption of NIS1 in the EU, an increase in the general level of cybersecurity has been achieved, but gaps also remain, which necessitated follow-up actions.

Secondly, the dissertation analyses Directive (EU) 2022/2555 (NIS2) – the updated version of the Network and Information Security Directive, adopted in December 2022 as a replacement for NIS1. The doctoral student makes a comparison between NIS1 and NIS2, pointing out how NIS2 builds on its predecessor: expands the scope by adding new sectors and types of vulnerable entities; introduces stricter requirements for risk management and accountability; strengthens coordination and information exchange between Member States; provides for more serious sanctions for non-compliance. It is rightly pointed out that NIS2 is part of the EU's response to increasing digitalisation and evolving cyber threats. The paper emphasises that NIS2 aims to address the weaknesses identified in NIS1 and to further enhance the level of cybersecurity in the Union in the years to come.

Along with NIS2, the dissertation also examines Directive (EU) 2022/2557 on the resilience of critical entities (CER). Although CER is more focused on the physical resilience of critical infrastructure, the author rightly places it within the overall digital security strategy, noting that it complements NIS2 and reflects the need for increased protection against new complex threats that key sectors face in the context of digitalization.

It is characteristic of the third chapter that for each of the analyzed directives, the author also presents information on its transposition into Bulgarian legislation. This gives additional practical value to the study. For example, it is mentioned that Directive 2016/1148 (NIS1) has been transposed into Bulgarian law through the Cybersecurity Act of 2018, and the main provisions of this law are discussed. In a similar way, national measures under the remaining directives are noted - whether and how they have been implemented in Bulgarian regulations. This approach shows the ability to connect the supranational framework with the national context, which is particularly valuable for assessing the effectiveness and applicability of European policies in our country.

In summary, the third chapter provides a comprehensive overview of the directive basis of European cybersecurity. The dissertation has systematically set out the content of each act, identified its objectives, scope, contribution and shortcomings, as well as its interaction with the others. At the end of the chapter, a Conclusion logically follows, in which the author synthesizes the conclusions drawn in the previous parts and confirms the thesis of the study. It is stated that the EU has made progress through various legislative measures, but the legal framework must develop dynamically in view of the emergence of new technologies and threats. The dissertation particularly emphasizes the need for more frequent updating of regulatory acts and proactive identification of emerging risks (for example, quantum computers as a future challenge for cybersecurity). General recommendations de lege ferenda are formulated - for updating the legal framework in relation to new technologies, for reducing fragmented implementation in different Member States, for strengthening coordination and exchange of good practices, etc. The conclusion is well-reasoned, shows that the set goal has been achieved, and clearly indicates the original contribution of the work: the first of its kind in our country, a comprehensive study of European cyber legislation, revealing its trends, problems, and opportunities for development.

Overall, the dissertation makes a very good impression with its structure, precision and comprehensiveness. The doctoral student demonstrates excellent awareness of the topic, confidently handles the conceptual apparatus of cybersecurity and EU law, is able to analyze and synthesize information from multiple sources. The text is written in an academic style, the argumentation is consistent, and the conclusions are convincingly substantiated. There is a skillful combination of the descriptive review of the regulatory framework with a critical analysis of its shortcomings and effectiveness. In this way, the doctoral

student achieves the set goal and proves her thesis that the existing European legal framework for cybersecurity, although advanced, needs further improvement in order to adequately respond to the rapidly changing environment.

3. Evaluation of scientific and applied scientific contributions

The contributions of Margarita Oysolova's dissertation can be systematized in two main areas: scientific (theoretical) contributions and applied (practical) contributions.

Scientific contributions

First of all, the work represents the first of its kind in Bulgarian specialized literature attempt to comprehensively study the secondary EU law in the field of cybersecurity. The doctoral candidate has carried out an impressive study in scope, including an analysis of 6 strategic documents, 8 regulations and 11 EU directives related to cybersecurity. The content of all these acts is presented in a synthesized form, which facilitates their understanding even by readers outside the legal community (e.g. IT specialists who have to implement these requirements). Such a broad scope and synthesis is a significant scientific contribution in itself, as it brings together the otherwise scattered regulatory framework in one place, providing the “big picture” of European cybersecurity policy.

In second place, the author has made an original comparative analysis of key documents: for example, the comparison between the two EU cybersecurity strategies (2013 and 2020) and the derivation of trends and changes in the policy approach; the comparison between the NIS1 Directive and the NIS2 Directive and the identification of specific improvements and extensions in the new directive. These comparisons contribute to scientific knowledge as they shed light on the evolution of concepts and priorities within the EU.

In third place, the doctoral candidate has identified the main problems and weaknesses in each of the reviewed regulatory acts and policies. This is not a simple descriptive enumeration, but is justified by an analysis of practice – it is indicated to what extent individual member states have managed to implement the requirements, where difficulties have been encountered, what amendments have been imposed at the EU level as a result of identified weaknesses. Thus, the work has a clear critical focus and goes beyond the framework of a compilation of texts – the author forms independent conclusions regarding the effectiveness of the existing framework.

In fourth place, concrete ideas de lege ferenda for improving the European cybersecurity framework are proposed. The doctoral student formulates a number of recommendations based on the findings of the analysis: the need for a more flexible mechanism for periodically updating the legislation in view of emerging new technologies (e.g. blockchain, quantum computers); unification and clarification of concepts and requirements to avoid uneven application in the Member States; strengthening cross-border coordination mechanisms in cyber incidents; integration of cyber ethics standards and raising awareness. These recommendations demonstrate an ability for predictive thinking and a contribution in theoretical terms – guidelines for the development of law are proposed, which can be the basis for future scientific discussions and legislative initiatives.

Last but not least, the interdisciplinary contribution of the work should be noted. The doctoral candidate combines legal analysis with knowledge from the field of information security and ethics. The inclusion of the concept of "cyberethics" and the discussion of the ethical and legal dimensions of cybersecurity in the EU strategic framework demonstrates an innovative approach to the topic, placing it in

a broader value context. This contributes to the scientific debates on the need to combine technological solutions with ethical and legal principles.

Scientific and applied contributions

Margarita Oysolova's work also has a clearly expressed applied significance.

First of all, the systematization of European cybersecurity legislation in one work is a practical convenience for various target groups – lawyers who work or are about to work on cybersecurity issues can use the dissertation as a reference book for the relevant acts and their basic provisions; technical experts in information security would find in it a comprehensible presentation of their legal obligations and frameworks; public authorities and politicians – a consolidated source when forming policies and draft laws in the field. The author herself explicitly notes that her aim is for the work to be useful and understandable not only for lawyers, but also for "non-lawyers, technical persons" and even for ordinary Internet users who are affected by cybersecurity issues. In this sense, the dissertation fulfils an educational and practical function.

Next, the analysis of the transposition of directives into national legislation is a valuable practical contribution. In this way, the work serves as a "bridge" between European and Bulgarian law – it shows where Bulgaria stands in the implementation of the requirements, which directives have already been implemented (e.g. through the Cybersecurity Act, the E-Government Act, amendments to sectoral laws, etc.), and whether there are any lags or difficulties. This is useful for national institutions tasked with the implementation of these policies, and can serve to identify areas that require additional efforts or amendments in our country. For example, if a directive (such as NIS2) is still in the process of transposition, Oysolova's analysis can guide the legislator on the key points to pay attention to.

Practical contribution are also de lege ferenda proposals, which have a specific focus. They could be used by the European institutions in future revisions of the regulatory framework or in the preparation of new strategies. The doctoral student's proposals, such as the inclusion of quantum security in policies, more frequent reviews of legislation, expert panels on digitalization, etc., are realistic and feasible measures. Although formulated in general terms, they provide constructive guidelines that show where the weak points are and how they could be addressed. This is a valuable contribution to practice because it translates scientific conclusions into potential actions.

As an overall assessment, it can be said that the contributions of the dissertation are significant both for the development of scientific theory in the field under consideration, and with immediate practical applicability. The work enriches the doctrine with new generalizations, classifications and ideas, and at the same time is able to support the practical process of lawmaking and law enforcement in the field of cybersecurity.

4. Evaluation of publications on the topic of the dissertation

Doctoral student Margarita Oysolova has presented three scientific publications that reflect the main research theses and results of the dissertation. All publications are thematically related to the dissertation work and represent parts of the researched issues, which shows the author's consistency and commitment to the topic throughout the entire period of study.

The first publication is a scientific report on the topic "Transposition of Directive (EU) 2016/1148 into Bulgarian legislation", included in the collection of reports of the XI National Conference of Doctoral

Students in the Field of Legal Sciences (2021). In this work, the doctoral student examines the process of introducing the requirements of Directive NIS1 (2016/1148) into national law, analyzing the Cybersecurity Act and related by-laws. The publication reflects parts of the third chapter of the dissertation, which examines the directives and their application in Bulgaria. In it, Oysolova reaches conclusions about the degree of compliance of Bulgarian legislation with European standards, points out the challenges (e.g. coordination between national competent authorities, the scope of designation of operators of essential services, etc.) and thus directly contributes to proving the thesis that although Bulgaria has transposed NIS1, further development (subsequently NIS2) requires additional efforts.

The second publication is a report "Cybersecurity Act", presented at the XII National Conference of Doctoral Students in the Field of Legal Sciences (2022). This report covers the analysis of Regulation (EU) 2019/881, dedicated to ENISA and cybersecurity certification - this same act is also discussed in detail in the second chapter of the dissertation. In the publication, the doctoral student has set out the main objectives and provisions of the "Cybersecurity Act", probably also considering the first steps in its implementation (since, in 2022 the first European certification schemes were already established). This report is valuable because it demonstrates that the author is up to date with the latest developments and participates in the scientific discourse on them even before the dissertation was finalized. The material supports the thesis of the dissertation, as it analyzes one of the key new EU tools for increasing cybersecurity - certification - and assesses its importance and challenges.

The third publication is “A Comparison between Directives 2016/1148 and 2022/2555 of the European Parliament and of the Council”, which at the time of submission of the documents was listed as forthcoming publication (2024). In it, Oysolova makes a direct comparison between the old and new Network and Information Security Directives (NIS1 and NIS2), summarizing in a synthesized form the similarities and differences. This article reflects very clearly the scientific contribution of the dissertation – namely the comparison of the two regimes and the conclusions on the need for changes. It is expected that the author will have pointed out in the publication that progress has been made since the adoption of NIS1, but gaps have been identified (limited scope, insufficient sanctions, lack of uniform security requirements, etc.), which NIS2 addresses by expanding the scope, stricter measures and increased supervision. This work practically brings to the fore one of the main theses of the dissertation - the development of European legislation continues evolutionary, with new acts building on previous ones to achieve a higher level of cyber resilience.

All three publications testify that the doctoral student has actively worked and discussed her topic in scientific forums, receiving, presumably, feedback and the opportunity to further improve her research. They also show that the main parts of the dissertation (analysis of the directives, analysis of the regulations) were subjected to a “pilot” presentation and criticism, which gives additional credibility to the results. The publications fully correspond to the topic of the dissertation, reflect her main contributions and are authored solely by the doctoral student, which means that she independently developed and presented these results. This meets the requirements for doctoral students for a minimum of publications on the topic and I can confidently say that the presented works cover and even build on the necessary minimum.

5. Evaluation of the abstract

The abstract of the dissertation is prepared precisely and in accordance with the established requirements for this type of academic document. The structure of the abstract is clear - it contains a general description of the dissertation, including the goal, subject, tasks, thesis, methodology and expected results; a description of the volume and structure of the work itself follows; the content of each chapter and the conclusion are briefly presented; finally, the contributions of the study and the publications on the topic are listed.

In view of the above, I believe that the abstract fully meets the requirements for an academic abstract accompanying a doctoral dissertation. It is structured correctly, written in a concise and clear style, and provides an overall picture of the content and contributions of the work, without going into unnecessary details. The abstract successfully fulfills its role of briefly presenting the research and achievements of the doctoral student, and for this reason I give it a positive assessment.

6. Notes and recommendations

Margarita Oysolova's dissertation has undeniable merits - a topical focus, a wide scope, depth of analysis and clearly formulated results. However, in the spirit of academic criticality and with the aim of future upgrading of the research (for example, when publishing as a monograph), I allow myself to make the following remarks and constructive recommendations:

1. *Regarding the scope of the study*. The doctoral student has included a very wide range of regulatory acts – practically all important strategies, regulations and directives, even indirectly related to cybersecurity. This comprehensive approach is commendable, but it carries the risk that the analysis in places will remain less in-depth. In some places in the work, the descriptive presentation dominates over the critical analysis due to the vast amount of material to cover. My recommendation is that, if published, the doctoral student should consider focusing on a narrower range of key acts or grouping them by thematic areas (for example, a separate consideration of the data protection framework, a separate consideration of the critical infrastructure framework, a separate consideration of criminal law aspects, etc.). This would allow for an even deeper examination of the internal connections and contradictions, without sacrificing completeness.
2. *Defining the concept of "cybersecurity"*. In the paper, the term "cybersecurity" is used in a broad context, encompassing many related areas (accessibility, electronic certification services, consumer protection, payment services, etc.). This reflects the reality that cybersecurity is pervasive, but it would be good to outline the scope of the term more clearly. For example, the reader may wonder why the Payment Services Directive or the Technical Standards Directive are considered here – the explanation is there, but it is implicit. It is advisable for the author to explicitly define or discuss the term "cybersecurity" at the beginning of the paper and to justify the criteria by which she decides which acts are "in the field of cybersecurity". This would prevent possible confusion and would strengthen the methodological framework of the study.
3. *Balance between normative and doctrinal analysis*. The dissertation is strong in legal (normative) analysis – the content of the acts and what has been done in practice has been studied in detail. However, at times there is a lack of a more in-depth discussion of the doctrinal sources and scientific views on the topic. For example, it would be useful to cite the opinion of authors on the effectiveness of NIS1 or criticisms from the scientific community towards GDPR in the context of cybersecurity. My recommendation is that in a more developed version of the work, the doctoral student integrate more comparative analysis with the opinions of established European experts and researchers (e.g. assessments from ENISA reports, academic articles on NIS2, analyses of the implementation of the Cybersecurity Act, etc.). This would give it even higher scientific value and would show a dialogue with the available literature, in addition to the normative texts.
4. *Analysis of the global context*. The focus of the dissertation is on EU law, which is justified given the topic and the scientific specialty. However, cybersecurity is a global issue and it would be interesting to take into account international efforts and standards that influence or correspond to EU law. For example, the Council of Europe Budapest Convention on Cybercrime, NATO Cyber Defense Framework, ISO/IEC standards for information security, UN guidelines in the digital sphere, etc. It is advisable in the introduction or conclusion, even if telegraphically, to make a connection between the European framework and the broader international context - this would

fully emphasize the understanding that EU efforts are part of the global picture and that there is interaction between the different levels of legal regulation of cybersecurity.

5. *Specification of some recommendations de lege ferenda*. In the concluding part, the doctoral candidate provides valuable recommendations for future actions. However, some of them are formulated relatively generally (e.g. “limiting uneven application” or “periodic reviews of legislation”). I would recommend that in a publication or report based on the dissertation, these ideas be developed more specifically – for example, proposing a mechanism for monitoring the implementation of the directives in all member states (perhaps through a special agency or extending the mandate of an existing structure); or an idea for adopting a cybersecurity “code” at EU level that would unify the main principles, instead of fragmented regulation. Also, the recommendation on quantum computers is very relevant – it could be supported with specifics, such as a call for the EU to fund research in the field of post-quantum cryptography and to adopt a legislative initiative on the topic. This would give the recommendations greater weight and applicability.

The remarks made above in no way belittle the qualities and merits of the dissertation work. They are intended solely as recommendations for its improvement, should the doctoral student decide to further develop and publish it as an academic publication or a series of articles. Overall, the work is of a high level and the remarks are rather intended to stimulate future research by the author in this very dynamic field.

7. Conclusion

The dissertation work of Margarita Evgenieva Oysolova meets all the requirements for content and quality set for doctoral dissertations. The topic is relevant and significant, the work has a clearly formulated thesis, which is logically sustained and consistently proven through analysis. The doctoral student demonstrates in-depth knowledge of the research area, mastery of the conceptual apparatus of cybersecurity and European law, as well as the ability to apply appropriate methods of scientific research (analysis, synthesis, comparative approach, historical, etc.). The conclusions in the work are justified and convincing, leaving no doubt about the validity of the scientific statements.

The author's interdisciplinary approach is particularly impressive - a combination of legal framework with technical and ethical aspects - which enriches the analysis and makes it relevant to a wider audience. The scientific and applied scientific contributions of the dissertation are undeniable: for the first time in our country, European cybersecurity legislation has been fully mapped; gaps have been identified and solutions have been proposed; the results can be directly used in practice (legislative and law enforcement).

I believe that the presented work fully meets the criteria for originality and significance. The dissertation demonstrates the doctoral student's creative abilities to summarize and analyze complex material, as well as to generate ideas for its development.

Based on all the above, I give my positive assessment of the dissertation work. I am convinced that Margarita Oysolova deserves to be awarded the educational and scientific degree "Doctor" in the professional field 3.6. Law (scientific specialty "International Law and International Relations"). I recommend that the esteemed scientific jury vote for awarding the requested degree.

07.10.2025 Sofia

Prof. George G. Dimitrov, PhD, DSc.
(Electronically signed)