

ПРИМЕРНА ГЛАВА ОТ КНИГАТА

„ПРОБЛЕМИ НА ДОКАЗВАНЕТО НА ГРАЖДАНСКА ОТГОВОРНОСТ В ЦИФРОВОТО ПРОСТРАНСТВО НА ЕС“¹

Въведение в цифровото пространство на ЕС

Тази част е посветена на понятието „цифрово пространство на ЕС“, разбрано като нов вид пространство на европейска интеграция със свои специфични обществени отношения и предизвикателства при регулиране. Зачитава се тезата, че цифровото пространство е част от вътрешния пазар на ЕС както в политически, така и в правен смисъл, но постепенно то става обект на самостоятелен слой интеграционна политика – дигиталната политика.

Разгледана е еволюцията на дигиталната политика на ЕС – от 80-те години на 20. век до днес, когато тя достига своята зряла фаза. Анализирана е по-специфично и политиката на ЕС по отношение на гражданската отговорност в цифровото пространство.

Очертават се основните предизвикателства пред нея. Зачитава се необходимостта от отклонения от тежестта и стандарта на доказване, като инструмент за справяне с предизвикателствата на дигиталната трансформация.

Цифровото пространство обозначава нов вид пространство в ЕС, което има своите особени характеристики и предизвикателства. Едно от най-съществените предизвикателства е създаването на доверие в технологиите и институциите на дигиталния

¹ © 2025 Димо Господинов, всички права запазени

Настоящата глава се споделя за промоционални и образователни цели. При цитиране или споделяне, моля, посочвайте автора. За повече информация и актуализации:

<https://www.dimogospodinov.com/book>

свят, които по природата си са не само нови за човека, но и неразбираеми. Институциите на Съюза осъзнават това и методично подхождат към цифровото пространство с различни политики, насочени към създаване и укрепване на доверието.

Ключов елемент от механизмите за създаване на доверие е гражданската отговорност, която е поставена под сериозен натиск от новите технологии. За да отговори на предизвикателствата, ЕС е готов, както винаги, да прояви изобретателност и иновативност. Започва реформа на рамката гражданската отговорност, чиято цел е да гарантира еквивалентно третиране на случаите от цифровото пространство с тези извън него.

Поради своите специфични функции отклоненията от тежестта и стандартът на доказване се оказват любим инструмент на ЕС в цифровото пространство, тъй като позволяват да се балансират икономическите интереси с ефективната защита на основни права и интереси. Равновесието се постига като на по-силната страна в дигиталното правоотношение – доставчици на цифрови услуги и съдържание, се прехвърля все повече отговорността да доказва факти от спорното правоотношение.

I. Цифровото пространство като част от вътрешния пазар

Цифровото пространство е обект на дигиталната политика на ЕС, която е част от развитието на вътрешния пазар, и представлява допълнителен слой на общностна интеграция, обусловен от функционирането на интеграционните процеси в нов тип пространство – цифровото. Това е вярно както в политически, така и в правен смисъл, тъй като компетентността на Съюза спрямо тези пространства произтича от едно и също основание. Това обстоятелство предопределя голяма част от принципите и приоритетите при регулиране на цифровото пространство. Все пак инициативите на общностните институции в дигиталната област постепенно се множат и еволюират, за да стигнат до днешния момент, когато цифровата политика на ЕС изглежда съвсем самостоятелна със свои собствени приоритети.

Една от причините за това обособяване са специфичните характеристики на предмета на регулиране – дигиталните технологии, и предизвикателствата от икономическо, социално, но и правно естество, които произтичат от този факт. Водещ принцип на политиката на ЕС е изграждането и поддържането на атмосфера на доверие в

цифровото пространство, за да се стимулира по-бързо възприемане на новите технологии и по-голям растеж на икономиката.

§ 21. Регулиране на цифровото пространство

1. Какво е цифрово пространство

Цифровото пространство² е нов вид пространство, дефинирано и обусловено от съществуването на информационни и комуникационни технологии (ИКТ). То е виртуално пространство, създадено от ИКТ и предпоставено от тяхната употреба под най-различна форма, при която възникват нови модели на взаимодействие между всякакъв род лица (физически, юридически, държавата)³. Това понятие е фокусирано върху пространственото измерение и в този смисъл не трябва да се бърка с „дигитална среда“, термин, обхващащ цялата екосистема, в която се извършва дигиталната интеракция, включително хардуер, софтуер и мрежова връзка⁴.

В това пространство кипи все повече икономическа дейност и то неминуемо става част на вътрешния пазар на ЕС. И тук, както и в аналоговата среда, са налице бариери пред икономическата интеграция на държавите членки от най-различно естество – икономически, технологични, физически, социални и други. Специфичното обаче е, че основното благо, което е обект на трансакции, както и преградите пред тях се разгръщат в цифровото пространство⁵. Тази качествено нова ситуация налага постепенно еволюиране на дигитална политика на ЕС.

2. Дигитална политика на ЕС

Дейностите, които ЕС предприема, за да се регулира цифровото пространство – актове за хармонизация на законодателството на държавите членки, инвестиционни програми и фондове, международни договори, стратегии, декларации и т.н., могат да се обобщят под понятието „дигитална политика“⁶. Тя е хоризонтална по своето естество,

² *Digital space*, еквивалентно на понятието „киберпространство“ (*cyber space*).

³ Дефиниция съгласно **Mărcuț, M.** *Crystallizing the EU Digital Policy ...*, p. 6.

⁴ Вж. дефиниция в чл. 2, пар. 1, т. 9 от Директива (ЕС) 2019/770 на Европейския парламент и на Съвета от 20 май 2019 г. за някои аспекти на договорите за предоставяне на цифрово съдържание и цифрови услуги (ОВ L 136, 22.5.2019, p. 1–27) (DCSD).

⁵ Например недоверие в новите технологии или страх от навлизане в личното пространство – вж. подробно изложение в **Mărcuț, M.** *Op. cit.*

⁶ *Digital policy*, вж. гл. 4 на **Mărcuț, M.** *Op. cit.*

насочена към всички сектори на икономическия и обществения живот⁷. Такава политика или компетентност не е предвидена специално в учредителните договори, но в рамките на вътрешния пазар са все по-значима част от активността на европейските институции.

§ 22. Развитие на дигиталната политика на ЕС

1. Зародиш на дигиталната политика

Това, което днес наричаме дигитална политика, има своят зародиш в т.нар. информационно общество – общностна политика, стартирала още през 1985 г. в изпълнение на новосъздадената компетентност на ЕИО по чл. 24 ЕЕА⁸, свързана с научните изследвания и технологичното развитие. В своята Рамкова програма за периода 1987–1991⁹ г. Европейската комисия си поставя за цел подготвяне на информационно и комуникационно общество, разбирано като създаване на синергии в ИКТ сектора чрез подпомагане на проучвания¹⁰.

Тази политика продължава своето развитие и през 90-те години, като до началото на 21. век тя постепенно е изменила акцента си от изследователска дейност към създаване на цифрова инфраструктура и справяне със социалните предизвикателства на дигиталната трансформация. Навлизането на интернет променя всички сфери на обществения живот и вече се заговаря за общество и икономика, базирани на знанието¹¹. Все по-големият мащаб на предизвикателствата, свързани с цифровото пространство, означава, че рамката на политиката по научни изследвания и технологично развитие е твърде тясна за съответната необходимост от хармонизация на общностното право. Постепенно дигиталната

⁷ Вж. Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите – Ново начало за Европа: Моят дневен ред за работни места, растеж, справедливост и демократична промяна. Политически насоки за следващата Европейска комисия. Страсбург, 15 юли 2014 г., стр. 6.

⁸ Единен европейски акт от Люксембург, 1985 г.

⁹ Решение на Съвета от 28 септември 1987 г. относно Рамковата програма за дейности на Общността в областта на научните изследвания и технологичното развитие (1987–1991).

¹⁰ Чл. 1 и т. 2.1 от Анекс II от Рамковата програма.

¹¹ Решение № 1513/2002/ЕО на Европейския парламент и на Съвета от 27 юни 2002 г. относно Шестата рамкова програма на Европейската общност за научни изследвания, технологично развитие и демонстрационни дейности, допринасящи за създаването на Европейското изследователско пространство и за иновациите (2002–2006).

проблематика се премества в политиката, свързана с вътрешния пазар^{12, 13}. Това е особено видимо след ограничаване на компетентността на Съюза по въпросите с научните изследвания и технологичното развитие с влизането в сила на Договора от Лисабон¹⁴.

2. Вътрешен пазар

Вътрешен пазар е понятие, описващо сливането на националните пазари на участващите в ЕС държави членки като форма на икономическа интеграция чрез прилагане на гарантираните основни свободи на движение (на стоки, хора, услуги и капитал), чрез гарантиране на свободна конкуренция и чрез приемането на мерки на хармонизация в различни области, предвидени в учредителните договори на ЕС¹⁵. Хармонизацията от своя страна представлява дейността на Съюза по приемане на общи правила чрез неговите институции и в рамките на предоставената му компетентност¹⁶. Основанията в договорите за такова нормотворчество са или общите по чл. 114 и 115 ДФЕС, или специални такива, уреждащи свободите на движение, както и различни секторни политики¹⁷.

3. Цифров единен пазар

Именно като част от вътрешния пазар дигиталната политика получава своя облик, израз на който е възникването на понятието „Цифров единен пазар“ (ЦЕП), което се използва за първи път през 2010 г. в Програма в областта на цифровите технологии за Европа (Програмата), част от Стратегията „Европа 2020“¹⁸. Основната цел на плана е извличането на „устойчиви икономически и обществени ползи от един ЦЕП, основан на бърз и ултрабърз интернет и приложения с висока оперативна съвместимост“¹⁹.

¹² Първите такива актове на хармонизация са Директивата за електронния подпис от 1999 г. и Директивата за електронната търговия от 2000 г.

¹³ По-подробно и задълбочено изложение на еволюцията на ЦЕП – от информационното общество до вътрешния пазар вж. **Mărcuț, M.** Crystalizing the EU Digital Policy: An Exploration into the Digital Single Market. Springer International Publishing, 2017, Chapter 2.

¹⁴ Става дума за това, че съгласно Договора от Лисабон (2009) компетентността на Съюза по въпросите на научните изследвания и технологичното развитие е споделена, но ограничена – чл. 4, пар. 3 ДФЕС.

¹⁵ Дефиницията се отнася и за „единен пазар“ и „общ пазар“, които се приемат за еквивалентни – вж. **Христов, Х.** Вътрешен пазар и основни свободи на движение в правото на ЕС. София: Сиела, 2018, стр. 25

¹⁶ Хармонизацията в широк смисъл включва както уеднаквяването на законодателствата (например с регламенти), така и хармонизирането им в тесен смисъл, както и тяхното координиране – пак там, стр. 46

¹⁷ Вж. по-подробно **Христов, Х.** Вътрешен пазар..., стр. 47 и сл.

¹⁸ Европа 2020, Стратегия за умен, устойчив и включващ растеж.

¹⁹ Програма в областта на цифровите технологии за Европа. Европейска комисия, 2010, Introduction, т. 1.

Признание за стратегическото значение на цифровото пространство и първи силен тласък на дигиталната политика идва през 2015 г. с новата комисия на председателя Юнкер, която приема своята стратегия за цифров единен пазар за Европа²⁰ (Стратегия). Според този документ ЦЕП е място, където „свободното движение на стоки, хора, услуги и капитал е гарантирано и хората и предприятията имат безпроблемен достъп до онлайн дейности в условията на лоялна конкуренция и високо равнище на защита на личните данни и на данните на потребителите, независимо от тяхната националност или мястото им на пребиваване²¹.

Видно е, че дефиницията на ЦЕП в голяма степен възпроизвежда понятието за вътрешен пазар по това, че е място, в което са гарантирани четирите основни свободи на движение заедно и защитата на конкуренцията. Отличителната характеристика обаче е, че той реферира към „онлайн дейности“, т.е. цифровото пространство, както и включва един нов слой защита – тази на данните²².

4. Развитие след ЦЕП

След изтичане на мандата на Комисията „Юнкер“ понятието ЦЕП все по-рядко се използва, за да обозначи дигиталната политика на ЕС²³. Днес в нейния обхват и съответния ресор на ЕК – „Европа, подготвена за цифровата ера“²⁴, както и в изпълнение на програмата „Цифрово десетилетие до 2030 г.“ влизат приоритети като ориентирана към човека дигитална среда, преодоляване на цифровото разделение между държавите членки, гарантиране цифровия суверенитет на съюза и други²⁵. Въпреки това актовете за хармонизация на законодателството в цифровото пространство продължават да се приемат

²⁰ Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите – Стратегия за цифров единен пазар за Европа (COM(2015) 192 final).

²¹ Стратегия за цифров единен пазар (Digital Single Market Strategy). Въведение, съгласно официалния превод

²² И това не е случайно, тъй като страхът от нарушаване на неприкосновеността на личното пространство е една от основните прегради пред масово включване на гражданите във виртуалната икономика – вж. Програма за цифровите технологии, 2010, стр. 12, фиг. 3.

²³ Ето един пример – The ubiquitous digital single market | Fact Sheets on the European Union | European Parliament. Достъпно на: <https://www.europarl.europa.eu/factsheets/en/sheet/43/the-ubiquitous-digital-single-market>

²⁴ Съгласно състава на Първата комисия на Урсула фон дер Лайен – https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en

²⁵ Вж. чл. 3 от Решение (ЕС) 2022/2481 на Европейския парламент и на Съвета от 14 декември 2022 г. за създаване на политическа програма „Цифрово десетилетие“ до 2030 г. (ОВ L 323, 19.12.2022, р. 4–26)

най-често на общите основания по чл. 114 и 115 ДФЕС²⁶, с някои значими изключения²⁷. Внимателният прочит на текста и мотивите на съответните актове показват, че икономическите съображения и стремежът за преодоляване на прегради в ЦЕП не са изоставени. Приоритетите и имената на стратегиите се променят, но същността на интеграционния процес се запазва.

II. Политики на ЕС в рамките на цифровото пространство

Европейската политика в дигиталната сфера възниква като необходимост да се посрещнат икономическите, политическите и демографските последици на цифровата революция, като едновременно с това се опазят европейските ценности. Цифровата трансформация нерядко влиза в конфликт с правата на човека, което ражда отговор в уникалната по рода си политика на ЕС, която търси баланс между икономически цели и опазване на права.

Както беше споменато по-рано, материалната компетентност на ЕС да осъществява политика в областта на цифровото пространство почива върху общите основания за регулиране на вътрешния пазар (чл. 114 и 115 ДФЕС), наричани имплицитни основания, както и специални норми като чл. 16 ДФЕС, наричани експлицитни или изрични основания²⁸.

В изпълнение на компетентността си ЕС осъществява нормативна дейност чрез разнообразен инструментариум от задължителни и незадължителни механизми. Сред задължителните инструменти се употребяват директивите и регламентите, незадължителните включват преди всичко кодекси за поведение, препоръки и насоки, които насърчават доброволно сътрудничество и саморегулация. В последните години се наблюдават все по-често т.нар. меки механизми като бели книги, етични принципи, както и инвестиционни програми, с които се прокарват нормативни изисквания²⁹. Това разнообразие от подходи цели да балансира иновациите със защитата на основните права и

²⁶ Например регламентите eIDAS, AIA, DSA, DMA и др.

²⁷ Например GDPR, приет на основание чл. 16 ДФЕС.

²⁸ В този смисъл *La politique européenne du numérique*, p. 256 et seq.

²⁹ Вж. например NextGenerationEU. Достъпно на: https://next-generation-eu.europa.eu/index_en

устойчивото развитие, като същевременно утвърждава ЕС като глобален лидер в дигиталните регулации³⁰.

С оглед своя фокус и приоритети, развитието на дигиталната политика на ЕС може условно да се раздели на две фази. Първата е до 2019 г., при която се поставят основните на регулаторната рамка и се преодоляват бариери пред ЦЕП. От първия мандат на Урсула фон дер Лайен нататък политиката на ЕС навлиза в своята зряла фаза, при която регулирането се засилва в подкрепа на безопасността на дигиталното пространство и цифровия суверенитет на Съюза³¹. В следващите страници ще се спра накратко на характеристиките на двата етапа и основните актове, които придават техния облик.

§ 23. Първи етап: до 2019 г.

Началото на дигиталната трансформация има своите първи признаци в бизнес организационните процеси още през 60-те и 70-те години на 20. век. Но тя истински си проличава през 90-те години, когато хората започват да използват цифрови средства за комуникация, лични взаимоотношения, забавления, консумация, образование, работа и т.н. По това време започват и първите стъпки от дигиталната политика на ЕС, която постепенно ще се развива, създавайки регулаторни рамки на основните типове отношения в цифровото пространство.

1. Първи стъпки

Първият стратегически документ на ЕС по темата е от 1997 г. и е озаглавен „Европейска инициатива в електронната търговия“³². Той има за цел повишаване на конкурентоспособността на Съюза на световния пазар чрез преодоляване на три ключови предизвикателства пред електронната търговия: обновяване на инфраструктурата, създаване на стимулираща регулаторна рамка и изграждане на подходяща бизнес среда. За постигане на тези цели е необходимо премахване на законодателни бариери, свързани с електронни разплащания, договори, съобщения, сигурност и защита на данните, защита на

³⁰ Цялостно изложение на проблематиката вж. *La politique européenne du numérique*, p. 231 et seq.

³¹ Преглед на еволюцията на дигиталната политика на ЕС, както и по-подробна аргументация на причините за разделянето ѝ на два етапа вж. **Stengg, W.** *Digital Policy in the EU: Towards a Human-Centred Digital Transformation*. Edward Elgar Publishing, 2024.

³² Съобщение на Комисията до Съвета, Европейския парламент, Икономическия и социален комитет и Комитета на регионите – Европейска инициатива в областта на електронната търговия (COM(97) 157 final).

интелектуалната собственост и други. Първите актове в подкрепа на тази политика са Директивата за електронната търговия³³, както и Директивата за електронните подписи³⁴.

2. Защита на данните

Регулирането на защитата на данните в ЕС започва с приемането на Директивата за защита на личните данни³⁵. Тази директива е заменена през 2016 г. с Регламента GDPR³⁶, приет на основание чл. 16 от Договора за функционирането на Европейския съюз и чл. 8 от Хартата на основните права на ЕС.

Растящите притеснения от последиците за неприкосновеността от бисквитки и други подобни интернет технологии е една от основните причини за приемането на Директивата ePrivacy³⁷, изискваща уебсайтовете да събират информирано съгласие, преди да съхранят информация върху устройствата на посетителите или извлекат такава от тях. 15 години по-късно е направено предложение за Регламент ePrivacy³⁸ със задачата да модернизира защитата на личните данни в дигиталната среда, но към днешна дата той остава все още неприет.

3. Повишаване на доверието при дигитални трансакции

През 2003 г. ЕК започва да задава в Евробарометър въпроси, свързани с електронната търговия. По това време само 16% от хората пазаруват онлайн, а на въпрос защо не го правят – 25% казват, че „нямат доверие в интернет“. На последващи въпроси какви са причините

³³ Директива 2000/31/ЕО на Европейския парламент и на Съвета от 8 юни 2000 г. относно някои правни аспекти на услугите на информационното общество и по-специално на електронната търговия на вътрешния пазар (ОВ L 178, 17.7.2000, р. 1–16) (Директива за електронната търговия).

³⁴ Директива 1999/93/ЕО на Европейския парламент и на Съвета от 13 декември 1999 г. относно обща рамка на Общността за електронните подписи (Директива за електронните подписи).

³⁵ Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. относно защитата на физическите лица при обработването на лични данни и относно свободното движение на тези данни (Директива за защита на данните) (ОВ L 281, 23.11.1995, р. 31–50).

³⁶ Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016, р. 1–88) (Регламент (ЕС) 2016/679 – GDPR).

³⁷ Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защитата на правото на неприкосновеност на личния живот в сектора на електронните комуникации (ОВ L 201, 31.7.2002, р. 37–47) (ePrivacy директива).

³⁸ Предложение за регламент на Европейския парламент и на Съвета относно зачитането на неприкосновеността на личния живот и защитата на личните данни в електронните съобщения и за отмяна на Директива 2002/58/ЕО (Регламент за неприкосновеността на личния живот и електронните съобщения) (COM/2017/010 final – 2017/03 (COD) (ePrivacy регламент)).

за недоверието, отговорът е: сигурността на плащането (73%), доверието в информацията в интернет (44%), проблеми, свързани с доставката (37%), възможността за гаранция или рекламация (36%) и накрая – анонимността на продавачите (26%)³⁹.

Ето защо до 2020 г. една голяма част от политиките за защита на потребителите са насочени към:

- 1) даване на достоверна информация⁴⁰;
- 2) осигуряване правото на отказ от поръчка, направена онлайн⁴¹;
- 3) подобряване възможностите за защита на потребителите чрез „Новата сделка за потребителите“⁴², извънсъдебно решаване на спорове⁴³, подобряване на трансграничното сътрудничество между регулаторните органи⁴⁴, колективни иски⁴⁵ и други.

³⁹ Вж. **Stengg, W.** *Digital Policy in the EU...*, p. 98

⁴⁰ Вж. например Директива 93/13/ЕИО, Директива 2005/29/ЕО, Директива 2011/83/ЕС на Европейския парламент и на Съвета от 25 октомври 2011 г. относно правата на потребителите, за изменение на Директива 93/13/ЕИО на Съвета и Директива 1999/44/ЕО на Европейския парламент и на Съвета и за отмяна на Директива 85/577/ЕИО на Съвета и Директива 97/7/ЕО на Европейския парламент и на Съвета (ОВ L 304, 22.11.2011, р. 64–88) (Директива за правата на потребителите – CRD), Директива (ЕС) 2019/2161 на Европейския парламент и на Съвета от 27 ноември 2019 г. за изменение на Директива 93/13/ЕИО на Съвета и на директиви 98/6/ЕО, 2005/29/ЕО и 2011/83/ЕС на Европейския парламент и на Съвета по отношение на доброто прилагане и модернизирането на правилата за защита на потребителите в Съюза (ОВ L 328, 18.12.2019, р. 7–28) (Модернизационна директива), Директивата за електронната търговия, GDPR, Регламент (ЕС) 2018/302 на Европейския парламент и на Съвета от 28 февруари 2018 г. за преодоляване на необоснованото блокиране на географски принцип и на други форми на дискриминация въз основа на националността, местопребиването или мястото на установяване на клиентите в рамките на вътрешния пазар и за изменение на регламенти (ЕО) № 2006/2004 и (ЕС) 2017/2394 и Директива 2009/22/ЕО (ОВ L 60I, 2.3.2018, р. 1–15) (Регламент за геоблокирането).

⁴¹ Вж. CRD, DCSD.

⁴² *New deal for consumers*, преведено на български като „Нов търговски механизъм за потребителите“, което не намирам за сполучливо, тъй като не отразява политическият нюанс, който *New deal* носи, вж. COM(2018) 183 final <https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52018DC0183> *New deal for consumers*.

⁴³ Създадена е Европейска потребителска мрежа; процедурата за алтернативно решаване на спорове по Директива 2013/11/ЕС на Европейския парламент и на Съвета от 21 май 2013 г. за алтернативно решаване на потребителски спорове и за изменение на Регламент (ЕО) № 2006/2004 и Директива 2009/22/ЕО (Директива за APC за потребители) (ОВ L 165, 18.6.2013, р. 63–79) (APC) и OPC платформата на ЕС – Регламент (ЕС) № 524/2013 на Европейския парламент и на Съвета от 21 май 2013 г. относно онлайн решаване на потребителски спорове и за изменение на Регламент (ЕО) № 2006/2004 и Директива 2009/22/ЕО (Регламент за OPC за потребители) (ОВ L 165, 18.6.2013, р. 1–12).

⁴⁴ Създаден е механизма по Сътрудничество при защита на потребителите (CPC) Регламент (ЕС) 2017/2394 на Европейския парламент и на Съвета от 12 декември 2017 г. относно сътрудничеството между националните органи, отговорни за прилагането на законодателството за защита на потребителите и за отмяна на Регламент (ЕО) № 2006/2004 (ОВ L 345, 27.12.2017, р. 1–26).

⁴⁵ Колективните иски дават възможност за защита на колективни интереси в области като защита на данните, финансови услуги, туризъм или други в областта на потребителското право – Директива (ЕС) 2020/1828 на Европейския парламент и на Съвета от 25 ноември 2020 г. относно представителни иски за защита на колективните интереси на потребителите и за отмяна на Директива 2009/22/ЕО (ОВ L 409, 4.12.2020, р. 1–27) (Директивата за колективните иски).

Като много съществена мярка в посока повишаване на доверието в дигиталните трансакции трябва да се спомене и Регламента eIDAS, който заменя Директивата за електронните подписи и разширява значително номенклатурата на електронните доказателства с електронния документ, електронния печат и други⁴⁶.

4. Борба с незаконното и увреждащото съдържание в интернет

В периода 2000–2019 г. се предприемат редица мерки за модериране на съдържанието в интернет, чиято цел е по-безопасна интернет среда⁴⁷. Освен вече споменатата Директива за електронната търговия, по-значимите актове, които са приети, са: Директивата за борба с детската порнография⁴⁸, Директивата за аудио-визуални медийни услуги⁴⁹, Директивата за авторското право в ЦЕП⁵⁰ и други. По това време е направено и предложението за Регламент за цифровите услуги (DSA), който е приет по-късно⁵¹.

§ 24. Втори етап: след 2019 г.

С началото на мандата на Първата комисия на Урсула фон дер Лайен се случва промяна в парадигмата на регулиране – от премахване на пречки пред развитието на цифровото пространство към неговото все по-засилено регулиране⁵². Причините са от икономическо и политическо естество, но те водят до много значими правни последици.

⁴⁶ Вж. Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ L 257, 28.8.2014 г., р. 73–114) (eIDAS), допълнен с Регламент (ЕС) 2024/1183 на Европейския парламент и на Съвета от 11 април 2024 г. за изменение на Регламент (ЕС) № 910/2014 по отношение на създаването на европейска рамка за цифрова самоличност (ОВ L 1183, 30.4.2024 г.) (eIDAS2).

⁴⁷ Вж. подробности в **Stengg, W. Digital Policy in the EU...**, p. 95–96

⁴⁸ Директива 2011/93/ЕС на Европейския парламент и на Съвета от 13 декември 2011 г. относно борбата със сексуалното насилие и сексуалната експлоатация на деца, както и с детската порнография, и за замяна на Рамково решение 2004/68/ПВР на Съвета (ОВ L 335, 17.12.2011, р. 1–14).

⁴⁹ Директива 2010/13/ЕС на Европейския парламент и на Съвета от 10 март 2010 година за координирането на някои разпоредби, установени в закони, подзаконови и административни актове на държавите-членки, отнасящи се до предоставянето на аудиовизуални медийни услуги (Директива за аудиовизуалните медийни услуги) (ОВ L 95, 15.4.2010, pp. 1–24).

⁵⁰ Директива DCSD.

⁵¹ Регламент DSA.

⁵² Концепцията е формулирана и разгърната, включително с подробни аргументи за причините за промяната на парадигмата в **Stengg, W. Digital Policy in the EU...**, p. 107 et seq.

1. Причините

GDPR създаде глобален стандарт при защита на данните със своя иновативен регулаторен подход и фокус върху основните права и служба на човечеството⁵³. Този успех вдъхна самочувствието на Европа, че да бъде пионер в дигиталната регулация вече не е недостатък. Лидерите на ЕС осъзнаха, че трябва да продължат с укротяването на „дигиталния звяр“, който изглеждаше да е поел контрола върху все по-цифровизирания свят⁵⁴.

В корена на всичко това, според Вернер Стенг, е отказването от идеята, че пазарните сили са достатъчни, за да решат съвременните политически и икономически проблеми в дигиталното пространство⁵⁵. Прекомерната власт на онлайн платформите и нарастващото недоверие към тях, в съчетание с предизвикателства като непрозрачността на технологиите, са недъзи, които няма да се излекуват с „повече пазар“.

Така ЕС реши да налага още по-смело своя модел в дигиталната икономика, при който регулацията се счита като източник на бизнес възможности, а не като пречка. За това говори един от първите стратегически документи на Комисията на Урсула фон дер Лайен – Бяла книга за изкуствения интелект⁵⁶. Регулаторната рамка е обобщена като „екосистема, базирана на доверие“. Доверието дава правна сигурност на бизнеса и мотивира потребителите да участват повече в дигиталната икономика. Хармонизацията е ключова, тъй като новите технологии по естеството си нямат пространствени ограничения, а без обща регулаторна рамка в целия ЕС за иноваторите ще е много трудно да съблюдават режимите на всички отделни държави членки. Декларираното в Бялата книга преследване на високи постижения и „атмосфера на доверие“⁵⁷ едновременно може да се каже за цялата законодателна програма на ЕС в последните години.

2. Новата дигитална стратегия на ЕК

На 19 февруари 2020 г., едновременно с Бялата книга, ЕК обявява и новата си стратегия в областта на дигиталната политика – „Изграждане на цифровото бъдеще на

⁵³ Вж. съобр. 4 GDPR.

⁵⁴ Вж. т. 3 от Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите: Изграждане на цифровото бъдеще на Европа.

⁵⁵ **Stengg, W.** *Digital Policy in the EU...*, p. 110 et seq.

⁵⁶ Бяла книга за изкуствения интелект – европейски подход за високи постижения и доверие (2020).

⁵⁷ Официалният превод от английски на *excellence and trust*.

Европа⁵⁸. Разликите с предходната политика на Юнкер – Стратегия за цифров единен пазар за Европа, са видими веднага. Първият и основен приоритет е наречен „Технология, която работи за хората“, а останалите са свързани с честната конкуренция и отвореното, устойчиво и демократично общество. Всичко това показва, че на участниците в цифровото пространство вече не се гледа като на зародиш, който трябва да се подпомага. Те вече са зрели и трябва да се укротят.

Политиката на ЕК следва така начертаната нова парадигма. Още в края на 2020 г. е приета стратегия за засилване прилагането на Хартата⁵⁹. Приоритетите са свързани с осигуряване на институционален, човешки, информационен и др. ресурс за повишаване ефективната защита на основните права на човека. Тази инициатива е последвана и от доклад за приложението на Хартата по отношение на дигиталната трансформация⁶⁰. Като завършек на това направление е приетата през 2022 Европейска декларация относно цифровите права и принципи за цифровото десетилетие⁶¹.

Ковид кризата от 2020–2022 г. нанася големи поражения върху европейската икономика, които налагат Дигиталната стратегия на ЕК да се допълни. Водещ фактор са огромните инвестиции от над 800 млрд. евро по Плана за възстановяване на Европа, голяма част от които са предназначени да отидат за дигитализация на бизнеса, публичните услуги, обучения и развитие на дигитални умения, проучвания и други⁶². В тази връзка е приет първо стратегическият документ Цифров компас до 2030 г.: Европейският път за цифровото десетилетие⁶³, а скоро след него и програмата „Цифрово десетилетие 2030“⁶⁴. Наред с другите приоритети, програмата си поставя за цел извършване на дигитална трансформация, която поставя в центъра си човека⁶⁵.

3. Актове

⁵⁸ Изграждане на цифровото бъдеще на Европа, COM(2020) 67 final.

⁵⁹ Стратегия за укрепване на прилагането на Хартата на основните права в Европейския съюз.

⁶⁰ Съобщение на Комисията до Европейския парламент и Съвета: Нов пакт за миграция и убежище (2020).

⁶¹ Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите: Европейска стратегия за данните (2020).

⁶² Вж. Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите: Актуализиране на новата индустриална стратегия за Европа (2021).

⁶³ Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите: Път към цифровото десетилетие: цифрова цел за 2030 г. (2021).

⁶⁴ Решение (ЕС) 2022/2481 на Европейския парламент и на Съвета от 14 декември 2022 г. за създаване на програма „Цифрова Европа“ и за отмяна на Решение (ЕС) 2015/2240.

⁶⁵ Вж. съобр. 4 ibidem.

В този период са приети множество актове в изпълнение на стратегическите документи и програми на Съюза, по-значимите от които могат да се групират в следните категории:

3.1. Цифрови платформи и пазари

В областта на цифровите платформи и пазари е приет Актът за цифрови услуги (DSA)⁶⁶, който регулира онлайн платформите с цел гарантиране на прозрачност и отчетност, включително премахване на незаконно съдържание и разкриване на алгоритми. Също така е приет Актът за цифровите пазари (DMA)⁶⁷, който е насочен към предприятия, контролиращи достъпа до пазара (*gatekeepers*) и предотвратяване на възможностите им да ограничават конкуренцията. Предприети са и законодателни мерки за подобряване на условията на работа, която се предоставя чрез онлайн платформи⁶⁸.

3.2. Киберсигурност и киберустойчивост

По това направление са приети закони като Акта за киберустойчивост⁶⁹, който въвежда изисквания за сигурност на продукти с цифрови елементи за повишаване на устойчивостта срещу киберзаплахи и Акта за киберсолидарност⁷⁰, свързан със споделянето на ресурси. Както и Директива NIS2⁷¹, актуализираща правилата за киберсигурност за по-широк кръг сектори, подобрявайки защитата на критична инфраструктура в ЕС.

3.3. Изкуствен интелект и възникващи технологии

Тази област е особено приоритетна за ЕС и актовете във връзка с нея ще бъдат разгледани допълнително в настоящото изследване. Тук само ще изброя на първо място

⁶⁶ Регламент (ЕС) 2022/2065 на Европейския парламент и на Съвета от 19 октомври 2022 г. относно единния пазар на цифрови услуги и за изменение на Директива 2000/31/ЕО (ОВ L 277, 27.10.2022, р. 1–102) (DSA).

⁶⁷ Регламент (ЕС) 2022/1925 на Европейския парламент и на Съвета от 14 септември 2022 г. за достъпни и справедливи пазари в цифровия сектор и за изменение на директиви (ЕС) 2019/1937 и (ЕС) 2020/1828 (ОВ L 265, 12.10.2022, р. 1–66) (DMA).

⁶⁸ Споменатата вече в първа част Директива (ЕС) 2024/2831

⁶⁹ Регламент (ЕС) 2024/2847 на Европейския парламент и на Съвета от 23 октомври 2024 г. относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и за изменение на регламенти (ЕС) № 168/2013 и (ЕС) 2019/1020 и Директива (ЕС) 2020/1828 (ОВ L 2847, 20.11.2024) (Акт за киберустойчивост).

⁷⁰ Регламент (ЕС) 2025/38 на Европейския парламент и на Съвета от 19 декември 2024 година относно мерки за засилване на солидарността и капацитета в Съюза за откриване, подготовка и реагиране на киберзаплахи и инциденти и за изменение на Регламент (ЕС) 2021/694 (Регламент за киберсолидарност), ОВ L 2025/38, 15.01.2025

⁷¹ Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (ОВ L 333, 27.12.2022, р. 80–152) (NIS2).

Акта за изкуствения интелект (AIA), който създава хоризонтална регулаторна рамка за ИИ. Наред с него са приети и редица актове, с които се реформират секторни правила в областта на безопасността на машините и други продукти, свързани с техните цифрови компоненти⁷². В областта на отговорността за изкуствен интелект и възникващи технологии е приета Директивата за отговорността за вреди от дефектни продукти⁷³ и се предложи Директива за вреди от изкуствен интелект⁷⁴.

3.4. Управление и споделяне на данни

В тази област е значим Актът за управление на данните (DGA)⁷⁵, който създава рамка за споделяне и повторна употреба на данни между бизнеса и държавата. Този регламент се допълва от Акта за данните (DA)⁷⁶, който установява правила за справедлив достъп до данни и техния обмен между частни лица.

3.5. Публични и трансгранични услуги

В тази категория впечатление прави допълнението на Регламента eIDAS, известно като eIDAS2⁷⁷, което подобрява рамката управлението на дигиталната идентичност в ЕС. Важен е и Актът за оперативно съвместима Европа⁷⁸, който подобрява оперативната съвместимост на публичните услуги в държавите – членки на ЕС.

Могат да се споменат и други актове, включително и други направления на регулация, но изброените са достатъчни, за да се изяснят приоритетите на европейския законодател в цифровото пространство в периода след 2019 г. Виден е стремежът към повече регулация и ограничаване на властта и самостоятелността на настанилите се в цифровото пространство големи играчи. Дори вече се заговаря за „дигитален

⁷² Например Регламент (ЕС) 2023/1230 на Европейския парламент и на Съвета от 14 юни 2023 г. относно машините и за отмяна на Директива 2006/42/ЕО на Европейския парламент и на Съвета и на Директива 73/361/ЕИО на Съвета (ОВ L 165, 29.6.2023, р. 1–102) (Регламент за машините)

⁷³ Директива PLD2.

⁷⁴ Предложение за директива AILD, което беше официално оттеглено от ЕК през февруари 2025-та

⁷⁵ Регламент (ЕС) 2022/868 на Европейския парламент и на Съвета от 30 май 2022 г. относно европейска рамка за управление на данните и за изменение на Регламент (ЕС) 2018/1724 (ОВ L 152, 3.6.2022, р. 1–44) – Акт за управление на данните (DGA).

⁷⁶ Регламент (ЕС) 2023/2854 на Европейския парламент и на Съвета от 13 декември 2023 г. относно хармонизирани правила за справедлив достъп до данни и за тяхното използване и за изменение на Регламент (ЕС) 2017/2394 и Директива (ЕС) 2020/1828 (ОВ L 2854, 22.12.2023) – Акт за данните (DA).

⁷⁷ Регламент 2024/1183/ЕС – eIDAS2.

⁷⁸ Регламент (ЕС) 2024/903 на Европейския парламент и на Съвета от 13 март 2024 г. за определяне на мерки за високо ниво на оперативна съвместимост на публичния сектор в целия Съюз (ОВ L 90, 22.3.2024, р. 1–26).

конституционализъм“, гарантиращ една инфосфера, където гражданите на ЕС могат да живеят и работят по-добре и по-устойчиво⁷⁹.

III. Политика на ЕС по отношение на гражданската отговорност в цифровото пространство

Гражданската отговорност е важен елемент от регулативната политика на ЕС в областта на цифровото пространство. Тя е механизъм за стимулиране на превантивно и предпазливо поведение от страна на задължените лица, както и средство за разпределяне на рисковете и неблагоприятните последици при вреди от дигитални дейности. В този смисъл, гражданската отговорност е осъзнавана като фактор за създаване на доверие в цифровите технологии, който заедно с инициативите за безопасността трябва да стимулира по-широко включване и икономически растеж.

Предметът на регулация в Цифровото пространство обаче е, меко казано, „нетрадиционен“ – със свои специфични предизвикателства и проблеми. Вследствие традиционната рамка за гражданска отговорност се оказва неадекватна при справянето със задачата да осигури справедливо обезщетение за пострадалите от цифровите технологии лица. Така ЕС е призван да „мисли извън рамката“ и да разработи нови модели на регулация, подходящи за дигиталния свят, съществен елемент от който са правните инструменти на тежестта и стандарта на доказване.

§ 25. Предизвикателства

1. Доверие

Обществото има нужда от доверие, за да функционира, но междучовешкото доверие и това в технологиите са различни неща. Доверието между хората е емоционално и се основава на личен опит, морални принципи и социални връзки, докато доверието към технологиите е рационално и зависи от тяхната надеждност, функционалност и прозрачност. Докато човешкото доверие изисква време за изграждане и може да бъде

⁷⁹ Самото понятие „конституционализъм“ и актовете, които се посочват като носители на „дигиталната конституция“, а именно DSA, DMA, AIA, GDPR, DGA и DA показват ясно чия власт се ограничава с това усилие. Вж. повече за концепцията **Floridi, L.** The European Legislation on AI: A Brief Analysis of its Philosophical Approach. *Philosophy & Technology*, 34, 215–222 (2021), p. 5.

дълбоко уязвимо, доверието в технологиите е по-крехко и се влияе от технически проблеми или липса на разбиране⁸⁰.

Съответно, изграждането на чувство на увереност в цифровите технологии е комплексна задача, която изисква и комплексни решения. Генерално погледнато, средствата, с които разполагаме за тази цел, са разделени в две групи: технологични и правни. В първата категория са мерки като прозрачност на алгоритмите, силна киберсигурност, надеждност на системите, етични правила, защитен достъп до данни и ясно информирание на потребителите⁸¹. Правните средства са различните законодателни актове, стандарти, рамки, насоки и надзор за тяхното прилагане⁸². Политиката на ЕС се осъществява предимно чрез нормативни инструменти, които могат да изискват или стимулират използването на технологични средства за изграждане на доверие, но могат и да налагат нетехнологични мерки като различните видове отговорности например.

Може да се каже, че антиподът на доверието е скептицизмът или дори страхът⁸³. Безспорно, историята показва, че всяко нововъведение се посреща малко или много с някаква съпротива⁸⁴. При цифровите технологии тяхната изначална непрозрачност в комбинация с ефимерността на бинарните електрически импулси, които изграждат основата им, будят най-малкото смущение и неразбиране. Винаги има опасност софтуерът например да се окаже с вградена „задна врата“, която го кара да прави неща извън неговото предназначение и без знанието на използващите го⁸⁵. А върху тази фундаментална несигурност процъфтяват и други предизвикателства, които подкопават доверието в дигиталните технологии.

2. Дигиталните рискове

⁸⁰ Вж. по-подробно по темата **Siau, K., Wang, W.** Building Trust in Artificial Intelligence, Machine Learning, and Robotics. *Cutter Business Technology Journal*, 31(2), 47–53 (2018), Chapter 3.

⁸¹ Ibidem, Chapter 2.

⁸² Boehme-Neßler, V. Law 4.0? Considerations on the Future of Law in the Digital Age. In: *Handbook Industry 4.0: Law, Technology, Society*, edited by W. Frenz, Springer, 2022, p. 275–288.

⁸³ Вж. съответно понятията „техноскептицизъм“ – <https://hpluspedia.org/wiki/Technoscepticism>; и „технофобия“ – <https://en.wikipedia.org/wiki/Technophobia>

⁸⁴ Някои от които особено организирани и агресивни като т.нар. лудити от 19. век – <https://en.wikipedia.org/wiki/Luddite>

⁸⁵ Например концепцията за троянския кон, развита от известния компютърен изследовател Кен Томпсън – **Thompson, K.** Reflections on Trusting Trust. *Communications of the ACM*, Vol. 27, No. 8, 1984, p. 761–763.

Дигиталните рискове са пряко свързани със свободата да използваме интернет, да употребяваме цифрови продукти и да вземаме други решения в живота си, които са засегнати от новите технологии⁸⁶. С натрупването на обществен опит се наслаждава и осъзнаване за това, че дигиталните рискове могат да представляват сериозна заплаха за здравето, безопасността и основните права, включително правото на неприкосновеност на личния живот, свободата на изразяване и сигурността⁸⁷.

Кибератаки като фишинг (*phishing*), рансъмуер (*ransomware*) и пробиви в сигурността на данните компрометират чувствителна лична и организационна информация, подкопавайки правото на поверителност и излагайки хората на риск от експлоатация. Злоупотребата с лични данни, често събирани без информирано съгласие, може да разруши доверието в технологията и да засегне автономността на личността. Алгоритмичните пристрастия и нерегулираните системи с изкуствен интелект създават риск от дискриминация, засягайки равенството и справедливостта в процесите на вземане на решения. Освен това, зависимостта от дигиталната инфраструктура създава уязвимости, тъй като нарушаването на достъпа до основни услуги, застрашава правото на информация на всеки човек, а понякога и възможността за ползване на жизненоважни ресурси.

3. Информационна асиметрия

Информационната асиметрия в дигиталния свят възниква, когато едната страна разполага с повече или по-добра информация от другата, което води до дисбаланс на силите и потенциална експлоатация⁸⁸. Например, компаниите често събират огромни количества данни за потребителите, което им позволява да прилагат таргетирана реклама или ценови стратегии, които потребителите може да не разбират или да не са съгласни с тях. По същия начин може да няма прозрачност относно това как функционират алгоритмите или системите с изкуствен интелект, което води до решения, които са неразбираеми или изкривени поради пристрастия и други проблеми с данните. Този дисбаланс може да подкопае доверието, да възпрепятства справедливата конкуренция и да задълбочи

⁸⁶ Вж. относно концепцията за дигиталните рискове – **Latil, A.** *Le droit du numérique. Une approche par les risques*. Paris: Dalloz, 2023, p. 33 et seq.

⁸⁷ Вж. повече за различните категории дигитални рискове – **Latil, A.** *Le droit du numérique ...*, p. 69 et seq.

⁸⁸ Вж. повече тук: https://en.wikipedia.org/wiki/Information_asymmetry

неравенствата, тъй като тези с повече информация могат да влияят непропорционално върху резултатите в пазарите, социалните взаимодействия и управлението⁸⁹.

4. Достъп до доказателства

Частен случай на информационната асиметрия е обстоятелството, че често страната, която се домогва да докаже факт, случил се в цифровото пространство, няма достъп до следите, които този факт е оставил след себе си. Това е така, тъй като дигиталната следа си има носител и този носител обикновено е в частни ръце. За да се събере цифровото доказателство като електронно съобщение, метаданни от активност в социални мрежи, данни за идентификация на лица и т.н., е необходимо съдействието на трето лице, много често това е самият нарушител⁹⁰. Неустойчивостта на цифровите следи ги прави също така много лесни за манипулиране или просто заличаване, което съществено изкривява съотношението на силите в полза на страната, която е собственик на средата, в която се развива правоотношението.

Този проблем се усложнява допълнително с факта, че принудителното запазване и изземване на доказателства в такива случаи може да налага взаимодействие между публични органи в различни юрисдикции, с техните различни процесуални закони и ограничителни правила. Доказателственото средство трябва да бъде запазено в автентичен вид, за да има стойност в съда, което е трудна техническа задача и създава множество възможности за оспорване отново от обикновено по-силната страна.

5. Икономически съображения

Допълнително предизвикателство е това, че въпреки всички рискове обществото има нужда от дигиталните технологии, за да запази глобалната си конкурентоспособност и да се ползва от всичките блага, които те носят със себе си. ЕС осъзнава това и всички актове, които предстои да бъдат разгледани, съдържат под една или друга форма и съображения за насърчаване на иновациите, подобряване на правната сигурност за бизнеса или преследване

⁸⁹ Така например липса на технически познания у потребителя го възпрепятства да установи наличието на изпълнение по договора – вж. съобр. 59 от DCSD.

⁹⁰ Подробно по темата вж. [FRA, Improving Access to Remedy ...](#), Chapter 2 Judicial remedies.

на други икономически цели⁹¹. Това обстоятелство усложнява задачата на европейския законодател, който, поставяйки човека в центъра, не може да си позволи свръхрегулация на бизнеса.

В това „ходене на въже“ над пропастта на рисковете ЕС трябва да изгради регулаторна рамка за гражданската отговорност, балансирайки между различни интереси, в нова ситуация, непозната досега. С присъщия си прогресивизъм Съюзът отговаря на тези предизвикателства по обичайния за себе си начин – чрез иновативни подходи на правна регулация.

§ 26. Тежестта и стандартът на доказване като подход за адаптиране на гражданската отговорност към цифровите предизвикателства

На всички тези предизвикателства ЕС отговоря чрез реформиране на рамката на гражданската отговорност. Идеята е тя да стане по-ефективна, разбирано като възможност реално пострадалите да защитят интересите си, поставени често в ситуация на по-слаба страна по дела, свързани с дигитални правоотношения. За целта се използват цяла палитра от правни инструменти, насочени към настройване на режима на отговорност така, че да е по-адекватен към действителността на цифровото пространство. Сред тях все по-предпочитани са институтите на тежестта и стандартът на доказване, или по-точно казано – правилата, предписващи отклонение от тях.

В предната част беше анализирано какво представляват тежестта и стандартът на доказване според правото на ЕС, кои са техните отклонения и какви функции изпълняват. Следващата трета част е посветена на въпросите защо и как се използват тези инструменти, но тук като заключение на тази част ще маркирам основните причини.

1. Справедливо разпределение на риска

Отклоненията от тежестта и стандарта на доказване водят до прехвърляне в някаква степен на риска, свързан с отговорността⁹². Той се изразява в това, от една страна, да не успее жертвата да получи справедливо възмездие, или от друга – някой да понесе отговорността да поправи едно негативно правно положение, без да го е причинил.

⁹¹ Вж. подробни аргументи за икономическата логика при регулиране на ИИ – **Buiten, M., A. de Streel, M. Peitz.** The Law and Economics of AI Liability. Computer Law & Security Review, Vol. 48, 2023.

⁹² Вж. съображенията за отклонения в §20

Съгласно принципа за справедливостта всеки трябва да понесе такава част от рисковете от дейността, която развива, съответна на ползите, които извлича от нея. Страната, на която е възложена по-тежка отговорност, е склонна да предприема повече предпазни мерки, за да не се стига до инциденти, и това е в полза на обществото⁹³.

Отговорността, разбира се, може да се утежни и с други средства, като например премахване на елементи от фактическия състав на правото на обезщетение, предвиждане на задължения за застраховане и други. Но нуждата от баланс на различни интереси и най-вече желанието да се стимулира иновацията и технологичният бизнес, изискват умерени подходи. А никой друг инструмент не е така гъвкав, както е комплексът от тежестта и стандарта на доказване. Тежестта например може да е обърната за един или няколко от елементите на фактическия състав на отговорността, но ако това е твърде радикално, може стандартът да се облекчи. Или да се направи комбинация между отклонение от ОПРТД с облекчаване на стандарта за обратно доказване и т.н. Вариантите са много и тепърва ще бъдат анализирани някои от тях.

2. Преодоляване на информационната асиметрия

Тежестта и стандартът на доказване помагат за справяне с информационната асиметрия, като или възлагат отговорността за предоставяне на доказателства на страната, която има по-добър достъп до тях, или по друг начин я стимулират да разкрива информация или предоставя доказателства. Така например ищецът по иск за вреди от нарушение в сигурността на личните му данни няма да е необходимо да доказва какви точно мерки за сигурност не е предприел администраторът, защото той няма откъде да ги знае⁹⁴. А в новата директива PLD2 пострадалият от дефектен продукт има право да изисква доказателства в подкрепа на иска си от ответника – производител, като в противен случай се презюмира дефект. В този смисъл е и концепцията за принципа на близост до доказателствата, който оправдава предпологане на факти или заключения на база поведението на страната, която има повече информация⁹⁵. Тези инструменти изравняват възможностите на страните,

⁹³ Вж. по темата **Kim, J.-Ch., B. Lee, S. H. Chun**. The Optimal Allocation of Burden of Proof and its Effect on Precaution Behavior. KAIST College of Business Working Paper Series No. 2008-002, 2008, p. 1–35.

⁹⁴ Вж. отговорността по чл. 82 GDPR.

⁹⁵ Вж. по темата за принципа на доказателствената близост (*proof proximity*) във **Volpin, C**. The Ball is in Your Court: Evidential Burden of Proof and the Proof-Proximity Principle in EU Competition Law. – In: Common Market Law Review, Vol. 51, No. 4, 2014, p. 1159–1185; вж. също **Karner, E**. The Function of the Burden ..., p. 72–73.

насърчават прозрачността и смекчават ефектите от неравномерното разпределение на информационните възможности в съдебните спорове.

3. Отговор на технологичните предизвикателства

Отделно от достъпа до доказателства, самите характеристики на дигиталните технологии могат да направят много трудни за доказване елементи на фактическия състав на отговорността като вина, дефект или причинно-следствена връзка. Пострадалите обикновено не са достатъчно технически подготвени, за да доказват нарушението. Поради това е справедливо част от риска за загубване на едно дело поради липса на достатъчно доказателства за някой неразгадаем проблем да се прехвърли върху икономически по-силната страна, която най-често е и по-добре информирана и може да се защити⁹⁶.

След всичко казано до тук, може да се заключи, че ЕС осъществява специфична политика на регулация на цифровото пространство в рамките на общата си политика за вътрешен пазар. Едно от големите предизвикателства пред нея е осигуряването на ефективни механизми за гражданска отговорност, които да гарантират нарастващия брой дигитални права и задължения. Различни причини и съображения водят до конкретни проблеми пред доказването на гражданската отговорност в цифровото пространство. Следователно, съюзът си поставя за цел да реформира нейната рамката в дигиталната си политика. В следващата част ще бъдат анализирани някои специални групи проблеми пред доказването и отговорът, който ЕС им дава.

⁹⁶ Вж. в този смисъл и **Wagner, G.** Verantwortlichkeit im Zeichen digitaler Techniken. – In: Versicherungsrecht, 2020, No. 12, part 1, p. 717–741.