DOI 10.69085/PSC2025070

ЗАЩИТА НА ОСНОВНИТЕ ПРАВА В ЦИФРОВАТА ЕРА: ПРЕДИЗВИКАТЕЛСТВА В КОНСТИТУЦИОННОТО ПРАВО ВЪВ ВРЪЗКА СЪС ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

ас. Тодор Рогошев
Пловдивски университет, България

Резюме: *Статията разглежда баланса между правото на личен живот и националната сигурност в условията на цифровата ера. Анализирани са конституционните и международноправните стандарти за защита на личната неприкосновеност, както и практиката на Конституционния съд, ЕСПЧ и Съда на ЕС. Отделено е внимание на предизвикателствата на киберсигурността, масовото събиране на данни и необходимостта от пропорционални мерки. В заключение се подчертава значението на превантивни решения и сътрудничество между държавата и частния сектор за устойчиво съчетаване на сигурността и основните права.*

Ключови думи: *права на човека, киберсигурност, право на личен живот, законно ограничение, ЕКПЧ*

PROTECTION OF FUNDAMENTAL RIGHTS IN THE DIGITAL ERA: CHALLENGES IN CONSTITUTIONAL LAW REGARDING THE PROTECTION OF PERSONAL DATA

Assist. Prof. Todor Rogoshev
University of Plovdiv, Bulgaria

Abstract: *The article examines the balance between the right to privacy and national security in the digital era. It analyzes constitutional and international legal standards for the protection of privacy, as well as the case law of the Constitutional Court, the European Court of Human Rights, and the Court of Justice of the European Union. Attention is given to the challenges of cybersecurity, mass data collection, and the need for proportionate measures. In conclusion, the importance of preventive solutions and cooperation between the state and the private sector is emphasized in order to achieve a sustainable balance between security and fundamental rights.*

Key words: *Human rights, cybersecurity, right to privacy, lawful restriction, ECHR*

1. Балансът между личните права и сигурността

В самите корени на „мощното дърво“[1] на модерната конституционна държава стоят две концепции – конституционализмът и индивидуалните права и свободи. Великите умове на Просвещението залагат идеите, които и до днес ръководят демократичните държави, посветени на идеята за върховенството на правото. Принципите на обществения договор и теорията за естествените права обаче пораждат и трения. Все пак в основата на обществения договор е постигането на някаква сигурност, било то под формата на държавата, която снабдява и подхранва индивидуалното и съвместното обществено развитие[2] или като Левиатан, който ни предпазва от естественото състояние на насилие чрез неговото монополизиране.[3] Сигурността гарантира и националния суверенитет, без който държавата не би могла да действа самостоятелно в управлението и грижата на своите граждани. С други думи, всяка държава трябва да намери равновесието между личните права и сигурността във всичките ѝ аспекти.

Въпросите на сигурността в исторически план винаги са били сравнително сложни. От управлението на държавни служители, натоварени с чувствителна информация, до откриването на граждани или чужденци, които носят риск за суверенитета и благосъстоянието на държавата. С развитието на модерните технологии тези проблеми на сигурността стават значително по-трудни за разрешаване. Рисковете, които преди няколко десетилетия са се развивали само в истинския, физически свят, днес имат и ново обиталище – цифровият свят, изграден от компютърни системи и свързан с интернет.

Настоящият доклад разглежда въпроса за баланса между личните права и сигурността в цифровата ера и търси отговор на въпроса по какъв начин влияят интернет, социалните мрежи, мобилните приложения и технологиите за наблюдение върху личната неприкосновеност. За целта следва да се разгледат конституционноправните задължения на държавата във връзка със сигурността, от една страна, но и с правото на личен живот, от друга. За пълно изследване на въпроса е необходимо неговото разглеждане в светлината на европейските тенденции, както и практиката на Конституционния съд, ЕСПЧ и СЕС.

[1] Вж Друмева, Е. Конституционно право. С., Сиела (Drumeva, E. Konstitutsionno pravo. S., Siela), 2025, с. 664.

[2] Вж. Locke, J. Second Treatise of Government. London, Black Swan, 1690. 159–162.

[3] Вж. Hobbes, T. Leviathan, or The Matter, Forme, & Power of a Common-Wealth Ecclesiastical and Civil. London, Green Dragon, 1651, p. 89.

2. Правото на личен живот

Правото на личен живот има много лица в Конституцията на Република България, от които няколко са от особен интерес за настоящата разработка. Съгласно чл. 30 всеки има право на лична свобода и неприкосновеност, а чл. 32 провъзгласява, че личният живот на гражданите е неприкосновен. Всеки има право на защита срещу незаконна намеса в личния и семейния му живот и срещу посегателство върху неговата чест, достойнство и добро име. Никой не може да бъде следен, фотографиран, филмиран, записван или подлаган на други подобни действия без негово знание или въпреки неговото изрично несъгласие освен в предвидените от закона случаи. Чл. 34 допълнително разширява това право, като гарантира неприкосновеността на свободата и тайната на кореспонденцията и другите съобщения.

Същите права са заложени и в редица международни актове, сред които Всеобщата декларация за правата на човека – чл. 12, Международният пакт за граждански и политически права – чл. 5 и чл. 17, Хартата на основните права на Европейския съюз – чл. 7, чл. 8 и чл. 52, § 1 и Конвенцията за защита на правата на човека и основните свободи (ЕКПЧ) – чл. 8. С оглед на идентичния характер и съдържание на тези права, в тяхната регламентация на конституционно ниво и в текстовете на посочените международни актове, последните два от които представляват и част от европейското законодателство, Конституционният съд намира, че при осъществяване на нормения контрол за конституционност следва да вземе предвид и тези международноправни норми в светлината на прогласените от тях принципи и стандарти, наред с практиката по тяхното прилагане на Европейския съд по правата на човека (ЕСПЧ).[4] Този подход е многократно потвърждаван в практиката на Конституционния съд, доколкото е възприет и от други предходни негови решения (вж. Решение № 7/1996 г. по к. д. № 1/1996 г., Решение № 1/1998 г. по к. д. № 17/1997 г., Решение № 2/1998 г. по к. д. № 15/1997 г., Решение № 4/2006 г. по к. д. № 11/2005 г., Решение № 3/2011 г. по к. д. № 19/2010 г., Решение № 1/2014 г. по к. д. № 22/2013 г., Решение № 3/2004 г. по к. д. № 3/2004 г., раздел V, т. 7).

Чл. 32 и 34 изрично предвиждат хипотези, в които тези права могат да бъдат ограничавани. Личният живот е ограничен от закона, видно и в двете алинеи, но без да се посочва изрично основание. Чл. 34, от друга страна, предвижда ограничение в случаите, когато това е необходимо за разкриване или предотвратяване на тежки престъп-

[4] Решение № 2 от 12.03.2015 г. на КС по к. д. № 8/2014 г., докладчик съдия Кети Маркова, ДВ, 23/2015 г.

ления. Според Конституционния съд в Решение № 2 от 2015 г. по к. д. № 8 от 2014 г. чл. 32, ал. 2 и чл. 34, ал. 2 от Конституцията изискват изключенията да са уредени от закон; да се допускат само с разрешение на съдебната власт; и само когато това се налага за разкриване и предотвратяване на тежки престъпления. Т.е. хипотезите на ограниченията в двете разпоредби се уеднаквяват. Следователно виждаме, че става дума за едни лични права, които са с особено висока степен на защита, заложена в Конституцията, ограничения на които се допускат в изчерпателно изброени случаи.

Идентичността между уредбата в Конституцията и международноправните актове, които бяха споменати, се вижда ясно и тук. Хартата, ЕКПЧ и Пактът – всички предвиждат в посочените разпоредби някакви форми на законни ограничения. В делото *Лъобоа срещу България*[5] ЕСПЧ приема, че законната намеса в упражняването на правата по чл. 8 от Конвенцията трябва да бъде „в съответствие със закона", да преследва една или повече от легитимните цели, предвидени във втората алинея, и да бъде „необходима в едно демократично общество". Това се доразвива в *Данилевич срещу Русия*,[6] където съдът приема, че понятието „необходимост" за целите на чл. 8 означава, че намесата трябва да отговаря на належаща обществена нужда и по-специално – да бъде пропорционална на преследваната легитимна цел. Идентичен е и похватът, който Конституционният съд е възприел при преценката дали има законни ограничения на конституционните права на гражданите.[7]

Следователно Конституцията на Република България и международноправните договори, по които тя е страна, защитават правото на личен живот и го прогласяват на най-високо ниво като привилегия, която следва да се брани от закона и да бъде ограничавана само в изключителни случаи.

3. Задълженията на държавата спрямо националната сигурност

Националната и индивидуалната сигурност са сред основните постулати, заложени в Конституцията. Самият преамбюл провъзгласява, че Конституцията е изградена върху правата на личността, нейното достойнство и **сигурност** като върховен принцип. Освен това се проявява чрез функциите на въоръжените сили (чл. 9) и на

[5] Лъобоа срещу България, ЕСПЧ, жалба № 67482/14, решение от 19.10.2017 г., пар. 65.
[6] Данилевич *срещу Русия*, ЕСПЧ, жалба № 31469/08, решение от 16.02.2021 г., пар. 54.
[7] Решение № 2 от 31.03.2011 г. на КС по к. д. № 2/2011 г., докладчик съдия Румен Ненков.

Министерския съвет (чл. 105), като е основна цел на външната политика на Република България. Точно по тази причина едно от изрично посочените основания, върху които могат да се ограничават личните конституционни права, е именно защитата на националната сигурност. (чл. 35, 37, 41). Тази сигурност се възприема и като сигурност на личността свободно да упражнява своите права. Така например са допустими ограничения на някои конституционни права за целите на превенция на престъпността, защита на правата и репутацията на други лица, на обществения морал и т.н. (чл. 39 – 41). По думите на Конституционния съд в своето Решение №5 от 1992 г. по к. д. №11 от същата година „*[д]ържавата като върховен носител на суверенитета и гарант на прокламираните в Конституцията граждански права е длъжна да осигури условията за свободно и безпрепятствено, във всяко отношение, упражняване на личното право*“. Разбира се, тук става дума за правото на свобода на религията.

Същият извод се потвърждава и в по-широк план от по-късното Решение № 7 от 1996 г. по к. д. № 1 от 1996 г., според което „*[т]ъй като Конституцията защитава и други ценности, респ. права и интереси, чието реализиране може да ги постави в конкуренция с разглежданото право, оправдано е да се допусне ограничаването му*“. Т.е. изглежда, че Конституционният съд възприема виждането, че за да се гарантира възможността гражданите да упражняват личните си права, може да е необходимо ограничаването на същите тези права.

Европейският съд за правата на човека застъпва сходно виждане при тълкуването на немалко от правата по Конвенцията.[8] Всъщност голяма част от предвидените от Конвенцията ограничения признават защитата на националната сигурност като легитимна цел.

Следва да се направи изводът, че сигурността като основна цел на държавата се разбира като сигурност в един общностен смисъл, но и в индивидуален смисъл. Т.е., от една страна, говорим за колективната сигурност на суверенитета, териториалната цялост, особените икономическите интереси на държавата и т.н. От друга страна, говорим за личната сигурност на всеки гражданин да живее и упражнява своите конституционни права свободно и без незаконна намеса от други субекти. Самите основания за ограничения във връзка с индивидуалните права често са и елемент на обществен интерес – например престъпност и тероризъм в контекста на националната сигурност. Въпросът, който се повдига, е докъде се простира тази възможност за ограничаване на правата?

[8] Сегерстедт-Виберг и други срещу Швеция, ЕСПЧ, жалба № 62332/00, решение от 6.06.2006 г.

4. Сблъсъкът между сигурността и правото на личен живот в Интернет

Тук идва моментът да засегнем основния проблем на доклада, а именно – кибертехнологиите и необходимостта от защита на националните кибермрежи. Основната характеристика на дейността в киберсферата е, че тя произхожда от компютърни системи и оперира във виртуалното пространство на интернет. Тази киберсреда е почти изцяло лишена от физическо присъствие. Единствената реална проекция са машините, чрез които съществува.[9] Поради това прилагането на същата логика, разследващи техники и тълкувания на правила, каквито са приложими в реалния свят, е предизвикателно. Три основни фактора правят кибердейността особено трудна за овладяване заплаха. Това са именно липсата на физически граници и географски ограничения, бързината, с която се извършва поведението, и възможността да се прикрие, изкриви или отклони източникът на атаката. В допълнение към тези фактори следва да се вземат предвид възможните цели и начинът на извършване на незаконната кибердейност.[10]

Хакерите по света имат достъп до редица инструменти, които правят дейността им във виртуалното пространство още по-трудна за проследяване, като прикриват източника на кибератаката или използват компютърни системи на трети страни за посредници за своите операции.[11] Прикриването най-често се осъществява чрез виртуална частна мрежа или VPN, която на практика използва „тунели" в киберпространството и така анонимизира източника на атаката.[12] VPN услугите днес са широко достъпни дори за обикновения потребител и се рекламират. Прокси сървърите работят по подобен начин, но вместо да създават виртуална мрежа, те пренасочват мрежовите пакети през легитимни комуникационни протоколи или съществуващи сървъри.[13] Накрая, Onion или Tor маршрутизацията

[9] Mačák, K. Is the International Law of Cyber Security in Crisis? – In: 8th International Conference on Cyber Conflict, Talin, NATO Cooperative Cyber Defence Centre of Excellence, 2016, 127–129.

[10] Lightfoot, S. Cases of Cyber Warfare in Conflict. – Contemporary Conflicts and Global Responses, [online], (DOI:10.13140/RG.2.2.18799.28327, 2018).

[11] Coco, A., Dias, T. D. 'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law. – European Journal of International Law, 2021, Vol. 32, No. 3, 771–805, p. 772.

[12] Ramadhani, E. Anonymity communication VPN and Tor: a comparative study. – Journal of Physics: Conference Series, 2018, Vol. 983, p. 1–2.

[13] Kropotov, V. et al. The Hacker Infrastructure and Underground Hosting: Services Used by Criminals. Trend Micro Research, 2017, p. 22–23.

също е метод за тунелиране,[14] който се базира на две стъпки: първо, пакетите се „прескачат“ или пренасочват през няколко местоположения и второ, между тези пренасочвания пакетите се криптират. Този тип маршрутизация обикновено се свързва с незаконен достъп до т.нар. „тъмен интернет“ и е лесно достъпна чрез приложения като Tor Browser.[15]

Компютрите са се развили значително от времето на релето – базираните електромеханични компютри и компютърните системи днес представляват огромни и сложни алгоритми. В тази сложност се крие и последното предизвикателство. За да се проследи незаконна дейност, е необходимо да се извърши техническо разследване, което изисква познания за това как системата работи и какви са нейните уязвимости. С по-високата сложност на системата обаче идва и по-голям шанс за уязвимост, за която често дори самите програмисти и оператори не подозират.[16] За да се открият тези уязвимости и начинът, по който действа зловредният софтуер, трябва да се инвестира значително време и човешки ресурси в обратното инженерство на зловредния софтуер, установяването на пробива в сигурността и определянето на щетите. Например разкриването на вируса Stuxnet изисква участието на редица компании, които работят върху конкретни компоненти на зловредния софтуер,[17] а изследователите правят нови открития повече от 10 години по-късно.[18] Всичко това – за зловреден софтуер с размер около 500 килобайта.[19] Целият този процес допълнително забавя разследването и засилва гореспоменатите проблеми.

Горепосочените средства позволяват на лица, които извършват дейност, застрашаваща националната и личната сигурност на гражданите, да го направят незабелязано или по начин, който прави намирането им значително по-трудно. България не е заела изрична позиция относно приложимостта на принципа за дължима грижа в киберпрост-

[14] Ramadhani, E. Anonymity communication VPN and Tor: a comparative study. – Journal of Physics: Conference Series, 2018, Vol. 983, p. 1, 2.

[15] Omar, Z. M. An Overview of Darknet, Rise and Challenges and Its Assumptions. – International Journal of Computer Science and Information Technology, 2020, Vol. 8(3), 110–116.

[16] Labicki, M. Cyberdeterrence and Cyberwar. Santa Monica, CA, RAND Corporation, 2009, p. 18.

[17] Lindsay, J. R. Stuxnet and the Limits of Cyber Warfare. – Security Studies, 2013, Vol. 22(3), 365–404.

[18] Seals, T. SAS 2019: 4 Stuxnet-Related APTs Form Gossip Girl, an Apex Threat Actor. – Threatpost, 2019 (https://threatpost.com/stuxnet-apts-gossip-girl/143595/).

[19] Rao, S. Stuxnet, A new Cyberwar weapon: Analysis from a technical point of view (2014) [онлайн], DOI: 10.13140/2.1.1419.5205.

ранството, но в своята Национална стратегия за киберсигурност[20] тя признава необходимостта от международно сътрудничество за предотвратяване на злонамерени кибероперации. Сътрудничеството включва обмен на опит, уведомления и технологични ресурси, които увеличават отбранителните способности в киберпространството.

Въпреки това, за да се спази принципът за дължима грижа и действителна превенция, от държавата се очаква да осъществява интензивен мониторинг на своята интернет инфраструктура, включително събиране и обработка на огромни обеми от данни.

Любопитно е в тази връзка Решение № 2 от 2015 г. по к. д. № 8 от 2014 г. на Конституционния съд. Според него запазването на данни от целия телекомуникационен трафик (фиксирана и мобилна телефония, интернет достъп, електронна поща и интернет телефония) без повод и с цел квалифицирана употреба за нуждите на предотвратяването, разкриването и разследването на тежки престъпления не може дефинитивно да се отрече. То не може да се третира като противоконституционно, ако конституционната проверка установи, че са спазени изискванията ограничението да е уредено със закон, да е в рамките на предвиденото с основния закон изключение, да е подчинено на легитимна/и цел/и от общ интерес, каквито несъмнено представляват борбата с тежките престъпления, повишаването на обществената сигурност, борбата с международния тероризъм и опазването на международния мир и сигурност, както и да е съобразен принципът за пропорционалност.

Казус, илюстриращ позицията на съда по този въпрос, би възникнал в случай, когато например извършител на терористичен акт, който до момента на извършване на деянието не е попадал в информационните масиви на полицията във връзка с други предходни свои криминални прояви, за да се е налагала проверка на данни от неговата комуникация, бъде заловен на местопрестъплението. Ако оспорената мярка не съществуваше, за да вменява на предприятията, предоставящи услугите, запазване на данните за целия протичащ трафик, то генерирането и проследяването им по отношение на това лице би могло да започне едва след като извършеното престъпление вече е факт и самоличността на дееца е установена. Ясно е, че в такъв случай информация по горепосочените въпроси, свързани с подготовката, организацията, самото извършване на престъплението и евентуалните съучастници, е невъзможно да бъде събрана, защото ще обх-

[20] Министерски съвет. Актуализирана национална стратегия за киберсигурност „Киберустойчива България 2023“. С., 2021.

ваща само периода от време, следващ престъплението и следователно няма как да обслужи разследването.

В този смисъл съпоставката на защитаваната цел и приложеното средство предпоставя извода, че по своята същност въведената мярка принципно се оказва съответна, необходима и подходяща, включително и през призмата на критерия за съразмерност на ограничението.

Не така обаче стои въпросът за срока на нейното експлоатиране, заложен в чл. 250а, ал. 1 Закона за електронните съобщения (ЗЕС) – 12 месеца, който при съобразяване с конкретната обществено-политическа ситуация Съдът оценява като несъразмерно дълъг и съществено надхвърлящ необходимото за постигане на дефинираните цели. Натрупването на едногодишна база данни от комуникационен трафик позволява тяхното използване не само за изготвянето на подробен личностен профил (с всички проблеми, които това създава), но и постигане на точна и детайлна диференциация на трайните, обичайни, инцидентни прояви на конкретното лице, неговите контакти, увлечения, интереси, включително с отграничаването на тези, представляващи прецедент в неговото поведение и реакции. Може да се систематизират по различни критерии местата, които то посещава трайно, често, рядко или инцидентно, както и да се направи точна идентификация на лицата, с които се среща. По същата схема могат да бъдат категоризирани и разграничени и неговите контакти – лични, служебни, професионални, културни и т.н. и то с оглед спецификата на данните – с една висока степен на точност по отношение интензитета на тяхното осъществяване. Очевидно е, че този срок съдържа всички белези на несъразмерност с целта на въведената мярка, което съществено рефлектира върху оценката за конституционност на целия законов режим на запазване на данните, достъпа до тях и възможното им използване.

По тези съображения Конституционният съд счита, че прекомерно дългият срок на запазване на данните самостоятелно компрометира конституционносъобразността на приетата мярка като цяло, тъй като при тази си регламентация, съобразно предвидения период на ограничението, тя се явява непропорционална. По тази причина КС обявява за противоконституционни чл. 250а – чл. 250е, чл. 251 и чл. 251а ЗЕС, според които се съхраняват трафичните данни и се използват за разследване на престъпления.

В този контекст решенията по делата *Schrems I* [21] и *Schrems II* [22] на Съда на ЕС са интересни. Въпреки че тези два случая касаят „ква-

[21] Schrems I, CEC, дело C-362/14, решение от 6.10.2015 г.
[22] Schrems II, CEC, дело C-311/18, решение от 16.07.2020 г.

валентното ниво на защита“ на личните данни в ЕС и САЩ, решенията силно се опират на правото в областта на човешките права. В Schrems I СЕС постановява, че защитата на личните данни играе важна роля в опазването на правото на личен живот съгласно член 7 от Хартата на основните права на Европейския съюз.

Днес държавите вече наблюдават киберпространството. Например Законът за чуждестранно разузнаване на САЩ (FISA) предвижда в секция 702 процедури за събиране на информация относно комуникации на чуждестранни разузнавателни данни. Програми за наблюдение срещу тероризъм и киберпрестъпност, като UPSTREAM, разрешени по този закон, не са насочени към отделни лица, а събират данни безразборно. Европейската комисия установява в Решение 2016/1250 (вече не е в сила), че субектите на наблюдение не се оценяват въз основа на вероятна причина или друг правен стандарт, а когато значимата цел на събирането е получаване на чуждестранна разузнавателна информация. Този тип събиране на данни за борба с престъпността и тероризма се нарича „масово“ събиране. Такова наблюдение обаче е изрично обявено за нарушение на правото на личен живот в няколко скорошни решения, сред които La Quadrature du Net[23] и Privacy International.[24]

С оглед на тези факти и съображения, СЕС анулира Решение 2016/1250 в делото Schrems II, тъй като установи, че FISA не предоставя достатъчна защита на правото на личен живот. Тези два случая показват само една част от напрежението, което може да възникне между задължението за дължима грижа в киберпространството и правата на човека. САЩ биха могли да твърдят, че такова наблюдение на данни е необходимо за борба с киберзаплахите, но тъй като то би нарушило правото на личен живот, ще остане незаконно. За разлика от физическия свят, където наблюдението може да бъде ограничено, киберпространството не може да бъде наблюдавано без значително въздействие върху личния живот.

Следователно при опита за баланс между правото на личен живот и осигуряването на националната сигурност се появява един изключителен проблем. От една страна, събирането на информация безразборно противоречи на правото на личен живот, но от друга страна, в киберсферата е почти невъзможно да се открият следи за дейности, застрашаващи националната сигурност, без подобно събиране на информация. Този проблем би могъл да се превъзмогне само и единствено чрез превантивни мерки, които включват синхронизирането

[23] La Quadrature du Net и др., СЕС, съединени дела C-511/18, C-512/18 и C-520/18, решение от 6.10.2020 г.
[24] Privacy International, СЕС, дело C-623/17, решение от 6.10.2020 г.

между действия в киберсферата и в истинския живот, за да може изследването на трафика на данни да бъде насочено към конкретно лице за конкретни действия. Вероятно най-важното е да се инвестира в системи за киберсигурност, които да правят невъзможно пробиването на важни компютърни системи. Последното е, за съжаление, чест феномен в България. Необходимо е сървърните системи да са изолирани и с ограничен достъп, за да може да се сведе до минимум рискът от кибератаки.

5. Заключение

В цифровата ера балансът между правото на личен живот и необходимостта от гарантиране на националната сигурност придобиват изключителна сложност. Конституционната и международноправната уредба признават висока степен на защита на личната неприкосновеност, но същевременно допускат ограничения, когато това е оправдано от обществения интерес и защитата на държавния суверенитет. С развитието на технологиите традиционните механизми за контрол и наблюдение се оказват недостатъчни, а новите инструменти за масово събиране на данни поставят под въпрос основните права на гражданите. Практиката на Конституционния съд, на ЕСПЧ и на Съда на ЕС показва, че всяка намеса трябва да бъде законосъобразна, пропорционална и необходима в едно демократично общество.

Изходът от този правен и етичен сблъсък може да се търси в съчетаването на превантивни технически мерки за киберсигурност с ясни законови гаранции за защита на личните данни. Само чрез такъв подход ще бъде възможно да се постигне устойчиво равновесие между сигурността на държавата и неприкосновеността на личния живот – две взаимосвързани ценности, които стоят в основата на съвременната конституционна демокрация.

За тази цел е необходимо инвестиране в технологиите и инвестиране в хората. България има един от най-силните цифрови сектори – разработките на софтуер са сред най-разпространените бизнеси в нашата страна. Повече от разумно е да се търси по-тясна съвместна дейност между държавата и частния сектор, за да се подсигури по-задълбочена киберсигурност. Това е един потенциал, който не е използван достатъчно, а би могъл значително да подобри националната сигурност, включително и сигурността, че гражданите ще се ползват от своите права в цифровата среда безпроблемно.