



Република България  
ИКОНОМИЧЕСКИ  
И СОЦИАЛЕН СЪВЕТ

## **РЕЗОЛЮЦИЯ**

на тема

**"Предизвикателства пред българските граждани от  
рисковете на глобалната цифрова среда"**

(разработена по собствена инициатива)

София, 2019 г.

Председателският съвет на Икономическия и социален съвет взе решение за разработване на резолюция на тема „Предизвикателства пред българските граждани от рисковете на глобалната цифрова среда”.

За докладчик беше определен Богомил Николов – член на ИСС от група III – други организации.

На свое заседание от 11 юли 2019 г. Пленарната сесия прие резолюцията.

## ПОЛЗВАНИ СЪКРАЩЕНИЯ

ЕИСК	Европейски икономически и социален комитет
ЕК	Европейска комисия
ЕС	Европейски съюз
ЕП	Европейски парламент
ОИСР	Организация за икономическо сътрудничество и развитие
ИИ	Изкуствен интелект
НСИ	Национален статистически институт

## **1. ИЗВОДИ И ПРЕПОРЪКИ**

- 1.1.** Икономическият и социален съвет (ИСС) отбелязва, че през последните 5 години използването на интернет в България нараства, като в този период броят на потребителите, ползващи мобилна широколентова връзка, се е увеличил над 4 пъти. Децата влизат за пръв път в интернет на все по-ранна възраст и тази граница устойчиво пада и за нашата страна. Същевременно данните сочат, че преди да навършат 11 години, близо 90% от тях вече са станали интернет потребители.
- 1.2.** ИСС констатира, че положителната тенденция на проникване и развитие на интернет достъпа и свързаните с него технологии създават редица предизвикателства относно липсата на умения за използване на цифровите технологии и изправят българските граждани пред непознати досега рискове и заплахи. Сред тях могат да се открият физическата безопасност, особено при децата; неприкосновеността на личното пространство и личната информация; кражбите на картови данни и измамите при плащания; фалшивите новини, зловредните влияния и радикализъм и др.
- 1.3.** ИСС изразява загриженост, че децата са изложени на най-големи рискове при използването на социалните мрежи. Сериозен проблем според ИСС са и прекомерната употреба на интернет и пристрастяването на съвременните деца към цифровите устройства.
- 1.4.** В този контекст ИСС препоръчва проблемите, произтичащи от цифровизацията и разрастването на употребата на интернет в България да се превърнат в обект на постоянно целево внимание и прилагане на специфични мерки и интегрирани политики от страна на държавата. Тези мерки приоритетно следва да са насочени към социално уязвимите групи от населението, като деца и възрастни граждани, които са изложени на значителни рискове.
- 1.5.** Според ИСС възможностите, които цифровизацията предоставя, могат да се реализират в пълна степен само ако се обединят усилията на всички заинтересовани национални институции, социалните партньори и структури на гражданското общество, както и на гражданите. Същевременно във всяка инициатива трябва да се отдели специално внимание на организирането на информационни кампании, за да се създаде култура на цифрова безопасност.
- 1.6.** Факт е, че интернет предоставя благодатна почва за прилагане на множество измами, които не се ограничават в рамките на нито една държава. Най-значимите сред тях са свързани с електронната търговия, фалшивата идентичност и инвестиционните измами.
- 1.7.** В този контекст ИСС предлага комплекс от мерки и инициативи, които далеч не изчерпват възможностите за действие, но фокусират вниманието върху съществени мерки и действия, които могат да доведат до осезаеми резултати.

- 1.8.** С оглед ограничаването на рисковете при пазаруване от онлайн търговци извън ЕС ИСС препоръчва провеждане на широки кампании от страна на контролните държавни органи и потребителските организации сред потребителите относно рисковете от пазаруване в сайтове, регистрирани извън ЕС. Целта е да бъдат информирани и обучени гражданите как да разпознават рисковите сайтове, как да се предпазват от измами, как да защитават компютрите и електронните устройства от нерегламентиран достъп при условията на онлайн търговията и др.
- 1.9.** ИСС акцентира на важността на сключването на споразумения от страна на националните/европейските органи за надзор на пазара с подобни органи в трети страни, където преобладаващо са регистрирани онлайн магазини – Китай, САЩ и др., с оглед постигане на договорености за защита правата на потребителите, ползващи тези магазини.
- 1.10.** ИСС настоява за прилагането на по-надежден контрол върху безопасността на продуктите, внасяни от търговци извън ЕС, което предполага по-широко сътрудничество с митническите власти, онлайн платформите, обучение на бизнеса и потребителите по въпросите на безопасността на продуктите и др.
- 1.11.** По отношение на киберсигурността ИСС счита, че България може активно да се включи в работата на създадените в рамките на ЕС Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и Мрежа от национални координационни центрове. Според ИСС е важно определянето на ясни условия за сътрудничество и отношения между Европейския център и националните центрове. Същевременно е необходимо националните центрове да бъдат финансирани от ЕС, за да се работи за намаляване на съществуващите различия между европейските държави.
- 1.12.** ИСС счита, че всяка стратегия за киберсигурност трябва да съдържа и мерки за повишаване на осведомеността и безопасното поведение на гражданите. Затова във всяка инициатива трябва да се отдели специално внимание на организирането на информационни кампании, за да се изгражда култура на цифрова безопасност.
- 1.13.** В тази връзка ИСС обръща внимание на потенциала на новата програма „Цифрова Европа“ през периода 2021 – 2027 г. и призовава българските институции за активно разясняване на възможностите за участие на социалните партньори и организациите на гражданското общество, особено по приоритетните направления киберсигурност и задълбочени цифрови умения. Подчертава също значението на развитието на цифрови умения и компетенции за повишаване възможностите за адаптация на човешките ресурси към променящите се изисквания на работните места и пазара на труда.

- 1.14.** ИСС обръща специално внимание и върху равнището на познания и умения на потребителите за боравене с цифрови технологии, като се отчитат особеностите на възрастта и социалната среда. Освен да познават правата, задълженията и отговорностите си, гражданите трябва да имат адекватни умения за боравене с цифровото съдържание. В този смисъл ИСС счита, че трябва да се насърчават инициативи за развиване на цифрова грамотност.
- 1.15.** ИСС подчертава изключителното значение на образованието и цифровите умения и препоръчва на институциите, в сътрудничество със социалните партньори, да работят за интегриране на интернет грамотността и уменията в учебните програми на всички етапи от образованието с акцент върху рисковете и подходящото поведение в онлайн среда.
- 1.16.** Според ИСС финансовата грамотност и образованието могат да играят важна роля за засилване защитата на потребителите, повишаване на осведомеността и информираността относно цифровите финанси, увеличаване на финансовата грамотност за използването на цифровите финанси и за засилване на общото доверие на потребителите в тях.
- 1.17.** ИСС и в други свои актове е изразявал подкрепа за развиването на мобилното здравеопазване, с което може да се постигне по-равноправен достъп до здравно обслужване за хората от отдалечени райони. Същевременно ИСС призовава за спазване на изискванията за безопасност на решенията в областта на мобилното здравеопазване, което би породило по-голямо доверие у гражданите.
- 1.18.** Изкуственият интелект (ИИ) навлиза бързо в съвременната икономика и често заменя хората в сектора на множество логистични и клиентски услуги. Същевременно се наблюдават безпокойство и недоверие от страна на гражданите дали ще запазят контрола над машината и контрола над своя живот. Във връзка с това ИСС апелира да се разработи и приеме национална стратегия относно ИИ в контекста на стратегията „Изкуствен интелект за Европа“ и както е предвидено в Координирания план за ИИ.

## **2. ВЪВЕДЕНИЕ**

- 2.1.** Проблемите и предизвикателствата за гражданите, произтичащи от използването на цифрови и интернет технологии в България досега не са били предмет на специализирани разработки на Икономическия и социален съвет. Изразявайки разбирането, че основна функция и грижа на държавата са повишаването на качеството на живот на всеки български гражданин и осигуряването на адекватна социална защита за уязвимите групи, ИСС счита, че бързото развитие на цифровите технологии поставя сериозни предизвикателства пред значима част от българските граждани.
- 2.2.** През последните години използването на интернет в България нараства систематично. Ако през 2014 г. достъп до интернет са имали 56,7% от

домакинствата, то през 2018 г. техният дял достига 72,1%. В същото време в страната намалява и делът на лицата, които никога не са използвали интернет - 26,7% през 2018 г. при 37,1% през 2014 г. и 70,6% през 2006 г.

- 2.3. В България особено силно впечатление правят ръстът и развитието на ширококоловия достъп до интернет през последните 5 години, като в този период броят на потребителите, ползващи мобилна ширококолова връзка, се е увеличил над 4 пъти. Същевременно относителният дял на домакинствата с достъп до интернет (72,1%) съвпада почти напълно с дела на тези с достъп до ширококолов достъп (71,5% за 2018 г.).<sup>1</sup>
- 2.4. ИСС отчита, че тези процеси са следствие както на интензивното технологично развитие, така и на действието на редица държавни политики, застъпени в Националната стратегия за развитие на ширококоловия достъп в Република България (2012 – 2015), Националният план за ширококолова инфраструктура за достъп от следващо поколение, разработен като програмен документ за ползване на средства от ЕС за програмен период 2014 – 2020 г., Националната програма „Цифрова България 2015 г.“ и др.
- 2.5. Високата скорост на проникване и развитие на интернет достъпа и свързаните с него технологии поставя редица предизвикателства пред българските граждани, свързани с липсата на умения за използване на цифровите технологии. ИСС изразява своята загриженост, че за голяма част от гражданите използването на тези технологии е ново и те не разполагат дори с минимална квалификация и опит за ефективното им и безопасно използване.
- 2.6. Според ИСС особено внимание трябва да се обърне на социално уязвимите групи от населението, като деца и възрастни граждани, за които използването на тези технологии представлява по-голямо предизвикателство и/или крие значителни рискове, свързани с физическата безопасност, икономическите интереси при пазаруване, изложеност на зловредни влияния, сигурност на личните данни и др.
- 2.7. ИСС изразява загриженост, че децата са изложени на най-големи рискове при използване на интернет. Докато умерената употреба на цифровите технологии може да е от полза за психичното благополучие на децата, то прекаленото им използване води до отрицателно въздействие и пристрастяване не толкова към цифровите устройства, колкото към цифровото съдържание (видео и интернет игри, форуми и др.), което при целенасочена употреба може да се използва за обучение и придобиване на знания. В този смисъл сериозен проблем според ИСС е прекомерната употреба на интернет не по предназначение. Това създава опасност за физическата и психическата неприкосновеност на децата и води до сериозно ограничаване на физическата им активност.

---

<sup>1</sup> НСИ, Използване на ИКТ от домакинствата, [https://infostat.nsi.bg/infostat/pages/module.jsf?x\\_2=240](https://infostat.nsi.bg/infostat/pages/module.jsf?x_2=240)

**2.8.** В тази връзка ИСС счита, че е необходимо проблемите, произтичащи от цифровизацията и разрастването на употребата на интернет в България, да се превърнат в обект на постоянно целево внимание и прилагане на специфични мерки и политики.

### **3. ИДЕНТИФИЦИРАНЕ НА РИСКОВЕТЕ ПРЕД БЪЛГАРСКИТЕ ГРАЖДАНИ, ПРОИЗТИЧАЩИ ОТ ИЗПОЛЗВАНЕТО НА ЦИФРОВИ И ИНТЕРНЕТ БАЗИРАНИ ТЕХНОЛОГИИ**

**3.1.** Скоростното разпространение и развитие на цифровите и интернет базираните технологии способстват за появата на множество нови и непознати досега рискове и заплахи за гражданите относно:

**3.1.1.** физическата безопасност, особено при децата (напр. случаи на заплашване или нападение от тези, с които контактуват онлайн);

**3.1.2.** фалшивите новини, идейните влияния и радикализма;

**3.1.3.** собствеността (напр. отдаване под наем през онлайн платформа);

**3.1.4.** личната информация - интернет технологиите превърнаха личните данни във високо търсена стока, която застрашава неприкосновеността на личното пространство;

**3.1.5.** финансовите рискове - кражба на картови данни, измами при плащания, заплащане за услуга, която никога не получават, и др.

#### **3.2. Рискове при онлайн пазаруване извън ЕС**

**3.2.1.** ИСС гледа положително на тенденциите на разширяване възможностите за дистанционно пазаруване в онлайн средата, защото пред потребителите се откриват възможности да пазаруват от сайтове не само на български или европейски търговци (от ЕС), но и на такива от всяка точка на света. ИСС подчертава, че европейските потребители разполагат с ясно регламентирани права за пазаруване онлайн, включващи:

- правото на преддоговорна информация;
- защитата от неравноправни клаузи;
- защитата от нелоялни търговски практики (в т.ч. заблуждаващи и агресивни);
- защитата на личните данни на потребителя;
- правото да получи пълно съответствие на стоката с договореното посредством законова и търговска гаранция;
- правото на връщане (отказ), без да посочва причина за това, без да дължи обезщетение или неустойка, в 14-дневен срок;
- правото на алтернативно решаване на спор, възникнал във взаимоотношението с търговец.



**3.2.2.** Същевременно ИСС напомня, че не така стои въпросът със защитата на потребителите и техните права при пазаруване от онлайн магазини, регистрирани извън ЕС. Основната причина е, че при тези пазарувания не действат защитите, които потребителят има при пазаруване в рамките на ЕС. Освен това правоприлагането е затруднено, тъй като контролните органи (национални или европейски) не могат да налагат санкции и да упражняват контролните си функции и правомощия извън рамките на ЕС.

**3.2.3.** ИСС обръща специално внимание върху основните рискове и проблеми при пазаруване от търговци извън ЕС:

3.2.3.1. Предоставяне на непълна или заблуждаваща информация за стоката и нейната цена (предлага се при изключително примамливи условия, което поражда съмнение за дефектен продукт, фалшив продукт или фалшива оферта).

3.2.3.2. Доставка на фалшиви стоки (имитация) – обикновено се разпознават по подозрително ниската цена; евтината опаковка, която не кореспондира с очаквания скъп продукт; липсата на характерни холограми, които някои марки ползват за защита на продуктите си.

3.2.3.3. Пазаруването от непознати търговци е предпоставка и риск за доставка на фалшификати - ако търговец, който за първи път срещаме в онлайн пространството, предлага модни аксесоари от последната колекция на половин цена, най-вероятно същият доставя имитации.

3.2.3.4. Вредните фалшиви отзиви създават опасност от безрезервно доверяване на неискрени онлайн мнения на клиенти, което може да е подвеждащо - клиентът може да е стимулиран да напише нещо положително в замяна на облага или самите търговци публикуват фалшиви отзиви.<sup>2</sup>

3.2.3.5. Плащане цената на стоката без наличие на необходимото доверие в отсрещната страна, поради което може съществено да се затрудни/да се направи невъзможно връщането на платената сума при проблем със закупената стока или при недоставянето ѝ.

3.2.3.6. Неравноправни клаузи и условия (липса на гаранция, липса на право на връщане и др.).

3.2.3.7. Липсваща, непълна или подвеждаща информация относно търговеца, поради което комуникацията с него при проблем е невъзможна.

---

<sup>2</sup> Пример: Проучване с тайни клиенти на английската асоциация на потребителите разкри цели мрежи от фейсбук групи, създадени да възстановяват на купувачите покупки от американски търговци срещу положителни отзиви и онлайн магазини, които изискват високи рейтинги от клиенти срещу възможност за връщане на стоки.

3.2.3.8. При пазаруване от търговци извън ЕС решаването на спорове и проблеми става много трудно, а често и невъзможно. Дори когато сайтът е на български или адресът завършва с .bg, няма гаранция, че той е с регистрация в България.

### **3.3. Сигурност на свързани с интернет устройства - „интернет на нещата“**

**3.3.1.** ИСС счита, че при условията на разрастващия се „интернет на нещата“, дефиниран като взаимно свързване чрез интернет на изчислителни устройства, вградени в ежедневните обекти, което им позволява да изпращат и получават данни, се предоставят нови възможности за потребителите, но същевременно се генерират непознати досега рискове относно сигурността и безопасността.

**3.3.2.** Интернет може да свързва устройства от различни производители, търговци на дребно или разработчици на софтуер. Това може да направи много по-трудно установяването кой е отговорен, когато нещо се обърка. Затова ИСС счита, че трябва да се работи за ясна и стабилна рамка за отговорност за продуктите. Трябва да е ясно кой субект отговаря за изпълнението и сигурността по време на пълния живот на свързания продукт.

**3.3.3.** След множество скандални разкрития по света за изтичане на данни чрез свързани устройства стана ясно, че трябва да се предприемат мерки, гарантиращи принципа, че собственикът на устройство трябва да контролира как и от кого се използват данните, които генерира. Настройките на всеки свързан продукт трябва да бъдат зададени по подразбиране на най-високото ниво на защита на личния живот, а потребителите трябва да са наясно с последиците от това как данните, събрани чрез интернет, могат да бъдат използвани.

**3.3.4.** Потребителите трябва да имат достъп до висококачествена и високоскоростна интернет връзка. Затова според ИСС следва да се обърне особено внимание на осигуряването на достъп за маргинализирани или уязвими групи потребители, в т.ч. в отдалечени географски райони и при спазване на принципа за неутралност на мрежата.

**3.3.5.** Също така следва да се гарантира, че потребителите получават ясна, кратка и лесно разбираема информация за свързаните продукти и по-специално за това, което един продукт може/не може да направи, без да е свързан, вместо широко разпространеното "съгласен съм с общите условия". Критичната информация трябва да бъде поставена на видно място преди покупката.

**3.3.6.** Цифровите технологии промениха естеството на много продукти поради свързания софтуер. ИСС счита, че функционалността на продуктите не

трябва да се ограничава от права върху софтуера или от липсата на актуализация и поддръжка, както и трябва да се гарантира работа без връзка с интернет.

**3.3.7.** Интернет на нещата предоставя на хакерите повече уязвимости. Съществуващото законодателство и стандарти за безопасност на продуктите се ограничават до безопасността на физическите устройства. ИСС споделя мнението, че за да се гарантира сигурността, следва да се преразгледа понятието „безопасност“ и законодателството да бъде актуализирано, отчитайки новите проблеми, свързани с киберсигурността, сигурността на данните и безопасността на продуктите.

### **3.4. Сигурност на онлайн разплащанията**

**3.4.1.** Успешното развитие на интернет базирана икономика предполага развити системи за онлайн разплащания и високо доверие на потребителите в тях. ИСС констатира, че понастоящем България е на първо място по използване на кешови разплащания при доставката на продукти, поръчани онлайн с 62% при средно за ЕС 18%.<sup>3</sup>

**3.4.2.** По данни на ОИСР през 2015 г. около 2,5% от гражданите на Франция и Великобритания са претърпели финансови загуби в резултат от неоторизирани/измамни онлайн разплащания в рамките на период от три месеца.<sup>4</sup> В условията на липса на подобни статистически данни за България не може категорично да се определи размерът на този проблем в нашата страна, още повече в контекста на споменатите преобладаващи разплащания в брой.

**3.4.3.** При разглеждането на сигурността на онлайн плащанията трябва да се отчетат особеностите в защитата при различните платежни механизми. Като цяло защитата при кредитните карти е по-висока, отколкото при дебитните карти и банковите преводи, тъй като потребителите имат възможност да оспорват плащания при проблеми с доставката. Според ИСС е необходимо да се положат усилия за информиране на потребителите относно съществуващите мерки и процедури при различните видове плащания, което може да способства и за намаляване на плащанията в кеш.

**3.4.4.** Без адекватна сигурност на плащанията данните, предоставени в контекста на плащанията за електронна търговия, могат да бъдат изгубени, откраднати или обект на друга злоупотреба, особено при използване на мобилни устройства, поради по-високия риск от изгубване, открадване или компрометиране. В тази връзка ИСС счита, че криптирането и динамичното

<sup>3</sup> Consumer Conditions Scoreboard: Consumers at home in the Single Market, 2015.

<sup>4</sup> OECD (2017a), OECD Digital Economy Outlook 2017, <http://dx.doi.org/10.1787/9789264276284-en>; OECD (2018d), ICT Access and Usage by Households and Individuals (database), <http://oe.cd/hhind>

удостоверяване на данни биха могли да помогнат за справяне с потенциални проблеми и за повишаване на доверието на потребителите в мобилните плащания.

### **3.5. Прилагане на изкуствен интелект в онлайн услуги**

**3.5.1.** Алгоритмите, основани на изкуствен интелект (ИИ), навлизат бързо в съвременната икономика. Те често напълно заменят хората при осигуряването на множество логистични и клиентски услуги, което често поражда недоверие и безпокойство у ползвателите им. Нещо повече, ИИ систематично се използва за профилиране и персонифициране на клиентите, което изисква обработката на лични и/или нелични данни.

**3.5.2.** Липсата на достатъчно знания и разбиране за това, какво означава изкуствен интелект, вероятно е в основата на безпокойствата и недоверието доколкото хората ще запазят контрола над машината и контрола над своя живот.

**3.5.3.** ИСС отбелязва, че след приемането на стратегия относно „Изкуствен интелект за Европа“, публикувана през април 2018 г., Европейската комисия(ЕК) предложи Координиран план за изкуствения интелект, с който се формулират мерки на равнище ЕС и на национално равнище в контекста на световната конкуренция. В плана наред с мерките за увеличаване на инвестициите, подобряване на наличността и достъпността на данните, подкрепа на талантите и уменията ЕК предлага да се формулират и мерки за гарантиране на доверието.

**3.5.4.** Във връзка с това ИСС апелира за навременно приемане на национална стратегия относно ИИ, както е предвидено в Координирания план за ИИ.

**3.5.5.** ИСС напомня, че в свое становище<sup>5</sup> ЕИСК призовава за по-добри статистически данни и повече научни изследвания относно последиците от ИИ за заетостта и труда, включително проучвания за специфичните за отраслите въздействия. Повече познания и разбиране за естеството и функционирането на ИИ са необходими също и за повишаване на доверието на хората въз основа на критично мислене.

**3.5.6.** ИСС изцяло подкрепя позицията на ЕИСК и счита, че мерките за преодоляване на недоверието в ИИ следва да отчитат както стимулирането на възможностите, произтичащи от технологиите, така и етичните, екологичните и социалните аспекти, свързани с тяхното налагане.

### **3.6. Отговорност на онлайн платформите**

**3.6.1.** развитието на онлайн платформите за информация и търговия също поставиха редица въпроси и създадоха опасения сред гражданите. Според

---

<sup>5</sup> Становище на ЕИСК, INT/877 Координиран план за изкуствения интелект.

проучване на Евробарометър от 2016 г.<sup>6</sup> 72% от потребителите имат притеснения относно събраните за тях данни. В същото време 56% признават, че не са прочели условията за ползване на онлайн платформите. От друга страна, 75% от гражданите считат, че е необходима повече прозрачност при подреждането на резултатите при търсене, идентифицирането на действителния доставчик на стока или услуга или фалшиви рецензии.

**3.6.2.** ИСС приветства усилията на ЕС за разработване и приемане на Регламент за онлайн платформите (Регламента), с който се създадоха предпоставки за равнопоставеност за съпоставими цифрови услуги, отговорно поведение на онлайн платформите, прозрачност и безпристрастност, отворени и недискриминиращи пазари в икономика, основана на данни.

**3.6.3.** ИСС подчертава и необходимостта от засилване на координацията между националните надзорни органи от държавите - членки на ЕС, с оглед осигуряване на ефективно прилагане на изискванията на Регламента.

**3.6.4.** ИСС счита също, че е необходима по-широка информационна кампания за информиране на българските граждани и МСП относно приетите изисквания към онлайн платформите с оглед ефективната защита на правата на граждани и фирми при ползването им.

### **3.7. Социални предизвикателства - рискове в социалните мрежи**

**3.7.1.** Интернет предоставя благодатна почва за прилагане на множество измами, които не се ограничават в рамките на нито една държава. Най-значимите сред тях са:

3.7.1.1. Измамите, свързани с електронна търговия, когато потребителите плащат за стоки, които след това се оказват фалшиви, дефектни или некачествени. В някои случаи стоките никога не биват доставяни.

3.7.1.2. Инвестиционните измами, когато се рекламира твърде добра инвестиционна възможност, като се използват новини и реклами, които изглеждат като от реално съществуващи източници. Потребителите, които са изкушени да инвестират в такива инвестиционни измами, могат да загубят съществена част от парите си.

3.7.1.3. Фалшивата идентичност, когато е налице представяне като автентична марка, истински приятели или роднини, за да се спечели доверието на потребителя и им се предлага да купуват стоки, да изпращат пари или да изтеглят зловерен софтуер на компютъра си.

---

<sup>6</sup> Специално проучване на Евробарометър 447 относно онлайн платформите (2016 г.).

**3.7.2.** Социалните мрежи от своя страна са поле за множество рискове, свързани предимно със:

3.7.2.1. Незаконно използване на лична информация от трети страни, които биха могли например да намерят начин да копират и обобщават потребителски профили, да събират лична финансова информация или да копират лична информация и да я използват за свои цели.

3.7.2.2. Кражба на самоличност, когато някой незаконно придобива и използва личните данни на друго лице по начин, който включва измама или заблуда, обикновено с цел извличане на икономическа изгода.

3.7.2.3. Кибер тормоз и преследване, когато е налице целево, умишлено, неуравновесено и престъпно използване на цифрови технологии с цел обида, публично унижение, разпространение на слухове и лъжи, както и преследване на лице в реалния му живот посредством цифрова технология.

**3.7.3.** Потребителите страдат от най-много измами, които проникват през WhatsApp и Facebook, следвани от Instagram и Twitter.<sup>7</sup>

### **3.8. Социални предизвикателства - рискове за децата**

**3.8.1.** Според национално представително изследване на Фондация „Приложни изследвания и комуникации“ от 2016 г. почти всички български деца (97%), на възраст между 9 и 17 години използват интернет, като същевременно наличието на деца в семейството съществено повишава вероятността за наличие на широколентов достъп до интернет връзка у дома. Възрастта, в която децата влизат за пръв път в интернет, устойчиво пада, като най-ранната възраст е 4 години (3%) и 5 години (6,8%). Почти една четвърт (24,3%) от децата са имали първия си контакт с Мрежата на седемгодишна възраст, а преди да навършат 11 години, близо 90% вече са станали интернет потребители. Средната възраст, на която децата за пръв път влизат в интернет през 2016 г., е 8 години, докато през 2010 е била 9.<sup>8</sup>

**3.8.2.** Изследването разкрива също, че децата използват интернет най-много за гледане на клипове 68,8%, използване на социални мрежи (64,9%), играене на игри онлайн (55,3%) и слушане на музика (54,2%). ИСС обръща внимание на констатацията, че за децата най-големи са рисковете при използване на социалните мрежи. Водещо място сред тях заемат контактите с непознати, неподходящото съдържание, виртуалният или сексуален

<sup>7</sup> Consumers International, Social media scams: Understanding the consumer experience to create a safer digital world, 2019.

<sup>8</sup> Онлайн поведение на децата в България: рискове и вреди, национално представително изследване, 2016 г., Фондация „Приложни изследвания и комуникации“  
[https://www.safenet.bg/images/sampleddata/files/Risks\\_Harm-BG.pdf](https://www.safenet.bg/images/sampleddata/files/Risks_Harm-BG.pdf)

тормоз. Според ИСС сериозен проблем са и прекомерната употреба на интернет и пристрастяването.

#### **4. ПРЕДЛОЖЕНИЯ ЗА ЗАСИЛВАНЕ НА ВЪЗМОЖНОСТИТЕ, ПРОИЗТИЧАЩИ ОТ ЦИФРОВИЗАЦИЯТА**

##### **4.1. Развитие на цифрова грамотност**

**4.1.1.** Като подчертава изключителното значение на образованието и цифровите умения, ИСС се присъединява към препоръката на ОИСР <sup>9</sup> към правителствата, че трябва да насърчават повишаването на осведомеността и образованието като основни инструменти за овластяване на родителите и децата например чрез:

- интегриране на интернет грамотността и уменията в учебните програми с акцент върху рисковете и подходящото поведение в онлайн среда;
- обучение и насърчаване на други заинтересовани страни да образуват и повишат осведомеността на децата и родителите;
- редовно измерване на развитието на тяхната интернет грамотност.

**4.1.2.** ИСС призовава за провеждане на обучение в цифрова грамотност на всички етапи от образованието. В него трябва да се отреди специален фокус върху онлайн безопасността, сигурността в интернет, критичното разбиране и оценка на информацията, онлайн етикетът и други социални умения.

##### **4.2. Цифрова грамотност във финансовите услуги**

**4.2.1.** Цифровите финансови услуги са технологии, включително електронни пари, мобилни финансови услуги, онлайн финансови услуги, банкова дейност без клонове и др., които са глобално явление. Те предлагат неограничени възможности за интегриране на по-бедните и финансово изключени слоеве от населението, които не са банкирали преди това, чрез: разширяване на достъпа, включително до нови видове финансови услуги при преодоляване на физическите инфраструктурни бариери; намаляване на разходите и осигуряване на по-достъпни финанси за всички; предлагане на по-удобни, по-бързи, сигурни и навременни сделки; и осигуряване на безпроблемно потребителско преживяване, съобразено с индивидуалните нужди.

**4.2.2.** Предизвикателствата за потребителите при достъпа и използването на цифровите финанси могат да произтичат от цялостната липса на информираност и знания за финансовите концепции или цифровите технологии. Съответно те могат да се дължат на: по-ниско ниво на обща

---

<sup>9</sup> Препоръка на ОИСР за децата от 2012 г., ОИСР, 2012 г.

грамотност; ограничена обща финансова грамотност; непознаване или липса на познания за финансовите услуги и съответното регулиране; липса на специфична осведоменост или познания за цифрови финанси; неадекватно ниво на общи цифрови умения и компетенции; и липса на познаване на технологиите и/или финансите.<sup>10</sup>

**4.2.3.** ИСС счита, че финансовата грамотност и образованието могат да играят важна роля за засилване защитата на потребителите, повишаване на осведомеността и информираността относно цифровите финанси, увеличаване на финансовата грамотност за използването на цифровите финанси и за засилване на общото доверие на потребителите в тях.

### **4.3. Цифрова грамотност в здравеопазването**

**4.3.1.** Експертни изчисления показват, че приблизително 15% от разходите за ползване на здравно обслужване могат да бъдат спестени чрез дистанционно наблюдение с помощта на решения в областта на мобилното здравеопазване.<sup>11</sup> ИСС споделя виждането, че мобилното здравеопазване може да допринесе за постигането на по-равноправен достъп до здравно обслужване, тъй като технологиите обхващат отдалечени райони и групи от хора, които биха имали затруднен достъп до здравно обслужване.

**4.3.2.** В тази връзка ИСС счита, че е необходима информационна кампания, която да подпомогне информираността на гражданите относно наличните възможности на електронното здравеопазване за електронен достъп до техните данни за извършени медицински манипулации, с цел личен контрол над злоупотребите към НЗОК.

**4.3.3.** Същевременно ИСС изразява загриженост относно гарантирането на безопасността на решенията в областта на мобилното здравеопазване и на приложенията, засягащи начина на живот и благосъстоянието, което обяснява потенциалната липса на доверие у гражданите. От друга страна, според ИСС безопасността може да се демонстрира, като се използват стандарти за безопасност на потребителите или специални знаци за качество.

**4.3.4.** Повод за загриженост будят и възможните случаи, когато гражданите биха използвали резултатите от дадено техническо решение или приложение в областта на мобилното здравеопазване, за да вземат самостоятелно решение, което може да застраши собственото им здраве, или когато дадено техническо решение в областта на мобилното здравеопазване погрешно сочи, че лицето е в добро здраве.

---

<sup>10</sup> OECD (2017), G20/OECD INFE Report on ensuring financial education and consumer protection for all in the digital age.

<sup>11</sup> Зелена книга относно мобилното здравеопазване, COM(2014)219.



#### **4.4. Цифрово изключване**

**4.4.1.** ИСС обръща специално внимание на факта, че нуждите на маргинализираните или уязвими потребители, както и на потребителите в неравностойно положение трябва да бъдат взети под внимание при разработката на платформите за онлайн търговия и процесите на електронната търговия, като плащания и доставки, за да се намали опасността от по-нататъшна маргинализация и социално изключване.

**4.4.2.** Във връзка с добиващата популярност на икономиката на споделянето е нужно да се отбележи, че една постоянно увеличаваща се група от потребители остава незасегната от предимствата на интернет технологията, що се отнася до споделяне и наем на функционален ресурс. Това е от изключителна важност не само в контекста на застаряващото население в България, но и предвид растящите цени на ресурсите по света.

#### **4.5. Неприкосновеност на личния живот и кореспонденция**

**4.5.1.** ИСС призовава за стриктно прилагане на високите стандарти за защита на личните данни и неприкосновеността на личния живот, установени в европейското законодателство, както в материалните разпоредби, така и в процесуалното законодателство. Гражданите трябва да могат да упражняват пълен контрол върху своите лични данни - как те се събират, използват и дали се споделят, както и да са в състояние да защитят неприкосновеността на личния си живот.

#### **4.6. Мрежова неутралност в България**

**4.6.1.** Неутралността на мрежата е принцип, при който всички електронни съобщения, които преминават през интернет, се третират еднакво без дискриминация, ограничение или намеса, независимо от подателя, получателя, вида, съдържанието, устройството, услугите или приложението.

**4.6.2.** България е сред седемте страни в ЕС, които са заложили на фиксирана относително ниска глоба (100 000 евро) при нарушения, свързани с неутралността на мрежата. Според ИСС, за да бъде възпираща и пропорционална на нарушението, е нужно санкцията да бъде базирана върху годишния оборот на установеното в нарушение дружество.

(п)

**проф. д-р Лалко Дулевски**

**ПРЕДСЕДАТЕЛ НА ИКОНОМИЧЕСКИ И СОЦИАЛЕН СЪВЕТ**