Права на децата в дигиталния свят. Приобщаващо цифрово образование.

Вероника Узунова

Children's Rights in the Digital World. Inclusive Digital Education.

Veronika Uzunova

Abstract:

Access to and use of the digital environment are essential for the realization of children’s rights and fundamental freedoms, for their inclusion, education, and participation, and for maintaining family and social relationships. If children lack access to the digital environment or if that access is limited due to poor connectivity, their ability to fully exercise their human rights may be compromised.

The shortcomings of educational systems and distance learning have had a particularly strong impact on students for whom the digital divide is most pronounced. As digital and learning spaces transform, a stronger foundation must be built to create sustainable and resilient systems.

Keywords: access, digital environment, rights, children, inclusive education, cybersecurity, digitization.

For contacts: Assist. Prof. Veronika Uzunova, PhD, Paisii Hilendarski University of Plovdiv, veronika.uzunova@uni-plovdiv.bg

ВЪВЕДЕНИЕ

„Нарушаването на детските права в онлайн среда се проявява под различни форми – кибертормоз, онлайн сексуална експлоатация, разпространение на лични данни, както и реч на омразата. Кибертормозът се утвърждава като едно от най-сериозните предизвикателства, тъй като води до сериозни последици за психичното и емоционалното здраве на децата – включително тревожност, депресия, социална изолация и дори склонност към самонараняване. Ето защо съществува спешна необходимост от създаване и прилагане на ефективни политики и механизми за защита на децата в дигиталната ера, както и от засилване на информираността сред родители, учители и самите млади хора“ (Стоева 2025).

Дигитализацията на множество процеси и използването на различни електронни услуги спестява време и ресурси на гражданите и бизнеса, оптимизира и работата на административните органи. Как обаче това влияе върху киберустойчивостта на системите, защитени ли са данните.

България като членка на Европейския съюз трябва да възприема всички регулации в сферата на киберсигурността, въвеждайки ги в националното законодателство. За съжаление събития като атаката срещу административните съдилища са ежедневие, което показва, че държавните институции са недостатъчно защитени. А държавната администрация и всички институции следват да бъдат едни от най-регулираните и защитените.

От години действа Законът за киберсигурност, има и допълнителна наредба за минимални изисквания в мрежовата информационна сигурност. Това означава, че нещата на хартия поне съществуват, остава да бъдат приложени адекватно.

ИЗЛОЖЕНИЕ

Както отбелязва Vincent-Lancrin, Stéphan (2022), „има два важни аспекта на дискусията за „дигитализация “в образованието, включително и дигитализацията на **приобщаващото образование**. Според него, първият въпрос относно дигитализацията на приобщаващото образование е свързан с връзката на образованието с потребностите на обществото и на пазара на труда като фокусира към решения, свързани с учебната програма; дигиталните умения на обучавани и обучаващи; и иновации с креативност, критично мислене, комуникация и сътрудничество във времена на широко разпространение на интелигентните технологии Вторият въпрос относно дигитализацията на приобщаващото образование се отнася до промените, които технологиите биха могли да предизвикат в предоставянето на образование, от ранна детска възраст до обучение за възрастни (по Vincent-Lancrin, 2022). „При осъществяване на дигиталното приобщаващо образование неминуемо се поставя за решаване проблематиката за киберсигурността му. Киберсигурността осигурява защита на потребителските профили, потребителските сърфирания в Интернет, потребителските данни и обмена на информация между отделните потребители.

Едно от най-популярните дефиниции на киберсигурността я определя като „организация и съвкупност от ресурси, процеси и структури, използвани за защита на киберпространството, от събития, които се нарушават де юре и де факто с правата на собствеността“ (Левтерова – Гаджалова - 2024).

Интерес представлява Решение № 2602 от 11.09.2024 г. на АдмС - Русе по адм. д. № 321/2021 г. за неоторизирания достъп до лични данни на милиони български граждани, съхранявани например в базите данни на НАП, Върховният административен съд на Република България е отправил преюдициално запитване до Съда на Европейския съюз като последния се е произнесъл с Решение от 14.12.2023 г. по образуваното пред него дело C-340/21. С решението е прието следното:

1) Членове 24 и 32 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година 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) трябва да се тълкуват в смисъл, че неразрешено разкриване на лични данни или неразрешен достъп до такива данни от "трета страна" по смисъла на член 4, точка 10 от този регламент сами по себе си не са достатъчни, за да се приеме, че приложените от съответния администратор технически и организационни мерки не са "подходящи" по смисъла на тези членове 24 и 32.

2) Член 32 от Регламент 2016/679 трябва да се тълкува в смисъл, че преценката дали приложените от администратора технически и организационни мерки по този член са подходящи трябва да бъде направена от националните юрисдикции конкретно, като се вземат предвид рисковете, свързани със съответното обработване, и като се прецени дали естеството, обхватът и прилагането на тези мерки са съобразени с тези рискове.

Съгласно чл. 4, § 7 от **Общ регламент относно защитата на данните**, според който Администратор означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя

целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка. В това си качество НАП следва задължително да спазва принципите, обективирани в чл. 5, § 1, букви "а" до "е". Необходимо е да се посочи, че принципа на цялостност и поверителност (буква "е") изисква личните данни да бъдат обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки.

Съгласно чл. 3, ал. 4 от Закона за киберсигурност, съгласно който субектите по чл. 4, ал. 1, т. 1 и 2 поддържат система за управление на сигурността на информацията, която включва следните минимални организационни мерки:

1. разпределение на отговорностите за мрежовата и информационната сигурност;
2. прилагане на политика за мрежовата и информационната сигурност;
3. управление на:
   а) риска;
   б) информационните активи, включително човешките ресурси;
   в) инцидентите;
   г) достъпите (физически и логически);
   д) измененията;
   е) непрекъснатостта на дейността и/или услугите (съществени, цифрови);
   ж) взаимодействията с трети страни.

Децата са най-уязвими и следва да се следи за претърпени неимуществени вреди и отрицателни емоции – срам, унижение, безпокойство, притеснение, особено при децата със специални образователни потребности.

Съществува и външна намеса относно компютърните игри и най-разнородни приложения, които използват децата като атака извършена от външни хакери, които са използвали съвременни техники и инструменти за проникване в системите на приложенията като са се възползвали от слабостите в системите и липсата на адекватни мерки за защита.

Вътрешни пропуски като липса на редовни актуализации на софтуер, неадекватни мерки за контрол на достъпа и недостатъчно обучение на персонала, може да улесни успешното проникване на хакерите. Личните и чувствителни данни в базата данни може да не са били криптирани, което ще увеличи риска от **изтичане на лични данни.** Съгласно чл. 4, т. 1 от Регламент (ЕС) 2016/679. „лични данни" означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни"); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната,

генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

Съгласно Решение № 51 на МС от 23.01.2023 г. за приемане на Национална програма за превенция на насилието и злоупотребата с деца (2023-2026 г.) и на План за действие за изпълнение на Националната програма за превенция на насилието и злоупотребата с деца (2023 - 2024 г.) в Цел 3, т. *4.4.* е уредено *изграждане* ***на приобщаващи модели и разбиране на различията****. Следва да се утвърдят и да се дадат добри практики за социализация на децата с комплексни нужди и множество увреждания и децата с психични страдания*. Те са най- уязвими при използване на Интернет пространството**.**

От изключително значение за рисковете в интернет среда е **Цел 9 от Национална програма "Цифрова България 2025", в която е уредено: гарантиране на правата на децата в цифровата среда.**

Основни мерки са:

- Организиране на информационни кампании за ограничаване на рисковете и отговорното поведение на децата в интернет среда;
- Развитие на сътрудничеството с академичните среди за въвеждане и развитие на обучение по медийна и цифрова грамотност;
- Създаване на информационни събития и кампании от членовете на Съвета на децата към Държавна агенция за закрила на детето за промотиране на цифрова компетентност и защита на правата на децата в цифрова среда;
- Борба със сексуалната експлоатация и злоупотреба с деца през компютърни системи.

ЗАКЛЮЧЕНИЕ

Най-добрият интерес на детето – всички действия, отнасящи се до деца в дигитална среда, следва да се подчиняват на принципа за най-добрия (най-висшия) интерес на детето, тъй като той е от първостепенно значение. Достъпът и използването на цифровата среда са важни за реализирането на правата и основните свободи на децата, за тяхното включване, образование, участие и за поддържане на семейните и социалните взаимоотношения. Ако децата нямат достъп до цифровата среда или когато този достъп е ограничен в резултат на лоша свързаност, способността им да упражняват в пълен обем своите човешки права може да бъде засегната.

Недостатъците на образователните системи, ученето от разстояние повлия особено силно на учащите, при които цифровото разделение е най-изразено. Когато се трансформират цифровите и учебните пространства трябва да се изгради по-добра основа за създаването на устойчиви и издържливи системи.

„Бързото развитие на новите технологии ни носи изключително много позитиви, а цялата вселена сякаш е събрана на едно място и можем да я носим навсякъде в джоба си. Модерният виртуален свят обаче **крие и своите рискове**, и то не само за индивидуалните потребители, а също така за бизнеса и най-вече за децата. Следва да се повиши информираността и познанията на учениците за рисковете в интернет пространството. Трябва да се формират умения за безопасно използване на мрежата и разпознаване на фалшиви новини.

ЛИТЕРАТУРА

[1] Левтерова – Гаджалова, Д., Тагарева, К., Сивакова, В. (2024). Наръчник за дигитално приобщаващо образование – настояще и бъдещи посоки. Университетско издателство „Паисий Хилендарски“. Пловдив. 24-25, ISBN: 978-619-202-964-7 и цит. там. лит.

[2] Стоева, Д. (2025). Нови заплахи за сигурността на България, балканите и европейския съюз. Университетско издателство „Св. св. Кирил и Методий“, Велико Търново, 146 -154. ISBN 978-619-208

[3]https://digitalk.bg/digitalk_awards/2025/02/07/4738603_kibersigurnost_v_epohata_na_burzata_digitalna/. (посетено на: 09.05.2026 г.).

[4] https://old-news.bnr.bg/post/101225066/inovativni-tehnologii-navlizat-barzo-v-advokatskite-kantori. (посетено на: 09.05.2026 г.).