

Gyermekek a kibertérben – online kockázatok klasszifikációja (4C)

Bevezetés

Köztudott, hogy a digitalizáció a gyermekek mindennapjainak is szerves részévé vált. A kiskorúak már az első éveikben kapcsolatba kerülhetnek az internettel, majd természetes módon életük minden színterét elkezdni átszöni. Az online jelenlét kétségkívül számtalan előnnyel jár, azonban kockázatokat is hordoz magával, melyek bekövetkezése károsan befolyásolhatja a gyermekek fejlődését. Az egyes kockázati típusok kategorizálása elősegítheti, hogy a kockázatokra olyan válaszingedményeket dolgozzunk ki és alkalmazzunk, melyek érdemben csökkentik a gyermekek kockázati kitettségének mértékét.

Az EU Kids Online projekt

Az elmúlt időszakban a gyerekeknek olyan kockázatokkal kellett – és vélhetően kell a jövőben is – szembenézniük, mint például az erőszakos és bántó tartalmak, zaklatás, megfélemlítés (cyberbullying), manipuláció, online kizsákmányolás (grooming), a szexuális bántalmazás és kihasználás. [1] Az Európai Bizottság Biztonságos Internet Programja által támogatott EU Kids Online 2009-es felmérés eredményei alapján tett először javaslatot egy olyan tipológiára (3C), amely három kategóriába sorolta be az online kockázatokat: tartalom (content), kapcsolat (contact) és viselkedés (conduct). [2]

A megváltozott környezet és a pandémia hatására új, frissített tipológia (4C) került kiadásra 2021-ben. Érdemes megfigyelni, hogy az említett kategóriákon belül felsorolt kockázatok egy része a gyermekeket érintő hagyományos kockázatok (pl. zaklatás, rasszizmus, szexuális kizsákmányolás) digitális változata. [3]

* Pécsi Tudományegyetem, „Oktatás és Társadalom” Neveléstudományi Doktori Iskola
Email: laszlo@bottyan.com

[1] Simsa T. (2021). Internetes szűrőszoftverek gyermek számára. *Infojegyzet.hu* 2021., (60.), [Letöltve: 2022. 10. 8.] https://www.parlament.hu/documents/10181/39233854/Infojegyzet_2021_60_internetes_szuroszoftverek.pdf/6be22509-0693-b14a-e08b-8a720f4d4d2a?t=1632477975305

[2] Livingstone, S.–Haddon, L. (2009): *EU kids online: final report 2009*.

[3] Livingstone, S.–Stoilova, M. (2021): *The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics)*. [Letöltve: 2022. 10. 8.] Hamburg: Leibniz-Institut für Medienforschung | Hans Bredow-Institut (HBI); <https://doi.org/10.21241/ssoar.71817>

[3] Livingstone, S.–Stoilova, M. (2021): *The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics)*. [Letöltve: 2022. 10. 8.] Hamburg: Leibniz-Institut für Medienforschung/ Hans Bredow-Institut (HBI); <https://doi.org/10.21241/ssoar.71817>

Kockázati kategóriák

Az egyes kockázati kategóriákat a fentebb hivatkozott felmérés a következők szerint részletezi:

- **Tartalom (Content):** olyan kockázat, amely esetén a gyermek káros, gyűlöletkeltő vagy illegális digitális tartalom címzettje, befogadója. Tartalmi kockázatok közé tartozik pl.: pornográf, erőszakos, rasszista, gyűlöletkeltő illegális tartalmak, reklám és spam, káros vagy félrevezető tanácsok, információk (pl. álhírek) fogadása;
- **Kapcsolat (Contact):** akkor beszélhetünk róla, amikor egy gyermek valamilyen interaktív kommunikáció áldozata lesz. Általában felnőtt kezdeményezi. Kapcsolati kockázatok közé tartozik pl.: zaklatás, üldözés grooming (behálózás), radikalizálás, vagy bármilyen ideológiai befolyásolás, személyes adatokkal való visszaélés;
- **Viselkedés (Conduct):** az a kockázat, amely esetén a gyermek konkrét tetteivel járul hozzá a káros tevékenységhez, azaz maga lesz az elkövető. Viselkedési kockázatok közé tartozik pl.: illegális tevékenységben való részvétel, például hackelés, mások megfélemlítése vagy zaklatása, szexuális zaklatás, káros, ártó tartalom (pl. pornográf) létrehozása vagy megosztása. [3]

A 2021-ben kiadott frissítés 4. C-je az ún. „**contract risk**”, amelynek fordításáról jelen írásom készítésének időpontjában nem találtam említést a hazai kiadványokban. Tágabb értelmezésben kötelmi jogi, szűkebb értelmezésben szerződéssel összefüggő, szerződésen alapuló kockázatnak lehetne nevezni. Ez esetben a gyermek, a digitális piac aktív résztvevője, fogyasztóként jelenik meg, ezért ezt kiemelő, jelen tanulmányomban fogyasztói kockázatként hivatkozom rá a továbbiakban.

– **Fogyasztó (Contract):** A leggyakoribb előfordulási formája, amikor egy gyermek „elfogad” (ideértve az akaratlanul, önkéntelenül, illetve tudtán kívül történő elfogadást is) bizonyos kereskedelmi- vagy szolgáltatási feltételeket valamilyen digitális termékre vagy szolgáltatásra vonatkozóan. Ilyenek pl.: csalás, szexuális célú streaming, online szerencsejáték. [3]

Az alábbi táblázatban láthatjuk összefoglalva az egyes kockázati kategóriákat alábontva egy további – agresszív, szexuális, értékalapú – rendszerezés szerint.

1. táblázat. Online kockázatok összesített táblázat

	Tartalom (Content) gyermek, mint fogadó	Kapcsolat (Contact) gyermek, mint részrtvevő	Viselkedés (Conduct) gyermek, mint kezdemenyező	Fogyasztó (Contract) gyerek, mint „szerződő fél”
Agresszív	erőszakos, gyűlöletkeltő tartalom	zaklatás, ül- dőzés, molesz- tálás	illegális tevékenység (pl. hackelés)	személyazo- nosság-lopás, csalás
Szexuális	pornográf, vagy testképzavaros tartalom	szexuális zakla- tás, grooming (behálózás)	szexuális zakla- tás, üzenetváltás	szexuális stream- ing, ember- kereskedelem
Értékek	káros, félrevezető információk	radikalizálás, ideológiai be- folyásolás	ártó tartalom létrehozása, megosztása	online szeren- csejáték

Forrás: Livingstone & Stoilova (2021).

Alapvető védekezési lehetőségek

Álláspontom szerint a fentebb ismertetett klasszifikáció jelentősége egyrésről abban áll, hogy a kockázati tényezők (kockázati csoportok) ismeretében meghatározhatók azok az alapvető intézkedések, melyek több, ugyanazon csoporthoz tartozó kockázatot csökkentenek. Másrésről az elméleti kategorizálás rámutat arra, hogy csak egyes kockázati tényezőket célzó intézkedések megtétele önmagában nem érhet célt, hanem mind a négy területen (tartalom, kapcsolat, viselkedés, fogyasztó) a minimális védekezési mechanizmusokat együttesen kell alkalmazni. Harmadrésről, amennyiben új kockázat jelenne meg, úgy valószínűsíthető, hogy ezen írásomban felsorolt védelmi intézkedések megtételével annak mértéke is csökkenthető.

Ezen alapvető intézkedések a következők szerint foglalhatóak össze:

- **Technikai védelem:** célszoftverek, pl. szűrőprogramok használata, amely képes elvégezni az internetes tartalom szelektálását és szűrését. A Nemzeti Média és Hírközlési Hatóság készített egy listát az ajánlott szűrőszoftverekről, amely magyar és angol nyelvű szoftverek elérhetőségét mutatja be. [1]

[1] Simsa T. (2021). Internetes szűrőszoftverek gyermek számára. *Infojegyzet.hu* 2021., (60.), [Letöltve: 2022. 10. 8.] https://www.parlament.hu/documents/10181/39233854/Infojegyzet_2021_60_internetes_szuroszoftverek.pdf/6be22509-0693-b14a-e08b-8a720f4d4d2a?t=163247797530

[3] Livingstone, S.–Stoilova, M. (2021): *The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics)*. [Letöltve: 2022. 10. 8.] Hamburg: Leibniz-Institut für Medienforschung | Hans Bredow-Institut (HBI); <https://doi.org/10.21241/soar.71817>

[4] Pongrácz, I. (2019): Gyermek a digitális világ útvesztőiben – Veszélyek és lehetőségek. *Miskolci Jogtudó*, 2019(2), Pp. 55–69. [Letöltve: 2022. 10. 20.] <https://jogtudo.uni-miskolc.hu/files/7394/>

- **Szülői felügyelet kialakítása:** az összes védelmi lehetőség közül a legfontosabb, a szülői támogatás, preventív és detektív értelemben. Preventív módon az online töltött tevékenység időbeli korlátozása és a hozzáférhetőség helyes megválasztása. Detektív módon pedig, hogy észleli, amikor a gyermek érzelmi fejlődésére valamilyen körülmény hatással van (például aggodalom, szorongás stb.);
- **Biztonságtudatosság növelése:** véleményem szerint még mindig nem részesül elegendő figyelemben a digitális kompetenciák mellett a biztonságtudatosság. Ennek keretében a főbb biztonsági követelmények megfogalmazásán és közvetítésén túl, azok átlátható, világos, megismertetése mutatkozik szükségserűnek, amely igazodik a gyermek érettségéhez. Ez járulhat hozzá ahhoz, hogy felismerjék milyen veszélyek leselkednek rájuk és legyen lehetőségük a kompetenciájuk folyamatos fejlesztésével megfelelő válaszintézkedésre.

Összefoglalás

Az elmúlt évek felmérései, statisztikái, továbbá a nemzetközi szervezetek ajánlásai megerősítik, hogy napjainkban a kibertérben való jelenlét erősen ki van téve az online kockázatoknak. A fiataloknak ugyanakkor az internet a természetes közeg, ennek kizárása nem lehet megoldás a problémára. [4] Kockázatmentes online környezet ugyan nem érhető el, de a tudatosság növelésével lehetőségünk nyílik a biztonságosabb környezet megteremtésére. Ehhez elengedhetetlen, hogy felismerjük, azonosítsuk és kategorizáljuk az egyes kockázatok, de legalább a főbb kockázati csoportokat, amelyekre megfelelő válaszintézkedésekkel reagálva növelhetjük a gyermekek digitális biztonságát. A fentiek alapján annyi bizonyosan előrebocsátható, hogy a biztonsági normák megfogalmazásában az oktatásügyekért felelős közigazgatási szerveknek, a közvetítésben pedig az egyes oktatási intézményeknek lesz még hangsúlyosabb szerepe a jövőben.