Török Tünde
bírósági titkár, PKKB
ORCID: -

KISKORÚAK SÉRELMÉRE ELKÖVETETT BŰNCSELEKMÉNYEK ÉS GYERMEKPORNOGRÁFIA AZ INTERNET SEGÍTSÉGÉVEL

Veszélyek az online térben

Absztrakt

A tanulmány az informatika és az internet világában elkövetett tisztességtelen cselekményeket elemzi, ahol a gyors technológiai fejlődés és a mesterséges intelligencia lépéshátrányba hozta a jogalkotót, gyengítve a kiberbűnözés szankcionálását. A magyar, uniós és nemzetközi jog –köztük a Budapesti Egyezmény – dogmatikai vizsgálatával tárgyalja a számítógéppel elkövetett bűncselekményeket (információs rendszer felhasználásával elkövetett csalás, adat megsértése, technikai védelem kijátszása) és a kiskorúak sérelmére elkövetett cselekményeket (kiskorú veszélyeztetése, gyermekpornográfia). Amellett érvel, hogy a szabályozás hiányosságai és a jogalkalmazói rutin hiánya gyakran vezet a felelősség feloldásához vagy a büntetési tételek elbagatellizálásához, aláásva az elrettentést és a prevenciót, miközben a sértett jelentős kárt szenved; a felmentés akár további elkövetésre is bátoríthat. Az európai válaszok bemutatásával rávilágít, hogy a határokon átívelő együttműködés büntethetővé tette a jogosulatlan hozzáférést és a tiltott pornográf tartalmat. Végkövetkeztetése, hogy a gyermekek digitális védelme a szülők és az állam közös felelőssége.

Tárgyszavak: kiberbűnözés, online gyermekvédelem, gyermekek szexuális kizsákmányolása, büntetőjog, Budapesti Egyezmény

CRIMES COMMITTED AGAINST MINORS AND CHILD PORNOGRAPHY VIA THE INTERNET

Abstract

This thesis analyses unlawful conduct in information technology and the internet, where rapid technological change and AI have left legislators a step behind, weakening the sanctioning of cybercrime. Through doctrinal analysis of Hungarian, EU and international law — including the Budapest Convention — it examines computer-enabled offences (information-system fraud, data breaches, circumvention of technical protections) and crimes against minors (endangerment of children, child pornography). It argues that gaps in legislation and inexperience in application frequently result in dropped charges or trivialised penalties, undermining deterrence and general prevention while leaving victims with significant harm; acquittals may even embolden further offending. Examining European responses, it shows how cross-border cooperation criminalised unauthorised access and illegal pornographic content. The thesis concludes that protecting children in the digital space is a shared responsibility of parents and the state and identifies the cooperation frameworks and jurisdictional rules governing such cases.

Keywords: cybercrime, online child protection, sexual exploitation of children, criminal law, Budapest Convention

DOI: 10.66103/KK.2026.3.5

1. Bevezető

A 21. század az információs technológia robbanásszerű fejlődését hozta el. Az állandóan „összekapcsolt" online világ a mindennapokba beépülve olyan kulturális és társadalmi változásokat indított el, ami a generációk közti szakadékot tovább mélyítve sokaknak rendkívül megnehezíti az alkalmazkodást. Még a felkészült IT szakemberek is gyakran a fejüket kapkodják a sokszor szinte havonta megjelenő új megoldások (mobil alkalmazások, felhős szolgáltatások, e-kereskedelem, kripto-fizetések stb.) láttán. Ezzel párhuzamosan szabályosan berobbant

az informatikába – és így az élet számos területére – az AI (mesterséges intelligencia), melynek társadalmi hatásait még a szakemberek is csak találgatják. Ebben a környezetben a jogalkotó – érthető - lépéshátránya súlyos következményekkel járhat, mivel ez korlátozza a számítógépes bűnözők tisztességtelen tevékenységének megfelelő szankcionálását.

Témaválasztásommal megvizsgálom a tisztességtelen cselekedeteket az informatika és az internet világában. Bemutatom az irányadó jogszabályokat, a jogellenes magatartást, az interneten elkövetett bűncselekmények büntetőjogi következményeit. Témaválasztásom indokát az adja, hogy a jogalkalmazók sok esetben olyan joghelyzetekbe kerülnek melyeket a jog alkotásakor még figyelmen kívül hagyott körülmények befolyásolnak. A helyes megítélésre nem áll elegendő rutin. Ezek együttes érvényesülése gyakran vezet a büntetőjogi felelősségek feloldásához, vagy a büntetési tételek elbagatellizálásához, miközben a sértettet ért anyagi vagy erkölcsi kár az esetek többségében jelentős mértékű. A bűncselekmények büntetés nélkül maradásának problematikája az, hogy nem jelent elrettenést a társadalom szélesebb körei számára, nem valósul meg a prevenciós hatás. A bíróságok viszont addig nem tudnak marasztaló ítéletet hozni, amíg nincs vonatkozó jogszabály. További problémát okoz, hogy a tettes felhatalmazást nyer a felmentő ítélet után a további folytatásra.

Részletesen bemutatom a kiskorúakra vonatkozó olyan bűncselekményeket, melyekben a gyermek sértettként jelennek meg. Kiemelkedő figyelmet fordítok a kiskorú veszélyeztetése, a kiskorú sértett részére elkövetett cselekmények, és a gyermekpornográfia tárgyalására.

A büntetőjog a következő számítógépes bűncselekményeket különíti el: információlopás, szabotázs, az adatok manipulálása, az adatok tisztességtelenül való megváltoztatása, jogosulatlan hozzáférés, jogosulatlan használat. A bűncselekmények vizsgálatánál egy elkülönült csoportot képeznek azon bűncselekmények, melyek a csaláshoz kapcsolódóan válnak bűncselekménnyé. Ilyenek a következőek: számítógépes csalás, adathamisítás, programokban, adatokban való kártétel, védett programok másolása.

A számítástechnikai bűncselekmények megvalósulásakor az elkövetés történhet szándékosan és gondatlanul is. A támadás történhet az adat, a szoftver vagy a hardver ellen. Előfordulhat olyan alakzatban is, amikor a szándékos elkövetést olyan kísérő bűncselekmény követi, amelyre már csak az elkövető gondatlan magatartása terjed ki. Esetlegesen olyan lehetőségeket teremt így a kevésbé „képzett" utódai számára, amellyel már könnyedén megvalósítható az újabb bűncselekmény. A bevezetőben említést kell tenni azon bűncselekményekről, melyek elkövetését elősegíti, illetve támogatja a rendszer sérülékenysége: az információs rendszer felhasználásával elkövetett csalás, adatok lopása, személyiségi jogok megsértése. Ilyenek: pornográfia, gyermekpornográfia elősegítése, rágalmazás,

zaklatás. Az internet által ezen bűncselekmények elkövetői is könnyebben elbújhatnak, mintha a materiális világban követnék el ezeket a cselekményeiket.

A számítástechnikai bűnözés elleni küzdelem Európai Uniós Központját az európai internetes bűnözés visszaszorítására hoztak létre. Célja, hogy megfékezze a személyhez fűződő jogok megsértését, valamint védelmezni hivatott a személyes adatok titkosságát. Olyan európai szervezetet hoztak létre, amely a határokon átívelően segítséget tud nyújtani a bűncselekmények áldozatainak. Az intézmény további célja a felvilágosítás és a prevenció. Az európai területen előrelépést jelentett a Budapesti Egyezmény létrejötte, amely nemzetközi szerződésként fontos előrelépést jelentett a magyar és nemzetközi büntetőjog területén is. A szerződéssel a számítógépes hálózatokba illetéktelenül belépők válnak büntethetővé, az elkövető hackereket így a tényállás büntethetővé teszi. A másik előrelépés, amely a szerződés létrejöttének köszönhető az, hogy a tiltott pornográf képek tárolása is büntethetőséget von maga után.

A részletes bemutatás arra szolgál, hogy minél szemléletesebb képet fessek a technológia okozta változásokról, előnyökről, hátrányokról, a könnyen megszerzett információmennyiség illetéktelen felhasználásáról és azon cselekményekről, melyek a számítógép által váltak elkövethetővé és elrejthetővé.

Meggyőződésem, hogy a szülői felelősségnek ki kell terjednie gyermek nevelése és felügyelete mellett a digitális térben való védelmére is. Az informatika teljes tiltása gyermekeink részére napjainkban gyakorlatilag nem kivitelezhető, így az azt használni engedő szülőt célszerű kötelezni arra, hogy gyermekét megóvja az informatikai bűnözéstől, különös tekintettel a gyermek fejlődését hátrányosan befolyásoló szexuális tartalmakra. A nevelő feladata szabályozni a gyermek egészséges életét, ellenőrizve és korlátozva a különböző adattartalmakhoz való hozzáférést annak életkorát figyelembe véve. Állam feladata pedig az, hogy a kiskorú veszélyeztetése bűncselekmény kapcsán szabályozza ennek megszegése esetén a szülők felelősségét.

„Nemcsak azért vagyunk felelősek, amit teszünk, hanem azért is, amit nem teszünk meg." (Lao-ce)

2. Az internet kialakulása, hatásai

Az internet manapság már olyan, mint bármelyik másik közműszolgáltatás, például, mint a villany-, a víz-, vagy a gázszolgáltatás. Bár azt hisszük ez napjaink terméke, azonban története hosszú időkre nyúlik vissza.

Ha biztosított az internet-hozzáférés otthonunkban, akkor akár hetekig ki sem kell lépnünk a lakásból, hogy tartsuk a kapcsolatot ismerőseinkkel, házhoz

szállíttassuk az ételeinket, ruhát vegyünk, dolgozzunk, tanulmányainkat végezzük. Ez a rendszer olyan gyors és könnyű információ-hozzáférést, és áramlást biztosít, amely az emberiség korábbi történelmében példa nélküli.[1] Az okostelefonok megjelenésével ráadásul az internetet - és ezzel gyakran szenzitív adatainkat - már a zsebünkben hordjuk. Ezt természetesen a bűnözői csoportok is kihasználják, akik észrevétlenül kereskednek lopott adatainkkal, személyiségünkkel, amellyel akár több százmillió dolláros károkat is okozhatnak.[2]

Az internet sokak szemében a felelősség nélküli kommunikáció és kapcsolatteremtés lehetőségeként nyilvánul meg. Ez talán még magánszemélyi viszonyokban sokszor kivitelezhető is lenne, hiszen szabadságjogunk korlátozhatatlanságát kérdőjelezné meg, ha gátolva lennénk ebben a tevékenységünkben. Az internet azonban - a hozzáférési költség csökkenése miatt - egyre szélesebb körben érhető el, és egyre szélesebb körben biztosít nyilvánosságot, kommunikációt, anonimitást és a szabad akarat kifejezését.

Az internet jelenleg már olyan gazdasági és üzleti tényező, amelyre tekintettel biztosítani kell a biztonságot a vállalkozások, a hitelezők, a befektetők és a gazdasági élet valamennyi szereplője részére.

Nem véletlenül az üzleti-gazdasági világ volt az első, amely felfigyelt az internet kommunikációs jelentőségére. Azonban, ha vállalkozások eladóként jelennek meg, szükségessé válik a koordinálás, valamint bizonyos szabályok kialakítása.

A szabályozást azonban úgy kell megalkotni, hogy a magánszemélyek számára maximálisan biztosítsa a szólás- és véleményszabadság jogát - lehetőség szerint minél kevesebb kötöttséggel.

Az internet jogi vonatkozása a legtöbb esetben a polgári jogi felelősségi - ahol már nem elég a polgári jogi szabályozás, ott a kriminológiai szabályokra alapoz.

Az internet használatának alap problémája, hogy egységes szabályozási rendszert kellene kialakítani minden jogterületen, különösen a büntetőjogon belül is. A problémák sokrétűek, a nemzetek eltérő nyelvéből, és sokféle milyenségéből az következik, hogy az egyes nemzeti jogrendszerek a fogalmakat másként értelmezik, és másként definiálják az egyes konkrét esetekben. Még az egyik kultúrában a szokásjog megengedi a gyermekek csonkítását a másikban erkölcsileg elítélendő és szigorú büntetést von maga után.

A megoldás a felvázolt problémára az lenne, ha közös szabályokat tudnánk alkotni, azonban a norma alkalmazása tagállami szinten eltérő lehetne.

1 Erre a megállapításra jutott az izraeli filozófus, Yuval Noah Harari is Homo Deus – A holnap rövid története című könyvében.

2 https://index.hu/tech/2018/02/09/lekapcsoltak_a_vilag_egyik_legnagyobb_kiberbunozoi_forumat/ - 2018. február 9-én írta meg az index.hu hírportál, hogy 36 személy ellen emeltek vádat, akik a világ egyik legnagyobb kiberbűnözői fórumán, az Infraudon tevékenykedtek. A vád szerint 4 millió lopott bankkártyaszámot adtak el, egy brit bank több százezer számlájához biztosítottak hozzáférést.

Az egyik legfontosabb jogi fogalom e tekintetben a véleménynyilvánítás szabadsága, amely az internet használatától adódóan elválaszthatatlan. Értelmezése azonban különösen sokrétű, ha például összevetjük az amerikai joggyakorlatot az európaival.[3]

Ezt az értelmezési problémát mindenképpen meg kellene oldani, hiszen az interneten a véleménynyilvánítás szabadságát sértő olyan tények, amelyek büntetőjogi felelősséget is maguk után vonnak, kifejezetten nagy számban találhatóak és számos jogi problémához vezetnek.[4] Az eltérő fogalomértelmezéseket a joggyakorlat által lehetne egységesíteni akképpen, ahogy a meglévő ügyekben a döntések megszülettek, időrendi sorrendben.

Az internet egységes nemzetközi szabályozásának hiánya elősegítette az úgynevezett „informatikai paradicsomok"[5] kialakulását[6]. A probléma a büntethetőség kérdésével áll kapcsolatban. Így kialakulnak olyan országok, ahol a jogrendszerek különbözősége miatt az informatikai bűnözők sorra valósítják meg azokat a deliktumokat, melyeknek sokkal kisebb a büntetőjogi felelőssége, továbbá a felelősségre vonás kockázata.

Erre a megoldási javaslatom szintén az egységes jogi szabályozás. Ezért igényel az informatikai büntetőjog a szokásosnál is hatékonyabb, odafigyelőbb nemzetközi fellépést. Az egységesítésre történtek nemzetközi kezdeményezések a jogi személyek büntetőjogi felelősségre vonásának egységesítését érintő normaalkotásban.[7]

2.1. Felelősség a search engine szolgáltatások esetében

A keresőmotor-szolgáltatók tevékenysége az interneten található, elképzelhetetlen mennyiségű és tömegű adathalmaz felhasználóbaráttá tételére irányul. Napjainkban a „Google a barátod" mondás mutatja be mennyire magától érthető számunkra, hogy a keresőmotorok szinte a teljes internetet indexálják, és pillanatokon belül bármilyen témába tartozó tartalmak teljes listáját adják visszsza. A keresőmotor-szolgáltatók a szolgáltatók nagy kategóriái közt egy köztes csoportot jelentenek. Helyzetüket bonyolítja, hogy nehezen dönthető el, hogy

3 Az Amerikai Egyesült Államokban a véleménynyilvánítás szabadsága európai szemmel nézve olyan mintha nem is volna ez alapvető szabadságjog.

4 Lásd: Gutnick-ügy (www.washingtonpost.com/wp-dyn/articles/A37437-2002Dec10.html Az alapvető szabadságjogok terjedelmét az egyes nemzetek alkotmányai szerint értelmezzük, ezért fontos a kérdés, miként lehet a jogrendszerenként eltérő fogalmakat egységesíteni.

5 Az „informatikai paradicsom" kifejezés olyan területet jelöl, ahol azért bűnöznek előszeretettel, mert nem büntetik vagy csupán nagyon kis valószínűséggel büntetik a cselekményt.

6 Szűts Márton: eEurope, Külgazdaság (Jogi melléklet), 2002/9. szám.

7 Európa Tanács Cybercrime Egyezményének 12. cikke. A rendelkezések a jogi személyt meghatározott esetekben tekintik büntetendőnek. Így, ha az elkövető természetes személyt a jogi személy képviseletének joga, a jogi személy nevében döntések meghozatalának joga, vagy a jogi személyen belüli ellenőrzés joga illette meg.

büntetőjogi felelősség milyen típusú tartalom – idegen, vagy saját – miatt terheli őket. A kérdés hátterében a linkek és hyperlink-ek kusza jogi helyzete áll. A kérdés megoldására az alábbi alternatívák születtek meg:

Az első alternatíva szerint felelőssé tehető azon weboldal szolgáltatója, akinek a weboldala hyperlink-eket tartalmaz, továbbá felelőssé tehető olyan tartalom megjelenítéséért is, amely az adott linken keresztül válik elérhetővé. A szolgáltatótól az általa linkelt tartalom folyamatos ellenőrzése nem várható el, ez túlzott felelősséget telepítene a weboldal-szolgáltatóra.

A következő elmélet szerint a szolgáltató egyáltalán nem felel azon hyperlink-ek tartalmáért, amelyek az oldalán kerültek elhelyezésre. Ez nyilvánvalóan egy meglehetősen szélsőséges elképzelés, hiszen a weboldal-szolgáltató mégis valamilyen szintű közvetítői szerepet játszik a jogsértő tartalom elérésében, illetve megjelenítésében.

A megoldás álláspontom szerint a két fenti alternatíva közt található.

A keresőmotor-szolgáltatások annyiban hasonlítanak az előbb ismertetett hyperlink hivatkozás(oka)t tartalmazó weboldalakhoz, hogy azok is hyperlink-hivatkozásokat jelenítenek meg, csak nagyobb mennyiségben, és irányítottan. A keresőmotorok két módszer mentén működnek, amelyek közt a lényeges különbség abban nyilvánul meg, hogy a hyperlink-hivatkozással fedett weboldal címkével történő ellátása (ún. labelling) a weboldal saját szolgáltatója, vagy egy központi szervezet által történik.

A keresőmotor érzékeli a begépelt (vagy másként bevitt) címkét, és saját programkódjának megfelelően kiszűri a kívánt linkeket. A keresőmotor tulajdonképpen egy program, amely matematikai módszerek révén szűri a weboldalakat, így csak az a személy vonható felelősségre, aki az adott keresőmotort használja, a keresőmotor megalkotója viszont nem. Ettől eltérő a felelősség akkor, ha a keresőmotor akként kerül programozásra, hogy ne a bevitt címkéknek megfelelő linkeket jelenítse meg, hanem olyan linkeket is, amelyek adott esetben más kategóriába tartoznak, vagy éppenséggel jogsértőek, súlyosabb esetben abszolút jogellenesek.[8] A nagy szolgáltatók esetenként gazdasági érdekeik mentén manipulálják a találati listát. Álláspontom szerint ezekben az esetekben a büntetőjogi felelősségre vonás bűnsegédi magatartásért képzelhető el.[9] Előfordulhat, hogy elmarad a tettesi cselekmény megvalósítása, azaz a felhasználó végül nem nyitja meg a hivatkozást. Ilyenkor a keresőmotor-szolgáltató eredménytelen részesi magatartása nem lesz szankcionálható.

8 Abszolút jogellenes tartalomnak minősül pl. a gyermekpornográfia, míg a relatív jogellenes tartalom csak az adott helyen és időben jogsértő, mint például a szerzői jogokat sértő tartalmak többsége.

9 Btk. 14. § (2) bekezdése szerint bűnsegéd az, aki a bűncselekmény elkövetéséhez másnak szándékosan segítséget nyújt. A keresőmotor szolgáltatója fizikai bűnsegélyt valósít meg akkor, amikor a jogsértő linkeket megjeleníti, ekkor a tettesi alapcselekmény külső feltételeinek megteremtésében működik közre.

Azonban a gyerekeknek szánt tartalom felhasználásának ellenőrzése jogosan lenne elvárható. Amennyiben azonban a szolgáltatót az ellenőrzésre szolgáló hamis személyes adattal láttak el, - a felhasználó korától eltérően a szülő más kort rögzít, - a szolgáltató felelőségét mentesítették. Ezt könnyű megérteni a következő egyszerű példán keresztül: a közösségi platformok az államok jogi szabályozását követően a 14 év alattiakat eltiltották például a Instagram használattól, mert az a gyermek életkorából adódóan károsan hathat a kisgyermek fejlődésére. Azonban, ha a szülő a gyermeke telefonján a születési időként olyan időpontot adott meg ahol már a gyermek betöltötte a korhatárt, a szolgáltató felelősége nem állapítható meg.

3. Kiskorú veszélyeztetése az internet használatával összefüggésben

Az információs technológia fejlődése az elmúlt évtizedekben alapvetően átalakította az emberek mindennapi életét. Az internet és a digitális eszközök használata ma már a társadalom működésének természetes részévé vált, és ez különösen igaz a fiatalabb generációk esetében. A gyermekek és a fiatalkorúak sokszor már egészen korai életkorban kapcsolatba kerülnek az online tartalmakkal, a közösségi médiafelületekkel és különböző digitális szolgáltatásokkal. Számukra az internet használata teljesen természetes, a kortársaikkal való kapcsolattartás, a tanulás és a szórakozás fontos eszköze.

3.1. A digitális környezet sajátosságai és a kiskorúak érintettsége

A szakirodalomban gyakran találkozunk a „digitális bennszülött" kifejezéssel, amely azokra a generációkra utal, akik már az internet és az okoseszközök világában szocializálódottak. A Z-generáció, valamint az utánuk következő Alfa-generáció tagjai készségszinten használják a mobilalkalmazásokat és az internetes kommunikációs csatornákat. A digitális környezetben való jártasságuk azonban nem jelenti azt, hogy minden esetben tisztában lennének az online térben rejlő veszélyekkel.[10]

A digitális környezet sajátossága, hogy az információ rendkívül gyorsan terjed. Ez kihatással van a fiatalok információfeldolgozási szokásaira és viselkedésére is. A folyamatosan változó, gyors ütemben érkező ingerekhez való alkalmazkodás következtében a gyermekek egyre nagyobb mennyiségű információt képesek

10 Z-generáció alatt jellemzően az 1995 és 2009 között, Alfa-generáción a 2010 után születetteket értjük. Pongrácz Ildikó: Gyermekek a digitális világ útvesztőiben – veszélyek és lehetőségek. Miskolci Jogtudó 2019/2. 55–69. 56–57. Elérhető: https://jogtudo.uni-miskolc.hu/files/7394/MJ2019iss2art6Pongracz.pdf

rövid idő alatt befogadni, és számukra természetessé válik több tevékenység párhuzamos végzése. Ez a jelenség ugyan bizonyos készségek fejlődését elősegítheti, ugyanakkor azzal is járhat, hogy a tartós figyelmet igénylő tevékenységek iránt csökken az érdeklődésük. A közösségi médiafelületeken és egyéb online platformokon a kapcsolattartás gyakran rövid üzenetekre, képi elemekre és hangulatjelekkel (emoji) kifejezett reakciókra korlátozódik. Ennek következtében a személyes kommunikációhoz szükséges készségek, így például az érzelmek árnyalt kifejezése vagy mások nonverbális jelzéseinek értelmezése háttérbe szorulhatnak.[11] Mindezek a sajátosságok számos előnyt hordoznak, ugyanakkor fokozzák a fiatalok kiszolgáltatottságát, és megkönnyítik, hogy különböző jogsértő magatartások sértettjeivé váljanak.[12]

3.2. Az online térben megjelenő veszélyek főbb típusai

Az internetes térben megjelenő veszélyek egyik leggyakoribb formája az online zaklatás (cyberbullying), amely a hagyományos iskolai bántalmazás digitális megfelelőjeként is értelmezhető. A közösségi médiafelületeken, üzenetküldő alkalmazásokban vagy online játékok során a gyermekek könnyen válhatnak sértő üzenetek, megalázó tartalmak vagy tartós pszichés nyomás célpontjává. Az ilyen jellegű magatartások súlyos érzelmi következményekkel járhatnak, és hosszabb távon a gyermek önértékelésére és mentális állapotára is negatív hatást gyakorolhatnak. További problémát jelent, hogy az interneten számos olyan tartalom is megtalálható, amely kiskorúak számára nem megfelelő. Az erőszakos vagy szexuális jellegű tartalmak, valamint a különböző káros magatartásformákat népszerűsítő oldalak könnyen elérhetők, különösen akkor, ha a gyermekek internet-használata nem áll megfelelő felügyelet alatt. Az online környezet sajátossága, hogy a tartalmakhoz való hozzáférés gyakran ellenőrizetlenül történik, így a gyermekek akár véletlenül is olyan információval találkozhatnak, amelyek fejlődésükre káros hatást gyakorolnak.[13] Külön kockázatot jelentenek az úgynevezett „kihívások" (például TikTok challenge-ek) is, amelyek során a felhasználók mások által közzétett viselkedéseket utánoznak, és azokat saját tartalomként

11 Pongrácz (2019) i.m. 57–58.

12 Meggyesfalvi Boglárka: Kockázati tényezők a digitális térben: A gyerekek internet- és közösségi média használata és az online áldozattá válás. Belügyi Szemle, 71. évf. 2023/12., 2163–2178. 2167. DOI: https://doi.org/10.38146/BSZ.2023.12.3

13 Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. EU Kids Online. 45., 53. DOI: 10.21953/lse.47fdeqj01ofo Elérhető: https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf;
WHO: One in six school-aged children experiences cyberbullying, finds new WHO/Europe study. 27 March 2024. Elérhető: https://www.who.int/europe/news/item/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study

megosztják. Bár egyes kihívások ártalmatlanok, mások kifejezetten veszélyesek lehetnek, mivel a kiskorúakat egészségkárosító, megalázó vagy akár jogellenes magatartások tanúsítására ösztönözhetik.[14]

Az internet használata lehetőséget teremt arra is, hogy felnőtt elkövetők kiskorúakkal lépjenek kapcsolatba. A digitális platformokon a kommunikáció nemcsak gyors, de lényegében korlátok nélküli és anonim. A felhasználók könnyen kapcsolatba léphetnek egymással, akár nagy távolság ellenére is. Emellett a személyazonosság elrejtése is egyszerű, ami megkönnyíti, hogy az elkövetők bizalmi kapcsolatot alakítsanak ki a gyermekekkel. Az ilyen helyzetek különösen veszélyesek, mert a kiskorúak gyakran nem látják át, hogy az online kapcsolatok mögött milyen szándékok állhatnak. Az online környezetre jellemző az is, hogy a digitális tartalmak előállítása és terjesztése rendkívül egyszerű. Ma már korlátozott eszközkészlettel (pl. AI generált video) is létrehozhatók és gyorsan megoszthatók olyan tartalmak, amelyek sérthetik a kiskorúak érdekeit. A szakirodalom ezt a jelenséget multiplikátorhatásnak nevezi. Ennek lényege, hogy egy-egy jogsértő tartalom rövid idő alatt sok emberhez eljuthat, ami növeli a sértettek kiszolgáltatottságát és a sérelem súlyát. A személyes adatok védelmének hiánya szintén komoly kockázatot jelent. A fiatalok sokszor nem gondolják végig, milyen következménye lehet annak, ha megosztják adataikat, fényképeiket vagy tartózkodási helyüket. Ezek az információk könnyen visszaélések alapjául szolgálhatnak. Az internet sajátossága, hogy az egyszer közzétett adatok felett a kontroll szinte végérvényesen elveszhet, ami tovább növeli a kiskorúak kitettségét[15] – mire a gyermek ráébred hibájára, már nem tudja azt meg nem történté tenni. Sokszor akár hónapokkal vagy évekkel később használják fel ellene; egy a pillanat hevében vagánynak tűnő megosztást, ami később – kontextus függvényében - a lejáratására is alkalmassá válhat.

Fontos kiemelni az internet anonimitását is. Ez lehetővé teszi, hogy a felhasználók elrejtsék személyazonosságukat, ugyanakkor megnehezíti a jogsértő magatartások felderítését. Az anonimitás érzete az elkövetőkben azt a benyomást keltheti, hogy cselekményeik következmények nélkül maradnak. Mindezek együtt olyan környezetet hoznak létre, amelyben a kiskorúak fokozott veszélynek vannak kitéve, és könnyebben válhatnak bűncselekmények sértettjeivé.[16]

Az internetes környezetben megjelenő veszélyek sokrétűsége miatt a gyermekek védelme összetett feladatot jelent. A büntetőjog e körben kiemelt szerepet tölt be, különösen azokban az esetekben, amikor a kiskorúak testi, értelmi vagy

14 Varga Árpád: A gyermekekre veszélyes online kihívások fogalma, jellemzői, okai és a hazai fiatalok érintettsége. Családi Jog 2023/4., 21-28. Online Szakcikk Adatbázis. Elérhető: https://szakcikkadatbazis.hu/doc/8258379

15 Meggyesfalvi (2023) i.m. 2167.

16 Meggyesfalvi (2023) i.m. 2167–2168.

erkölcsi fejlődése kerül veszélybe. Ezt a védelmi célt szolgálja a kiskorú veszélyeztetésének tényállása, amely azokat a magatartásokat rendeli büntetni, amelyek alkalmasak a gyermek fejlődésének hátrányos befolyásolására. A következőkben ezért azt vizsgálom, hogy az online térben megvalósuló magatartások milyen módon értékelhetők a kiskorú veszélyeztetésének tényállása szempontjából.

3.3. Kiskorú veszélyeztetésének tényállása

A kiskorú veszélyeztetésének tényállása a gyermek fejlődésének büntetőjogi védelmét szolgálja. A Btk. 208. § két egymástól elkülöníthető tényállást foglal magában: egyrészt a gondozási kötelezettség súlyos megszegésén alapuló alakzatot, másrészt azt az esetkört, amikor nagykorú személy a kiskorút jogsértő vagy káros életmód irányába tereli.[17] Az (1) bekezdésben írt tényállásnál a jogi tárgy a kiskorú testi, értelmi, erkölcsi és érzelmi fejlődése, a (2) bekezdésben foglaltnál pedig a tizennyolcadik életévét be nem töltött személy erkölcsi fejlődése áll a védelem középpontjában.[18]

3.3.1. Az első alakzat: gondozási kötelezettség súlyos megszegése

Az első alakzat esetében a sértett a polgári jogi szabályok szerinti kiskorú.[19] A bűncselekmény lényege, hogy az a személy, aki a gyermek nevelésére, felügyeletére vagy gondozására köteles, e kötelezettségét súlyosan megszegi, és ezzel a kiskorú fejlődését veszélyezteti. Mivel kerettényállásról van szó, a releváns kötelezettségek többféle forrásból eredhetnek: alapulhatnak polgári jogi jogviszonyon (például bébiszitter megbízása), foglalkoztatási jogviszonyon (például tanár esetében)[20], vagy hatósági döntésen (például gyámrendelés során). E kötelezettségek köre azonban nem korlátozódik kizárólag formális jogviszonyokra.[21] A bírói gyakorlat szerint felelősség terhelheti azt a személyt is, aki ténylegesen kerül olyan helyzetbe, hogy a kiskorúról gondoskodnia kell, még akkor is, ha erre kifejezett megbízás nem jött létre.[22] Ennek megfelelően a gyermekkel közös háztartásban élő személyek (például a nevelőszülő, a gyám házastársa vagy élettársa) is kötelesek részt venni a kiskorú nevelésében, felügyeletében és gondozásában,

17 A Btk. 208. §-t lásd a Mellékletben.
18 *Szomora Zsolt*: Kiskorú veszélyeztetése. In: Karsai Krisztina: Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez, 2025. július 1. időállapotú, 2025. évi Jogtár-formátumú kiadás.
19 2013. évi V. törvény a Polgári Törvénykönyvről (a továbbiakban: Ptk.) 2:10. §.
20 Kúria Bfv.II.231/2017/6.
21 Szomora (2025) Kiskorú veszélyeztetése… i.m.
22 *Kiss Annamária:* A kiskorú veszélyeztetése bűntettének első alakzatához kapcsolódó ítélkezési gyakorlat elemző bemutatása. Glossa Iuridica, 2025/1-2., 291-320. Online Szakcikk Adatbázis. Elérhető: https://szakcikkadatbazis.hu/doc/1280009. https://doi.org/10.55194/GI.2025.1-2.15

így adott esetben a Btk. 208. § (1) bekezdés szerinti bűncselekmény elkövetőivé válhatnak.[23]

A kiskorú veszélyeztetésének megállapításához önmagában nem elegendő a kötelezettség megszegése, hanem annak egyben súlyosnak is kell lennie. A súlyosság megítélése mindig az adott ügy körülményei alapján történik. Ide tartozhat az alapvető gondozási feladatok tartós elmulasztása, a gyermekkel szembeni bántalmazás, vagy olyan magatartások tanúsítása, amelyek alkalmasak arra, hogy a kiskorú fejlődését kedvezőtlen irányba befolyásolják. A kötelességszegés megvalósulhat aktív magatartással és mulasztással is. A gyakorlatban gyakran éppen a tartós odafigyelés hiánya, a felügyelet elmulasztása vagy a káros hatásokkal szembeni közömbösség vezet a veszélyhelyzet kialakulásához.[24]

A bírói gyakorlat a nevelési, gondozási és felügyeleti kötelezettséget tágabban értelmezi. Ide tartozik a gyermek életkörülményeinek folyamatos figyelemmel kísérése, a megfelelő testi és lelki fejlődés feltételeinek biztosítása, valamint az alapvető szükségletek kielégítése. A kötelezettség magában foglalja azt is, hogy a gondozásra köteles személy a lehetséges veszélyeket felismerje és elhárítsa. Ennek tartalma nem minden esetben azonos, hanem a gyermek életkorához és egyéni körülményeihez igazodik.[25] A gyakorlat azt is hangsúlyozza, hogy a nevelési és felügyeleti kötelezettség kiterjed a pszichés és testi veszélyek megelőzésére is.[26]

A kiskorú veszélyeztetésének megállapításához az is szükséges, hogy a súlyos kötelességszegés és a kialakuló veszélyhelyzet között okozati kapcsolat álljon fenn. Vagyis a gyermek fejlődését fenyegető helyzetnek a kötelesség megszegéséből kell következnie.[27]

A bűncselekmény csak szándékosan követhető el. Ez azt jelenti, hogy az elkövetőnek tisztában kell lennie azzal, hogy kiskorúról van szó, valamint azzal is, hogy milyen kötelezettségek terhelik, és magatartása alkalmas a gyermek fejlődésének veszélyeztetésére. A gyakorlatban ez sokszor abban nyilvánul meg, hogy az elkövető a lehetséges következményekkel tisztában van, de azokkal szemben közömbös marad. Amennyiben a szándékosság hiányzik, a kiskorú veszélyeztetése nem állapítható meg, ilyenkor legfeljebb más, gondatlanságból elkövetett bűncselekmény jöhet szóba. A bűncselekmény befejezetté válásához a veszélyhelyzet kialakulása szükséges, ugyanakkor nem követelmény, hogy tényleges károsodás

23 Kúria Bfv.1420/2024/8. [42].
24 Szomora (2025) Kiskorú veszélyeztetése… i.m.
25 *Makai Katinka:* A gyermekek érdekeit sértő és a család ellen tanúsított magatartások büntetőjogi és polgári jogi vetületei I. rész, Büntetőjogi Szemle 2020/2., 57-65. Online Szakcikk Adatbázis. Elérhető: https://szakcikkadatbazis.hu/doc/2723906.
26 Kiss (2025) i.m.; BH2008.7.177. (Legf. Bír. Bfv.I.380/2007.)
27 Szomora (2025) Kiskorú veszélyeztetése… i.m.

is bekövetkezzen. Elméletileg a kísérlet is elképzelhető, azonban ennek a gyakorlatban csekély a jelentősége.[28]

A fenti szempontok az online környezetben is érvényesek, azonban ott sajátos módon jelennek meg. A bírói gyakorlatban az ilyen esetek egyelőre kevésbé fordulnak elő. Álláspontom szerint ugyanakkor súlyos kötelességszegés lehet például, ha a kiskorú nevelésére vagy felügyeletére köteles személy tartósan nem ellenőrzi a gyermek internet-használatát, eltűri, hogy a kiskorú számára nyilvánvalóan káros tartalmakkal találkozzon, vagy nem akadályozza meg, hogy a gyermek ismeretlen személyekkel lépjen kapcsolatba. Hasonlóan értékelhető az is, ha a gondozásra köteles személy maga járul hozzá a gyermek kiszolgáltatott helyzetének kialakulásához, például a kiskorúval kapcsolatos személyes tartalmak felelőtlen megosztásával.

Egyre gyakrabban merül fel a kérdés, hogy a szülő által a kiskorúról megosztott képek, videók vagy egyéb személyes tartalmak elérhetik-e a büntetőjogi felelősség szintjét. Önmagában a gyermekről készült tartalmak közzététele a családi körön kívül (sharenting[29] = share + parenting) - a gyermek beleegyezése nélkül - nem jogellenes, bizonyos esetekben azonban felmerülhet a kiskorú veszélyeztetésének megvalósulása.[30] Súlyos kötelességszegésről lehet szó különösen akkor, ha a szülő vagy más gondozásra köteles személy olyan tartalmakat tesz közzé, amelyek a kiskorú kiszolgáltatottságát növelik, vagy alkalmasak arra, hogy a gyermek fejlődését hátrányosan befolyásolják. Ide tartozhat például a gyermek megalázó helyzetben történő bemutatása, a személyes adatok széles körben hozzáférhetővé tétele, vagy olyan képek közzététele, amelyek visszaélésre adhatnak lehetőséget. Ugyanakkor – amint arra fentebb is utaltam – minden esetben egyedileg, a körülmények mérlegelésével kell megítélni, hogy a kötelezettségszegés mennyiben tekinthető súlyosnak, és fennáll-e a veszélyhelyzet.

Érdemes megjegyezni, hogy ezen a területen a jogi szabályozás nemzetközi szinten sem tekinthető még kiforrottnak. A jelenlegi keretek sok esetben nehezen tudják kezelni az online térben megjelenő új kockázatokat, és kevésbé veszik figyelembe a szülők digitális tudatosságát, illetve annak hiányát. Mindezek miatt különösen fontos a megelőzés: a szülők - és általában a társadalom

28 Csapucha Bernadett: A veszélyeztetési eredmény értelmezése a kiskorú veszélyeztetése törvényi tényállásában. Büntetőjogi Szemle 2021/1., 15-23. Online Szakcikk Adatbázis. Elérhető: https://szakcikkadatbazis.hu/doc/6615031.

29 UNICEF: https://www.unicef.org/parenting/child-care/sharenting.

30 A sharenting kérdése elsődlegesen a gyermek személyiségi jogaival, különösen a magánélethez és a képmáshoz való jogával összefüggésben merülhet fel, a szülői tartalommegosztás adott esetben e jogok sérelmét eredményezheti.
Nagy Nelli: A sharenting megakadályozása: A gyermekek jogainak érvényesítése a szülői felügyeleti jog korlátozásával szemben. Arsboni. 2025. május 12. Elérhető: https://arsboni.hu/a-sharenting-megakadalyozasa-a-gyermekek-jogainak-ervenyesitese-a-szuloi-felugyeleti-jog-korlatozasaval-szemben/.

- tájékoztatása és a figyelemfelkeltés jelenleg az egyik leghatékonyabb eszköz a kiskorúak védelmében.[31]

3.3.2. A második alakzat: a kiskorú jogellenes vagy káros irányba befolyásolása

A kiskorú veszélyeztetésének második alakzata eltérő jellegű magatartásokat fog át. Ebben az esetben nem a gondozási kötelezettség megszegése áll a középpontban, hanem az, hogy egy nagykorú személy a kiskorút jogsértő vagy a fejlődésére káros életmód irányába tereli, vagy ilyen magatartásra próbálja rábírni. A sértett ez esetben a tizennyolcadik életévét be nem töltött személy, függetlenül polgári jogi státuszától (például az esetleges házasságkötésétől). Ez a tényállás olyan eseteket szankcionál, amikor az elkövető aktívan hat a kiskorú viselkedésére, és ezzel annak erkölcsi fejlődését veszélyezteti. A Btk. súlyosabban rendeli büntetni, ha a nagykorú személy a kiskorút bűncselekmény vagy szabálysértés elkövetésére próbálja rábírni, illetve züllött életmód folytatására ösztönzi. Ugyancsak magasabb a büntetési tétel akkor, ha az elkövető a kiskorút bűncselekmény elkövetéséhez „felajánlja", vagyis más számára ilyen célból rendelkezésre bocsátja. Már a rábírásra törekvés is elegendő a felelősség megállapításához, nem szükséges, hogy a kiskorú ténylegesen jogsértő magatartást tanúsítson.[32]

Az online térben ennek különös jelentősége lehet, mivel a digitális platformok alkalmasak arra, hogy a kiskorúakat különböző jogellenes vagy káros tevékenységek irányába befolyásolják. Ilyen lehet például, ha valaki a kiskorút bűncselekmény elkövetésére ösztönzi, vagy olyan életmód felé tereli, amely a fejlődésére káros hatással van.

A digitális térben különösen gyakori jelenség az úgynevezett grooming[33] (behálózás). Ennek során a felnőtt elkövető lépésről lépésre alakít ki bizalmi kapcsolatot a kiskorúval, majd ezt kihasználva próbálja befolyásolni őt. A kapcsolat sokszor ártalmatlan beszélgetéssel indul, később azonban egyre személyesebb irányba halad, és akár jogsértő vagy a gyermek számára káros helyzetekhez is vezethet. Az elkövető tudatosan építi fel ezt a folyamatot, és a megszerzett bizalmat arra használja, hogy a kiskorút különböző magatartásokra rávegye.[34] Az elkövető gyakori céljai: szexuális zaklatás, emberkereskedelem, csalás, pénzügyi előnyök megszerzése, vagy lopás. Ez jól illeszkedik a törvényi tényálláshoz,

31 *Bezáková, Zuzana – Madleňák, Adam – Švec, Marek:* Security Risks Of Sharing Content Based On Minors By Their Family Members On Social Media In Times Of Technology Interference. Media Literacy and Academic Research, Vol. 4, No. 1, April 2021. 64–65. Elérhető: https://www.mlar.sk/wp-content/uploads/2021/04/4_Bezakova_Madlenak_Svec.pdf.

32 Btk. 208. § (2) bek.; Szomora (2025) Kiskorú veszélyeztetése… i.m.

33 https://health.clevelandclinic.org/what-is-grooming.

34 Police.hu: Grooming: Ragadozók a kibertérben. A Rendőrség hivatalos honlapja. Elérhető: https://www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag/grooming-ragadozok-a-kiberterben.

hiszen már a rábírásra irányuló törekvés is elegendő lehet a felelősség megállapításához.

Az ilyen helyzetek gyakran konkrét online felületeken alakulnak ki. A közösségi oldalak, üzenetküldő alkalmazások vagy az online játékokhoz kapcsolódó chatfelületek (például Discord)[35] lehetővé teszik, hogy a felhasználók közvetlenül kapcsolatba lépjenek egymással. A kommunikáció sokszor zárt csoportokban vagy privát üzenetekben zajlik, ami nehezíti a külső kontrollt. Manapság gyakori a peer-to-peer network használata, amely egy olyan hálózat, ahol a beszélgetést folytató személyek eszközei központi szerverek kihagyásával közvetlenül kapcsolódnak össze. Ehhez, ha hozzávesszük a felhasznált – gyakran katonai szintű – titkosítást, akkor látható, hogy a visszaélések felderítése külső hatóság által rendkívül nehézkes. Az áldozatok sokszor a szégyen érzése miatt, még a károk bekövetkezése után sem, fordulnak szüleikhez. Az is gyakori, hogy az elkövetők valótlan adatokat adnak meg magukról, így a kiskorú nem tudja, kivel áll valójában kapcsolatban. Ez a környezet kedvez annak, hogy a felnőttek hosszabb időn keresztül hatást gyakoroljanak a kiskorúakra, és őket káros vagy akár jogellenes magatartásokra próbálják rávenni.[36]

Az online befolyásolás sokféle formát ölthet. Előfordulhat például, hogy az elkövető valamilyen előny ígéretével próbálja rávenni a kiskorút különböző tevékenységekre, vagy éppen olyan viselkedési mintákat közvetít felé, amelyek a fejlődésére kedvezőtlen hatással lehetnek. A közösségi média sajátossága, hogy ezek a hatások gyakran észrevétlenül épülnek be a mindennapi kommunikációba, így a kiskorú számára nehezebben felismerhetők.

Fontos ugyanakkor, hogy az online térben megvalósuló befolyásolás nem minden esetben illeszthető be egyetlen büntetőjogi tényállás keretei közé. Az elkövetés során gyakran több, egymással összefüggő jogsértő magatartás jelenik meg, amelyek adott esetben külön-külön is büntetendők lehetnek. Ilyen lehet például a zaklatás, a gyermekpornográfiához kapcsolódó cselekmények, a szeméremsértés, a zsarolás vagy a személyes adattal való visszaélés. Az ilyen jellegű ráhatás összességében alkalmas lehet arra, hogy a kiskorú erkölcsi fejlődését veszélyeztesse, ezért a tényállás alkalmazása ezekben az esetekben is felmerülhet.[37]

35 Az elkövetést megkönnyíti, hogy a Discord jelenleg még nem ellenőrzi a felhasználók életkorát, és 2026 februári sajtóhírek szerint az életkor-ellenőrzést csak 2026 második félévében tervezi bevezetni. Hvg.hu: Meghátrált a Discord, egyelőre nem vezetik be a vitatott életkor-ellenőrzést. 2026.02.25. Elérhető: https://hvg.hu/tudomany/20260225_discord-eletkor-ellenorzes-bevezetes-halasztasa-valtoztatasok.

36 *Varga Árpád:* A gyermekek online szexuális kizsákmányolása elleni küzdelem egyes szabályozási tendenciái és európai irányvonalai. Iustum Aequum Salutare XXI. 2025. 2. 175–190. XXI. 2025. 2. 175–190.178–179. Elérhető: https://publikacio.ppke.hu/id/eprint/2802/1/2025-02_10_Varga.pdf; https://doi.org/10.69695/ias.2025.2.10
Kherkher, Steve: Suing Discord for Child Exploitation. November 25, 2025. Elérhető: https://www.kherkhergarcia.com/suing-discord-for-child-exploitation/

37 Varga (2025) i.m. 183.

3.3.3. Jogalkotási javaslat – egy új (3) bekezdés

(3) Az (1) bekezdés szerint minősül, ha az informatikai rendszer vagy internet használat során a gyermeket veszélynek teszi ki, nevelésének megkönnyítése, gyermek felügyeletének biztosítása céljából informatikai eszközt a gyermek használatára átad- és ezzel kiskorú testi, értelmi, erkölcsi vagy érzelmi fejlődését veszélyezteti.

Súlyosabban minősül: ha ezzel betegséget idéz elő vagy 14 év alatti sértett sérelmére követi el.

Magyarázat:

Testi, értelmi fejlődés kockázatai: digitális autizmus – a gyermek nem tanul meg beszélni, illetve jelentős elmaradást mutat kortársaihoz képest.

Erkölcsi fejlődés: a gyermek felügyeletéért felelős személy szándékosan, vagy gondatlanságból hagyja, hogy a gyermek pornográf tartalmakat nézzen ezáltal eltorzítva annak szekszuális fejlődését.

Érzelmi fejlődés kockázatai: a gyermek nem tud az életkorának megfelelő kötődést és kapcsolatokat teremteni, nonverbális úton érzelmeket kifejezni.

EM: életkor beállításának gondatlanságból nem tesz eleget, vagy meghamísítja azt.

EM: ellenőrzés nélküli használatot engedélyez - Parents controll

4. Gyermekpornográfia mesterséges intelligenciával generált szereplőkkel

A gyermekpornográfia a gyermekek szexuális kizsákmányolásának egyik legsúlyosabb formája, amely sok esetben gazdasági érdekekkel is összekapcsolódik. A technológiai fejlődés tovább növeli a kockázatokat. Az online környezet lehetővé teszi a tartalmak gyors és széles körű terjesztését, valamint olyan új módszerek megjelenését, melyekkel az elkövetők megpróbálják kijátszani a jogi szabályozást.[38] Mindez indokolttá teszi, hogy a gyermekpornográfiával kapcsolatos büntetőjogi szabályokat a digitális környezet sajátosságaira figyelemmel értelmezzük.

4.1. A gyermekpornográfia törvényi tényállása

A gyermekpornográfia tényállása a kiskorúak szexuális kizsákmányolásával szembeni büntetőjogi fellépés egyik legfontosabb eszköze. A Btk. 204. § lényegében

38 *Mezei Kitti*: Az online gyermekpornográfia és a büntetőjog. Ügyészek Lapja 28. évf. 2021/4. 19–30. 19. Elérhető: https://real.mtak.hu/135281/1/mezei_UL_2021_4beliv.pdf

minden olyan magatartást szankcionál, amely a tizennyolcadik életévét be nem töltött személyt ábrázoló pornográf felvételekhez kapcsolódik. Ide tartozik különösen az ilyen felvételek megszerzése és tartása, azok továbbadása vagy hozzáférhetővé tétele, valamint a felvételek készítése, terjesztése és kereskedelme. A törvény differenciáltan kezeli az egyes elkövetési magatartásokat: a puszta megszerzés és tartás is büntetendő, ugyanakkor a készítéshez, terjesztéshez vagy nagy nyilvánosság számára történő hozzáférhetővé tételhez súlyosabb büntetési tételek kapcsolódnak. A jogalkotó különös súllyal értékeli azokat az eseteket, amikor a sértett tizenkettedik életévét sem töltötte be, illetve amikor az elkövető a gyermek kiszolgáltatott helyzetét, vagy a vele fennálló nevelési, felügyeleti vagy hatalmi viszonyt használja ki. A tényállás nemcsak a már elkészült felvételekhez kapcsolódó magatartásokat fogja át, hanem kiterjed az előkészületi jellegű cselekményekre is, például az anyagi eszközök biztosítására vagy a kiskorú pornográf szereplésre történő felhívására. Jelentősége van annak is, hogy a törvény a pornográf felvétel fogalmát kifejezetten kiterjeszti a nem létező személyek valósághű ábrázolására is, ami az új technológiák, különösen a mesterséges intelligencia alkalmazása szempontjából bír kiemelt jelentőséggel.[39]

A gyermekpornográfia tényállásához szorosan kapcsolódik a pornográf műsorokra vonatkozó szabályozás. A Btk. 204/A. § azokat a magatartásokat rendeli büntetni, amelyek során kiskorú személy pornográf jellegű élő előadásban, műsorban vesz részt, illetve ilyen szereplésre felhívják, vagy annak megszervezésében közreműködnek. A szabályozás így nemcsak a rögzített felvételekhez kapcsolódó visszaéléseket fedi le, hanem az élő, gyakran online közvetített tartalmakat is. Ez a tényállás különösen az internetes környezetben jelentős, ahol a pornográf tartalmak nemcsak rögzített formában, hanem élő közvetítések során is megjelenhetnek, ezzel fokozva a kiskorúak kitettségét.[40]

4.2. Klasszikus elkövetési magatartások a digitális környezetben

A bírói gyakorlat alapján a gyermekpornográfiával kapcsolatos bűncselekmények több, jól körülhatárolható elkövetési formában jelennek meg. Ezek az esetek jól mutatják, hogy a tényállás a digitális környezetben is széles körben alkalmazható. Gyakori elkövetési mód, hogy az elkövető online kommunikáció során – sok esetben fenyegetéssel vagy nyomásgyakorlással – veszi rá a kiskorút arra, hogy magáról szexuális tartalmú felvételeket készítsen és azokat elküldje. A bírói gyakorlatban ismert olyan eset, amikor a terhelt közösségi oldalon

39 A Btk. 204. §-t lásd a Mellékletben.; Szomora Zsolt: Gyermekpornográfia. In: Karsai Krisztina: Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez, 2025. július 1. időállapotú, 2025. évi Jogtár-formátumú kiadás.

40 A Btk. 204/A. §-t lásd a Mellékletben.; Szomora (2025) Gyermekpornográfia… i.m.

keresztül kényszerítette a gyermekkorú sértettet arra, hogy egyre intimebb képeket készítsen magáról, majd ezeket saját számítógépén tárolta, miközben további, internetről beszerzett gyermekpornográf felvételeket is birtokolt.[41] Szintén tipikus elkövetési magatartás a tiltott felvételek internetes feltöltése és továbbítása. Előfordult, hogy az elkövető nagyszámú, kiskorúakat ábrázoló pornográf képfelvételt töltött fel online tárhelyre, illetve elektronikus levél útján továbbított más személyek részére, ezzel szélesebb körben hozzáférhetővé téve azokat.[42] Tipikus elkövetési mód az is, amikor a terhelt másoktól kapott felvételeket ment le és tárol a saját eszközein. Ilyen ügyekben a terheltek több tucat, kiskorúakat szexuális cselekmény közben ábrázoló képet és videót tartottak számítógépeiken, amelyek különböző forrásokból – jellemzően internetes kapcsolatok útján – kerültek hozzájuk.[43]

Ezek az esetek jól mutatják, hogy a hazai ítélkezési gyakorlatban egyelőre az ilyen jellegű, klasszikusnak mondható elkövetési magatartások fordulnak elő digitális környezetben.[44] Ez azonban nem jelenti azt, hogy a jogalkalmazásnak ne kellene felkészülnie a technológiai fejlődéssel együtt járó új jelenségekre, így különösen a mesterséges intelligenciával összefüggő elkövetési formákra.

4.3. A gyermekpornográfia új megjelenési formái a mesterséges intelligencia korában

A mesterséges intelligenciával összefüggő elkövetési formák megértéséhez szükséges röviden áttekinteni a gyermekpornográfia nemzetközi fogalmát és annak fejlődését. A gyermekpornográfia fogalmát a nemzetközi jogi dokumentumok is hasonló alapokon határozzák meg, ugyanakkor az egyes államok között bizonyos eltérések figyelhetők meg.[45] A Budapesti Egyezmény[46] és a Lanzarote Egyezmény[47] egyaránt abból indul ki, hogy gyermekpornográfiának minősül minden olyan vizuális tartalom, amely kiskorút ábrázol kifejezetten szexuális jellegű helyzetben, illetve ide sorolhatók azok az ábrázolások is, amelyek kiskorúnak tűnő vagy valósághűen megjelenített személyeket mutatnak be. A szabályozás

41 Egri Törvényszék 4.Bf.248/2015/8.
42 Ajkai Járásbíróság B.54/2014/18.
43 Nyíregyházi Járásbíróság 2.B.1190/2015/4.
44 2/2018. BJE szám.
45 Mezei (2021) i.m. 21–22.
46 Az Európa Tanács egyezménye a számítástechnikai bűnözésről; 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről (a továbbiakban: Budapesti Egyezmény) 9. cikk 2. bekezdés.
47 Az Európa Tanács egyezménye a gyermekek védelméről a szexuális kizsákmányolás és a szexuális bántalmazás ellen; 2015. évi XCII. törvény az Európa Tanácsnak a gyermekek szexuális kizsákmányolás és szexuális zaklatás elleni védelméről szóló Egyezménye kihirdetéséről, valamint ezzel összefüggésben egyes törvények módosításáról (a továbbiakban: Lanzarote Egyezmény) 20. cikk 2. bekezdés.

ugyanakkor mozgásteret hagy az államoknak abban, hogy a kizárólag fiktív vagy mesterségesen előállított tartalmakat milyen körben rendelik büntetni.[48]

A technológiai fejlődés következtében egyre inkább elterjed az úgynevezett virtuális és pszeudo-gyermekpornográfia. Előbbi körébe tartoznak a számítógéppel generált képek, rajzok vagy animációk, míg utóbbi esetben valós képek digitális manipulációjáról van szó, például amikor egy felnőtt testét úgy módosítják, hogy az kiskorúénak tűnjön. Új jelenségként kell számolni a mesterséges intelligenciával létrehozott, úgynevezett „deepfake" tartalmakkal is, amelyek valósághűen képesek egy személyt pornográf helyzetben feltüntetni. Ezeknek a tartalmaknak a megítélése nem egységes, azonban egyre inkább az a szemlélet erősödik, hogy a valósághűen megjelenített, nem létező kiskorúakat ábrázoló felvételek is büntetőjogi relevanciával bírhatnak. Ennek oka, hogy bár közvetlen fizikai sérelem nem minden esetben mutatható ki, az ilyen tartalmak hozzájárulhatnak a gyermekek szexuális kizsákmányolásának normalizálásához, erősíthetik az elkövetői hajlandóságot, valamint szerepet játszhatnak a grooming folyamatokban is. Mindezek miatt a jogalkotás egyre inkább arra törekszik, hogy a technológiai fejlődés által létrehozott új formákat is a büntetőjogi védelem körébe vonja.[49]

Igazodva a nemzetközi tendenciákhoz, a Btk. 204. § (8) bekezdése a pornográf felvétel fogalmát úgy határozza meg, hogy abba már nemcsak a valós kiskorúakat ábrázoló tartalmak tartoznak bele, hanem a nem létező személyek valósághű ábrázolásai is. Ez azt jelenti, hogy a büntetőjogi felelősség nem kerülhető meg pusztán arra hivatkozással, hogy a felvételen szereplő „gyermek" nem valós személy. A jogalkotó ezzel a megoldással kiterjesztette a védelem körét, a szabályozás így már nemcsak a hagyományos fényképfelvételekre vonatkoztatható, hanem minden olyan ábrázolásra, amely alkalmas a kiskorú felismerhető megjelenítésére. Ez azt jelenti, hogy valós személy esetében nem feltétel a teljes valósághűség: elegendő, ha az ábrázolt személy beazonosítható. Ennek megfelelően akár rajz vagy festmény is megalapozhatja a büntetőjogi felelősséget, ha azon konkrét kiskorú felismerhető módon jelenik meg. Ezzel párhuzamosan új elemként jelent meg a nem létező személyek valósághű ábrázolásának büntethetősége. A jogalkotó e körben a valósághoz megtévesztésig hasonló ábrázolásokat kívánja lefedni, vagyis azokat az eseteket, amikor nem állapítható meg egyértelműen, hogy a képen szereplő személy valós-e vagy sem. Ez a gyakorlatban elsősorban a mesterséges intelligenciával létrehozott, úgynevezett „deepfake" tartalmakhoz kapcsolódik.[50]

A virtuális gyermekpornográfia elleni fellépés nem pusztán elméleti kérdés. Bár ezekben az esetekben jellemzően nem ér közvetlen fizikai sérelem egyetlen

48 Mezei (2021) i.m. 22.
49 Mezei (2021) i.m. 23.
50 Szomora (2025) Gyermekpornográfia… i.m.; A Büntető Törvénykönyvről szóló 2012. évi C. törvény indokolása. A 204. §-hoz.

kiskorút sem, a jelenség mégis komoly veszélyeket hordoz. A virtuális tartalmak felhasználhatók a gyermekekkel való kapcsolatfelvétel során, és alkalmasak arra is, hogy a kiskorúakat fokozatosan bevonják szexuális jellegű kommunikációba vagy tevékenységekbe. Az elkövetők oldalán pedig hozzájárulhatnak a kiskorúak iránti szexuális érdeklődés megerősödéséhez, valamint csökkenthetik az ilyen magatartásokkal szembeni belső gátakat. A kutatások szerint az ilyen jellegű, akár mesterségesen előállított tartalmak fogyasztása hosszabb távon növelheti annak kockázatát, hogy az érintettek valós személyek sérelmére is hasonló cselekményeket kövessenek el.[51]

A jelenség társadalmi szinten is problémát jelent. A gyermekek szexuális célú ábrázolásának elterjedése hozzájárulhat ahhoz, hogy a gyermekeket szexuális tárgyként megjelenítő tartalmak iránti kereslet fennmaradjon, és ezzel közvetve a valós kiskorúak kizsákmányolásának piaca is életben maradjon. Emellett az ilyen tartalmak normalizálhatják a gyermekek tárgyiasítását, és gyengíthetik a társadalmi elutasítást a hasonló jellegű visszaélésekkel szemben.[52]

A mesterséges intelligencia alkalmazása nemcsak új elkövetési formák megjelenéséhez vezet, hanem általánosabb kockázatokat is felvet a bűnözés szempontjából. A tapasztalatok azt mutatják, hogy a generatív MI-rendszerek képesek részletes, logikusan felépített és akár kreatív válaszokat is adni olyan kérdésekre, amelyek bűncselekmények megtervezésére vagy végrehajtására irányulnak. Ez azt jelenti, hogy az ilyen rendszerek – akár közvetve, kifejezett szándék nélkül is – hozzájárulhatnak a jogellenes magatartások előkészítéséhez, miközben azok felderítését is megnehezíthetik.[53]

Bár a fejlesztők folyamatosan törekednek arra, hogy az ilyen rendszerek kiszűrjék a káros vagy jogellenes felhasználási módokat, a gyakorlatban ezek a korlátok nem minden esetben bizonyulnak elégségesnek. A mesterséges intelligencia sajátossága, hogy ugyanaz az eszköz egyszerre szolgálhat hasznos és káros célokat: miközben számos területen elősegíti a fejlődést, egyúttal lehetőséget ad a visszaélésekre is.[54]

Ez különösen indokolttá teszi, hogy a jogalkotás és a jogalkalmazás ne csak az egyes konkrét bűncselekményekre reagáljon, hanem a technológia általános kockázatait is figyelembe vegye. A gyermekpornográfia és más szexuális bűncselekmények esetében ez azt jelenti, hogy a mesterséges intelligencia által nyújtott

51 Ambrus István: A mesterséges intelligencia és a büntetőjog. Állam- és Jogtudomány LXI. évf. 2020/4. 4–23. 22. Elérhető: https://real.mtak.hu/118745/1/2020-04_AMBRUS-tan.pdf.

52 Mezei (2021) i.m. 24.

53 *Solt Ágnes – Virág György*: „Azt hittem, barátok vagyunk" Kódolt megtévesztés, avagy a mesterséges intelligenciafelhasználása a bűnelkövetésben. Kriminológiai Tanulmányok 62. Országos Kriminológiai Intézet, 2025, 30–47. 45. Elérhető: https://okri.hu/images/stories/KT/KT62_2025/002_Solt-Virag.pdf https://doi.org/10.58655/KT.62.2025-2

54 Solt – Virág (2025) i.m. 46.

új lehetőségeket a büntetőjogi védelem szempontjából is értékelni kell, és szükség esetén a szabályozást ehhez kell igazítani.

5. Záró gondolatok

Jelen írásomban kísérletet tettem annak bemutatására, hogy a számítástechnikai, illetve az internetes bűncselekmények milyen összetettek, megoldásuk milyen komplex lehet. Az elkövetők gyakran magasan kvalifikált, vagy az átlagosnál intelligensebb személyek, akik a virtuális világot kihasználva arctalanul tudnak több millió forintos, vagy akár dolláros károkat okozni, nem beszélve azon bűncselekmény típusokról – mint például a gyermekpornográfia – amelyek a sértett személyek egész életét tehetik tönkre. A technikai fejlődés rendkívül gyors, napról napra jelennek meg új technikai vívmányok, amelyeket ugyanilyen gyorsasággal találnak meg a bűnözők is, hogy cselekményeik eszközévé, színterévé tegyék azokat. A bűncselekményeket gyakran határokon átívelve követik el, a sértetteknek igen magas száma lehet, és rengeteg ország érintett. Így a jogalkotók és jogalkalmazók vállán hatalmas felelősség nyugszik, nem csak abban, hogy megfelelően lépést tartsanak a bűnelkövetőkkel, de abban is, hogy megfelelő nemzetközi egyezményekkel, és intézményekkel felvegyék a harcot a bűnözőkkel szemben. Erre láthatunk pozitív példákat, mint a Budapesti Egyezmény, vagy az Európai Kiberbűnözés Elleni Központ megalakulása. Azonban, ha valóban komolyan gondoljuk és mindenek felett érvényesíteni kívánjuk gyermekeink érdekeiket - a „The best interests of the child”[55] filozófiáját követve - a jogalkotásban is gyorsítanunk kellene, elfogadva a technikai világ száguldásának kihívásait.

Felhasznált Irodalom

Ambrus István: A mesterséges intelligencia és a büntetőjog. Állam- és Jogtudomány LXI. évf. 2020/4. 4–23. Elérhető: https://real.mtak.hu/118745/1/2020-04_AMBRUS-tan.pdf

Bezáková, Zuzana – Madleňák, Adam – Švec, Marek: Security Risks Of Sharing Content Based On Minors By Their Family Members On Social Media In Times Of Technology Interference. Media Literacy and Academic Research,

55 ENSZ Gyerekjogi Egyezményének 3. cikkéből ered: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

Vol. 4, No. 1, April 2021. 64–65. Elérhető: https://www.mlar.sk/wp-content/uploads/2021/04/4_Bezakova_Madlenak_Svec.pdf

Csapucha Bernadett: A veszélyeztetési eredmény értelmezése a kiskorú veszélyeztetése törvényi tényállásában. Büntetőjogi Szemle 2021/1., 15-23. Online Szakcikk Adatbázis. Elérhető: https://szakcikkadatbazis.hu/doc/6615031

Hvg.hu: Meghátrált a Discord, egyelőre nem vezetik be a vitatott életkor-ellenőrzést. 2026.02.25. Elérhető: https://hvg.hu/tudomany/20260225_discord-eletkor-ellenorzes-bevezetes-halasztasa-valtoztatasok

Kherkher, Steve: Suing Discord for Child Exploitation. November 25, 2025. Elérhető: https://www.kherkhergarcia.com/suing-discord-for-child-exploitation/

Kiss Annamária: A kiskorú veszélyeztetése bűntettének első alakzatához kapcsolódó ítélkezési gyakorlat elemző bemutatása. Glossa Iuridica, 2025/1-2., 291-320. Online Szakcikk Adatbázis. https://doi.org/10.55194/GI.2025.1-2.15 Elérhető: https://szakcikkadatbazis.hu/doc/1280009

Makai Katinka: A gyermekek érdekeit sértő és a család ellen tanúsított magatartások büntetőjogi és polgári jogi vetületei I. rész, Büntetőjogi Szemle 2020/2., 57-65. Online Szakcikk Adatbázis. Elérhető: https://szakcikkadatbazis.hu/doc/2723906

Meggyesfalvi Boglárka: Kockázati tényezők a digitális térben: A gyerekek internet- és közösségi média használata és az online áldozattá válás. Belügyi Szemle, 71. évf. 2023/12., 2163–2178. https://doi.org/10.38146/BSZ.2023.12.3

Mezei Kitti: Az online gyermekpornográfia és a büntetőjog. Ügyészek Lapja 28. évf. 2021/4. 19–30. 19. Elérhető: https://real.mtak.hu/135281/1/mezei_UL_2021_4beliv.pdf

Nagy Nelli: A sharenting megakadályozása: A gyermekek jogainak érvényesítése a szülői felügyeleti jog korlátozásával szemben. Arsboni. 2025. május 12. Elérhető: https://arsboni.hu/a-sharenting-megakadalyozasa-a-gyermekek-jogainak-ervenyesitese-a-szuloi-felugyeleti-jog-korlatozasaval-szemben/

Police.hu: Grooming: Ragadozók a kibertérben | A Rendőrség hivatalos honlapja. Elérhető: https://www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag/grooming-ragadozok-a-kiberterben

Pongrácz Ildikó: Gyermekek a digitális világ útvesztőiben – veszélyek és lehetőségek. Miskolci Jogtudó 2019/2. 55–69. Elérhető: https://jogtudo.uni-miskolc.hu/files/7394/MJ2019iss2art6Pongracz.pdf

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. EU Kids Online. 45., 53. https://doi.org/10.21953/lse.47fdeqj01ofo Elérhető: https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf

Solt Ágnes – Virág György: „Azt hittem, barátok vagyunk" Kódolt megtévesztés, avagy a mesterséges intelligenciafelhasználása a bűnelkövetésben. Kriminológiai Tanulmányok 62. Országos Kriminológiai Intézet, 2025, 30–47. Elérhető: https://okri.hu/images/stories/KT/KT62_2025/002_Solt-Virag.pdf, https://doi.org/10.58655/KT.62.2025-2

Szomora Zsolt: Kiskorú veszélyeztetése. In: Karsai Krisztina: Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez, 2025. július 1. időállapotú, 2025. évi Jogtár-formátumú kiadás.

Szomora Zsolt: Gyermekpornográfia. In: Karsai Krisztina: Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez, 2025. július 1. időállapotú, 2025. évi Jogtár-formátumú kiadás.

Varga Árpád: A gyermekekre veszélyes online kihívások fogalma, jellemzői, okai és a hazai fiatalok érintettsége. Családi Jog 2023/4., 21-28. Online Szakcikk Adatbázis. Elérhető: https://szakcikkadatbazis.hu/doc/8258379

Varga Árpád: A gyermekek online szexuális kizsákmányolása elleni küzdelem egyes szabályozási tendenciái és európai irányvonalai. Iustum Aequum Salutare XXI. 2025. 2. 175–190. XXI. 2025. 2. 175–190.178–179. Elérhető:https://publikacio.ppke.hu/id/eprint/2802/1/2025-02_10_Varga.pdf; https://doi.org/10.69695/ias.2025.2.10

WHO: One in six school-aged children experiences cyberbullying, finds new WHO/Europe study. 27 March 2024. Elérhető: https://www.who.int/europe/news/item/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study