Szemléletformáló füzetek
DJP Mentorok részére
2017

11 // Gyermekek a digitális világban I. – Biztonság

Nemzeti Fejlesztési Minisztérium
digitális jólét program hálózat
KIFÜ
SZÉCHENYI 2020
Magyarország Kormánya
Európai Unió
Európai Regionális Fejlesztési Alap
BEFEKTETÉS A JÖVŐBE

GYERMEKEK A DIGITÁLIS VILÁGBAN I. – BIZTONSÁG

Miközben csak kapkodjuk a fejünket, és több-kevesebb sikerrel próbálunk folyamatosan alkalmazkodni a gyorsuló digitalizációs forradalom újabb és újabb technikai újdonságaihoz, gyermekeink már jórészt ma is a digitális világban élnek. A digitális világban – éppúgy, mint életünkben – ugyanúgy fontos, hogy megtanuljuk és megtanítsuk a viselkedési normákat, azaz mi és gyermekeink is tudatos felhasználókká váljunk.

Soha nem volt még olyan az emberi történelem során, hogy az egymást követő generációk élete, technikai környezete ennyire különbözött volna. Generációk sora tudott mindig érvényes tudást átadni a következőnek, hiszen mind technikai, mind társadalmi környezetük szinte változatlan volt.

Nap mint nap érezzük, hogy a világ változása felgyorsult, így a digitalizációs átmenet korában egyre kevésbé értjük a következő generációk – így gyermekeink – életét, vágyait. Egyre nehezebben tudunk hatni rájuk, és egyre kevésbé ismerjük fel a rájuk leselkedő esetleges veszélyeket.

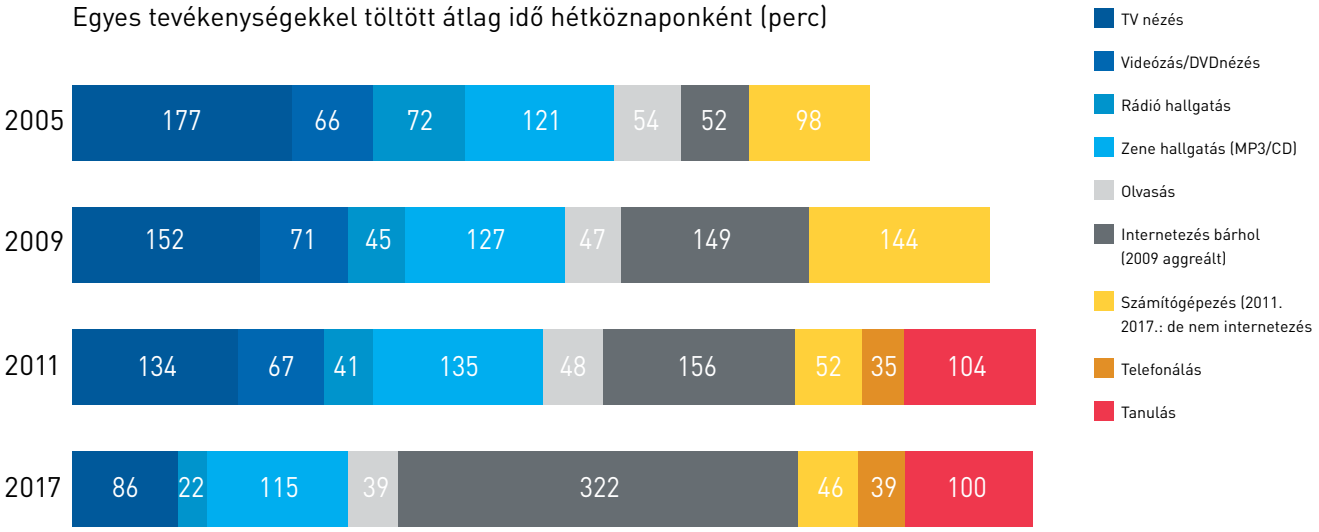
Ezért különösen fontos, hogy a lehető legmélyebb ismeretekkel rendelkezzünk mindazokról a lehetőségekről és kockázatokról, melyek a gyermekek életére kihatnak.

Mindig online

Az internetelérés és számítógépes penetráció gyors növekedésével napjainkban a legtöbb magyar család rendelkezik valamilyen számítástechnikai eszközzel és internet-hozzáféréssel; csupán a gyermekek kis része él olyan családban, ahol nincs internet, illetve valamilyen számítógép, okostelefon.

Ezzel párhuzamosan alig több mint 10 év alatt drasztikusan átalakult a gyerekek szabadidős időmérlege is: míg egy évtizede a legtöbb időt tv-nézéssel töltötték, mára a tv-t – más szabadidős tevékenységekkel együtt – elsöpörte az internet. A Nemzetközi Gyermekmentő Szolgálat IX. Nemzetközi Médiakonferenciájára készült részére készült „20 év kutatás a médiáról és a gyerekekről” című kutatás adatai szerint 2017-ben átlagosan napi több mint 5 órát töltenek az interneten. Azt, hogy az internet átvette a többi médiafelület szerepét, jól jelzi, hogy a gyerekek közel fele a tv-sorozatokat is online fogyasztja.

SZABADIDŐ ÉS MÉDIA



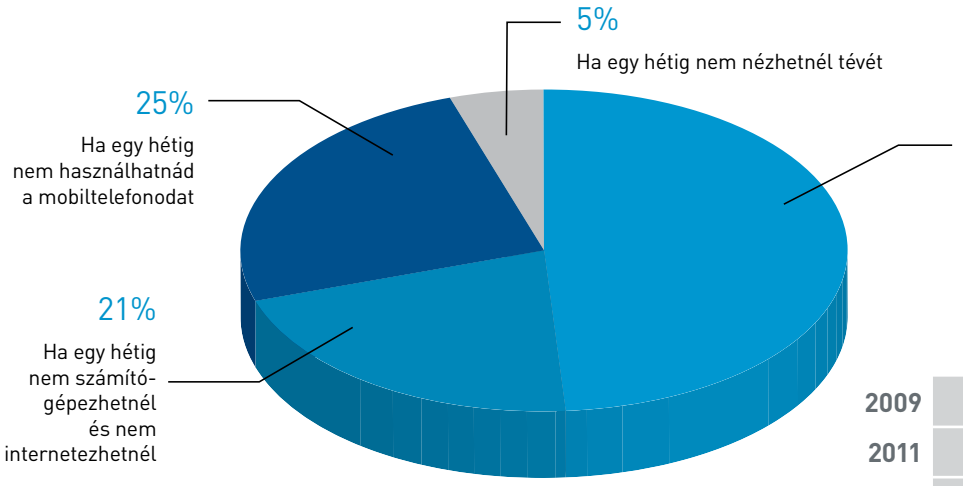
Forrás: Nemzetközi Gyermekmentő Szolgálat (2017)

A digitalizáció és a közösségi felületek egyértelműen megváltoztatták a gyerekek szocializációs környezetét is: a megfelelő korosztályokban gyakorlatilag mindenki fenn van valamely éppen népszerű közösségi oldalon, és az ottani kommunikációs eszközök használatával szinte folyamatosan online kapcsolatban is vannak.

Ilyen mértékű jelenlét révén a média mint fő szocializációs ágens jelenik meg az életükben, háttérbe is szorítva akár a hagyományosabb szocializációs közvetítő csatornákat, mint például a családot vagy az iskolát, sőt még a kortárscsoportot is. Az internet, a folyamatos elérés lassan fontosabbá válik minden másnál.

BARÁTSÁG 2.0

Válaszd ki azt a büntetést, amelyiket személy szerint a legsúlyosabbnak érzel! (%)



2009	6	10	22	61
2011	7	10	25	58
2017	5	25	21	49

Forrás: Nemzetközi Gyermekmentő Szolgálat (2017)

A gyermekeket az internet használatából fakadó hatások értelmezésére és esetleges veszélyek felismerésére és elhárítására a szülőknek csak korlátozott mértékben van módjuk, hiszen többségüknek nincs megfelelő ismerete ehhez. Az iskolában és a gyermekvédelem intézményeiben ugyan dolgoznak a médiahatással, illetve a gyermekek viselkedési sajátosságaival foglalkozó szakemberek, de az ő eszközeik korlátozottak a gyermekek médiafogyasztási szokásainak befolyásolásában. Kétségtelen tehát, hogy a társadalom legszélesebb összefogására van szükség ahhoz, hogy hatékonyan kezeljük az eszközök használatából eredő legkülönbözőbb problémákat (pl.: az állandó használat, vagy a különböző felhasználókra leselkedő veszélyek), illetve hogy az infokommunikációs technológiákat – a digitális oktatás meghonosításával – a gyermekek fejlesztésének szolgálatába állítsuk.

Általában a digitális kockázatokról

A gyerekek internethasználatának elterjedésével számos olyan újfajta kockázatforrás is megjelent, amely a mindennapi (offline) világban ismeretlen volt. Éppen ebből is adódóan az online tér különös, sok esetben első pillantásra fel sem ismerhető kockázatokat is rejt magában, amellyel együtt mind a védekezés, mind pedig a segítségnyújtás nehezebb feladatot jelent.

A kockázatokkal szembeni hatékony védekezéshez így elengedhetetlen legalább az alapvető ismeretek elsajátítása. Ezen ismereteknek ki kell terjedniük a káros tartalmak, illetve magatartások felismerésére és ennek megfelelő kezelésére, a rendelkezésre álló védelmi eszközök és mechanizmusok ismeretére, továbbá a segítségnyújtásban szerepet vállaló, valódi szaktudással bíró intézmények igénybevételének lehetőségére. Fontos megjegyezni, hogy az említett készségek elsajátítása nem kizárólag a gyermekek számára elengedhetetlen: az internethasználat rejtette kockázatokkal a szülőknek, pedagógusoknak éppúgy tisztában kell lenniük és nekik is tudatos felhasználókká kell válniuk.

Az alábbiakban az internethasználat során leggyakrabban felmerülő kockázatokról ejtünk szót, kitérve a rendelkezésre álló védelmi megoldások alkalmazására, elérhetőségére. Noha a napi szintű internetezés vitathatatlanul leginkább kockázatoknak kitett csoportját a gyermekek jelentik, az összegyűjtött példák között számos olyan is található, amely kortól függetlenül, mindenki számára valós kockázatokat jelenthet (lásd például az internetfüggőség vagy az adatvédelmi jogsértések kérdését). Éppen ezért az alábbiakban a lehetséges megoldások, támpontok széles skáláját is kínáljuk.

Az internethasználattal kapcsolatos leggyakrabban felmerülő kockázatok

Az internethasználat során felmerülő kockázatok köre, megjelenési formái, hatásai igen sokrétűek. Egy részükre igaz, hogy a mindennapi életben is előforduló jelenségek online megfelelőiként (lásd például az online zaklatást vagy megfélemlítést) értékelhetők, ugyanakkor más esetekben a károkozás reális lehetősége az internet adta specialitásokból ered.

Erre tekintettel a kockázatok az alábbiak szerint csoportosíthatók:

1. az internethasználat mint tevékenység okozta sérelmek;
2. az interneten közzétett tartalmak kockázatai és
3. más személyek (internethasználók) káros magatartása.

1. Az internethasználat önmagában rejlő kockázatai

Ebben a körben azokat az internethasználat rejtette kockázatokat érdemes megemlíteni, amelyek bármiféle külső tényező, károkozásra irányuló szándék hiányában is képesek hátrányos következményeket okozni a felhasználó számára, főként az ismeretek hiányára visszavezethetően.

Elsőként beszéljünk az internethasználat kapcsán bizonyos esetekben könnyen kialakuló függőség (addikció) kérdéséről. Erre talán a legjobb példaként az online játékok szolgálnak, amelyek, még ha önmagukban nem is jelentenek kockázatot (értve ezalatt, hogy káros tartalmat nem hordoznak), de a korlátok nélküli használatuk a gyerekek fejlődésére nézve hosszú távon károsnak mutatkozhatnak.

Hasonlóan függőséget jelenthet a közösségi médiában való aktív, rendszeres jelenlét igénye, ez ugyanis egy idő után nem csak kényszerként jelentkezik és a személyiségre nézve gyakorol káros hatást (például személyes kapcsolatok megszűnése, személyes kommunikáció és kapcsolatteremtés készségének érezhető romlása), de e körben említhető a számos ál- és hamis információ nem megfelelő kezelésének problémája is (az álhírek jelenségéről bővebben a sorozat 10. füzetében olvashatsz).

A VIDEOJÁTÉKOK OKOZTA FÜGGŐSÉG

Az online videojátékok okozta függőség kockázatos jelenséggé képes válni, amely mind fizikai, mind pszichés tekintetben könnyen káros hatásokat válthat ki a fiatalokból. A fizikai problémák megnyilvánulhatnak mozgás- vagy érzékszervi betegségekben, míg a mentális hatások eredményeképpen a gyermekek könnyen elveszíthetik kapcsolatukat a való világgal, a szociális kapcsolataikra gyakorolt hátrányos hatások mellett pedig a játéktól való eltiltás akár elvonási tünetekkel is járhat.

Szintén ebbe a témakörbe tartozik, elsősorban az ismeretek hiányára visszavezethető kockázatok azon köre, amelyek az online fizetési lehetőségek kapcsán jelentkezhetnek. Napjainkban igen egyszerűen lehet olyan módon vásárolni, szolgáltatást megrendelni, illetve szerződést kötni, amelyből a későbbiek során bármilyen teljesítési (konkrétan például fizetési) kötelezettség keletkezik a felhasználó számára. Gyakran előfordul, hogy a tájékozatlan vagy akár csak figyelmetlen internethasználó (gyermek) olyan kötelezettséget vállal, amelyet valójában nem szándékozott, rosszabb esetben nem is tud teljesíteni.

2. Káros internetes tartalmak

Ide azokat az internetes tartalmakat soroljuk, amelyek önmagukban nem minősülnek jogellenesnek, egyes korosztályok számára azonban – elsősorban szellemi fejlettségükre tekintettel – hátrányos hatást gyakorolhatnak. Ezek a tartalmak jellegüket tekintve jellemzően a nyílt szexualitást (pornográfiát), illetve az erőszakot közvetlen formában ábrázoló elemek, de emellett olyan témák feldolgozása is alapot adhat az ilyen besorolásra, amelyeket a gyermekek szintén nem képesek megfelelően kezelni, értelmezni (pl. erőszak). Az efféle tartalmakat tekintve alapvető elvárás, hogy esetükben a szolgáltatók valamilyen technikai eszközzel biztosítsák, hogy a gyermekek lehetőség szerint ne férjenek hozzá, ugyanakkor azok a felnőttek számára továbbra is hozzáférhetők legyenek.

JOGELLENES ÉS KÁROS TARTALMAK ELHATÁROLÁSA

Az online tartalmakkal (és egyéb magatartásokkal) szembeni védekezés során a velük szemben történő fellépés módja, lehetőségei tekintetében megkülönböztetjük a jogellenes és a káros tartalmakat. Az első körbe azok a tartalmak sorolhatók, amelyek a hatályos jogszabályokba, így elsődlegesen a Büntető törvénykönyvbe, illetve a Polgári törvénykönyvbe ütköznek, azaz közzétételükre jogszerűen semmilyen formában nem kerülhet sor (például zaklatás, pedofil tartalmak, más képmásának jogosulatlan felhasználása, becsületsértő tartalom közzététele). A káros tartalom az előzőkkel ellentétben jogszerűen megjelenhet, azonban tekintettel arra, hogy a kiskorúak egészséges fejlődésére kedvezőtlen befolyást képes gyakorolni, ezért a jogalkotók általában velük szemben a hozzáférés korlátozását követelik meg.

3. Káros magatartások

A kockázatok e körében azokat az internet elterjedésével együtt megjelenő jelenségeket, magatartásokat kell megemlíteni, amelyek az online tér egyes sajátosságait kihasználva alkalmasak károkozásra. Az alábbiakban említésre kerülő magatartásformák jelentős részben önmagukban is alkalmasak a károkozásra, míg egy részük csupán „előkészületi” cselekményként értékelhetők, a tényleges sérelemre aztán a maga fizikai valóságában kerül sor (e magatartások felsorolása kapcsán a Digitális Gyermekvédelmi Stratégiában foglaltakat vettük alapul, a stratégiáról e fejezetben még részletesen szólunk).

Az elsőként említésre érdemes magatartásforma a számos formában megnyilvánuló cyberbullying (vagy online megfélemlítés). Az online tér egyik legnagyobb problémájává nőtte ki magát, amely sokkal eredményesebben és hatásosabban félemlíti meg az áldozatot, mint a fizikai erőszak.

Az online megfélemlítés, zaklatás napjainkban ismert, jelentősebbnek mondható megnyilvánulási formái az alábbiak:

- flaming (égetés): dühös és trágár nyelvezet használatával támadó jellegű hozzászólások küldése nagy nyilvánosság előtt;
- harassment (zaklatás): sorozatosan és hosszabb ideig fennálló szándékos sérelemokozás, jellemzően támadó, sértő, felzaklató üzenetek küldésével, amely célja lehet a fiatal megalázása, fenyegetése, nevetségessé tétele, kiközösítése, lejáratása, negatív színben feltüntetése;
- denigation (befeketítés): a hírnév rontására alkalmas pletykák vagy szóbeszéd küldése, kiposztolása, terjesztése valakiről;
- exclusion (kiközösítés): az online közösség egy tagjának az adott csoportból való kirekesztésére irányuló szándék;
- outing (kibeszélés): titkok, pletykák vagy egyéb személyes információk engedély nélküli megosztása másokkal;
- trickery (trükközés, becsapás): személyes adatok csalással, megtévesztéssel történő megszerzése valakitől, majd ezeknek az információknak, adatoknak a közösséggel való megosztása;
- cyberstalking (online megfigyelés): az áldozat online szokásainak megfigyelése, folyamatos figyelemmel kísérése és támadó jellegű kijátszása, fenyegető, megfélemlítő üzenetek küldése és ezek felhasználása félelemkeltésre;
- cyberthreats (online fenyegetések): közvetlen fenyegetések, nyugtalanító kijelentések, amelyekből úgy tűnik, hogy a szerző másban vagy esetleg magában kárt kíván tenni (esetleg öngyilkosságot szándékozik elkövetni);
- sexting (szexting): saját magáról készített, szexuálisan provokatív kép vagy nyíltan szexuális tartalmú szöveg online elküldése másnak, majd az ilyen felvételek széles nyilvánossággal való megosztása.

Szintén itt érdemes röviden említést tenni az internetes pedofília veszélyéről. Ebben az esetben ugyan az online tér csak az előkészülethez nyújt megfelelő terepet az elkövető számára, ugyanis hamis profilok mögé rejtőzve könnyen más személynek – legtöbb esetben szintén gyermeknek – kiadva magukat próbálhatják meg a gyermekek tapasztalatlanságát kihasználni.

Adatvédelem

Érdemes szót ejteni az adatvédelmi visszaélések problematikájáról, ennek is napjainkban egyik igen gyakran megvalósuló formájáról, az online adathalászatról (phishing), amely egy, a felhasználók megtévesztését szolgáló módszer arra, hogy felfedjék személyes és pénzügyi adataikat félrevezető e-mail üzeneteken vagy internetes oldalakon keresztül. A személyiséglopás

mint internetes úton elkövetett bűncselekmény az utóbbi években terjedt el igazán, és nagyrészt az adathalászathoz és a közösségi oldalakhoz köthető. Ennek során az elkövetők az áldozat valamennyi releváns személyes adatát, illetve sok esetben bizalmas információit is megszerzik, amely eredményeképpen pedig valódi értelemben vett károkozásra (például online vásárlásra, hitelfelvételre vagy egyéb kötelezettségvállalásra) is sor kerülhet.

A kockázatokkal szembeni védekezés hatékony formái

Az előző pont alatt említett kockázatokkal szembeni védelmi mechanizmusok alapvetően kétirányúak lehetnek: egyfelől a gyermekek (illetve valamennyi internethasználó) felkészítése a lehetséges kockázatokra, azok elkerülésére, a rendelkezésre álló segítség igénybevételére, másfelől pedig az állam által – és jellemzően jogszabályok útján megkövetelt – kötelezően alkalmazandó technikai megoldások megkövetelése.

A gyermekek tudatosságának növelése

Az internet kockázataival szembeni védelem egyik legfontosabb formáját a gyermekek kellő szintű ismereteinek megteremtése jelenti, amely következtében fel tudják ismerni és ennek következtében el tudják kerülni az internetezés során felmerülő káros, kockázatos tartalmakat. Ez a kompetencia szoros összefüggésben értelmezendő a biztonságos internethasználatot elősegítő technikai megoldások ismeretével, azaz az egyes biztonsági megoldások (például a 18 éven aluliaknak nem ajánlott tartalmak előtt az e jellegükre való figyelemfelhívás) felismerése az internethasználat során is kiemelt szempontnak számít.

A kockázatok elkerülése mellett a gyermekeknek a káros tartalmakkal való szembetalálkozásuk során ugyanúgy rendelkezniük kell az alapvető készségekkel. Ez a gyakorlatban elsősorban a számukra nem ajánlott vagy kifejezetten kockázatos tartalmakkal, magatartásokkal történő szembesülés felismerésében, másodlagosan pedig a kockázatok megfelelő fórumok felé (például Hotline-ok, állami szervek, pedagógus) való bejelentésében nyilvánul meg – ezzel is hozzájárulva esetlegesen kevésbé felkészült társaik megóvásához.

Technikai és jogi megoldások mint a védelem eszközei

Elsőként a szolgáltatók által kötelezően alkalmazandó szűrőszoftver-megoldásokról érdemes szót ejteni. Az elektronikus hírközlési törvény értelmében[1] az internetszolgáltatók kötelesek kiskorúak védelmét lehetővé tevő, magyar nyelvű, könnyen telepíthető és használható szoftver internetes honlapjáról való ingyenes letölthetőségét, illetve ingyenes használhatóságát biztosítani[2]. Ezen technikai megoldás biztosítja, hogy a gyermekek egészséges fejlődésére káros, illetve esetenként kifejezetten jogellenes internetes tartalmak számukra ne legyenek elérhetők.

1 *Lásd az elektronikus hírközlésről szóló 2003. évi C. törvény 149/A. § (1) bekezdését.*
2 *A jelenleg a piacon elérhető szűrőszoftverek listáját lásd az alábbi linken: http://nmhh.hu/dokumentum/173242/szuroszoftverek.pdf.*

A szoftver előnye, hogy azzal az egyes tartalmak korlátozása mellett számos egyéb beállítás is eszközölhető, így például a gyermekek internethasználatára fordított (napi) időkeret vagy idősáv is beállítható.

A médiaszabályozás által megkövetelt[3] hatékony műszaki megoldások szolgáltatók (és műsorterjesztők) általi alkalmazása – e tekintetben a szűrőszoftverekhez hasonlóan – az interneten elérhető káros tartalmak jogszabályban meghatározott körének a hozzáférhetetlenné tételét, de legalábbis megnehezítését kívánják szolgálni.

AJÁNLÁS A HATÉKONY MŰSZAKI MEGOLDÁSOKRA

A hatékony műszaki megoldásokkal kapcsolatosan a Nemzeti Média- és Hírközlési Hatóság Médiatanácsa által kiadott ajánlás a jogszabályi követelmények betartása érdekében többféle javaslatot megfogalmaz. Így például, amennyiben a médiatartalom tizennyolc éven aluliaknak nem ajánlott tartalmat, illetve pornográfiát vagy szélsőséges, indokolatlan erőszakot tartalmaz, a médiaszolgáltató az életkor-ellenőrzéssel egyidejűleg, azonos helyen, jól láthatóan hívja fel a néző figyelmét a kiskorúakra vonatkozó kockázatokra, például az alábbi szöveg megjelenítésével: „Figyelem! Ez a médiatartalom kiskorúakra káros elemeket is tartalmaz. Amennyiben azt szeretné, hogy az Ön környezetében kiskorúak hasonló tartalmakhoz csak egyedi kód megadásával – azaz kiskorúak kizárása mellett – férjenek hozzá, kérjük, használjon szűrőprogramot! Szűrőprogram letöltése és további információk itt (tájékoztató oldal URL hivatkozása)."

A hatékony műszaki megoldásokhoz mind céljában, mind megjelenési formájában nagymértékben hasonlító megoldást ír elő az elektronikus kereskedelmi törvény[4], miszerint a médiaszabályozás előzőkben említett hatályán kívül eső azon internetes tartalmakat, amelyek súlyosan károsíthatják a kiskorúak egészséges fejlődését, a szolgáltató kizárólag e tényre történő figyelemfelhívás mellett teheti közzé. Mindemellett a hatályos törvényi előírások e klasszifikációs kötelezettség alkalmazása által azt is biztosítják, hogy a kiskorúak fejlődésére káros internetes tartalmak az előzőkben említett szűrőszoftver révén felismerhetők – és ezáltal szűrhetők – legyenek.

Indokolt még említést tenni azon jogvédelmi eszközről, amely a kifejezetten internetes úton és gyermekek sérelmére elkövetett jogsértések gyors és hatékony orvoslását hivatott szolgálni. Az úgynevezett értesítési-eltávolítási eljárás (notice and take down) igénybevételével a személyiségi jogok kiskorú jogosultjai, illetve a kiskorú jogosultak törvényes képviselői egy precízen szabályozott eljárási rend szerint, még a polgári peres, vagy a büntetőeljárás előtt vagy helyett, hatékony módon képesek lehetnek fellépni a kiskorúak személyiségi jogainak védelme érdekében. Az eljárás eredményeképpen – a szolgáltatóval történő egyeztetést követően – lehetőség nyílik a kiskorú személyiségi jogait sértő tartalmak (információ) eltávolítására.

3 *Lásd a médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény 11. §-át.*
4 *Lásd az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 4/A. § (1) bekezdését.*

Segítségkérés formái és csatornái

Kiemelt jelentőséggel bír, hogy abban az esetben, amennyiben a fiatalok – az előzőkben vázolt védelmi mechanizmus alkalmazása ellenére – mégis káros tartalommal találkoznak, esetleg már áldozattá válásukra is sor került, ne csak ismerjék, de bátran igénybe is merjék venni azokat a fórumokat, ahol számukra megnyugtató segítséget tudnak nyújtani. Segítséggel elsősorban a gyermekekhez legközelebb álló személyek (szülők, gondviselő, pedagógusok), az állami szervek és civil szervezetek, illetve a káros tartalmak bejelentésére szolgáló Hotline-ok szolgálhatnak.

A szülők és a pedagógusok szerepe

Vitathatatlan, hogy a szülőkre és pedagógusokra kiemelt szerep és felelősség hárul a megfelelő szintű segítségnyújtásban, amely természetesen feltételezi az említett személyi kör felkészültségét, az internet nyújtotta kockázatok és lehetséges hatásuk ismeretét, és nem utolsósorban a hatékony problémamegoldás módját és formáját. Amiképpen ugyanis a mindennapi életben, úgy az online világban is hasonló mértékű támogatás, segítség várható el elsősorban a szülők (illetve általánosságban véve a család) részéről a problémák megfelelő kezelésében, a károk enyhítésében.

Hasonlóképpen elvitathatatlan a pedagógusok szerepe is. A pedagógus számos esetben, például fiatalok közötti zaklatások, megfélemlítések esetében szinte valamennyi résztvevővel, érintettel (így az áldozattal, elkövetőkkel) közvetlen kapcsolatban áll. Ebből a helyzetből adódóan a pedagógus nemcsak a konfliktus észlelésében, de annak megoldásában is kulcsszereplő. A pedagógusokkal szembeni elvárás tehát az ismeretek átadása mellett az oktatási rendszer keretei között működő vita- és konfliktuskezelési mechanizmusokban való aktív részvételben is megmutatkozik.

ONLINE SZEMLÉLETFORMÁLÓ SZOLGÁLTATÁSOK

A Tabby projekt[5] célja az online és az elektronikus eszközök használata során fellépő kockázatok tudatosítása, a biztonságos webhasználat kialakítása, valamint az önvédelmet szolgáló információk és készségek átadása a tanulók, pedagógusok, iskolapszichológusok és a szülők számára.
A felületen található egy kérdőív, melynek kitöltése segítséget nyújt az internetes bántalmazás – különösen az online fenyegetés, a zaklatás, valamint a szexuális tartalmú SMS-ek – korai felismerésében és megelőzésében. Segítségével a diákok maguk is fel tudják mérni az őket érő internetes fenyegetések kockázati szintjét és saját online viselkedésüket.
Továbbá az itt található jó gyakorlatok, oktató videók és az online bulliyng kézikönyv[6] mind segítenek annak eldöntésében, hogy a fiatalokat érintő online fenyegetések mennyire komolyak, igényelnek-e közvetlen felügyeletet, megfigyelést, illetve beavatkozást.
forrás: http://hun.tabby.eu/

5 http://hun.tabby.eu/
6 http://hun.tabby.eu/uploads/1/6/8/6/16865702/booklet_hun.pdf

Az otthonaneten.hu a család minden tagjának segít abban, hogy az internet otthon is a megfelelő helyet foglalja el mindenki életében.
A kisebb és a nagyobb gyerekeknek is segít, hogy könnyen, szórakozva fedezhessék fel és biztonságosan barangolhassanak az internet világában. Továbbá a szülőknek is információt, segítséget nyújt a megismeréséhez, a megértéséhez.
Rajzfilmek, ismeretterjesztő filmek, videók, zenék, játékok segítik a tanulást, a legfontosabb tudnivalók megismerését. A netetikettet, az internet ránk leselkedő veszélyeit is megismerhetik az oldalra látogatók.
A szülőkhöz szóló pszichológiai témájú írások tanácsokat adnak a nettel kapcsolatos nehéz helyzetek megoldásához is.
Forrás: http://otthonaneten.hu/

Egy gondolat erejéig visszautalva a tudatosság kérdésére: látható, hogy az internethasználat valamennyi szegmense során elengedhetetlen feltétel az ismeretek kellő szintű elsajátítása, amely a tapasztalt felnőttek saját maguk és a gyermekek megóvása mellett a másoknak való segítségnyújtásban is jelentkezik.

Az állami és civil szféra

Az állami szervek, hatóságok jogszabály adta feladatukból kötelesek aktívan kivenni részüket mind a gyermekek biztonságát szolgálni hivatott jogszabályi előírások betartásának felügyeletét, mind pedig a bekövetkezett sérelmek esetén azok orvoslása mellett az elkövetők kellő szintű, ugyanakkor a sérelem sajátosságaihoz mérten arányos jogkövetkezmény alkalmazását. Az alábbiakban összegyűjtöttük a legfontosabb olyan állami szereplőket (és feladataikat), akikhez segítségkéréssel fordulhatnak az arra rászorulók[7].

- Bűnüldöző szervek: a rendőrség bűnfelderítési, bűnmegelőzési feladatkörében általános bűnügyi nyomozó hatósági jogkört gyakorol, végzi a bűncselekmények megelőzését, megakadályozását és felderítését, ezen túl gyakorolja a szabálysértési hatósági jogköröket[8].
- Nemzeti Adatvédelmi és Információszabadság Hatóság: súlyos adatvédelmi jogsértések gyanúja esetén hatósági eljárást indíthat, melynek során határozatban elrendelheti a jogellenesen kezelt adatok zárolását, megsemmisítését, megtilthatja az adatok kezelését vagy adatvédelmi bírságot is kiszabhat[9].
- Nemzeti Média- és Hírközlési Hatóság: a hatóság által működtetett Bűvösvölgy Médiaértés-oktató Központ feladata, hogy bemutassa a gyermekeknek, hogyan használhatják tudatosabban és a kockázatokat elkerülve a médiát[10]. A szintén a hatóság égisze alatt működő Internet Hotline szolgáltatás[11] pedig az interneten található jogellenes, illetve a kiskorúak számára káros tartalmak bejelentésére biztosít lehetőséget[12].

7 *Ezzel kapcsolatosan részletesebben lásd a Digitális Gyermekvédelmi Stratégia 30–37. oldalait.*
8 *Internetes elérhetőség: www.police.hu.*
9 *Internetes elérhetőség: www.naih.hu.*
10 *Internetes elérhetőség: www.nmhh.hu.*
11 *Erről lásd még a következő pont alatt írtakat.*
12 *Internetes elérhetőség: www.buvosvolgy.hu.*

- Nemzeti Média- és Hírközlési Hatóság Médiatanácsa: hatósági felügyeletet gyakorol a médiaszabályozás gyermekek és kiskorúak védelmére vonatkozó előírásainak érvényesülése tekintetében, emellett kezdeményező szerepet vállal a médiaműveltség, a médiatudatosság magyarországi fejlesztésében[13].
- Gyermekvédelmi Internet-kerekasztal: a kerekasztal az NMHH elnökének huszonegy tagú, javaslattevő, véleményező, tanácsadó testülete a médiatartalom-szolgáltatók, az elektronikus kereskedelmi szolgáltatók és az elektronikus hírközlési szolgáltatók jogkövető magatartását elősegítő ajánlások, állásfoglalások kiadására jogosult, feladata továbbá a kiskorúak és szüleik médiatudatosságát növelő intézkedések kezdeményezése. A testület a hozzá beérkezett bejelentések alapján jogosult egyedi ügyeket is megvizsgálni, és azok általánosított tapasztalatai alapján ajánlást vagy állásfoglalást kiadni[14].
- Alapvető Jogok Biztosának Hivatala: a hatóságok tevékenysége során felmerült, az alapvető jogokkal kapcsolatos visszásságok megszüntetése érdekében hivatalból eljárást folytathat, amely természetes személyek pontosan meg nem határozható, nagyobb csoportját érintő visszásság kivizsgálására vagy egy alapvető jog érvényesülésének átfogó vizsgálatára irányulhat[15].
- Oktatási Jogok Biztosának Hivatala: a biztos a gyermeket, a tanulót, a hallgatót, a kutatót, a pedagógust, az oktatót, a szülőt, valamint azok közösségeit megillető, oktatással kapcsolatos állampolgári jogok érvényesülésének elősegítésében működik közre. Eljárásának tárgya lehet olyan egyedi ügyben hozott határozat vagy intézkedés, valamint határozat (intézkedés) elmulasztása, amely bizonyos, a gyermek, a tanuló, a szülő, a pedagógus, a hallgató, a kutató, illetve az oktató számára biztosított jogokat sért vagy a sérelem közvetlen lehetőségét idézi elő[16].

Az állami szervek mellett kiemelkedő jelentőséggel bírnak a kifejezetten a gyermekvédelem terén tevékenykedő társadalmi szervezetek, amelyek speciálisan gyermekek és az internethasználattal összefüggő releváns kérdésekkel foglalkoznak. E szervezetek elsősorban az oktatás, azon belül is a megelőzés, a segítségnyújtás vagy az áldozatkezelés problematikájával foglalkoznak. Az említett szervezetek körében megemlíthető példaként a Nemzetközi Gyermekmentő Szolgálat, a Kék Vonal Gyermekkrízis Alapítvány, az Eszter Alapítvány, a Hintalovon Alapítvány, a Nagycsaládosok Országos Egyesülete, a Médiaunió Alapítvány, a Gyermekmédia Egyesület, a Médiasmart Közhasznú Nonprofit Kft., az Egyszervolt Alapítvány, az Országos Gyermekvédő Liga vagy az UNICEF Magyar Bizottság Alapítvány.

13 Internetes elérhetőség: www.mediatanacs.hu.
14 Internetes elérhetőség: http://nmhh.hu/cikk/187273/Gyermekvedelmi_Internetkerekasztal
15 Internetes elérhetőség: www.ajbh.hu.
16 Internetes elérhetőség: www.oktbiztos.hu.

Hotline-ok

A Hotline-ok olyan bejelentési pontokként működnek, melyek különféle kategóriákban mind jogellenes, mind pedig a kiskorúakra nézve káros tartalmak bejelentését teszik lehetővé. Az ilyen Hotline-ok működésének jellemzője, hogy a valóban sérelmes tartalmak esetén felhívják az érintett szolgáltatót a panasszal érintett tartalom eltávolítására, elősegítve az önkéntes jogkövetés megvalósulását. Hangsúlyozandó, hogy a Hotline-ok tényleges hatósági jogkör hiányában nem tudják kötelezni a szolgáltatókat az egyes tartalmak tényleges eltávolítására, így együttműködés hiányában a sokszor hosszadalmasabb hatósági és bírósági eljárások kezdeményezése válik szükségessé.

HOTLINE-OK AZ INTERNETEN

Hazánkban két jelentősebbnek mondható Hotline működik, a 2011 óta az NMHH által üzemeltetett Internet Hotline,[17] és az NISZ Nemzeti Infokommunikációs Szolgáltató által üzemeltetett Biztonságosinternet Hotline[18]. Az oldalakon keresztül számos kategóriában lehet jogsértő(nek vélt) tartalmakat bejelenteni úgy, mint például: pedofil tartalom; rasszista, idegengyűlöletre uszító tartalom; erőszakot megjelenítő tartalom; drogfogyasztásra csábító tartalom; zaklatás, megfélemlítés; hozzájárulás nélkül közzétett sértő tartalom. A tapasztalatok alapján elmondható, hogy a hazai tartalom- és tárhelyszolgáltatók jellemzően együttműködnek, és a jogsértő tartalmat hozzáférhetetlenné teszik, illetve a kiskorúakra káros tartalmak esetén elhelyezik a szükséges korhatárfigyelmeztetést.

2017 nyarán nyitotta meg „kapuit" az Igazságügyi Minisztérium alá tartozó Áldozatsegítő Központ[19], mely 24 órás ügyelettel információadási, áldozatirányítási, kapcsolat-felvételi, érzelmi segítségnyújtási helyszínként működik, valamint előzetesen (telefonon, e-mail-on) egyeztetett időpontban fogadja a felnőtteket, fiatalokat és gyermekeket egyaránt, érzelmi segítségnyújtás és tájékoztatás céljából.

Pedagógusoknak a tudatos felhasználóvá válás oktatásához a magyar nyelven is elérhető Web We Want – Internet, ahogy mi szeretnénk[20] című kiadvány nyújt segítséget, melynek tanári és tanulói kézikönyve felhasználható tanórák keretében is. A tanulói kézikönyvet fiatalok dolgozták ki kortársaik számára, a tanári kézikönyv óraterveit pedig Európában és azon kívül dolgozó tanárok dolgozták ki tanárok számára. Hivatalos képviselet: www.saferinternet.hu, www.biztonsagosinternet.hu.

A jogtudatosság növelése

Igen hatékony „eszköz" lehet a bekövetkezett sérelmek orvoslása terén a jogtudatosság növelése. Az ennek birtokában lévő gyermek képes felismerni azokat a cselekedeteket, amelyek jogellenesek, és ebből adódóan elkövetésük akár (súlyos) jogi következményekkel is járhat.

17 Internetes elérhetőség: www.internethotline.hu.
18 Internetes elérhetőség: www.biztonsagosinternet.hu.
19 Internetes elérhetőség: http://aldozatsegitokozpont.im.gov.hu/
20 Internetes elérhetőség: http://www.webwewant.eu/hu/web/guest/inicio

A jogsérelem felismerése és megfelelő kezelése esetén ugyanis a kiskorú tisztában van azzal, hogy jogellenes cselekmény áldozatává vált (vagy ennek közvetlen lehetősége fennáll). Ezen túl a jogtudatosságnak köszönhetően ismeri a rendelkezésre álló jogorvoslati fórumokat, és tekintettel arra, hogy bizalommal van az ismert intézmények iránt, megteszi a szükséges lépéseket a sérelem orvoslására.

A jogtudatosság – ahogyan általában véve az internethasználathoz kapcsolódó ismeretek – hiányának egyik legjelentősebb negatív hozadéka a látencia, azaz hogy a káros magatartások, illetve a kockázatos online tartalmak az ellenük fellépni képes személyek, szervezetek előtt rejtve maradnak. A legmegfelelőbb intézkedések, védekezési mechanizmusok sem érnek semmit, amennyiben azok a szükséges helyzetben – legfőképpen az ismeretek hiányára visszavezethetően – nem kerülnek alkalmazásra.

eBIZTONSÁG MINŐSÍTÉS KÖZNEVELÉSI INTÉZMÉNYEKNEK[21]

A mai fiatalok közösségi oldalakhoz csatlakoznak, közösségeket alakítanak ki és online tartalmakat hoznak létre és osztanak meg. Az iskolák feladatai közé tartozik, hogy a tanítási és tanulási folyamat részeként biztonságos környezetet és hozzáférést teremtsenek. Lehetőség van csatlakozni az eBiztonság közösséghez, ahol többet megtudhat a témáról, valamint megoszthatja tapasztalatait, ezáltal segítve más pedagógusokat is. A felhasználók, szakértők ötleteket, dokumentumokat és tapasztalatokat cserélnek az eBiztonság témakörében, segítenek egymásnak és jó gyakorlatokat osztanak meg egymással.

Az eBiztonság Minősítést a European Schoolnet hozta létre. Célja, hogy biztonságosabb, inspirálóbb környezetet nyújtson a tanárok és a diákok számára.

Az iskolák nemzetközileg elismert szabványokkal való összehasonlítás alapján felmérhetik saját eBiztonsági gyakorlataik szintjét. Az iskola eredményei alapján egy akcióterv kerül kidolgozásra az eBiztonság magasabb szinjtének elérése érdekében, aminek a következő lépése az eBiztonság Minősítés Akkreditáció, miután a szükséges változtatásokat megtették.

A portál az iskolákat folyamatosan bővülő forráslistával látja el: eBiztonsági tanácsadás és segítségnyújtás, adatlapok, követelmények listája és minták.

Forrás: https://www.facebook.com/ebiztonsag

Összegzés

A gyermekek számára kockázatot jelentő online tartalmak és egyéb magatartások igen széles skálán mozognak, ahogyan az ezek elkerülését szolgáló eszközök, technikai megoldások, illetve e célból működő intézmények. A valóban hatékony védelem, illetve a bekövetkezett sérelem esetén történő gyors és eredményes sérelemkezelés kizárólag széles körű ismeretek birtokában lévő gyermekekkel valósulhat meg. Éppen ezért igen fontos annak felismerése, hogy az internethasználattal összefüggésben alkalmazott védelem nem a korlátozás eszköze kíván lenni, hanem éppen ellenkezőleg, a gyermekek biztonságban tudását kívánja elősegíteni.

21 https://www.facebook.com/ebiztonsag

A DIGITÁLIS GYERMEKVÉDELMI STRATÉGIA CÉLJAI ÉS ESZKÖZEI

A Digitális Gyermekvédelmi Stratégia (DGYS) központi célkitűzése, hogy a gyermekek biztonságosan és értékteremtő módon használják az internetet.

A fiatalok intenzív médiafogyasztási szokásait figyelembe véve, az online térben rájuk leselkedő kockázatok kezelésének érdekében hangsúlyossá vált a médiatudatosság fejlesztése. Az ehhez szükséges ismeretek és képességek elsajátításához az alábbi területeken határozott meg feladatokat a stratégia: a tudatos internethasználat támogatása, az online tér veszélyeivel szembeni védelem erősítése és a sérelmek káros következményeinek enyhítése, valamint a megfelelő jogkövetkezmények alkalmazása.

Ahhoz, hogy ez a célkitűzés eredményesen megvalósuljon, a megvalósításba minden érintettet, azaz a szülőket, a civil szervezeteket és az oktatási intézményeket is be kell vonni. A tudástranszferben fontos feladat jut a kortársaknak.

A megfelelő szintű tudás megszerzése mellett cél a kellő hatékonyságú védelmi mechanizmusok felállítása és működtetése, illetve a sérelmek megfelelő kezelése.

A gyermekek médiaműveltségének fejlesztése az aktuális állapot felmérésére támaszkodva tervezhető, és a továbbiakban is rendszeres elemzéseket igényel. Vizsgálat tárgyát képezi a gyermekek médiaműveltségének értékelése, a pedagógiai módszertani megoldások, a gyermekek digitális vásárlási szokásainak kiértékelése, mert csak erre építve válhat hatékonnyá a stratégia megvalósítása.

Gyermekek médiaműveltségének fejlesztése érdekében tervezik médiahetek beépítését a Digitális Témahét programkínálatába, illetve tehetséggondozást a médiaműveltség terén.

A fentiek értelmében szükségessé vált a médiát oktató tanárok képzésének és továbbképzésének átalakítása, mely a biztonságos és etikus internethasználattal, az online megfélemlítéssel, bántalmazás kockázatainak megismerésével, megelőzésével és kezelésével ismerteti meg a pedagógusokat. A stratégia lehetővé kívánja tenni a médiaműveltség-képzésben való részvételt a szülők számára is. Speciális képzést igényel az igazságszolgáltatás, illetve a gyermekvédelem területén dolgozók képzése is.

Valamennyi érintett szereplő számára lehetővé kell tenni a hasznos információkhoz való egyszerű hozzáférést egy gyűjtőhonlap kialakításával. A nyilvánosság számára elérhető tájékoztató anyagok hitelesítését szakértői testület végzi majd.

A biztonságos internethasználat elősegítését szűrőszoftverek fejlesztésével, biztonságos internetszolgáltatással, hatékony műszaki megoldások alkalmazásával, a szolgáltatók nagyobb társadalmi szerepvállalásával, gyermekeknek készülő tartalmak gyártásának támogatásával kívánják szorgalmazni.

Ezt a célt szolgálja a kiskorúak számára ajánlott (white list) és káros (black list) tartalmakat hordozó internetes oldalak listájának összeállítása, folyamatos aktualizálása és az ezekhez kapcsolódó újabb szűrőszoftverek fejlesztése.

A stratégia a megoldások alkalmazási körének kiterjesztésénél olyan külföldi bevált védelmi intézkedéseket is számba vesz, mint például a hálózati szintű tartalomszűrési funkciók elvárását a szolgáltatóktól, illetve olyan műszaki megoldások (PIN-kód, személyazonosság igazolásának előírása) elterjesztésének kötelezővé tétele vagy a szolgáltatók ösztönzése a tudatos internetezéssel kapcsolatos társadalmi szerepvállalás hatékonyabb felvállalására.

Az online veszélyek megelőzésében és a problémák kezelésében a büntetőjogi eszközök alkalmazása helyett a nevelést, az iskolai szintű szankciókat javasolja a stratégia elsődleges megoldási formaként alkalmazni, a pedagógusok megfelelő felkészítésével.

A stratégia a gyermekek kellő szintű biztonságának és védelmének megteremtése körében nem kizárólag tiltásokkal, korlátozásokkal kíván megfelelő terepet biztosítani az online térben, hanem ösztönözni kívánja a kifejezetten a fiatalok számára készült, a média tudatos használatára (információbiztonság, adatkezelés, adatbiztonság, felelős, etikus médiahasználat) vonatkozó médiatartalmak gyártását.

Miután sok esetben elkerülhetetlen a káros esetek bekövetkezte, ezért a károk enyhítésére is figyelmet kell szentelni a sérelemkezelés módjának megfelelő megválasztásával. A vitarendezés alternatív formájaként, a jogi eljárások mellett, a nevelési, oktatási intézményekben működő egyeztetési eljárások lefolytatására is mód van. A stratégia szükségesnek tartja az ilyen típusú mechanizmusok alkalmazási körének kibővítését.

A fiatalkorúak által elkövetett bullying típusú jogsértések esetén a stratégia a Büntető törvénykönyv által lehetővé tett jóvátételi eljárás mellett a megelőzésben résztvevő szereplőknek (például iskolának) biztosítani kívánja a büntetőjogon kívüli mediáció igénybevételét is. A pedagógusonak megfelelő felvilágosítást kell kapniuk az alternatív konfliktuskezelési eljárások (pl. resztoratív sérelemkezelés) igénybevételéről, a szolgáltatást nyújtó civil szervezetekről és szakemberekről.

A stratégia az online zaklatás eseteit a büntetőjogon kívüli területen, az igazgatási és az oktatási jog területén is szabályozni kívánja.

A tapasztalatok szerint a sérelmet elszenvedettek jellemzően nincsenek tisztában a jogszabályok által biztosított efféle eljárási lehetőségekkel, és ebből adódóan igénybevételükre is csak elvétve kerül sor. A stratégia megfogalmazott célkitűzései között éppen ezért elsődleges fontosságúnak tekinti ezen eljárási formák ismertségének növelését a tudatos médiahasználat oktatásának keretei között, illetve tájékoztató kampányok keretében.

A stratégia, mint a fentiek alapján látható, a gyermekek mellett jóval szélesebb személyi kört szólít meg, és alapvető fontosságú szerepet szán a médiaműveltség, médiatudatosság fejlesztésének. Az online tér biztonságos és felelősségteljes használata, illetve a rendelkezésre álló források kihasználása érdekében az elsődleges hangsúlyt nem a terület (további) szabályozásában, hanem alapvetően a „felhasználók" képességeinek fejlesztésében látja.

Kedves Mentor!

Végül engedj meg a kézikönyv használatával kapcsolatban néhány technikai megjegyzést.

A kézikönyv anyagát 2017. október 13-án zártuk le, így elképzelhető, hogy azóta megváltozott egy-egy jogszabály, gazdasági adat vagy internetes elérhetőség.

Kérjük, a füzetek nyomtatása során gondolj környezetünkre, és amennyiben lehet, takarékoskodj a papírral. Ha nem a teljes füzetet szeretnéd kinyomtatni, hanem csak egy-egy oldalt vagy fejezetet, akkor a PDF olvasó „Nyomtatás" menüpontjában állítsd be a kívánt oldalak oldalszámát.

Ha DJP mentori munkád során bármilyen nehézségbe ütközöl, vagy olyan megoldásra találsz, amelynek más kollégák is hasznát vehetnék, kérjük, fordulj hozzánk bizalommal az alábbi elérhetőségeken:

Digitális Jólét Koordinációs Központ Ügyfélszolgálat:

telefonszám: +36 70 6695648
e-mail cím: ugyfelszolgalat.djkk@neum.hu
facebook: https://www.facebook.com/groups/1908308209418637/

GINOP 3.3.1–16 azonosítószámú projekt „Digitális Jólét Program Pontok fejlesztése" című pályázat ügyfélszolgálat:

e-mail cím: ugyfelszolgalat.ginop331@kifu.gov.hu
weboldal: www.kifu.gov.hu

IMPRESSZUM
Szerkesztette: Szenes Gábor
Kézirat lezárva: 2017. október 13.
Kiadó: Kormányzati Informatikai Fejlesztési Ügynökség

Kapcsolat: info@kifu.gov.hu