Adatvédelmi kézikönyv pedagógusoknak

2015

Készült az ARCADES projekt tagjainak közreműködésével

A kiadvány létrehozásában közreműködtek:

Árvay Viktor

Kozma Laura

Márkus Petra

Nagy Kata

Szántó Zsófia

Sziklay Júlia

Tordai Zsófia

Szerkesztette:

Tordai Zsófia

ISBN 978-963-12-3670-5

Tartalom

1. Fejezet: Bevezetés a magánélet védelmébe

Tartalom:

Mi is az a privát szféra? A virtuális és valós magánéletünk védelme.

Célok:

- a magánszférával összefüggésben más emberek viselkedésére és eltérő élethelyzetekre tudatosan reagáló magatartásforma kialakítása;
- a magánélet védelméhez való jogra vonatkozó kifejezések magyarázata;
- annak hangsúlyozása, hogy miért fontos ez mind a valós, mind a virtuális világban.

Alapvetés:

Egy ember életében a gyermekkor különleges időszak. Ekkor ismerkedünk meg a világgal és önmagunkkal, majd kezdünk kialakítani egyéb emberi kapcsolatokat is, melyek alapja a barátság és a bizalom. Ezért biztosítani kell, hogy a fiatal "emberpalánta" harmónikus, szeretetteljes és biztonságos légkörben nevelkedjen és tanuljon meg tisztelni másokat is. Minden gyermeknek, függetlenül attól, hogy a világ mely részén él, joga van az élethez, a fejlődéshez és ahhoz, hogy szabadságban, valamint az emberi méltóságot, a magánéletet és a személyes adatok védelmét tisztelő környezetben nőjön fel.

A könyv szerzői fontosnak tartják felhívni a figyelmet arra, hogy a mai világunkban milyen érték a magánélet és a személyes adatok védelme. A gyermekeknek és fiataloknak meg kellene tanulniuk úgy használni a modern technológia vívmányait, hogy közben nem feledkeznek el a biztonságról és a veszélyek elkerüléséről virtuális terepen sem.

A civilizációnk kivételes ütemű fejlődése, a modern technológia és az információáramlás különféle módozatai állandóan új minőségű és léptékű kihívásokat hoznak magukkal. Különösen igaz ez a gyermekek és fiatalok esetében, hiszen az internethez már bárki hozzáférhet, ugyanakkor a másik oldalon az emberi méltóság és a belőle származtatható jogok – így a magánélet védelméhez és az adatvédelemhez való jogok – egy demokratikus államban az egész jogrendszer alapját kell, hogy képezzzék.

A magánélet tág fogalom, az egyedülléttől kezdve az intimitásig, vagy az önálló döntések kialakításáig sok minden belefér. A külvilág oldaláról pedig háborítatlanságot szeretnénk elérni, vagyis, hogy mások – értve ezalatt szülőket, barátokat, tanárokat, vagy akár tágabb környezetünket, az államot is – ne zavarjanak.

A *pszichológusok* is ismerik ezt a lelki szükségletet és védendő értékként kezelik. Olyan tényezőként, melynek biztosítása azért fontos egy ember számára, mert csak így érezheti magát biztonságban, nyugalomban. A pszichológia megkülönböztet *zárt privát szférát* – intimszférát –, ahol a saját testi, szexuális vagy érzékeny érzelmi viszonyaink védelmében fontos a titkosság, titkolózás, mások távoltartása, valamint *nyitott privát szférát*, ahol az egyénhez tartozó területre a mások által történő behatolás csakis az érintett engedélyével, hozzájárulásával történhet (például nyilvánosan hangoztatott nézetek, személyhez köthető termékek esetében – lásd szabadalmak, szerzői jogi termékek).

A témával foglalkozó *szociológusok* az egyén eltérő társadalmi szerepeihez kapcsolva különválasztják az emberi élet köz- és magánterét.

Végül a jog is felismerte a magánéletet, mint védendő jogi tárgyat és 1888-ban Thomas M. Cooley amerikai legfelsőbb bírósági bíró a **"háborítatlansághoz való jogként"** definiálta is azt.

Az európai alkotmányos rendelkezések értelmében mindenkinek joga van ahhoz, hogy személyes adatai fölött rendelkezzen, titkait, szokásait, magatartását és személyes kapcsolatait titokban tartsa. A védelem főleg – de nem kizárólag – rajtunk múlik.

Szükségünk van egy védett magántérre, ugyanakkor számos helyzet arra sarkall, hogy önként hozzunk nyilvánosságra információkat magunkról és másokról. Sokszor egyszerűen nem vagyunk urai a helyzetnek, **a modern technológiai fejlődés komolyan veszélyezteti magánszféránkat.** A kultúránkat ért változások, a technikai fejlődés és a globalizáció miatt a hatások és kihívások állandóan változnak. Az egyén társadalmi helyzetére, feladataira, jogaira és kötelezettségeire vonatkozó nézetek azonban Európa-szerte egy tőről fakadnak, ez az oka annak, hogy a magánéletet fenyegető veszélyekre adandó jogi válaszok – különösen az Európai Unión belül – is hasonlóak.

Fogalmak: magánélet, magánélethez való jog

Alkotmányos alapjogról van szó. Eredetileg amerikai jogtudósok – V. Brandeis és E. Warren – a 19. században a tömegmédia gátlástalansága elé próbáltak falat húzni a "háborítatlansághoz", titokban tartáshoz, exkluzivitáshoz való jog megfogalmazásával. A jogfejlődés során számos új értelmezés is teret kapott, így az intimitás mellett megjelent a családi élet, az emberi kapcsolatok, más személyiségi jogok védelmének igénye is, valamint a másik oldalon az állam védelmi kötelezettsége.

Megtörtént esetek, példák:

Vitassák meg és elemezzék a magánéletet érintő egyes emberi magatartásokat (pl. kíváncsiskodás, pletyka stb.), ezek következményeit és hatásait.

- *Kati informatika órán ellátogatott egy közösségi oldalra, és a szünet alatt úgy ment ki az osztályteremből, hogy nem jelentkezett ki a honlapról. Az osztálytársai úgy gondolták, itt a jó alkalom egy kis viccelődésre: álinformációkat küldtek ki a nevében. A lány eleinte csak mosolygott a társai által írt megjegyzéseken, de később mások is elkezdték az álhírt kommentelni és Kati családjáról egy olyan valótlan történet bontakozott ki, ami már komolyan kellemetlen volt számára.*

- *A jómódú Kovácsék házában betörők jártak. A rendőrség a nyomozás során minden fontos körülményt megvizsgált. A család gyermeke egy rendkívül nyitott és dicsekvő fiú, aki az interneten számos alkalommal hencegett már – fotókkal illusztrálva – azzal, hogy milyen drága ajándékokat, márkás ruhákat, elektronikai felszereléseket kap szüleitől. Ezek a netre feltöltött információk jó tippek voltak a betörőknek.*

- *A diákok épp tornaórára öltöztek át, amikor Mónika a mobiljával csinált egy fényképet barátnőjéről, és gondolkodás nélkül felrakta a netre. Nem akart ártani neki, jó viccnek gondolta a dolgot. Pár perc múlva meggondolta magát és leszedte, de ekkor már késő volt: a vetkőző lány képe kommentekkel együtt gyorsan terjedt és egy kinyomtatott változatot valaki még az iskola folyosóján is elhelyezett. Nagy botrány kerekedett, Mónika barátnője sokat sírt a kép miatt. Talán mégsem volt jó vicc a fotózkodás?*

- *Egy iskolai fogalmazásnál a következő témát kellett feldolgozni: "Ki vagyok én és mit tartok fontosnak?" Anna osztálytársai – távollétében – átkutatták a táskáját, kivették a füzetét és mikor Anna visszatért az osztályterembe, épp nagy hangon röhögtek azokon a mondatokon, amelyekben Anna próbálta identitását és a számára fontos értékeket megfogalmazni. Anna zokogva menekült ki a teremből.*

- *Simon mobilját a nappaliban felejtette és anyja épp arra járt, mikor sms érkezett. Nem bírt kíváncsiságának ellenállni és beleolvasott az üzenetekbe. Nagyon meglepődött, mert Simon nem mesélte el otthon, hogy barátnője van és szerelmes.*

Beszélgessenek róla!

- Volt már bárkinek olyan személyes élménye, mikor a magánéletükbe tört be valaki? Milyen körülmények között került sor erre? Milyen érzésekre emlékeznek vissza?
- Tisztában vagyunk azzal, hogy a többiek mit gondolnak rólunk? Milyen információkat osztunk meg magunkról online, és mások mit tudnak meg ebből?
- Előfordult már, hogy beleegyezésünk nélkül feltettek egy képet, vagy írtak rólunk a neten? Tisztában vagyunk azzal, hogy ez nem jogszerű?
- Van-e joga a tanárnak vagy szülőnek ahhoz, hogy beleolvasson a gyerek levelezésébe, vagy abba a szövegbe, amit feltölt magáról?
- Használunk adatvédelmi beállításokat?
- Hogy lehet a valós (offline) és az online világban megvédeni a magánszféránkat? Melyik egyszerűbb?
- Hogy tudjuk elkerülni az online érkező zaklató kérdéseket?
- Vajon ma a netre feltett információ befolyásolhatja-e a későbbi életünk bármilyen módon (például jövőbeli párkapcsolatot, vagy karriert)?

Javasolt helyzetgyakorlatok:

1. Az osztály bejön a terembe és a gyerekeknek egymást, valamint a tanárt/ igazgatót/vendéget üdvözölniük kell. Más-más köszönési módot fognak alkalmazni ("Helló!' "Cső!" "Jóreggelt kívánok!" "Csókolom!", valamint puszi, kézfogás, hátbaveregetés, átölelés stb.) attól függően, hogy milyen viszonyban vannak az adott személlyel és az mennyiben várja el/fogadja szívesen például a testi érintkezést.

2. Tegyék fel a kérdést, hogy a hozzánk közel álló személyekhez miért és hogyan viszonyulunk fizikailag is? Milyen érzéseket váltana ki belőlünk, ha olyan valaki jönne túl közel hozzánk, akit nem kedvelünk, aki idegen, vagy egyszerűen nem számolunk azzal, hogy megérinthet minket? Hangsúlyozzuk, hogy mindenkinek

szüksége van egy védett térre maga köré, ami biztonságot jelent számára, és aminek az illetéktelen személy által történő megsértése viszolygást és egyéb kellemetlen reakciókat vált ki az emberből.

3. Írjuk fel a táblára a "magánélet" szót és kérjünk szabad asszociációt a gyerekektől.

4. Egy diák írja fel egy papírra, hogy milyen információkat tud osztálytársáról, majd hasonlítsa össze azokkal az adatokkal, amiket a neten lehet róla összegyűjteni. Végül kérdezzék meg az osztályt, hogy ki tud még egyéb fontos dolgot az adott személyről mondani. A begyűjtött adatokból alkossanak közösen egy szemlyiségprofilt (kategóriák: kinézet, azonosító adatok, hobbik, személyiségjegyek, barátok stb.) és jelöljék meg, hogy melyik adat milyen forrásból származik. Vitassák meg, hogy mi okozott meglepetést, az érintett személy tudott-e a neten fellelhető összes információról, esetleg volt-e a nyilvános forrásokban olyan, amit jobb (okosabb) lett volna bizalmasan kezelni. Hangsúlyozzuk, hogy jogunk van a személyes adataink sorsa fölött rendelkezni és nem szabad az érintett tudta és beleegyezése nélkül róla adatokat nyilvánosságra hozni (például fényképét bárhová feltölteni).

Figyelem! Csak önként jelentkező diákról lehet kutatni, ennek hiányában a feladatot mindenkinek anonim módon, egy névvel meg nem jelölt ismerősével kapcsolatban szabad csak elvégezni!

5. Kérdezzük meg és írjuk fel kulcsszavakban a táblára azokat az eseteket, melyek a magánéletünk sérelmével járnak (testi érintés, hozzánk tartozó tárgyak átkutatása, rólunk szóló információk nyilvánosságra hozatala, telefonbeszélgetés lehallgatása, leveleinkbe való beleolvasás stb.) Hangsúlyozzuk, hogy ezek mind sértik a privátszférát!

   Csoportokban a gyerekek dolgozzák ki, hogy mi a védelem lényege és a jog milyen lehetőségeket biztosít számukra. Hogyan kerülnek a róluk szóló információk a netre és milyen fajta adatoknál kellene ezt mindenképpen elkerülni/megakadályozni?

Hangsúlyozzuk, hogy a nyilvánosságra került személyes adatokhoz idegenek is hozzáférhetnek és a rosszindulatú felhasználásnak nincs időbeli korlátja. Jogunk van ahhoz, hogy bizonyos dolgokat titokban tartsunk, és ezzel a joggal élni is kell!

6. Nem szabad elfelejteni, hogy a jogot – jogszerűen – korlátozni is lehet, ennek azonban vannak formai és tartalmi követelményei. A szülő, tanár, iskola, orvos vagy akár az állam néha akaratunk ellenére is gyűjthet vagy felhasználhat személyes adatokat például fertőző betegségek elkerülése, gyógyítása, bűncselekmények megakadályozása vagy a szülői kötelezettségek teljesítése érdekében. Gyűjtsenek a gyerekek és vitassanak meg olyan példákat, mikor a korlátozás szerintük is indokolt.

7. Alkossanak a gyerekek vizuális alkotásokat (például poszter, karikatúra stb.) a témáról, melyeket be lehet később mutatni.

2. Fejezet: Bevezetés a személyes adatok védelmébe

Tartalom:

Az adatvédelmi jogok és kötelezettségek összessége.

Célok:

- ismeretterjesztés az adatvédelemről;
- a személyes adat személyes jellegének hangsúlyozása;
- jogtudatosítás az érintetti jogokkal és az adatkezelői kötelezettségekkel összefüggésben.

Hasznos definíciók:

Néhány alapfogalmat tisztázni kell (például személyes adat, adatalany, adatvédelem). A jog az adatalanyokat jogokkal ruházza fel, az adatokat felhasználókat ugyanakkor kötelezettségekkel terheli.

Az érintettek/adatalanyok jogai: az információs önrendelkezési jog magában foglalja

- a meghatározott célból történő tisztességes adatkezelés követelményét;
- az adatkezeléshez való hozzájárulás szükségességét;
- a hozzáférés lehetőségét (például másolathoz);
- a pontatlan, helytelen adat kijavításához való jogot;
- a törléshez való jogot;
- jogsértés esetén a panasz lehetőségét (például az adatvédelmi hatóságnál).

Az adatkezelők kötelezettségeinek alapja: az adatkezelésre vonatkozó szabályok tiszteletben tartása. Így

- az adatok megszerzése és feldolgozása tisztességes módon kell, hogy történjen;
- az adatokat tárolni és felhasználni csak meghatározott cél(ok) érdekében lehet;
- az adatok legyenek pontosak, teljesek és naprakészek;
- az adatokat biztonságosan és csak addig tárolják, amíg ez szükséges;
- a személyes adatok legyenek megfelelőek, relevánsak és nem túlzottak;
- kérés esetén főszabályként az adatalany kaphasson saját adatairól másolatot.

Személyes adat: az érintettre vonatkozó minden információ, különösen neve és személyazonosító száma vagy bármilyen más fizikai, lelki, szellemi, gazdasági, kulturális vagy társadalmi jellemzője, illetve egyéb olyan következtetés, amiből a személyt azonosítani lehet.

Érintett/adatalany: bárki élő személy, akit közvetlenül vagy közvetve a rá jellemző személyes adat segítségével azonosítani lehet.

Adatvédelem: a magánélet védelméből levezetett emberi jog, mely azonban bizonyos esetekben más jogok – például a véleménynyilvánításhoz való jog – érdekében korlátozható (vagyis nem abszolút).

Magánélet védelme: egy demokratikus társadalomban alapvető jog.

Adatkezelés: személyes adaton végrehajtott bármely művelet, különösen az adatok felvétele, gyűjtése, osztályozása, raktározása, módosítása, felhasználása, nyilvánosságra hozatala, törlése, ideiglenes blokkolása, megsemmisítése, jövőbeli felhasználás megakadályozása. Ide tartozik többek között a fényképezés, audió vagy vizuális felvétel készítése, testi jellemzők rögzítése (például ujjlenyomat vagy tenyérnyomat, illetve DNS mintavétel, írisz szkennelés stb.).

Adatkezelő: az a személy vagy szervezet, aki vagy ami meghatározza az adatkezelés célját és dönt a személyes adatok felhasználásáról.

Adatfeldolgozó: az a személy, vagy szervezet, aki vagy ami az adatkezelő utasításának megfelelően és érdekében az adatokat technikai értelemben feldolgozza.

Megtörtént esetek, példák:

A) Jogok

1. Jog a felejtéshez (NAIH-Google eset)

A panaszos egyetemista azért fordult az adatvédelmi hatósághoz, mert felfedezte, hogy ha a nevét beírja a Google keresőbe, akkor számos olyan képet kap találatként, mely az arcát náci szimbólumokkal együtt ábrázolja. Ezeket a képeket az egyetem film-történeti óráján alkották, és mivel a képekkel való összekapcsolás számára egyértelműen kellemetlen következményekkel járt (például álláskeresésnél), először megkereste a Google-t, hogy a program a képekkel összefüggésben "felejtse el a nevét". Elutasították, majd a NAIH felszólítására a Google a képek és a név közötti összekapcsolást végül megszüntette.

2. Tájékoztatáshoz való jog (CCTV – zárt kameraláncú rendszer)

Mikor egy iskolában kamera rendszert szerelnek fel, a diákokat minden lényeges körülményről – az adatkezelő neve és címe, jogalap, mennyi ideig tárolják a felvételeket, az adatalanyoknak milyen jogaik vannak és hová fordulhatnak – előzetesen tájékoztatni kell. Fontos, hogy a kamerák működéséről piktogramos táblákat is ki kell helyezni.

3. Az adatok hordozhatósága (az e-mail címek átvitelének kérdése)

Mikor valaki elektronikus levelezőrendszert cserél, fontos számára, hogy az e-mailjeinek adatait és dokumentumait (például címlista, mellékletek stb.) könnyen átvihesse az új szolgáltatóhoz.

B) Kötelezettségek

1. Adatvédelmi beállítások

Az adatvédelmi beállításokról való gondoskodás elsődleges adatkezelői kötelezettség. Online szolgáltatások esetében (például Facebook) alapvető jogunk, hogy meghatározzuk az adatvédelmi beállításokat, vagyis hogy adatainkhoz ki és hogyan férhet hozzá. Ezek közül a legfontosabbak, hogy ki léphet kapcsolatba velünk, más felhasználók mit láthatnak

a tevékenységünkből, személyes profiloldalunkra ki rakhat ki megjegyzést (kommentet). Gyakorlati tény, hogy egy nem nyilvános profilnál idegenek kellemetlenkedéseitől kevésbé kell tartani.

2. Adatbiztonság (Hotel Wi-Fi csalások esete)

Mikor rácsatlakozunk egy nyilvános Wi-Fi hálózatra (például egy étteremben), mindig ellenőrizzük, hogy valódi és biztonságos oldalakat nyitunk-e meg (a legtöbb böngésző program figyelmeztet a veszélyre, a megbízható URL címek – vagyis webhely címek – zölden jelennek meg).

Beszélgessenek róla!

- Érte már valakinek sérelem a személyes adatait? Ha igen, hogyan?
- A Facebookra milyen személyes adatokat teszünk fel? Milyen jogsértés történhet itt? Mit tehetünk ilyen esetben?
- Vajon az iskolai dolgozat személyes adat?
- Ha diákok az órán egymással levelezneknek, az személyes adat? A tanár elveheti a teleírt cetlit? Beleolvashat?
- Milyen személyes adatok vannak a neten? A Google keresőbe írják be a tanulók a saját nevüket és közösen nézzék át a találatokat!
- Valaki látott már online szolgáltatáshoz kapcsolódó adatvédelmi szabályzatot? Esetleg el is olvasta, mielőtt megadta volna személyes adatait?
- Fájl-megosztó rendszerek, levelezőprogramok vagy más, előzetes regisztrációt megkövetelő online szolgáltatások igénybevételekor használjuk az adatvédelmi beállításokat?
- Fel tudunk sorolni a felhasználói fiókot védő adatbiztonságot szolgáló megoldásokat (például megfelelő – számot, nagybetűt is tartalmazó – jelszavak, weboldalról történő kijelentkezés, weboldal biztonsági ellenőrzése, profil nyilvánosságának korlátozása stb.)?

Javasolt helyzetgyakorlatok:

1. Ellenőrizd a Facebook-os adatvédelmi beállításaid!

2. Tegyük fel, hogy a közösségi oldalakon a profilod teljesen nyilvános – milyen kockázatokat fedezel fel?

3. Alkoss profilt egy híres emberről!

4. Mindig olvasd el az adatvédelmi nyilatkozatokat, mielőtt megadsz személyes adatot!

5. Írj adatvédelmi naplót: mi történt a neten található személyes adataimmal az elmúlt héten/két hétben/hónapban? Milyen és mennyi információt osztottam meg magamról? Az adott időszakban mit írt/írhatott más (ismerős vagy ismeretlen) rólam? Megadtam valahol a nevemet, e-mail vagy lakcímemet? Bejelentkeztem internetes oldalakra? Le/feltöltöttem fájlokat a számítógépemre? Használtam applikációkat a mobilomon?

6. Nézzenek együtt figyelemfelhívó videókat (magyar és angol nyelven):

- Vastag Tamás: Egy biztos hely: http://www.youtube.com/watch?v=gc8s581LJws
  és
  http://naih.hu/files/NAIH---TCR-video.mp4
- https://www.youtube.com/watch?v=9dRK8T-ny94

7. Kiscsoportos munka: a gyerekek kisebb testvérüknek 5 percben hogyan magyaráznák el az adatvédelem lényegét és fontosságát?

8. Olvassanak át együtt egy adatvédelmi szabályzatot és emeljék ki az egyes pontok következményeit.

Fontos tudni!

1. Ha egy szolgáltató személyes adatot kér tőlünk, akkor nekünk is jogunk van a tájékoztatáshoz, az adatok kijavításához vagy akár törléséhez.
2. Mikor az adatkezelés nem kötelező, a hozzájárulás szabadon megtagadható.
3. A kellemetlen vagy kínos adatok törlését kérhetjük a tartalomszolgáltatótól.

Ajánlott információforrás:

- Az adatvédelmi hatóság honlapja (www.naih.hu).

3. Fejezet: A magánélet védelmének és a személyes adatok védelmének jelentősége

Tartalom:

Miért fontosak ezek a témák? Miért kapnak alapjogi védelmet? A megfigyelés miért lehet probléma?

Cél:

A különféle élethelyzetek tudatos felismerésére és megfelelő válaszadásra nevelés. A téma fontosságára és a kiszolgáltatottság veszélyeire történő figyelemfelhívás.

Alapvetés:

Az adatvédelem a magánélethez való jog része, mely alapvető emberi jog. Nem csak egy elvont fogalom, de a mindennapok része az orvosi rendelőben, a boltban, játék vagy facebookozás közben személyes információkat is közlünk. Minél inkább kapcsolatba szeretnénk kerülni másokkal, annál több személyes adatot adunk ki magunkról. Akár részletesek, akár általánosak, jogi értelemben ezek az adatok személyesnek minősülnek, hiszen személyünkkel közvetlenül vagy közvetetten kapcsolatba hozhatók, így ez alapján az adatalanyt már megilleti a jogi védelem. Az internet egyik fő vonzereje a rajta keresztül fellelhető személyes információk mennyisége, melyre a jognak is válaszokat kell találnia.

A személyes adatoknak gazdasági értékük is van, erre a cégek és a marketing-reklámszakemberek már régen rájöttek, ezért kapunk annyi kéretlen és aggresszív elektronikus reklámot, hirdetést spamek vagy célzott megkeresések formájában.

Technikailag nagyon sok megoldás létezik már a felhasználók nyomon követésére, elég, ha valaki internetezik, e-fizetési eszközöket használ, vagy egyébként egy elektronikus rendszer hatókörébe kerül (például köztéri kamerák felveszik, turistaként kedvezményes city kártyát vásárol, vagy hitelkártyájára terhelés érkezik). Minden egyes használat egy elektronikus nyomot hagy hátra, amin könnyű azonosítani és lekövetni az adott személy szokásait vagy mozgását.

Az új technológiák robbanásszerű fejlődésének korában a magánélet és az adatvédelem nagyon kiszolgáltatott és sérülékeny. Ezért különösen fontos a fiatalok körében a tudatosítás és tájékoztatás, hiszen ők az állandó netezés során különösen hajlamosak – akár értelmetlen módon is – személyes információkat idegenek számára elérhetővé tenni, nyilvánosságra hozni. Természetes és nincs abban semmi rossz, ha boldog pillanatainkat fényképeken, vagy más módon ismerőseinkkel meg akarjuk osztani, de tisztában kell lennünk ennek következményeivel és vigyázni kell arra, hogy ezzel senkit ne bántsunk meg. Megalázó fényképeket például, ami most vagy a jövőben kínosan érinthet valakit, nem szabad feltölteni!

A gyerekeknek és fiataloknak eszükbe kell vésni, hogy ha egyszer az interneten nyilvánosságra hoznak egy információt, azt már bárki láthatja és az örökre ott is marad. A személyes adatok védelme online térben nem egy egyszerű feladat, sokkal hatékonyabb a bajt okosan megelőzni és a kockázatokat tudatosan elkerülni.

A kockázatok közé tartozik, hogy a nyilvánosságra hozott információval könnyen vissza lehet élni. Egy fényképet gyerekjáték megváltoztatni, manipulálni, más környezetbe helyezni. Mémezéssel például nevetségessé lehet tenni bárkit, de súlyos esetben egy ellopott kép személyiséglopás, vagy pedofília eszközévé is válhat.

Vajon a gyerekek vagy akár szüleik gondolnak ezekre a kockázatokra, amikor büszkén feltöltenek a netre egy fotót?

A gyerekekkel beszélgetni kell arról, hogy igazán szükséges-e és ha igen, vajon milyen mértékben magukról, családjukról vagy ismerőseikről információkat nyilvánosságra hozni. Az adatvédelem legfontosabb szabálya, hogy az érintett önkéntes hozzájárulása szükséges az adatkezeléshez – vagyis a fényképeken szereplő személyeket meg kell kérdezni, hogy nem zavarja-e őket, ha kikerülnek a netre. A fényképek ráadásul sokszor többletinformációt is hordoznak, anyagi helyzetre, családi kapcsolatokra, sebezhetőségre utalhatnak.

A magánszférához való jogot kölcsönösen tisztelni kell, csak így támaszthatunk mi is elvárásokat és, ha valaki azt kéri tőlünk, hogy a számára kínos módon nyilvánosságra került személyes adatait (fénykép, komment stb.) töröljük, tegyük ezt meg azonnal.

A magánszférához való jogot a nyilvánosság mellett a megfigyelés is veszélyezteti. A bűncselekmények számának növekedésére a kamerák köztéri vagy iskolákban történő felszerelése jó válasznak tűnt a nagyvárosokban. Adatvédelmi szempontból a személyekről, vagy egy személyhez köthető tárgyról (például gépjármű) készített felvételek ugyanúgy személyes adatok, mint a leírt információk. Ezért a kamerázás – különösen a gyermekekről, fiatalokról készített felvételek – adatkezelésének jogi hátterére, a megfelelő jogi szabályozásra különös figyelmet kell fordítani.

Hasznos alapfogalmak:

- magánélethez való jog
- személyes adatok védelméhez való jog

Megtörtént esetek, példák:

- *Viki a barátaival közös nyaralásról készített fényképeket feltöltötte a közösségi oldalára. Előtte azonban meg kellett volna kérdeznie őket, hogy nincs-e kifogásuk ez ellen!*

- *Matyi bulizós korszakát éli, egy átmulatott éjszaka után iskola helyett a haverokkal inkább a közeli tópartot választotta és erről a Facebookon be is számolt. Anyjának délután elárulta, hogy lógott a suliból és szüleitől kierőltette az igazolást, melyben "betegségre" hivatkoztak. Osztályfőnöke később számonkérte a szülőkön, hogy miért falaztak a gyereknek, hiszen a tanárok is látták a beszámolót a kellemes tóparti délelőttről. Borzasztó kellemetlen helyzet volt ez mindenkinek.*

- *Kati, Marci barátnője. Egy hétvégén Kati családjával elutazott, de "kárpótlásul" küldött magáról egy friss képet, amiben csak melltartót visel. Marci büszkén elküldte a képet barátjának, aki fel is tette azt a közösségi oldalra. 250 megjegyzés*

érkezett a képhez, köztük sok (alpári stílusban) a lány melleinek nagyságát, formáját kritizálta. Kati szégyenében napokig nem mert iskolába menni, és azóta sem beszél a fiúval.

Beszélgessenek róla!

- Miért fontos számunkra a magánélet és az adatvédelem?
- Tudjuk, hogy milyen típusú személyes adatokat hozunk nyilvánosságra online?
- Tisztában vagyunk a kockázatokkal és azzal, hogyan védekezhetünk ezek ellen?

Javasolt helyzetgyakorlatok:

1. Hangsúlyozni kell, hogy az internet a modern világban az önkép kiteljesítésének fontos eszköze. A közösségi hálózatok segítségével korlátlanul bemutathatjuk eredményeinket, új kapcsolatokat építhetünk ki és kreatívak lehetünk. A rólunk mások előtt kialakult képet befolyásolja on-line tevékenységünk is: ha dokumentumokat nyilvánosságra hozunk, webes fórumokon témához hozzászólunk, kommentelünk vagy egyszerűen bizonyos oldalakra ellátogatunk. Tegyük fel a kérdést: mennyire fontos ez számunkra?

2. Csoport feladatként kérjük meg a gyermekeket, elemezzék ki, vajon az általuk hagyott "digitális lábnyomot" megismerve, másokban milyen benyomás alakulhat ki róluk? Vitassák meg azt is, hogy vajon az ismerősökkel való kapcsolattartáshoz valóban szükséges-e ilyen mennyiségű és minőségű személyes információ megosztása?

3. A következő feladat során nyomtassunk ki privát képeket az internetről (például nyaralásról vagy barátokkal készített közös fotókat). A csoportok egy-egy fotó és a hozzá tartozó szöveg (cím, comment) információtartalmát elemezzék ki. Ezután minden csoport válasszon ki egy közösségi oldalt (Twitter, Facebook stb.) és a saját tapasztalataik, valamint az elolvasott adatvédelmi szabályok alapján vizsgálják meg, hogy az adott közösségi oldalon:
   - jellemzően milyen személyes adatok szerepelnek;
   - milyen formátumban (képi, szöveges, videó stb.);
   - milyen adatvédelmi kockázatokkal lehet az adott helyen számolni (pl. adatvesztés, visszaélések stb.);
   - milyen rokonszenves vagy jó megoldásokkal lehet találkozni?

4. Végül hangsúlyozzuk, hogy a legfontosabb a saját felelősség, nem másoktól vagy egy technikától kell védelmet várni, hanem tudatosan, saját döntéseink alapján kell biztonságosan internetezni.

4. Fejezet: Ki és honnan szerezheti meg személyes adatainkat?

Tartalom:

Ki akarja megszerezni a személyes adatainkat? A személyes adat fogalma. Mi a különbség a személyes adat és a különleges adat között és miért kell másképpen védeni őket? Ki gyűjti a személyes adatokat és mi az adatkezelés, adatgyűjtés célja? Ki tudhat arról, hogy mit csinálunk az interneten?

Cél:

Fel kell hívni a gyermekek figyelmét a személyes adat fogalmára, a személyes adatok védelmének fontosságára, és arra, hogy miért élvez néhány adatfajta speciális védelmet!

Alapvetés:

A modern technikák fejlődésével párhuzamosan egyre nagyobb szerepet kap az internet és egyre több időt szentelünk online életünknek. Egy honlapra történő belépés már gyűjthető információ, így előfordulhat, hogy úgy tudnak meg mások rólunk valamit, hogy nem is osztunk meg személyes adatokat. Az információ forrása lehet maga az adatalany, lehet egy harmadik fél, bizonyos adatokat pedig automatikusan gyűjtenek be.

Nem szabad elfelejtenünk, hogy az internet számos lehetőséget biztosít a magánélet és a személyes adatok elleni visszaélésekhez (például adatok kiszivárogtatása, erőszak, rágalmazás, csalás, személyiséglopás, spam-küldés, káros tartalmak terjesztése, hamis információk közlése).

Alapvető fontosságú, hogy a szülők és a pedagógusok kiemelt figyelmet fordítsanak a gyermekek biztonságára, hiszen a felnőtteknek a társas érintkezésről több tudásuk és tapasztalatuk van. Az önmérséklet, a tudatosság és a józanész a legfontosabb tényező ebben a küzdelemben, azonban épp ezek a tulajdonságok azok, amelyekkel a fiatal felhasználók nem (feltétlenül) rendelkeznek.

Az interneten szinte mindent megosztunk magunkról: a fotóktól és linkektől kezdve a legbelsőbb személyes információkig, hol és mit csinálunk éppen, mik a terveink, gondolataink a jövőre nézve. Ennek alapján bárki megismerhet minket, az életünket, a szenvedélyeinket és a kapcsolatainkat. A különféle nyilvántartásokban megbújó információmorzsákat csak hozzá kell kapcsolni egy adott személyhez, és máris személyes adat keletkezik.

A személyes adat speciális kategóriája a különleges adatok köre. Különleges adat „a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat”[1]. A különleges adatok a törvény értelmében csak akkor kezelhetőek, ha:

[1] Infotv. 3 § 3 a)

- az adatalany írásos hozzájárulását adta, vagy
- törvény a kötelező adatkezelést előírta (nagyon nyomós közérdekből például járványok megakadályozása vagy terrorfenyegetés elhárítása miatt).

Azt is észben kell tartanunk, hogy a személyes adat nagyon értékes árucikké válhat, amit rossz szándékú emberek nem csak legális, elfogadható módon próbálnak megszerezni, hanem akár bűncselekmény útján is. Néhány módszer egészen egyszerű (például az információt beolvassák dokumentumokból vagy kidobott elektromos eszközökből, kicsalják magától az érdeklődőktől), mások azonban kifinomultabb IT technikákat alkalmaznak (feltárt adatok után keresnek az interneten, vagy számítógépeket törnek fel).

Felhasználói fiókok létrehozása, regisztráció különböző honlapokon, online levelezőrendszerek, közösségi hálózatok, online játékportálok, e-mail cím létrehozása – ezek azok a szituációk, amelyekben leggyakrabban kiadjuk az adatainkat. Mindig érdemes átgondolni, hogy valóban használni akarjuk-e az adott szolgáltatást és tisztességes üzlet-e cserébe az adatainkat megosztani egy ilyen széles felületen? Tényleg szükséges megadni az adatainkat, vagy önkéntesen vagyunk túlbuzgók? Mikor nem várható el tőlünk az adatok kiszolgáltatása és mikor minősíthető ez egyenesen veszélyesnek?

Beszélgessenek róla!

- Tudod, mik azok a személyes adatok? Melyik személyes adat igényel speciális védelmet?
- Miért kell védenünk az adatainkat és a rólunk szóló információkat?
- Figyelned kell arra, hogy ki gyűjt rólad információkat és mire használja fel ezeket?
- Be lehet-e azonosítani valakit látszólag irreleváns adatok alapján (pl.: van egy pöttyös, sárga ruhája)? Mondjanak példákat arra, hogy adott osztályban kiről mi lehet releváns információ.
- Milyen információkat nem szabad megosztani az interneten?

Javasolt helyzetgyakorlat:

A gyerekek csoportmunkában írják le a gondolataikat a következő kérdésekről:

- Egy személy mely adata, milyen szituációban adható meg eltérő életszakaszokban:

- születéstől általános iskoláig
- gimnáziumtól egyetemig
- egyetemi tanulmányok során
- munkába állástól nyugdíjig
- nyugdíjazás után

- Bizonyos online szolgáltatások rendszeres használatakor milyen adatokat kell és/vagy szokás megadni?

- online játékba történő bejelentkezés
- közösségi hálózatokra történő regisztráció
- kérdőívek kitöltése
- kapcsolattartás a barátokkal

5. Fejezet: Hogyan maradhatnak a titkaink biztonságban?

Cél:

A gyermekeket nem csupán arra kell megtanítani, hogyan és miért kell bizonyos információkat privát módon kezelni, de azt is lényeges elsajátítaniuk, hogyan akadályozhatják meg személyes adataik nemkívánatos közzétételét, megosztását és mit kell tenni akkor, ha ez mégis bekövetkezik.

Alapvetés:

Hogyan lehet az okos eszközöket valóban okosan használni és adatalanyként milyen jogaink, adatkezelőként pedig – például egy közösségi oldalon – milyen kötelezettségeink vannak?

Lehetséges veszélyek:

- *Személyiséglopás*: különböző technikák (például adathalászat, hacking, adatbányászat, pszichológiai manipuláció) által az elkövetők elegendő személyes adathoz juthatnak ahhoz, hogy ellopják egy gyermek személyazonosságát és további visszaéléseket kövessenek el.

- *Zsarolás*: valaki kínos vagy esetleg nyíltan szexuális tartalmú fényképekkel zsarolhatja a gyermeket.

- *Online zaklatás*: ismerős vagy ismeretlen gyűjthet áldozatáról olyan adatokat, melyekkel később ő zaklatható.

Ha egy gyermek személyes adatai akarata ellenére vagy gondatlanság következtében kerülnek nyilvánosságra, az hatással lehet az emberi méltóságára, önbecsülésére és a magánéletére is. Az adatokkal való visszaélés anyagi (például hitelkártyával vagy hűségkártyával való csalásnál) és súlyos pszichológiai következményekkel is járhat (különösen az online és szexuális zaklatás esetében).

Védekezés a veszélyekkel szemben:

Az interneten való böngészés és az online kommunikálás során hajlamosak vagyunk a biztonság hamis illúziójába ringatni magunkat. Ugyanakkor tisztában kell lenni azzal, hogy a nem titkosított kommunikációs eszközök használata során gyakorlatilag bárki, nagyobb erőfeszítés nélkül bepillantást nyerhet bármilyen beszélgetésbe.

A digitális környezetben két fő megoldás van a hatékony adatvédelemre: egyrészt a technikai védekezés az adatbiztonság növelésével, másrészt a felhasználó tudatosságának növelése, vagyis hogy figyeljen arra, kivel milyen információt oszt meg és ne tegyen közzé érzékeny adatokat.

A védekező magatartás első számú szabály. Mivel az internet nem felejt, és ami egyszer felkerült, az örökre ott is marad, a gyermekeknek nem lenne szabad semmilyen olyan személyes adatot megosztaniuk, amelyet nem egy szélesebb közönségnek szánnak. A posztolt tartalmak felett később már nem lehet kontrollt gyakorolni, egy barátból válhat

ellenség, bárki bújhat egy „kreált” profil mögé azzal a céllal, hogy személyes adatokat szedjen ki a gyanútlan áldozatokból és bárki lophat adatokat a gyerekek számítógépéről, vagy egy cégtől, amely tárolja az adott információkat. Ezek a veszélyek nem csupán a közösségi oldalak használata folytán leselkednek ránk, hanem bármilyen online szolgáltatás kapcsán, legyen az akár e-mail, keresőoldal, szöveges és videó üzenetek, felhő alapú szolgáltatások, vagy privátnak hitt fényképalbumok.

Egy másik jó megoldás, ha rendszeresen ellenőrizzük a közösségi oldalakon, blogokon, fényképmegosztó portálokon a megadott biztonsági beállításainkat, mielőtt posztolunk valamit. Ez az egyik kulcsa a saját adataink felett gyakorolt hatalomnak: vagyis hogy tudjuk, kivel mit osztunk meg.

Azért, hogy a titkok valóban titkok maradjanak, a régebben közzétett információkról sem szabad megfeledkezni. Könnyű elveszteni a fonalat azzal kapcsolatban, hogy kivel, mikor, milyen személyes adatot osztottunk meg, azonban mindenkinek joga van hozzáférni a saját adataihoz, és akár követelni, hogy azokat javítsák, töröljék, vagy tiltsák le. Ezek a jogosultságok biztosítják az emberek számára a magánélethez való jog gyakorlását és személyes adataik védelmét.

Hangsúlyozandó: a személyes adatokat biztonságban kell tartani. Az adatkezelő és a felhasználó közös feladata, hogy ennek érdekében a szükséges intézkedéseket megtegyék. Már viszonylag korán el kell kezdeni a gyermekek tudatos számítógép-használatra való nevelését, hogy tudják, hogyan óvhatják meg eszközeiket a támadásoktól. Minden olyan digitális berendezést, amely csatlakozik az internethez, szükséges ellátni a megfelelő szoftver védelemmel (vírusirtók, anti-malware programok, tűzfal beállítások) és kellően erős jelszavakkal. A jelszó legyen összetett, egy jelszó csak egy eszközt védjen, és feleljen meg néhány alapvető és egyszerű kód-alapszabálynak (lásd Tippek bekezdés).

Végezetül fontos kiemelni: a gyerekeknek tudniuk kell, hogy ha bármiféle visszaélés történik a személyes adataikkal kapcsolatban, forduljanak egy felnőtthöz – szülőhöz, tanárhoz, vagy olyasvalakihez, akiben megbíznak –, aki ténylegesen segíthet a probléma orvoslásában.

Hasznos definíciók:

Adatbiztonság: technikai eszközök segítségével az adatok biztonságának és titkosságának biztosítása a felhasználó viselkedéséhez igazodva.

Személyiséglopás: más „személyiségének” eltulajdonítása oly módon, hogy az elkövető elegendő személyes információt gyűjt az áldozatról ahhoz, hogy el tudja hitetni magáról, hogy ő az adott személy. Miután feltételezik róla, hogy ő valóban az, akinek kiadja magát, a tolvaj még több adatot tudhat meg.

Online zaklatás: mikor valaki digitális eszközökön keresztül rendszeresen zaklat, gyötör, fenyeget vagy megaláz egy másik személyt.

Megtörtént eset, példa:

- *Két barátnő megosztotta egymással a hallgatói tanulmányi rendszerben használt jelszavát, egyrészt ezzel is kifejezve bizalmukat a másik felé, másrészt óvatosságból,*

hátha egyikük elfelejti a jelszavát. Anna nemtörődömségből ugyanazt a jelszót használja valamennyi közösségi oldalához, Marina pedig kíváncsiságból megnézi, a barátnőjétől kapott kulcs nyitja-e az összes többi használt oldal zárját. Sikerrel is jár, amikor azonban bejelentkezik Anna közösségi oldalára, véletlenül ráklikkel a „jegyezze meg a jelszót" opcióra. Marina testvére később ugyanazt a számítógépet használja, és rájön, hogy hozzáférése van Anna online profiljához. Úgy dönt, megtréfálja a lányt, és kiposztol egy képet a nevében egy fiatal tanárról, amelyen az éppen egy fiatal lánnyal csókolózik, a fotó alá a férfi telefonszámát is odaírja, követelve, hogy az „hagyjon fel a pedofil viselkedéssel".

Beszélgessenek róla!

- Hogyan éreznéd magad, ha egyik barátod megosztaná egy titkodat a többi osztálytársaddal, például, hogy kibe vagy szerelmes?
- Hogyan választasz jelszót az online szolgáltatásokhoz? Megosztod a jelszavadat a barátaiddal?
- Szoktál figyelni a biztonsági beállításokra a Facebookon, ask.fm-en, vagy más oldalon, illetve szoktad módosítani azokat?
- Mit tennél, ha tudnád, hogy egy barátod online zaklatás áldozatává vált? Kihez fordulnál segítségért?
- Mit gondolsz, biztonságban vannak az adataid azoknál a szervezeteknél, amelyekre rábíztad őket? Vajon lehetséges, hogy adataidat illetéktelenek szerzik meg, vagy megfelelő védelemben részesülnek?
- Milyen következményekkel járhat, ha ellopják a személyes adataid, vagy ha személyiséglopás áldozatává válsz?
- Másképpen viselkedsz az interneten egy felhasználói név álcája mögött? Miben mások a reakcióid és stílusod akkor, mint amikor a saját neved alatt nyilvánulsz meg?

Javasolt helyzetgyakorlat:

Próbáljanak ki közösen egy jelszóerősség-ellenőrző programot, hogy kiderüljön, mennyire biztonságos a jelszavuk.

Tanácsok a legkisebbeknek és idősebbeknek egyaránt:

Amit minden gyermeknek tudnia kell a témával kapcsolatban:

- Mindig gondold meg, mielőtt megosztasz magadról valamit másokkal! Kellően megbízható az a személy ahhoz, hogy titkaid biztonságban legyenek nála?
- Mindig használj vírusirtót a számítógépeden, tableteden és okostelefonodon is!
- Ne nyiss meg olyan e-mailt vagy csatolmányt, amelynek küldőjét nem ismered, vagy nem megbízható forrásból származnak!
- Sose válaszolj olyan emberek üzeneteire, akiket nem ismersz!
- Sose adj meg személyes információkat olyanoknak, akiket nem ismersz, legyen az akár az utcán, akár az interneten!
- Mielőtt megadnád a telefonszámod egy alkalmazás vagy játék használatához, mindig győződj meg arról, hogy az alkalmazás vagy játék nem fog pénzt levonni a számládról!

Amit minden kamasznak tudnia kell a témával kapcsolatban:

- Sose küldj magadról meztelen vagy kínos képeket! Nem tudhatod, mikor kerülnek nyilvánosságra.
- Okostelefonodat védd számkóddal!
- Ne oszd meg telefonszámodat az interneten vagy közösségi oldalakon!
- A közösségi oldalakon használj felhasználónevet!
- Használj jelszókezelő alkalmazást!
- Mielőtt új profilt hoznál létre egy közösségi oldalon, mindig nézd meg, milyen szabályok szerint kezeli a szolgáltató a privát adatokat! Olvasd el az oldal használatára vonatkozó feltételeket, illetve, hogy lehetséges-e az adataid törlése, ha úgy kívánod.
- Olvasd el az általános szerződési feltételeket, hogy kiderüljön, megoszthatja-e másokkal is adataidat a szolgáltató.
- Mielőtt letöltenél egy applikációt, mindig ellenőrizd, milyen adatokhoz fog hozzáférést kérni! Töröld azokat az alkalmazásokat, amelyeket már nem használsz!

Tippek a megbízható jelszóhoz:

- Személyes adatod, háziállatod vagy kedvenc együttesed neve nem alkalmas jelszónak, mert ezeket bárki, aki csak kicsit is jobban ismer, könnyen kitalálhatja.
- Ne őrizd a jelszavadat a számítógéped közelében!
- A jelszó legalább 8 karakter hosszú legyen, és tartalmazzon kis-és nagybetűket, illetve számokat is.
- Ne használj olyan karaktereket, amelyek egymás mellett találhatóak a billentyűzeten, vagy az ábécében (pl. qwertz, asdfg, abcde, 12345).
- Rendszeresen változtasd meg jelszavadat!
- Ne felejts el kijelentkezni, ha mások által is használt számítógépről interneteztél!
- Könnyen megjegyezheted a jelszavad, ha egy mondaton alapszik, például: Imádom Az Erős Jelszavakkal Védett Privát Szférámat (IAEJVPSZ). Ha még számokat is adsz hozzá, a jelszavad még biztosabb (IAEJVPSZ917).

6. Fejezet: Dönts okosan!

Cél:

E fejezet célja, hogy felhívja a figyelmet az adatkezeléshez való *hozzájárulás* fontosságára. Fontos, hogy átgondoljuk, személyes adataink kezelése vajon a mi érdekünkben történik-e és milyen következményei lehetnek a hozzájárulásnak, vagy a hozzájárulás megtagadásának.

Alapvetés:

1. A hozzájárulás fogalma

Főszabályként személyes adataink csak megalapozott, jogszerű okból kezelhetők. A jogszerűség alapesete az egyén hozzájárulása, amivel tulajdonképpen azt fejezi ki, hogy az adott körülmények között egyetért az adatai kezelésével. A hozzájárulás megadható szóban, írásban vagy egyéb más megfelelő módon (például ráutaló magatartással). A beleegyezés alapja az egyértelmű, önkéntes és tájékozott döntés, nem fogadható el a kényszer vagy megtévesztés. Fontos, hogy mások személyes adatait sem szabad a beleegyezésük nélkül közzétenni és, ha ez mégis megtörtént és az illető ezt kéri, gondoskodni kell a helyzet orvoslásáról (a kép levételéről, a komment törléséről stb.)

Érdemes odafigyelni arra, hogy számos közösségi oldalnál hiányos vagy hibás a biztonsági (alap)beállítás, a nyilvános részeket érdemes átállítani zártra/privátra. Az önként adott hozzájárulás ebben az esetben azt jelenti, hogy a gyermeknek vagy a szüleinek ellenőrizni kell az adatvédelmi beállításokat és ki kell választani a számukra legalkalmasabb eszközt.

2. A gyermekek és tinédzserek hozzájárulása

Számos ország joga meghatározza azt a minimum korhatárt, amikor a fiatalok már képesek önálló jognyilatkozatot tenni és már nem kell ehhez szülői hozzájárulást kérniük. Magyarországon néhány adatkezelő, például a közösségi oldalak, saját maguk állapítanak meg alsó korhatárt (Facebooknál ez 13 év!) ameddig szülői hozzájárulás szükséges. Más kérdés, hogy ez mennyire hatékony és ellenőrizhető.

A magyar jog előírja a 14 év alatti gyermek véleményének kikérését, de ekkor még a szülő dönt, 14-16 év között a szülővel közösen tett, 16 év felett pedig már önállóan a gyermek jognyilatkozata lesz érvényes az adatkezeléseknél.

Ha a gyermek még nem adhat önállóan érvényes jognyilatkozatot, akkor a szüleinek kell ezt megtenni helyette. A szülőknek a gyermek érdekét kell legfőképp figyelembe venniük, de a gyermekek véleményét is meg kell hallgatniuk. Úgy kell meghozniuk a döntést, hogy az összhangba kerüljön egyrészt a gyermek nézőpontjával, vágyaival, másrészt érettségével és korával.

A nyilatkozattételi képességgel rendelkező fiatalokat pedig arra kell ösztönözni, hogy körültekintően járjanak el, amikor hozzájárulnak személyes adataik kezeléséhez és átadják

az irányítást a személyes információik felett. Arra is gondolniuk kell, hogy elég információval rendelkezzenek egy megalapozott döntés meghozatalához, különösen ügyeljenek arra, hogy miért van szüksége az adatkezelőnek az ő adataira, mit fog vele csinálni és meddig tárolja majd őket. A fiataloknak nem szabad elfelejteniük: a beleegyezésnek önkéntesnek kell lennie.

3. A hozzájárulás visszavonható

Amikor hozzájárulásunkat adjuk személyes adataink védelméhez, tudnunk kell: a hozzájárulás bármikor visszavonható. Bármelyik fél adja meg a hozzájárulást (akár a szülő, akár a gyermek), joga van visszavonni azt. Az adatkezelőnek tiszteletben kell tartani a kérést és azonnal fel kell hagynia adatkezelési tevékenységével. Például, ha valaki közzétesz egy fotót a gyermek beleegyezésével egy közösségi oldalon, de a fiatal később meggondolja magát, a képet feltöltő személynek azonnal törölnie kell a képet.

Azt is fontos tudni, hogy ha a szülő egyezett bele az adatkezelésbe a gyermek nevében, a megfelelő kor elérése után a gyermek maga is visszavonhatja ezt a hozzájárulást.

4. Az adatvédelmi szabályzatok: miért fontos elolvasni őket és mit jelentenek?

Csaknem minden online szolgáltató ad egy tájékoztatást arról, hogy milyen feltételei vannak a szolgáltatásai igénybevételének. Az elnevezés változó: *„A szolgáltatás feltételei", „A használat feltételei", „Adatvédelmi nyilatkozat", „Privacy policy"*. Innen tájékozódhat a felhasználó az adatkezelés minden kérdéséről: milyen adatokat, ki kezel, milyen okból, mennyi ideig, mi történik az adatokkal a fiók törlése vagy deaktiválása után. Ezen információk ismerete, a feltételek elolvasása nélkül adott beleegyezés tulajdonképpen nem önkéntes illetve semmiképpen sem megalapozott. A következmény pedig a magánszféra önkéntes leszűkítése, megsemmisítése.

Hasznos fogalmak:

- **Opt-in:** tudatos és aktív hozzájárulás az adatkezeléshez (például egy mező „check-box" kipipálásával)
- **Opt-out:** csak a tiltást kell jelezni, a tiltás elmaradásával passzív „zöld jelzés" az adatkezelő részére

Megtörtént eset, példa:

- *A 12 éves Márk és testvére egyedül voltak otthon, mikor csörgött a telefon és Márknak egy kedves női hang gratulált a két napos családi belépő nyereményhez egy kalandparkba. Ehhez csak néhány adatot kellett megadni azért, hogy a hölgy elküldhesse a jegyeket: a telefonáló megkérdezte Márk szüleinek a nevét, telefonszámát és a lakcímüket. Ezután azt kérdezte, van-e a szülőknek hitelkártyájuk. Márk igennel válaszolt és elmondta: a számítógép mellett tartják, hogy online vásárlásnál használhassák. A hölgy megkérte Márkot, hogy végső lépésként olvassa fel a kártya számát és a hátoldalon lévő három jegyű kódot, hogy beazonosítsák: tényleg ők a nyertesek. Márk örömmel teljesítette a kérést.*

Beszélgessenek róla!

Tegyük fel, hogy valaki nem foglalkozik az adatvédelmi kockázatokkal és például a közösségi oldalon a beállításoknál az „ismerősök ismerősei” lehetőséget választja. Ha 100 barátja van és mindegyik barátnak 100 további ismerőse, akkor már 10.000 ember láthatja a személyes adatait!

Javasolt helyzetgyakorlatok:

1. Egy kiválasztott közösségi oldalon nézzük meg, hol lehet az adatkezelések tiltásáról dönteni.

2. Nézzük meg együtt, hogy mások (barátok, szülők, ismeretlenek) milyen személyes adatokat látnak a profilunkon.

3. Egy gyakorló feladat során játsszák el a gyerekek, hogy egészségügyi adatokat kivel és milyen szituációkban kell/lehet/tilos megosztani.

Ajánlott kiegészítő anyagok:

A legifjabbaknak az EU összes nyelvén elérhető egy mesesorozat a http://www.sheeplive.eu oldalon: http://uk.sheeplive.eu/fairytales/unknown-mobile-phone-subtitles.

7. Fejezet: Profilok

Cél:

A profilkészítés egyre jelentősebb a bankok, a biztosító társaságok, az online kereskedők és szolgáltatók gyakorlatában. Milyen szituációkban készülhetnek rólunk is profilok és hogyan lehet módosítani azt?

Alapvetés:

1. *Mi az a profilozás?*

A profilalkotás folyamata során információkat gyűjtenek egy személyről, kiértékelik azokat (többek között tényekből következtetéseket, feltételezéseket vonnak le), majd a hasonló karakterű, értékrendű, tevékenységű egyéneket kategóriákba, profilokba sorolják. A profil alapján személyre szabott tanácsadást és szolgáltatásokat is kínálnak (például gazdag embereknek luxuscikkeket), de a bűnözői profilkészítés bevett gyakorlat a kriminológiában is.

2. *Valaki felhasználja az adataimat profilozási célokra? Milyen adatok ezek?*

A profilalkotás gazdasági haszonszerzéssel jár, mert a személyre szabott szolgáltatást vagy terméket jobban el lehet adni. Rendkívül sokszínű adathalmaz kerül begyűjtésre: név, e-mail cím, vásárlási és internetezési szokások, látogatott oldalak neve, kifizetett számlák, egészségügyi információk.

Az online szolgáltatók (kereső motorok, közösségi oldalak, fórumok és online kereskedők) szinte mindig együtt dolgoznak profilozókkal. Ennek oka, hogy online környezetben rendkívül egyszerű az információgyűjtés, hiszen digitális lábnyomot hagyunk magunk után minden mozdulatunkkal. Így könnyű információkhoz jutni rólunk: mit csinálunk, kivel beszélgetünk, milyen termékeket vásárolunk vagy használunk, mit olvasunk az e-book olvasónkon, hol nyaralunk stb. A szolgáltatók ezután olyan reklámokat és tartalmakat tárnak elénk, amelyekről azt gondolják, érdekelhetnek minket. Még a termékek árait is megváltoztathatják, ha elemzésük szerint hajlandóak vagyunk akár többet is fizetni az adott termékért. Csak olyan tartalmak jelennek meg előttünk, amelyek mások szerint érdekelnek minket, vagyis azt látjuk, amit a profilozók látni engednek. Azt azonban nem veszik figyelembe, ha változik az ízlésünk vagy esetleg más is érdekelne minket.

3. *Melyek a profilozás veszélyei?*

Mindenek előtt az, hogy nincs arról tudomásunk, hogy profil készül rólunk, információkat gyűjtenek és kezelnek velük kapcsolatban és ezeket kategóriákba sorolják.

Problémát jelent, ha a kategorizálás rossz adatokon és hibás feltételezéseken alapul. A nem megfelelő szolgáltatásokat és elfogadhatatlan kölcsönajánlatokat azok kapják, akik negatív kategóriába kerültek és esélyük sincs rá, hogy az adatok kijavítását kérjék.

A profilozó technológiák az egyén viselkedésének és preferenciáinak kiterjedt feltérképezését teszik lehetővé. A profilok olyan személyes információkat is feltárhatnak, amelyekről talán még maga az alany sem tudott. Az emberek talán azért sem érzik közvetlenül az adatgyűjtés kellemetlen hatásait, mert nem látják az információk alapján megalkotott képet.

Ezért minden profilozó tevékenység az adatgyűjtéstől a kategorizálásáig az alany tudtával kell, hogy történjen!

4. Mit tehetek a profilozás ellen?

Senkiről nem készülhet profil, ha ő maga nem tud arról, hogy adatgyűjtés és adatfeldolgozás alanya lett. Csak akkor történhet meg az elemzés az engedélye nélkül, ha törvény erre lehetőséget biztosít.

Jogunk van információkat kapni arról, hogy milyen forrásból, ki, milyen adatokat gyűjt róla, azokat mire használja, és ha készültek profilok, milyen kategóriákat használtak!
Jogunk van ahhoz, hogy kérjük a jogellenesen gyűjtött adat törlését, illetve a hibás adat javítását!

Megtörtént esetek, példák:

- *Egy 16 éves hűségkártya-tulajdonos vásárlási adatait a kereskedő gondosan begyűjti, elemzi és rövid időn belül terhes anyukáknak szóló hirdetéseket kap. A család reklamál, ekkor kiderül, hogy a lány tényleg várandós, csak nem szólt róla, ugyanakkor már vásárolt néhány várandósoknak való terméket.*

- *Anna apukája rákos lett, a lány pedig rákeresett a betegségre az interneten, hogy megtudja: milyen az apa állapota, milyen veszélyek fenyegetik, és hogyan tud neki segíteni. Egy évvel később az apa szerencsésen meggyógyul, ennek ellenére Anna a betegséggel és egészséggel kapcsolatos ajánlásokat kapott minden alkalommal, amikor az interneten keresgél.*

  vagy

  Néhány hónappal később az édesapa elhunyt, de az online szolgáltatók még hosszú ideig emlékeztették Annát a történtekre, mivel folyamatosan kapta az egészség/betegség témájában az ajánlatokat.

Beszélgessenek róla!

- Hogyan érint, amikor a korábbi kereséseid alapján kapsz ajánlatokat? Örülsz neki, mert kényelmes vagy inkább kellemetlen?
- Ha személyre vagy névre szóló ajánlatokat kapsz, nincs az az érzésed, hogy az internet túl sokat tud rólad?
- Tudtad, hogy folyamatosan lábnyomokat hagyunk az interneten és ezeket a lábnyomokat sokan fel is térképezik?

- Kaptál már valaha tájékoztatást arról, hogy felhasználják az adataidat profilkészítéshez? Kaptál ezután olyan ajánlatokat, amelyek a te ízlésedet tükrözték?
- Ha egy szervezet hibás/helytelen adatokat tárolna rólad, felhívnád őket és kérnéd, hogy helyesbítsék azt?
- Próbáld meg elképzelni, milyen kínos lenne neked, ha valakinek rossz információi lennének rólad!

Javasolt helyzetgyakorlat:

Egy-két tanuló mondja el: milyen honlapokat szokott látogatni, milyen híreket olvas, milyen tartalmakat néz meg. A többiek képzeljék el, hogy online kereskedők és próbálják meg kitalálni a megadott információkból, hogy milyen termékek érdeklik őket. Helyesek voltak a következtetések?

Tippek:

Minden gyereknek tudnia kell, hogy az online szolgáltatóknak érdekükben áll információkat gyűjteni róluk, például: milyen klub kártyákkal rendelkeznek, milyen játékokat játszanak, milyen adatlapokat néznek meg a közösségi oldalakon, stb. Ezen információk alapján a szolgáltatók képesek megmondani, milyen információk és tartalmak érdekelhetik a felhasználót. Nagyon fontos kijavítani a hibásan begyűjtött információkat.

8. Fejezet: Digitális lábnyom

Cél:

Egy olyan tudatos viselkedés kialakítása, amellyel kevesebb információt osztunk meg magunkról az interneten. Figyelem: az interneten tulajdonképpen nem létezik anonimitás!

Alapvetés:

Az internet nem felejt. A kereső motorok szerepe. Az online jelenlét feltérképezése. A felejtés joga. Hogyan reagáljunk súlyos, vagy sürgős esetekben?

A digitális lábnyom a virtuális világban történő tevékenységünk nyoma, azt mutatja, hogy milyen honlapokat látogattunk meg, milyen elérési utakat használtunk, milyen oldalakat nyitottunk meg (különböző domain nevek alatt vagy anélkül), milyen szavakra kerestünk rá, milyen keresési eredményeink vannak és mit választunk ki ezen eredmények közül. Természetesen a digitális lábnyom magába foglalja a megadott adatainkat direkt és indirekt módon (pl. alkalmazások során) közzétett adatokat is.

Még ha mi nem is osztunk meg semmi személyeset magunkról, akkor is előfordulhat, hogy az információink más emberek vagy vállalatok számára elérhetőek lesznek. Személyes adatainkat sokan eltérő módokon gyűjtik: mobil hálózatok üzemeltetőitől, mobil telefonok és szoftverek létrehozóitól, internet-elérési pontok szolgáltatóitól, tanácsadó ügynökségektől.

Az internet az anonimitás hamis érzését kelti. A tájékozottság hiánya – nem tudjuk, hogy milyen adataink és hogyan gyűjthetők be online – ösztönzőleg hat ránk és önként osztunk meg személyes adatokat. Valójában minden egyes kapcsolódáskor néhány információ eltárolódik. Ezen adatok alapján bárki könnyen beazonosítható az interneten. Online anonimitás tulajdonképpen nem létezik, a neten hagyott információk különösen nehezen törölhetők, néha ez nem is lehetséges. Mivel egyre több időt töltünk online tevékenységgel, így a nagy netes adatbázis rólunk is folyamatosan növekszik.

Hasznos fogalmak:

Digitális lábnyom: egy adott személlyel kapcsolatos információk, amelyeket internetszolgáltatók szervereiről és honlapok tulajdonosaitól gyűjtöttek. Ezek lehetnek például: fotók, nevek, vásárlási információk, blog bejegyzések, vagy olyan adatok, amelyeket önkéntelenül adunk meg, például IP cím vagy az operációs rendszer adatai.

A felejtés joga: jogunk van ahhoz, hogy ne jelenjen meg az interneten olyan információ rólunk, amelyet nem akarunk – kivéve, ha ezt törvény írja elő (pl.: parlamenti képviselők vagyonnyilatkozat-közzétételi kötelezettsége).

Süti (cookie): egy kis információ, amelyet kinyitáskor a honlap küld és a felhasználó böngészője tárol. A sütik emlékeznek a böngészési beállításokra (pl.: bejelentkezések, választott nyelv) vagy további információkat küldenek az oldal szerverére (pl.: biztonsági

beállítások, kosár tartalma). Törvény arra kötelezi a honlapok tulajdonosait, hogy jól látható helyen informálják a látogatókat a sütik használatáról és arról, hogyan tudják kikapcsolni azokat.

Megtörtént esetek, példák:

- *Az EU Bírósága 2014-ben szigorú döntést hozott egy ügyben, melyet egy spanyol állampolgár és a spanyol adatvédelmi hatóság indított a Google ellen 2010-ben. A spanyol férfi sérelmezte, hogy a nevére irányuló keresést követően a találati listán egy 16 évvel korábbi újságcikk jelenik meg, mely arról szól, hogy köztartozás miatt elárverezték a házát. A férfi azzal érvelt, hogy már visszafizette a tartozást és kellemetlen számára az ügy. Az ítélet kimondta, hogy a Google adatkezelőnek minősül, és mint ilyen, felelős az emberek magánéletéért, vagyis a Google köteles a találatot törölni. A gyakorlatban a hasonló kérések kb. harmada teljesül csak.*

- *A NAIH-nál panasszal élt egy egyetemi hallgató, aki a Google-tól - élve a felejtéshez való joggal – azt kérte, hogy a Google keresője ne kapcsolja össze nevét az egyetemi filmtörténeti óra keretében készült felvételekkel, melyeken ő náci szimbólumokkal a háttérben szerepel. A Google-nak írt levelét első körben elutasították. A Hatóság felszólítására megszűnt a kifogásolt jogsérelem és a Google keresője már nem adja ki találatként nevét a képekhez.*

9. Fejezet: Veszélyek és kockázatok

Tartalom:

Mi rossz történhet, ha a gyerekek, kamaszok az interneten kommunikálnak? Szabaduljunk meg a spam-ektől! Ne ess áldozatául az adathalászoknak! Gyűlöletbeszéd. Online zaklatás. A sexting veszélyei. Mit tegyünk, ha megtörtént a baj?

Hasznos fogalmak:

Spam: kéretlen üzenetek (főleg reklámok, körlevelek), melyeket elektronikus üzenetküldő rendszereken keresztül továbbítanak.

Adathalászat (phising): a legtöbb cég rendelkezik már saját netes felülettel annak érdekében, hogy szolgáltatásaikat népszerűsítsék és még könnyebben elérhetővé váljanak az ügyfelek számára. A rosszindulatú információgyűjtés egyik módja az úgynevezett pszichológiai manipuláció (social engineering), amely az emberi hiszékenységet használja ki. A különböző szoftverek és hardware-ek által támasztott biztonsági korlátokat kikerülve hozzáférést nyernek az áldozat számítógépéhez és az azon tárolt adatokhoz. Az információs technológia, a biztonsági szabályozások elégtelensége, vagy a munkavállaló tudatlansága mind szerepet játszhatnak egy sikeres adathalász-támadás megvalósulásában. A mesterkedés célja legtöbbször az, hogy a támadó rejtett kémprogramokat vagy más ártó programokat telepítsen a számítógépre, vagy, hogy rábírja a felhasználót, hogy adja meg jelszavát illetve valamilyen bizalmas pénzügyi vagy személyes adatot.

Gyűlöletbeszéd: az Európa Tanács által megfogalmazott definíció szerint: *"minden olyan kifejezési forma, amely fajgyűlöletet, idegengyűlöletet, antiszemitizmust vagy intoleranción alapuló másfajta gyűlöletet – ideértve az agresszív nacionalizmusban és etnocentrizmusban kifejeződő intoleranciát, a kisebbségekkel, migránsokkal és bevándorlókkal szembeni hátrányos megkülönbözetést és ellenségességet – terjeszt, igazol, támogat vagy arra izgat".*

Internetes zaklatás (cyberbullying): elektronikus eszközök használatán keresztül, visszatérő (vagy állandó) zaklatásban megtestesülő ellenséges magatartás. Az online zaklatást mindig szándékosan, ismétlődően, az elektronikus eszközök agresszív módon történő használatával egyedül vagy csoportosan követik el egy meghatározott áldozat sérelmére, hogy így okozzanak neki erkölcsi sérülést, vagy hozzák kellemetlen helyzetbe.

Sexting: erotikus képek vagy videók küldése és/vagy fogadása elektronikus eszközök segítségével. A fiatal generációk körében széleskörűen elterjedt jelenség az utóbbi időben.

Megtörtént esetek, példák:

- ***Spam:*** *2011 januárjában az ombudsman gyermekjogi oldalára jelentkezett be az a panaszos, aki sérelmezte, hogy gyermekkorú felhasználóknak is továbbít az egyik levelezőrendszer (freemail) pénisznagyobbításra vonatkozó reklámot tartalmazó kéretlen elektronikus levelet. Szerinte nem fogadható el az a védekezés, hogy a felhasználók életkorát a regisztrálásukkor megadott adatok alapján kezelik, hiszen az ott megadott információk hitelességét nem ellenőrizték, sőt, jogi értelemben az ott megadottak nem is tekinthetők nyilatkozatnak. Ellenben bűncselekmény, a*

gyermekjogok tömeges megsértése, ha e reklámok szórása ilyen megbízhatatlan adatokon alapul. Hatásköri korlátai miatt az ombudsman vizsgálatot nem tudott indítani, de a panaszos levelét megküldte a Magyar Tartalomipari Szövetségnek (MATISZ) és a Magyar Reklámszövetségnek is. A MATISZ elnöke válaszában vázolta, hogy 2002-2003 között az USA-ban és Európában is életbe léptek a spam kezelésére hivatott törvényi szabályozások, ennek ellenére mára a globális e-mail forgalom 90-95%-át a spam-ek teszik ki, vagyis a probléma hatékony megoldása továbbra is várat magára. A felhasználói érdektelenség és tudatlanság is közrejátszik, hiszen a spam-ek terjesztéséért felelős hálózatok jelentős része fertőzött személyi számítógépekből áll. A MATISZ tudomása szerint az USA-ban a spam terjesztéséért elsődlegesen felelős ún. botnet-ek felderítését és lekapcsolását, üzemeltetőik és a fertőző botnet-komponensek fejlesztőinek elfogását és elítélését tartják a leghatékonyabb megoldásnak.

- ***Adathalászat (phising):** 2009 januárjában Bryan Rutbergtől adathalászok csalták ki Facebook jelszavát. Rutberg azt gyanítja, a probléma okozója egy olyan e-mail volt, amely arra kérte, kattintson egy linkre, mely a Facebook fiókjához fogja irányítani. A linkre kattintva egy olyan hamis oldalra került, amely megszólalásig hasonlított a valódi Facebook nyitóoldalra, így gyanútlanul begépelte felhasználónevét és jelszavát. A támadó aztán átvette a hatalmat Rutberg fiókja felett, és üzeneteket küldött barátainak azzal, hogy kirabolták, és küldjenek neki pénzt egy internetes banki szolgáltatón keresztül. Egyik ismerőse át is utalt egy összeget, ezáltal egy adathalász támadásának közvetett, egy csalásnak pedig közvetlen áldozatává vált. Ilyen csalások például a „Nigériai" vagy a „419", melyek mind megbízható embereket céloznak meg.*

- ***Internetes zaklatás (cyberbullying):** Az internetes zaklatás jelenségére egy 2006-ban öngyilkosságot elkövető amerikai kislány esete hívta fel a figyelmet. A tragédia azért történt, mert a vád szerint egy anya a lányával együtt segített a 13 éves áldozat megvezetésében egy online közösségi portálon, amikor rendszeres e-mail váltások során elhitették vele, hogy egy 16 éves fiúval flörtöl. A két tinédzser később vitába keveredett, a 13 éves lány pedig végső elkeseredésében felakasztotta magát. A közvélemény felháborodását az váltotta ki, hogy az ügyészség eleinte egyszerűen nem tudott vádat emelni a gyanúsított anya ellen, mert nem találtak olyan vádpontot, ami az online zaklatást kimerítette volna. Végül a nőt összeesküvés és számítógépes rendszerek jogtalan használata miatt állították bíróság elé. Mivel az egész ügy a MySpace oldalain játszódott le, felvetődött a közösségi portál felelőssége is. Az eset után Matt Blunt, Missouri állam kormányzója aláírta az internetes zaklatás büntetéséről szóló törvényt, amely hivatalosan 2008. augusztus 28-án lépett hatályba, és amely kimondja, hogy az online sértegetőkre vagy molesztálókra akár 500 dolláros pénzbüntetést és 90 napig terjedő elzárást is ki lehet szabni. Sajnos a cyberbullying halálos áldozatainak száma napról-napra nő, és a médiában megjelenő hírek alapján jellemzően 13-15 év körüli kislányokat hajszolnak öngyilkosságba a gonosz és jellemzően anonim megjegyzések.*

- ***Sexting:** A fiatalok szexualitással összefüggésben is felhasználják az IT eszközöket kapcsolattartásra, érdeklődésük bővítésére. Azonban bűncselekményt követ el, ha valaki az igényét úgy igyekszik kielégíteni, hogy 18 év alatti személyekről készített képeket tölt le korra, nemre és érdeklődésre való tekintet nélkül. Előfordulnak azonban olyan esetek is, amikor a párok (a felnőttekhez hasonlóan) felvételt*

készítenek az intim együttlétről, amely szintén bűncselekmény, még akkor is, ha önmagukról, egymás beleegyezésével készítik el. Megtörtént, hogy egy 16 éves lány a párjának szándékozott kedveskedni, vágyát fokozni, ezért a laptopjába épített webkamera segítségével az MSN-en a fiú részére „műsort" adott, amelyen önmagát elégítette ki meztelenül. Ezzel bűncselekményt követett el. A lány esetében a készítéssel és közzététellel 2-8 évig terjedő, a fiú esetében 3 évig terjedő szabadságvesztéssel büntethető bűncselekményről van szó. Természetesen az ilyen esetek egyedi mérlegelést igényelnek. Teljesen más megítélés alá esik, amikor bulikon és/vagy buliból készülnek felvétel(ek) és azok kerülnek továbbításra, megosztásra. Jelenleg a jogi szabályozás nem kielégítő. Ami viszont ennél is súlyosabb, hogy a fiatalok sem képesek ezeket megfelelően kezelni, hiszen egyrészt buli, másrészt „ciki" ha nem vesz részt benne, harmadrészt bizonyos felvételek igen komoly pénzkereseti lehetőséget jelentenek.

Beszélgessenek róla!

1. Spam

- Gyakran kapsz e-mailben kéretlen reklámokat?
- Meg szoktál nyitni olyan üzeneteket, amelyek küldőjét nem ismered?
- Tudod, hogyan lehet szűrni a spam-eket?
- Került már valamelyikőtök kellemetlen szituációba spam üzenetek miatt? Ha igen, mit tett?

Tipp:

- Minden nem kívánt üzenetet törölj, legyen az akár álláslehetőség, szerencsejáték hirdetés, utazási vagy termékajánlat!
- A mellékleteket ne nyisd meg!
- Megfelelően állítsd be a levelezőrendszer szűrőprogramját!
- Használj olyan naprakész vírusirtó programot, amely rendelkezik spam-szűrő funkcióval is!
- A tartalma vagy mennyisége miatt zavaró eseteket jelenteni kell a hatáskörrel rendelkező hatóságnak!

2. Adathalászat (phising)

- Gyakran csatlakozol nyilvános Wi-Fi hálózathoz?
- Tudod, milyen veszélyeket rejthet magában a nyilvános Wi-Fi használata?
- Szoktál internetbank szolgáltatást használni, vagy online áruházakban vásárolni?
- Odafigyelsz, hogy kijelentkezz a már nem használt oldalakról?
- Megnézed, hogy az éppen látogatott oldal ellenőrzött-e?

Tipp:

- Soha ne adj meg személyes adatokat e-mailen vagy weboldalakon keresztül, ha nem vagy biztos abban, ki vagy miért kéri őket!
- Soha ne telepíts nem megbízható forrásból származó alkalmazásokat vagy szoftvereket!

- Mindig legyen naprakész vírusirtó telepítve a számítógépre, illetve ajánlatos a tűzfalat is használni annak érdekében, hogy ne települhessenek ártó programok a gépre!
- Mielőtt megadnád a személyes adataidat egy online felületen, mindig ellenőrizd a biztonsági és adatvédelmi szabályzatokat!
- Ha bűncselekmény történt, fordulj a rendőrséghez!

3. Gyűlöletbeszéd

- Kényelmetlenül érzed magad, ha olyan emberrel találkozol, aki más nemzetiségű vagy vallású, mint te? Hangot adsz a véleményednek?
- Láttál már az interneten olyan posztokat vagy kommenteket, amelyek célja mások sértegetése vagy kirekesztése volt?
- Tudod, mi számít gyűlöletbeszédnek? Járhat bármilyen büntetőjogi következménnyel?
- Mit gondolsz, csak a szóbeli sértések minősülnek gyűlöletbeszédnek?

Tipp:

- A gyerekekkel meg kell értetni, hogy nem attól lesz valaki népszerű vagy elfogadott a társai között, ha másokat kellemetlen szituációba hoz vagy kiközösít.

4. Internetes zaklatás (cyberbullying)

- Van olyan barátod, akit csak az interneten keresztül ismersz? Mit teszel, ha egy ismeretlen személy kezdeményez veled beszélgetést valamelyik online felületen?
- Hallottál már online zaklatásról?
- Ha még nem, mit gondolsz, mit jelent? Ha már hallottál ilyesmiről, veled vagy valamelyik ismerősöddel történt már hasonló? Mi történt pontosan, és hogyan reagáltatok?

Tipp:

- Ne nyiss meg ismeretlen személytől származó üzenetet, de legalábbis kérdezz körbe a barátaidnál, rokonaidnál ismerik-e az illetőt!
- Sose találkozz egyedül, felnőtt társasága nélkül olyan személlyel, akit csak az internetről ismersz. Ha épp senki sem tud elkísérni, mindenképp szólj egy ismerős felnőttnek a találkozóról. Célszerű az első találkozót egy nyilvános helyre, például egy forgalmas kávézóba szervezni!
- Az éppen használaton kívül lévő webkamera is rejthet magában veszélyeket, ha például egy hackertámadás során tudtunk és beleegyezésünk nélkül rögzítenek vele képet!
- Ha bármilyen incidens történik, a hatóságok, szülők vagy tanárok jelentsék a problémát a weboldal üzemeltetőjének!

5. Sexting

- Szerinted menő fürdőruhás fényképeket posztolni az interneten?
- Küldtél vagy kaptál már valaha erotikus fényképet vagy videót?
- Tudod, mi a valódi sorsa a törölt fotóknak?
- Mit gondolsz, az e-mailben küldött fényképeket csak a címzett láthatja?

Tipp:

- Fel kell hívni a figyelmet arra, hogy nem csak a fényképek és videók megosztása, továbbítása és a letöltése lehet veszélyes, de maga az elkészítésük is!
- **18 év alattiakról készült erotikus tartalmak nyilvánosságra hozatala és továbbítása büntetőjogi felelősséggel jár akkor is, ha a nyilvánosságra hozó vagy továbbító szintén kiskorú!**
- A gyerekeket meg kell tanítani arra, hogyan ne hozzák magukat olyan helyzetbe, amelyet később megbánhatnak. Az interneten megosztott bizalmas képek a későbbiek során – például iskolai felvételi vagy álláskeresés esetén – még okozhatnak kellemetlenségeket!
- A gyermekekben tudatosítani kell, hogy ha valami egyszer felkerült az internetre, az ott is marad. Például ha valaki erotikus anyagot tölt fel magáról az egyik közösségi oldalra (vagy bármilyen más online felületre), nagy az esélye, hogy még az eredeti tartalom törlését követően is megjelenhet más weboldalakon, ha valaki korábban letöltötte!
- Ha a gyerek vagy fiatal magáról erotikus képet vagy videót talál egy honlapon, jelentheti azt a szolgáltatónak, és kérheti annak eltávolítását.

Javasolt helyzetgyakorlat:

Adatvédelmi kvíz

1. *Az interneten megismerkedtél egy nagyon vonzó fiúval/lánnyal. Beszélgettek már egy ideje, amikor megkér, küldj magadról képet.*
   a) *A profilképem úgyis olyan jó, végre találkozhatnánk is.*
   b) *A legrosszabb, ami történhet, hogy nem tetszem neki.*
   c) *Biztosan nem küldök képet, elvégre a profilképemen láthatja, hogyan nézek ki. Mire kéne neki még kép?*

2. *Olyan ember jelöl be a Facebookon, akivel még soha sem találkoztál.*
   a) *Visszaigazolom, hogy több ismerősöm legyen.*
   b) *Elgondolkodom, hátha mégis ismerem valahonnan.*
   c) *Nem igazolom vissza. Sosem találkoztunk, nem is értem, miért jelölt be.*

3. *Megjelenik egy újságcikk: mémek posztolása a legújabb trend a neten.*
   a) *Az meg mi a fene?*
   b) *Valamit hallottam a suliban, cikis képekkel kapcsolatos.*
   c) *Ez az, amikor fájlokat, főleg fényképeket küldözgetnek az interneten abból a célból, hogy felhasználók széles rétegét szórakoztassák kínos szituációkban készült vagy manipulált képekkel, illetve hamis hírekkel?*

4. *15 éves vagy, és egy olyan weboldalra tévedsz, amely mielőtt beengedne, megkérdezi: Elmúltál már 18?*
    a) *Szerintem felesleges feltenni ezt a kérdést.*
    b) *Ugyan még csak 15 vagyok, de el tudom dönteni, hogy meglátogatok-e egy honlapot vagy sem.*
    c) *Lehet, hogy jobban teszem, ha megkímélem magam valami kellemetlenségtől, ami az oldalra való belépéssel járna?*

5. *Ahhoz, hogy játszhass, meg kell adnod a bankszámla számod egy online játékban.*
    a) *Nem érdekel, megadom, a lényeg, hogy játszhassak.*
    b) *Nem is tudom. Lehet, hogy előbb megkérdezek valakit, aki már tapasztalt a témában.*
    c) *Kizárt dolog, hogy megadjam, azonnal egy kereskedelmi oldalra irányítana a honlap.*

6. *Észreveszed, hogy egy barátnőd bikinis képeket posztolt magáról.*
    a) *Én is készítek magamról párat, és gyorsan fel is töltöm.*
    b) *Kizárt dolog, hogy bikinis képeket töltsek fel magamról, de azért posztolok néhány ütős fotót.*
    c) *Sokan letölthetik a fotómat a netről, hogy aztán szórakozhassanak. Nem akarom, hogy bárkinek is fényképei legyenek rólam a gépén.*

7. *Kapsz egy e-mailt, amiben arról értesítenek, hogy egzotikus utazást nyertél. Csupán néhány személyes adatot kell megadnod, és már át is veheted a nyereményed. A kért információk: név, lakóhely, telefonszám, bankszámla szám, személyi igazolvány szám, adószám.*
    a) *El se hiszem, hogy ekkora szerencse ért! Gyorsan elküldöm a kért adatokat, és már megyek is csomagolni.*
    b) *Vajon hogyan lettem pont én kiválasztva egy ilyen nyereményre? Na mindegy, egy próbát megér.*
    c) *Ó, persze, biztosan. Ez színtiszta beugratás, semmilyen adatot nem fogok küldeni nekik.*

8. *Egy barátod elmeséli, hogy valaki a nevében küldözget e-maileket az osztálytársaitoknak.*
    a) *Hagyjuk már! Mégis hogyan tudna más bejelentkezni a fiókjába?*
    b) *Gondolom megadta a jelszavát valakinek, aki most így vicceli meg.*
    c) *Manapság sajnos nem nehéz feltörni valakinek az e-mail fiókját.*

9. *Az iskolában azt tanultátok, hogy a fénykép személyes adatnak minősül.*
    a) *Nem, ez nem igaz. Személyes adat csak a név, a lakóhely, a személyi igazolvány szám, és a hasonlók. Ezt mindenki tudja.*
    b) *Csak akkor minősül személyes adatnak, ha szerepel mellette a neve is annak, akiről készült.*
    c) *Természetesen személyes adatnak minősül, hiszen bárkit be lehet így azonosítani.*

10. *Egy barátod személyes adataival visszaéltek. Elmeséli, hogy a NAIH-hoz fordult segítségért.*
    a) *Nem tudom, mi az.*
    b) *Azt hiszem, az valami nemzetközi szerv, amely az adatokkal foglalkozik.*
    c) *Ha jól tudom, az a magyar adatvédelmi hatóság.*

11. *Egy szórakozóhelyen elkérik a telefonszámod.*
    a) *Megadom, szeretek új embereket megismerni.*
    b) *Rendben van a dolog, maximum nem veszem fel, ha sokat hívogatnak.*
    c) *Már elég sztorit hallottam a zaklatásokról. Inkább nem adom meg a számom.*

12. *A 14 éves húgod csak szülői felügyelet mellett netezhet.*
    a) *Sajnálom szegényt, hogy nem internetezhet szabadon.*
    b) *Minek ott ülni mellette, utólag úgyis le lehet ellenőrizni, milyen oldalakat látogatott.*
    c) *Biztos, hogy nem épp a legkellemesebb így netezni, de ily módon legalább elkerülhető, hogy olyasmit lásson, ami nem neki való.*

13. *Egy barátod kínos fotót posztol rólad az interneten.*
    a) *Kicsit mérges leszek, de megkérem, hogy törölje a képet, és minden rendben lesz.*
    b) *Én is feltöltök róla egy fényképet.*
    c) *Remek… Soha az életben nem tüntetem el azt a képet.*

14. *Azért regisztráltam a Facebookra, hogy*
    a) *egyre több és több emberrel találkozzam, fotókat töltsek fel magamról, videókat osszak meg, a mindennapi tevékenységeimről posztoljak.*
    b) *nehogy lemaradjak. Szinte mindenki fent van a Facebookon, ahol őrült ismerősgyűjtési verseny zajlik.*
    c) *barátokat és régen látott ismerősöket keressek.*

15. *Ha megkérdezik, gondoskodom-e a személyes adataim védelméről, a válaszom egyértelmű igen, mivel*
    a) *a személyes információmat csak kedves emberekkel osztom meg.*
    b) *csak akkor adok meg adatokat, ha kérik, automatikusan sosem.*
    c) *alapos indok nélkül senkinek sem adok meg személyes információkat.*

Eredmények:

<u>Ha a legtöbb válaszod a):</u>

A válaszaid alapján jobban oda kellene figyelned adataid védelmére. Nem tudod felmérni, milyen káros következményekkel járhat, ha meggondolatlanul adod meg a telefonszámodat, vagy fotókat posztolsz magadról a közösségi oldalakon. Tájékozódj az adatvédelem lehetőségeiről és a veszélyekről!

<u>Ha a legtöbb válaszod b):</u>

A válaszaid azt mutatják, hogy korábban már hallottál az adatvédelemről, vagy legalábbis jó érzéked van ahhoz, hogyan kerülheted el a személyes adatok meggondolatlan közlését. Bizonyos esetekben gyanítod, ha valami nem stimmel, mikor a személyes adataidat kéri valaki, de végül általában beadod a derekad. Adatvédelmi ismereteidet még bővíteni kell!

<u>Ha a legtöbb válaszod c):</u>

Gratulálunk, sikeresen teljesítetted az adatvédelmi kvízt! A válaszaid egyértelműen azt mutatják, hogy tisztában vagy az adatainkra leselkedő veszélyekkel. Még a való életben, a mindennapi szituációkban is kellőképpen meg tudod ítélni, hogy a közzététel mikor megalapozott, és mikor vezethet kellemetlenségekhez. Csak így tovább!

10. Fejezet: Segítő szervezetek

Tartalom:

Hogyan érvényesíthetjük a személyes adatok védelméhez való jogunkat? Miben segíthet az adatvédelmi hatóság?

Cél:

A segítő szervezetek bemutatása, különös tekintettel az adatvédelmi hatóságra.

Alapvetés:

Ahhoz, hogy pontosan értsük, mit kell védeni, fontos lenne a személyes adatok védelméhez való jog definíciójának átismétlése.

A jogszerű adatkezelés ismérvei:

1. A személyes adatok kezelése főszabályként az érintett/adatalany hozzájárulása alapján történik,
2. kötelező adatkezelést indokolt esetben csak törvény rendelhet el,
3. az adatkezelés csak meghatározott célból történhet,
4. az adatok legyenek pontosak, teljesek, naprakészek, a hibás adat kijavítása kérhető,
5. az adatbiztonságért az adatkezelő (és az adatfeldolgozó) felel,
6. a már nem szükséges adatok törlésre kerülnek, a törlést az adatalany is kérheti,
7. a tárolt személyes adatok megfelelőek, relevánsak, szükségesek,
8. a tárolt adatok legyenek hozzáférhetőek (például lehessen másolatot kérni),
9. az adatalanyt főszabályként megilleti a részletes tájékoztatáshoz való jog,
10. adatvédelmi jogsértés gyanújának felmerülése esetén az érintett az adatvédelmi hatósághoz vagy bírósághoz fordulhat.

Hasznos fogalmak:

Adatvédelmi hatóság: független állami szerv, amelynek feladata, hogy biztosítsa a személyes adatok (és Magyarországon emellett a közérdekű adatok nyilvánosságához való jog) védelmét. Az EU országaiban szinte kivétel nélkül mindenhol működik egy ilyen hatóság. Bárki élhet panasszal és az eljárás ingyenes.

Az adatvédelmi hatóságok:

- előírhatják a hibás adat kijavítását
- elrendelhetik a jogszerűtlenül kezelt személyes adatok korlátozását, törlését vagy megsemmisítését
- megtilthatják a személyes adatok jogszerűtlen kezelését, feldolgozását
- megtilthatják a személyes adatok más országokba való továbbítását
- elrendelhetik az adatalanyok értesítését, ha azt az adatkezelő jogellenesen megtagadta
- bírságot szabhatnak ki
- büntetőeljárást kezdeményezhetnek, vagy más hatóság együttműködését kérhetik
- elendelhetik, hogy döntésük nagy nyilvánosságot kapjon, ha ezzel az adatalanyok szélesebb rétegének jogvédelmét segítik elő.

Megtörtént esetek, példák:

- *A Hatóság 2013-ban vizsgálatot indított felnőtt online társkereső oldalak ellen (pl. randivonal, onlyyou, tavkapcs), mert kb. 3500 10-15 év közötti gyermek adatlapja is szerepelt a „kínálatban". Sem jogi, sem egyéb értelemben nincs keresnivalójuk tizenéves kislányoknak és fiúknak felnőtt társkeresők között, ezért a jogsértő oldalak üzemeltetőit a Hatóság több millió forint bírsággal sújtotta.*

- *Korábban az adatvédelmi biztoshoz is már tucatjával érkeztek szülői és érintetti panaszok, mert szépségkirálynő választáson való részvétel miatt elküldött fürdőruhás képek később felbukkantak jellemzően pornográf vagy hasonló stílusú oldalakon. A törlési kérelmekre pedig ilyen fajta válaszok érkeztek: „Innen soha a büdös életben nem fogsz lekerülni" vagy „Ha felkerültél az oldalra és emiatt szomorú vagy, írj nekünk és talán levesszük a képeidet az oldalról. Mivel bunkók vagyunk, és a szép szóból nem értünk, minél inkább mocskolódsz, annál biztosabb, hogy sikerrel jársz". Ezekben a becsületsértő, bűncselekményi szintet elérő esetekben mindenképpen rendőrséghez kell fordulni és büntetőeljárást kell kezdeményezni.*

Beszélgessenek róla!

- Éltél már a gyakorlatban adatvédelmi jogaiddal? Ha igen, milyen módon? Ha nem, miért nem?
- Hallottál már valaha a NAIH-ról vagy az adatvédelmi biztosról?
- Ha jogaid sérülnének, fordulnál panaszoddal a NAIH-hoz?

Javasolt helyzetgyakorlatok:

1. Nézzék meg a NAIH weboldalát!

2. Játszanak szerepjátékot, amelynek tárgya egy adatvédelmi panasz benyújtása: valaki a panaszost, más pedig az adatvédelmi hatóság munkatársának véleményét formálja meg.

Tippek:

A gyerekeket bátorítani kell, hogy baj esetén ne forduljanak magukba, hanem kérjenek segítséget egy felnőttől. Tudatosítani kell, hogy az interneten bárki adataival történhet visszaélés, ugyanezzel a problémával biztos, hogy sok millió más áldozat is küszködik, nincs egyedül és mindenre van megoldás, jogorvoslat!

A Nemzeti Adatvédelmi- és Információszabadság Hatóság honlapja: www.naih.hu,

valamint további **segítő szervezetek**:

Kihez fordulhatok?	Elérhetőség	Milyen ügyben?
Nemzeti Adatvédelmi és Információszabadság Hatóság www.naih.hu	1125 Budapest, Szilágyi Erzsébet fasor 22/C. Tel: +36 -1-391-1400 E-mail: ugyfelszolgalat@naih.hu	Ha személyes adatok védelmével (adatvédelem) vagy a közérdekű adatok nyilvánosságával (információszabadság) kapcsolatos alkotmányos jogaival összefüggő kérdése van vagy ezeket a jogait sérelem érte vagy érheti.
Alapvető Jogok Biztosa www.ajbh.hu	1051 Budapest, Nádor utca 22. Tel: (06-1-) 475-7100 E-mail: panasz@ajbh.hu vagy külön gyerekeknek: kerdesemvan@obh.hu	Amennyiben egy hatóság tevékenysége vagy mulasztása alapvető jogot sértt vagy közvetlenül sérthet.
Nemzeti Média-és Hírközlési Hatóság www.nmhh.hu	1133 Budapest, Visegrádi u. 106. Tel: (06-1) 468 0673 E-mail: info@nmhh.hu	Ha hírközlési szolgáltatók ellen kíván panaszt benyújtani (például mobiltelefon-, internet-, postai szolgáltatásokkal kapcsolatban, kéretlen elektronikus hirdetés, spam bejelentése), illetve médiatartalom-szolgáltatók elleni panaszok esetén (például televízió- és rádióműsorokkal, ún. lekérhető médiatartalmakkal, nyomtatott és internetes sajtóban megjelenő tartalmakkal és egyéb internetes tartalmakkal kapcsolatban).
Nemzeti Média-és Hírközlési Hatóság Internet Hotline www.internethotline.hu	1015 Budapest, Ostrom u. 23-25. E-mail: internethotline@internethotline.hu	Jogellenes, illetve gyerekekre veszélyes vagy káros internetes tartalom bejelentése az Internet Hotline bejelentő felületén (http://internethotline.hu/tart/index/31/Bejelentes) és az internethotline@internethotline.hu e-mail címen van lehetőség.
Kék-Vonal Gyermekkrízis Alapítvány www.kek-vonal.hu	1364 Budapest, Pf.: 125. Tel: +36-1-354-1029 E-mail: info@kek-vonal.hu	Ha a gyermekek bajban vannak, vagy ha segítségre lenne szükségük és úgy érzik egy kívülálló, független személlyel szeretnének beszélgetni. Ingyenesen és anonim módon hívható a 116-111-es szám.