Témák és ötletek az információkezelés tanítására

Holló Csaba

chollo@inf.u-szeged.hu
SZTE TTIK Informatikai Intézet

Absztrakt. Az információs társadalom fejlődésével az információ egyre nagyobb értékkel bír, ami indokolja az információkezelés tanításának fontosságát. Ennek megfelelően az információkezelés különböző aspektusai a 2020-as NAT-ban is megjelennek. Jelen cikkben bemutatásra kerül néhány téma és ötlet az információkezelés tanítására.

Kulcsszavak: információs társadalom, információkezelés, információbiztonság.

1. Bevezetés

Viszonylag közismert az információkezelés fontossága, és annak szükségessége is, hogy ezt az tudást a diákok is megszerezzék ([1, 2, 3]). Az információkezelésről, biztonságról, beállítási és védekezési lehetőségekről, illetve azok tanításáról számos irodalom megjelent (például a [4] tananyagai, [5, 6]). Egy cikk nem alkalmas arra, hogy ilyen mennyiségű tartalom tanításának minden részletét tárgyalja, ezért bizonyos témákra egyáltalán nem, vagy csak felületesen térek ki. Az érintett témákban sem cél minden tárgyalandó ismeret felsorolása, csupán szeretnék a cikkben, illetve a mellékelt irodalmakon keresztül olyan tartalmakat megemlíteni, szempontokat, illetve gyakorlati ötleteket adni, amelyek az információkezeléshez tartozó témakörök tanítása során hasznosak lehetnek. A cikkben nem fogok kitérni arra sem, hogy a jelenlegi kerettanterveket figyelembe véve mely témákat, mikor, milyen óraszámban lehetne tanítani, ugyanis ennek részletes elemzése egy külön cikket igényelne. Annyit viszont fontosnak gondolok megemlíteni, hogy a kerettantervben leírtaknak megfelelően az információkezelés témaköréhez tartozó ismeretekre érdemes többször, azokat átismételve és fokozatosan bővítve tárgyalva visszatérni, annál is inkább, mert ennek a tudásnak számos elemére a diákoknak különböző korosztályokat átívelően (esetlegesen különböző mértékben) folyamatosan szükségük lehet, a képességek és normák kifejlődéséhez pedig fokozatos mélyítésre és gyakorlásra van szükség.

2. Szakmódszertani szempontok

Az információs technológiákhoz tartozó tanítandó ismeretek mennyisége az utóbbi időben jelentősen megnőtt, új kihívás elé állítva a tanárokat. Ugyanis, a hagyományos témakörök tanításakor többnyire elegendő volt arról meggyőződni, hogy a diákok megfelelően elsajátították a tananyagot, akkor valószínűsíthető volt, hogy szükség esetén a tanultakat használni is fogják. Az információs technológiához tartozó ismeretek esetén azonban, mivel a tanárnak nagyon kevés rálátása van a diákok online tevékenységére, el kellene érni, hogy a diákok valós helyzetekben a tanár hiányában is felismerjék, hogy hogyan kellene eljárni, és főleg hajlandóak legyenek azt megtenni akkor is, ha az olyan plusz munkával jár, ami nélkül a feladatot ugyan meg tudják oldani, csak kevésbé biztonságosan vagy etikusan. Ehhez pedig az kell, hogy kialakuljanak bennük alapvető biztonsági és etikai normák, és ily módon ők is fontosnak tartsák a tanultak betartását. Ez a tanulásnak egy olyan módja, amikor az attitűd kialakítása legalább olyan fontos, mint a kompetenciák megszerzése, hiszen megfelelő attitűd hiányában a használatlan kompetenciák értéktelenek. Kérdés, hogy az attitűd kialakulását hogyan lehet elérni?

Természetesen ez is ott kezdődik, hogy a diáknak meg kell értenie, hogy milyen mechanizmusok játszódnak le, el kell sajátítania a szükséges ismereteket, és tudnia kell azokat alkalmazni.

Ugyanakkor nem mindegy, hogy ezeket az ismereteket hogyan dolgozzuk fel, mert „szárazon" elmondva nagyon hamar a feledés homályába merülhetnek. Igyekeznünk kell az ismereteket a diákok mindennapjaihoz kötni, érdekesen, és lehetőleg oly módon, hogy érzelmeket is kiváltsunk belőlük, mert az a tudást maradandóbbá teszi ([7]), és segít az etikai normák kialakításában is. Ennek érdekében igyekszem a cikkben, illetve a rendhagyó módon jelentős mennyiségben kevésbé tudományos cikkeket is tartalmazó irodalomjegyzékben, konkrét hétköznapi példákat, érdekes videók elérését is mellékelni.

Törley Gábor a [8] cikkében rámutat arra, hogy a biztonságtudatossággal kapcsolatos ismeretek tanításánál is igyekeznünk kell a Bloom-féle taxonómia minél magasabb szintjét elérni. Ez a többi információkezelési ismeret esetén is így van, és logikus összefüggésben van a meggyőzés sikerességével. Ugyanis, az elemzés, értékelés és teremtés szintjein egyre nagyobb esélyünk van a diákok meggyőzésére, és ily módon a biztonsági és etikai normák kialakítására.

A meggyőzés csak akkor elképzelhető, hogyha ismerjük és meg tudjuk cáfolni az esetlegesen a diákokat ebben gátló ellenérveket, amihez szükségszerű, hogy a diákok kifejtsék a véleményüket, ütköztessék az érveiket, értékeljenek, és megoldásokon gondolkodjanak. Ehhez pedig nem elegendő „leadni" az anyagot, hanem beszélgetni kell a diákokkal, és olyan viszonyban kell lenni velük, illetve olyan légkört kell teremteni az osztályban és az órán, hogy merjék kimondani a gondolataikat.

3. Az információ megbízhatósága

3.1. Hitelesség és megbízhatóság

Érdemes közérthetően és praktikusan definiálnunk az információ hitelesség és megbízhatóság fogalmát. Az információ hiteles, ha a közzétevője megbízható és hitelesíti (felel érte) ([9]). Viszont érdemes figyelembe venni, hogy az általában megbízható közzétevő is tévedhet. Ezért az információ megbízhatósága a hitelességnél erősebb elvárás, ami szükségessé teszi annak igazságtartalmának vizsgálatát több forrás, korábbi (tudományos) ismeretek, illetve racionális érvek alapján.

3.2. Bizalom tényezők

Hasznos megnézni a legfontosabb olyan tényezőket, amelyek növelik a bizalmat az olvasóban. Ilyenek lehetnek a design (profi megjelenés), az, hogy a tartalom az olvasó által már valószínűleg ismert információkra épít, érvelési hibáktól mentes, logikus, áttekinthető és átlátható felépítésű, a szerző elismert (megbízhatónak gondolt emberek bíznak már benne), a tartalom tárgyilagos (legalábbis látszólag elfogultságmentes), és alá van támasztva további szakirodalmakkal, referenciákkal. Az ilyen tényezőkről több okból is érdemes beszélni. Egyrészt azért, mert az információk közzétételénél fontos ezekre figyelni, ha azt szeretnénk, hogy mások megbízhatónak gondolják az általunk közzétett tartalmat. Másrészt olvasóként jó, ha ezek hiánya gyanút ébreszt bennünk. Harmadrészt pedig, a profi átverők használják is az ilyen tényezőket a bizalom megnyerésére, tehát csak ezek miatt még nem célszerű elhinni a tartalmat.

3.3. A média hitelessége

Bár ezt a témát a Vizuális kultúra, illetve a Mozgóképkultúra és médiaismeret tantárgyak is érintik, mégis érdemes néhány szót szólni arról, hogy hogyan működik az online média, hogyan lehet megélni vagy legalábbis pénzt szerezni (konkurencia, mennyiség a minőség rovására, szenzációhajhász és kattintásvadász oldalak, pl. [10]), a névtelenség és felelősség kérdéséről, és arról, hogy ezek hogyan függenek össze a valótlan információk megjelenésével és terjesztésével.

3.4. A közösségi oldalak szerepe

Sokan alapvetően a közösségi oldalakról, az azokban megjelenő megosztások alapján tájékozódnak, ezért fontos beszélni arról, hogy ez hogyan vezethet nem megfelelő ismeretszerzéshez.

Az ismerősök a híreket a saját „szemüvegükön” keresztül szűrik és módosíthatják is. Amint a [11, 12] cikkekben ismertetett tanulmányból kiderül, a felhasználók a kamuhíreket 70%-al nagyobb valószínűséggel osztják meg, általában a bennük levő több újdonság és élénk érzelmi reakciók miatt, ezért sokkal gyorsabban terjednek, mint az igaz hírek. Továbbá, bizonyos esetekben az álhírek melegágya lehet az is, hogy egyes vélekedések szerint valamilyen jellegű cenzúra miatt az igazságok nem kapnak napvilágot, és ezért a valótlanságot terjesztő ismerősök megosztásai hihetőbbeknek tűnnek.

A közösségi oldalakra másik jellemző jelenség a véleménybuborék kialakulása. A közösségi oldalakon az algoritmusok azon dolgoznak, hogy a felhasználó minél több időt töltsön az oldalon, ezért igyekeznek olyan megosztásokat beválogatni, amelyek valószínűleg tetszeni fognak a felhasználónak, vagy pedig (meglepő, esetlegesen szélsőséges tartalmukkal) felkeltik annak a figyelmét ([13]). Továbbá, a felhasználó is szűri az ismerőseit, többnyire azokkal barátkozik, kommunikál többet, és azoknak a megosztásait olvassa el, akikkel jelentős mértékben egyetért. Az ily módon kialakuló közösségek „nem látják egymást”, ezért hiányzik az egészséges vita is a tisztánlátáshoz. A hiányos tájékozódáson túl ez azért is probléma, mert annak elfogadása, hogy a nekem ellentmondó vitapartner nem ellenség, hanem egy másik szemszögből neki is lehet igaza, annak belátása, hogy ily módon a kulturált vita egy lehetőség a mélyebb megértéshez, illetve az ezeken alapuló kölcsönösen elfogadható megoldáskeresés képességének kialakítása, alapvető fontosságúak (lennének) a civilizált együttműködéshez, a problémák erőszakkal történő kezelésének elkerüléséhez.

3.5. Lehetőségek a megbízhatóság ellenőrzésére

Célszerű a közzétevő vizsgálatával kezdeni. Megbízhatók-e az eddig közzétett (megosztott) tartalmai: vannak-e ilyen tapasztalataink, vagy van-e ilyen jellegű információnk mások értékeléseiből, szerepel-e átverős oldalak listájában vagy jelez-e ilyen problémát az erre vonatkozó böngészőbővítmény? Feltételezhetően van-e megfelelő szaktudása a közzétevőnek, vagy a megosztott tartalom szerzőjének a tartalommal kapcsolatban? Lehet-e szándéka (érdeke) megtévesztésre?

Ezután célszerű megnézni, hogy elévült-e a tartalom? A legmaradandóbb a saját élmény, ezért érdemes a diákokkal olyan tartalomra kerestetni, amelyre az első találat tartalma már nem érvényes. Érdemes mutatni a tanulóknak olyan tartalmat is, amelyben félrevezetés céljából használnak olyan cikket, amely elavult vagy a tartalma könnyen félreértelmezhető, mint például az [14]-ben bemutatott 1976-os cikk a koronavírussal kapcsolatban.

A megbízhatóság eldöntésében fontos annak mérlegelése is, hogy a tartalom tényt állít vagy véleményt fogalmaz meg, ezért érdemes ezt konkrét tartalmakkal gyakorolni. Tudatosítani kell a tanulókban, hogy megfogalmazásaikban ők is figyeljenek a kettő közötti különbségre, mert a téves tényállításnak komolyabb jogi következményei is lehetnek.

Tipikus módszer az információ megbízhatóságának ellenőrzésére, hogy több forrást is megnézünk. Itt viszont érdemes figyelembe venni, hogy a tartalmakat sok esetben a források is átvehetik egymástól (a komolyabb médiumok ezeket lehivatkozzák), tehát a többi forrás megbízhatóságát is értékelni kell, ugyanakkor hogyha hamis a tartalom, akkor van esélyünk olyan forrást is találni, amely cáfolja a valótlan vagy elferdített tartalmat.

Konkrét példákon keresztül be lehet mutatni a kamuhír-propaganda mögött rejlő taktikákat és jellegzetességeket, mint például érzelmekre ható tartalom, támadás valakik ellen, vagy más identitásának eltulajdonítása. Érdemes tudatosítani a tanulókban, hogy az elkövetők egyes esetekben akár nyilvánvaló jogtalanságokat is bevállalnak, arra számítva, hogy a sértettnek nem éri meg a leleplezésükhöz és jogi lépésekhez szükséges pénzt és energiát ráálldozni, vagy ha mégis, az elkövetőknek akkor is megérheti az esetleges jogi következményeket is megkockáztatni (például a reklámbevétel nagyobb lehet, mint a sértett esetleges hosszas pereskedésének következménye [15]). A tanulók a kamuhír taktikákat játékosan is gyakorolhatják (például a [16, 17, 18] cikkekben leírt módon, vagy az alhirvadasz.hu oldalon) azért, hogy majd felhasználóként ezeket könnyebben felismerjék. Fontos

továbbá a diákok figyelmét arra is felhívni, hogy a megfelelő tájékozódáshoz vegyék figyelembe a véleménybuborék jelenségét, illetve azt is, hogy a képek és videók is lehetnek manipulálva ([19]). Az ilyen manipulálások technikáiról és felismeréséről a diákok a Vizuális kultúra, illetve a Mozgóképkultúra és médiaismeret tantárgyakban is tanulnak, viszont legalábbis a mesterséges intelligencia ilyen jellegű alkalmazásairól a Digitális kultúra tantárgyban is célszerű lenne beszélni, érdekes történetek és videók felhasználásával, mint pl. a [20, 21, 22].

További ötleteket az álhírek felismerésére a [23, 24, 25., 26, 27, 28] cikkekben találunk.

A legfontosabb azonban, hogy az embernek igénye legyen a megbízható információkra, és hajlandó legyen az ehhez szükséges lépéseket megtenni, ugyanakkor valószínűleg ezt a legnehezebb elérni, ezért fontos arról is beszélgetni, hogy milyen következményei lehetnek a valótlan információk alapján történő döntéseknek és cselekedeteknek.

4. Az információ megosztása

4.1. Az információ értéke

A további tartalmak megalapozásaként érdemes megbeszélni néhány példát arra, hogy miért értékes az információ.

Ha nem jutunk egy információ birtokába, akkor eleshetünk lehetőségektől, tévesen ítélhetünk meg helyzeteket, illetve helytelen döntéseket hozhatunk.

Az információ manapság fizetőeszköz is ingyenesnek hirdetett szolgáltatásokhoz azáltal, hogy a regisztráció, illetve a szolgáltatások használata során adatokat osztunk meg magunkról, amelyeket a szolgáltatók eladhatnak olyanoknak, akik ezeket valamilyen célból fel szeretnék használni. Ugyanis, az információk, olyanok is, amikről nem is gondolnánk, felhasználhatók mások érdekében, vagy ellenük, például hasznos tudományos kutatásokra, de befolyásolásra, zsarolásra is. Az ártatlannak látszó információk felhasználására egy példa a [29] cikkben olvasható Chris "Birdman" Andersen esete, amikor az egyik áldozat életkorának ismerete kulcsfontosságú információ volt a zsaroláshoz, ezúttal pénzszerzés érdekében. A későbbi fejezetekben további példákat is látni fogunk az információk felhasználhatóságára.

4.2. Az információk gyűjtése

Érdemes beszélni azokról a lehetőségekről, hogy mások hogyan gyűjthetnek információt rólunk.

Nyilvánvaló, hogy amikor részt veszünk egy jelenléti eseményen, vagy nyilvános helyen cselekszünk valamit, akkor mások látnak, hallanak minket. Mivel az online térben kevésbé érzékeljük mások jelenlétét, ezért valamivel kevésbé tudatosulhat bennünk az, hogy online tevékenységeink során is ugyanez történik.

A fentieknél még kevésbé nyilvánvaló, hogy az internetes szolgáltatásokat nyújtó oldalak hogyan gyűjtik rólunk az információkat. Egyrészt, rengeteg adatot szolgáltatunk a nyilvános profiljainkban, különböző közösségi oldalakon, keresésekben, applikációkban megadott információkkal, lépésszámláló, naptár, helymeghatározás és más programok használatával. Érdekes feladat lehet a diákoknak az, hogy keresőben rákeressenek saját magukra, illetve lekérjék a róluk tárolt adatokat a Google Takeout szolgáltatásban, vagy a közösségi oldal fiókjukban. Másrészt, érdemes tisztázni, hogy a sütik ([30]), amelyek elvileg a kényelmünket szolgálják, további adatokat gyűjtenek be rólunk, amelyeket nem feltétlen csak annak az oldalnak szolgáltatnak, amelyet meglátogattunk, és amelyen ezeket engedélyeztük, hanem más oldalaknak is, amelyeket az általunk meglátogatott oldal erre feljogosít, például azért cserébe, hogy azok szolgáltatásait használja. A Lightbeam böngészőkiegészítővel látványosan szemléltetni tudjuk, hogy egyes oldalak hogyan osztják meg egymással a rólunk gyűjtött adatokat ([31]), érdemes ezt a diákokkal kipróbálni.

Az információk gyűjtésének megbeszélése jó alkalom arra, hogy definiáljuk a személyes adatok és az adatvédelem fogalmait. A [32] definíciója alapján a személyes adat „bármely meghatározott, azonosított vagy azonosítható természetes személlyel [érintett] kapcsolatba hozható adat és az adatból levonható, az érintettre vonatkozó következtetés", az adatvédelem pedig „a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége". Megjegyzendő, hogy a [32] definíciója szerint, a személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek az adat és az érintett közötti kapcsolat helyreállításhoz szükségesek. Az adatvédelemmel kapcsolatos további kérdésekről a [33] irodalomban olvashatunk.

4.3. Megosztással kapcsolatos veszélyek

Az előzőekben leírt módon a cégek (különösen az olyan nagyok, mint a Google vagy Facebook) rengeteg adatot begyűjtenek. Érdemes tisztában lenni azzal is, hogy a látszólag személytelen adatok (általában ilyenek azok is, amiket a sütik gyűjtenek) egymással összekapcsolva, már személyes (azaz hozzánk köthető) adatokká válhatnak ([34]). Kimutatták például, hogy az amerikai lakosság 87%-át be lehet azonosítani kizárólag az irányítószámuk, nemük és születési dátumuk alapján ([35]). Ily módon az interneten is megjelenő tevékenységek (mit, mennyi ideig olvasunk, mire kattintunk, mit lájkolunk és mit nem, miket posztolunk, kereséseink, vásárlásaink, GPS koordinátáink), ismerőseink, törzsvásárlói kártyák, nyereményjátékok stb. elemzése révén az adatbrókerek nem csak felhasználói csoportokat képezhetnek, amelyeknek célzott üzeneteket (például reklámokat) lehet küldeni, de az információkat esetlegesen egészségünkre, vagy személyiségünkre vonatkozó személyes adatként is eladhatják, ami biztosítás, munkavállalás és más helyzetekben hátrányosan érinthet minket úgy, hogy nem is feltétlen lesz tudomásunk a történtekről ([36]). Persze, jogszabályok (például GDPR, illetve adatvédelmi törvények) korlátozzák a gyűjthető és tárolható adatokat és azok felhasználását ([33, 37]), de különösen felhasználói tudatosság hiányában ezek nem nyújtanak elegendő védelmet, továbbá általában sokkal könnyebb a problémákat megelőzni, mint kezelni. Ezért fontos tisztázni a személyes adatok fogalmát és az adatvédelmi tudnivalókat, amire az említett témakörök és példák jó lehetőséget nyújthatnak. Nyilvánvalóan manapság már nem lehet az online világból kiiratkozni, de azt megtehetjük, hogy legalább akkor, amikor erre lehetőségünk van, átgondoljuk, hogy milyen adatokat vagyunk hajlandóak megosztani magunkról, például érdemes-e részt vennünk egy nyereményjátékon, attól függően is, hogy milyen információkat kérnek cserébe.

Természetesen az adatainkat nem csak a nagy cégek vagy adatbrókerek gyűjthetik. A [38] videóban láthatunk példát arra, hogy hogyan lehet visszaélni egy nyereményjáték ürügyén megadott adatokkal. Ennek kapcsán is lehet beszélgetni arról, hogy miért érdemes különböző helyeken különböző jelszavakat használni, a kétfaktoros azonosításról, de a közzétett adataink nyilvánosságának korlátozásáról is. Utóbbi kapcsán érdemes megemlíteni, hogy a közzétett, önmagukban ártalmatlan adataink is felhasználhatók arra, hogy csaló szándékkal nekünk küldött levélben elaltassák bennünk a gyanút, mivel annak olvasásakor azt gondolhatjuk, hogy ha valaki ennyi mindent tud rólunk, akkor biztosan ismer.

Talán kevésbé közismert veszélyként Gyurkó Szilvia hívta fel a figyelmet a [39] interjúban a következőkre. „Az #iamalone hashtag a legerősebb triggerje a pedofiloknak, mert pontosan tudják, hogy ott lesz a másik oldalon egy 13 éves kiskamasz, aki azt érzi, hogy nagyon egyedül van, senki nem szereti, baja van az élettel. Ha ráír, hogy milyen gyönyörű, vagy hogy „mutass többet magadból!", akkor öt perc alatt rá tudja őt venni, hogy küldjön egy felvételt, amivel utána tudja zsarolni. És mivel egyedül van, senkitől nem fog tudni segítséget kérni.". Fontos tehát a gyerekek figyelmét felhívni arra, hogy a hashtagek is elárulhatnak róluk olyan információkat, melyek potenciális veszélyt jelenthetnek.

Hasonlóképpen szembesülhetnek a diákok a közösségi oldalakon megosztott tartalmak kellemetlen következményeivel a [40] videó megnézése kapcsán is, ami átvezet annak megbeszélésére, hogy

hogyan élhetnek vissza akár az ismerősök is a megosztott információkkal és tartalmakkal. Tipikus példa erre, amikor általunk bizalmasan megosztott titkokat vagy képeket az ismerős az engedélyünk nélkül közzétesz vagy azok közzétételével zsarol. Ennek az egyik leggyakoribb példája, amikor a fiatalok körében meglehetősen gyakori szextingelésből ([41]), vagy korábbi intim viszonyból szerzett képeket tesznek közzé, akár pornográf oldalakon is telefonszámmal együtt. Az áldozat nevetségessé tétele sok esetben zaklatásba is átmehet, és az áldozatnak nehéz lelki terhet jelent, akár depressziót, vagy öngyilkossági gondolatokat is okozhat ([42]).

A [29] cikkben részletesen olvashatunk arról, hogy a rólunk megszerzett adatok birtokában hogyan lehet álprofilt készíteni és azzal visszaélni. Ezek áttekintése mellett érdemes megbeszélni, hogy melyek azok az információk, amelyek felhasználhatók arra, hogy az álprofil valóságosnak tűnjön, és amelyekre ily módon figyelni kell, hogy lehetőség szerint minél kevesebb ilyen információ jusson illetéktelenek birtokába.

Tudatosítani kell a diákokban, hogy az előzőekben leírtak miatt is fontos az általuk használt szolgáltatások (első sorban a közösségi oldalak) beállításait úgy módosítani, hogy az adataikhoz való hozzáféréseket megfelelően korlátozzák.

4.4. Szólásszabadság és felelősség

Az információ közlése kapcsán érdemes beszélni a szólásszabadság korlátairól. Arra, hogy hol a határ a véleménynyilvánítás és a hivatal vagy mások becsületének sértése között, nincs világszinten egységes szabályozás, például az Egyesült Államokban a szólásszabadságnak van nagyobb súlya, míg az EU-ban a személyiségi jogoknak ([43]), továbbá, ez a konkrét helyzettől is függ, bizonyos esetekben az érintett köteles többet eltűrni (például, ha közszereplő),de ez nem azt jelenti, hogy korlátlanul lehet másokat sértegetni. Különbség van a hamis tényállítás és a vélemény között is, például az [44] oldal éveken keresztül erre történő hivatkozással működhetett. Továbbá, vannak etikai szabályok is, amelyeket a közösségi létben be kell tartani akkor is, ha azt nem jogszabály írja elő, erre példaként érdemes megbeszélni a diákokkal, hogy nekik mennyire bántó lenne, hogyha például mások a hátuk mögött csúfolnák őket, tehát olyant ne tegyenek, aminek elszenvedői ők sem szeretnének lenni.

A felelősség témakörével már foglalkoztunk, a korábbiakban láttuk, hogy a megosztásokkal személyiségi jogokat vagy szerzői jogot sérthetünk. De azt a felelősséget is át kell gondolnunk, hogy az általunk megosztott információkkal másokat befolyásolunk, aminek súlyos következményei lehetnek. Aktualitásként lehet itt a koronavírussal kapcsolatos álhírekre is gondolni, de a fiatalokhoz talán közelebb álló példaként lehet a West-Balkán diszkótragédiáról ([45, 46]) is beszélni, ahol a pánik és az ebből következő tragédia alapja az volt, hogy valaki valótlanul késelést kiáltott, egyesek szerint a közösségi médiában is ezt osztották ([47]). Függetlenül attól, hogy a közösségi média megosztás igaz volt-e, az eset alkalmas annak megbeszélésére, hogy egy valótlan hír megosztásának hogyan lehetnek akár súlyos következményei. Érdemes tisztázni, hogy a felelősség akkor is fennáll, hogyha az adott információt nem mi osztjuk meg elsőként, hanem tovább osztjuk. Hogyha pedig egy (pl. Facebook) csoport adminisztrátorai vagyunk, akkor fokozott felelősségünk van abban, hogy hogyan kezeljük a csoport adatait, például a tagok beleegyezése nélkül egy eredetileg zárt csoportot nem tehetünk nyilvánossá még csak kizárólag kutatási célból vagy technikai okokból néhány percre sem. Ez a példa pedig átvezet annak tisztázására, hogy a kisebb nyilvánosság (például egy zárt Facebook csoportban való megosztás) csökkenti a cselekmény súlyát, de nem semmisíti meg azt. Konkrét példaként beszélhetünk egy romániai iskolában történt esetről ([48]), ahol Facebook csoportban tanárokat sértő szövegeket és képeket osztottak meg. Minden résztvevő büntetést kapott, de az adminisztrátor büntetése súlyosabb volt, mert ő felelt azért, ami a csoportban történt és nyilván tudott róla. Viszont általában a kommentekért első sorban a szerző a felelős, az adminisztrátor akkor, ha tudomására jut, és nem távolítja el a jogtalan (például a másokat sértő) tartalmakat.

4.5. A digitális lábnyom

A digitális lábnyom digitálisan tárolt személyes adat. A korábbi fejezetekben részletesen tárgyaltuk az általunk megosztott, illetve rólunk gyűjthető információkat, melyek mind a digitális lábnyom részei. Ebben a fejezetben ezt azzal egészíteném ki, hogy egyes szolgáltatásoknál (levelezésnél, közösségi oldalaknál) nyilatkozhatunk arról, hogy mi történjen az adatainkkal, a profilunkkal a halálunk után ([49]). Ez a diákoknak életkorukból kifolyólag többnyire inkább családtagjaik tekintetében lehet érdekes, ugyanakkor ennek kapcsán lehet beszélni az elhunyt személyek adatainak kezeléséről, illetve a mesterséges intelligencia alkalmazásáról is, a digitális lábnyomok alapján az elhunyt személy megteremtéséről a digitális térben, illetve annak etikai és pszichológiai tényezőiről ([49, 50, 51, 52]).

4.6. A megosztás előnyei

Az előző fejezetekben részletesen beszéltünk az információmegosztás veszélyeiről, de a diákok jogosan gondolnák elfogultnak a hozzáállásunkat, ha nem beszélnénk az előnyeiről is.

Nem nehéz olyan példákat találni, amikor valakinek előnye származott abból, hogy más által (legalábbis vele) megosztott információ birtokába jutott. De a megosztás előnyeihez tartozik a sikerek megosztásának lehetősége, illetve a közösségi értékelés is, mert ezek bizonyos esetekben motiválhatják a diákot jobb minőségű munkára, nem feledkezve meg arról, hogy az viszont káros lehet, ha a diák az önértékelését kizárólag a visszajelzésektől teszi függővé. Hasonlóképpen, amint az előzőekben tárgyaltuk, veszélyeik mellett hasznosak is lehetnek a megosztott információk alapján nyújtott szolgáltatások, például az, ha a szolgáltatók a preferenciáinkról begyűjtött információk alapján ajánlanak további minket érdeklő tartalmakat.

Végül, az is nyilvánvaló, hogy az általunk készített és megosztott tartalmak érdekesek, értékesek, hasznosak lehetnek mások, illetve az utókor számára is, erre egy szokatlan példa a [53] emlékoldal, mely egyben kordokumentum is.

4.7. Megosztás előtt

Ajánlott átgondolni, hogy az adott tartalmat miért és kikkel szeretnénk megosztani, és a megosztást annak megfelelően korlátozni.

Érdemes felhívni a diákok figyelmét arra, hogy csak olyasmit érdemes közzétenni, amiben biztosak vagyunk, hogy később sem fogjuk megbánni, mert nem biztos, hogy később lehetőségünk lesz törölni, hiszen más személyek vagy oldalak is készíthetnek arról másolatot. Gondolni kell arra, hogy mi is változunk, a környezetünk is változik, és ami ma jónak tűnik, azt egy idő után vállalhatatlannak érezhetjük, vagy hátrányosan érinthet. Továbbá, ha tudjuk is törölni, ha valakit megbántottunk vele, azt nem lehet meg nem történtté tenni.

Ajánlott átgondolni, hogy a megosztásból a többiek mit tudhatnak meg rólunk, és az felhasználható lehet-e ellenünk.

Figyelni kell arra is, hogy megosztásainkkal nem csak magunknak, hanem másoknak is árthatunk. Lehet, hogy az információ, kép, videó tulajdonosa, vagy a rajta szereplő személyek, valamilyen okból nem szeretnék, hogy azt megosszuk, és a megosztással árthatunk is anélkül, hogy ez szándékunkban állna. Érdemes a diákokkal megbeszélni, hogy voltak-e ilyen jellegű élményeik.

Természetesen ki kell térni a megosztás adatvédelmi és szerzői jogi vonatkozásaira is, hiszen a másokkal kapcsolatos információk megosztása személyes adatok kezelésének minősül, és ily módon a megosztáshoz is ki kell kérnünk az érintettek beleegyezését.

Érdemes a diákokkal megismertetni azon információkezeléssel kapcsolatos jogszabályi részleteket és büntetési tételeket, amelyekben elkövetőként vagy sértettként ők is érintettek lehetnek.

5. Adatbiztonság

A [32] definíciója szerint az adatbiztonság „az adatok jogosulatlan megszerzése, módosítása és megsemmisítése elleni műszaki és szervezési megoldások rendszere."

Ebben a témakörben célszerű beszélni a lehetséges támadásokról és kockázatokról (vírusok, férgek, trójai programok, kémprogramok, lánclevél, spam, adathalászat, biztonsági rések stb.), illetve arról, hogy ilyen támadások célpontjai olyan más szolgáltatók is lehetnek, ahol a mi jelszavainkat tárolják, és ezért ajánlott, hogy különböző oldalakon különböző jelszavakat használjunk, ráadásul ezek nehezen feltörhetők legyenek ([54, 55]) és azokat rendszeresen változtassuk meg. Sok erős jelszót megjegyezni viszont csak akkor lehet, ha ezeket valamilyen algoritmus szerint találjuk ki (például [56]), segíthet a kétfaktoros azonosítás ([57, 58]) használata, melynek azonban kockázatai is vannak ([59, 60]), illetve használhatunk jelszókezelő programot is. További lehetőség a biometrikus azonosítás ([61]), ami sokféleképpen azonosíthat (például ujjlenyomat, retina, hang, DNS, arc, de akár gépelés, járás, mozgás alapján is), és aminek a digitálisan megváltoztatott verzióját célszerű tárolni azért, hogy ellopás esetén megváltoztatható legyen. Érdemes megmutatni, hogy vannak olyan oldalak, ahol becslést kaphatunk arra, hogy mennyi idő alatt törhető fel egy adott jelszó (például https://www.security.org/how-secure-is-my-password/), ahol meg lehet nézni, hogy adott jelszó szerepel-e az általuk gyűjtött feltört jelszavak adatbázisában (például haveibeenpwned.com/), illetve ahol segítséget kaphatunk zsarolóprogramok ellen (pl. https://www.nomoreransom.org/hu/).

Az adatbiztonság témakörében számos további internetes szolgáltatás (például elektronikus ügyintézés, kereskedelem, bankolás stb.) biztonságára is ki kell térni, melyek részletezése azonban meghaladná ezen cikk kereteit, de jónéhány tartalmi ötletet kaphatunk a [62] videóban, amelyek megbeszélését érdemes kiegészíteni tényleges történetekkel, illetve a diákok tapasztalataival, mert a megbeszéltek akkor lesznek maradandóak, hogyha konkrét példákhoz kapcsolódnak.

6. Szerzői jogok

Különösen a mai fiatalok körében a megosztás természetes és gyakori jelenség, és sok esetben nem gondolják át ennek hátterét, nem csak biztonság, másoknak okozott esetleges kár, hanem szerzői jogi szempontból sem, ezért is fontos erről beszélni.

A kerettantervben a szerzői jog explicit módon nem szerepel, csak a hivatkozás szabályai, jogosultságok, és az etikus információkezelés ([63, 64]), amibe viszont véleményem szerint a szerzői jog több megközelítéssel is beletartozik. Egyrészt, a szerző és a szerzői jog meghatározása szoros kapcsolatban áll egymás munkájának a tiszteletével, függetlenül attól, hogy azt mennyire gondoljuk értékesnek, továbbá a hivatkozások is csak ennek kontextusában nyernek értelmet. Dolgozataikban a diákok is felhasználják mások munkáit, ezért beszélnünk kell a felhasználás kategóriáiról, különös tekintettel a szabad felhasználás oktatási lehetőségeire és korlátaira ([65]), és nem csak általánosságban, hanem konkrét eseteket megbeszélve, mint például az Európai Unió Bíróságának ítélete az iskolai dolgozatban használt és közzétett fotó kapcsán ([66]), vagy a Jerusalema kihívással kapcsolatos szerzői jogok ([67]). Természetesen a megoldást is meg kell mutatunk, azaz célszerű ismertetni olyan oldalakat is, ahonnan zenéket, képeket, illetve videókat ingyenes le lehet letölteni (mint például a [68, 69] cikkekben ismertetettek, továbbá ncs.io, free-stock-music.com, danosongs.com, pixabay.com, depositphotos.com, unsplash.com, pexels.com, foter.com, gratisography.com stb.).

Beszélnünk kell az internetes szolgáltatások felhasználási feltételeiről, a számukra átruházott jogkörökről, továbbá a programok licencelési kategóriáiról, a letölthető digitális termékek használatáról és megosztásáról is ([70]), lehetőleg a diákok által is használt programokat és tartalmakat használva példaként.

7. Összefoglalás

Az információs társadalom fejlődésének következtében az információkezelés témakörében a diákokkal jelentős mennyiségű ismeretet szükséges megbeszélnünk, melyeknek jelen cikkben csak egy részét érintettük, különböző mélységekben, első sorban felvillantva bizonyos ismereteket, összefüggéseket és ezekhez köthető mindennapi példákat. Remélhetőleg ezek a tartalmak elgondolkodtatják a diákokat, segítik az egyes témák megértését elmélyíteni, az ismeretek megbeszélését a Bloom-féle taxonómia minél magasabb szintjére emelni, és ily módon a kívánt biztonsági és etikai normákat jobban kialakítani. Lehetőség szerint ezek kiegészíthetők a [8]-ban is említett más eszközökkel (virtuális valóság, szimuláció, társas- és szituációs játékok, színházi nevelés, pszichodráma stb.), illetve továbblépésként ilyenek kifejlesztésével. Végül pedig, más megközelítésből visszatérve a Bloom-féle taxonómiára, azért is fontos, hogy a diákok képesek legyenek az ismereteket megfelelő minőségben érteni, használni, értékelni, és megoldásokat kidolgozni a felmerülő problémákra, mert a fejlődő információs technológia kihívásainak a jelenlegi diákok általi kezelése a jövőben jelentősen befolyásolhatja az életminőséget.

Irodalom

1. Dzindzisz Sztefan: *Iskolákban tanítaná a kormány, mi a fake news*, 2018. január 15., https://www.napi.hu/tech/iskolakban-tanitana-a-kormany-mi-a-fake-news.654724.html?utm_source=index.hu&utm_medium=doboz&utm_campaign=link&fbclid=IwAR2i_lyETfx-hz96M0TEfQADNl1aQUS01iZYqLcOa6RWOfVdNp_-JPDx-gA& (utoljára megtekintve: 2021.11.09.)
2. Political Capital: *Álhírek elleni küzdelem az oktatásban*, 2019.11.28, https://politicalcapital.hu/hireink.php?article_read=1&article_id=2476 (utoljára megtekintve: 2021.11.09.)
3. Bálint Kata, Hunyadi Bulcsú, Krekó Péter, László Róbert, Molnár Csaba: *Álhírek elleni küzdelem az oktatásban*, Budapest, 2019. november, https://politicalcapital.hu/pc-admin/source/documents/pc_alhirek_elleni_kuzdelem_az_oktatasban_20191128.pdf (utoljára megtekintve: 2021.11.09.)
4. NJSZT: *Tananyagok*, https://njszt.hu/hu/form/tananyag-letoltese?tananyag=konyv_it_biztonsag_2019 (utoljára megtekintve: 2021.11.09.)
5. Dr. Abonyi-Tóth Andor, Dr. Turcsányi-Szabó Márta: *A digitális írástudás fejlesztésének lehetőségei*, https://dl-sulinet.educatio.hu/download/letoltheto-dokumentumok/Digitalis-irastudas.pdf (utoljára megtekintve: 2021.11.09.)
6. Európa Pont: *Harc az álhírek ellen*, https://europapont.blog.hu/2018/03/13/harc_az_alhirek_ellen (utoljára megtekintve: 2021.11.03.)
7. Freund Tamás: *Agyhullámok, tanulás, kreativitás*, In: Pedagógiai Esték, Szeged, 2016. 11. 22., https://www.youtube.com/watch?v=J13f5so7y2c (utoljára megtekintve: 2021.11.09.)
8. Törley Gábor: *A biztonságtudatosság oktatási módszerei: a bevonódás szerepe*, In: „Közigazgatás Napja Konferencia 2021" című tanulmánykötetben megjelent tanulmány, 2021.
9. Prusi: *Szakdolgozat az információk hitelességéről*, 2017. 09. 02., https://prusi.blog.hu/2017/09/02/szakdolgozat_az_informaciok_hitelessegerol_i (utoljára megtekintve: 2021.11.03.)
10. Hanula Zsolt: *Majdnem megtanultam három nyelvet egy hónap alatt*, https://index.hu/tech/2016/08/29/majdnem_megtanultam_harom_nyelvet_egy_honap_alatt/ (utoljára megtekintve: 2021.11.06.)

11. *Feketén-fehéren kiderült: szívesen osztunk meg kamuhíreket.* In: HVG, 2018.03.18. https://hvg.hu/tudomany/20180318_kamuhirek_terjedese_a_twitteren_mit_kutatas (utoljára megtekintve: 2021.11.06.)
12. Soroush Vosoughi, Deb Roy, Sinan Aral: *The spread of true and false news online*. In: SCIENCE, 2018.03.09., Vol 359, Issue 6380, pp. 1146-1151, DOI: 10.1126/science.aap9559, https://www.science.org/doi/10.1126/science.aap9559 (utoljára megtekintve: 2021.11.06.)
13. Lovász Dávid: *A véleménybuborék jelensége a közösségi médiában*. In: Kalauz, PTE Könyvtár és Tudásközpont, 2017. 12. 15., https://kalauz.lib.pte.hu/velemenybuborek-jelensege-kozossegi-mediaban/ (utoljára megtekintve: 2021.11.06.)
14. Marinov Iván: *Koronavírus: mit bizonyít a neten terjedő 1976-os cikk?* 2020. 08. 17., https://www.urbanlegends.hu/2020/08/koronavirus-mit-bizonyit-a-neten-terjedo-1976-os-cikk/ (utoljára megtekintve: 2021.11.03.)
15. *Együtt nyomoznak és perelnek Liptaiék: milliós csalás áldozatai lettek*. Bors, 2017.11.21., https://www.borsonline.hu/celeb/egyutt-nyomoznak-es-perelnek-liptaiek-millios-csalas-aldozatai-lettek/143306 (utoljára megtekintve: 2021.11.06.)
16. Mák Gabi: *Gyárts te is kamu híreket!* https://divany.hu/eletem/2018/02/22/gyarts_te_is_kamu_hireket/ (utoljára megtekintve: 2021.11.06.)
17. Marinov Iván: *Hogy állsz a tényekkel? – Igaz/Hamis kvíz gyerekeknek.* https://www.urbanlegends.hu/2021/10/annamarie-bon-fake-konyv-kviz/?fbclid=IwAR3X_s2lCSlYxE9vQanOB-jSQsGx4Rt3sDzsRah8mXn8FCT0egQWlKHw6ZA (utoljára megtekintve: 2021.11.06.)
18. *Ezt a vizsgát kötelezővé tennénk az érettségin: pofonegyszerű játékkal kell felismerni a kamuhíreket*. In: HVG, 2017. 07. 18., https://hvg.hu/tudomany/20170718_factitious_kamu_hirek_hoax_atveros_oldalak_alhirek_jatek (utoljára megtekintve: 2021.11.06.)
19. *Így verhet át a média!* In: 6 lépés https://youtu.be/w_HY4dIiON4 (utoljára megtekintve: 2021.11.06.)
20. *Erre is képes a mesterséges intelligencia!* 2019.12.13., https://youtu.be/tkimwiVzF5c (utoljára megtekintve: 2021.11.09.)
21. *Nem létező személyek készítése*. In: PosztmodeM, 2019. máj. 24., https://youtu.be/UyiIeV_B81c (utoljára megtekintve: 2021.11.09.)
22. Molnár Csaba: *Először csaltak ki pénzt deepfake hanggal, és rögtön van magyar szál*. 2019.09.05., https://index.hu/techtud/2019/09/05/eloszor_csaltak_ki_penzt_deepfake_hanggal_es_rogton_van_magyar_szal/?fbclid=IwAR2kSPHfMdIEzTNf9c2HmyfBymqUlyEWxt_j1Se4WQTFnjvLUJaNX9WlVrw (utoljára megtekintve: 2021.11.09.)
23. Fülöp Hajnalka: *Álhíre.*, In: GimiMore Plus, 2019.11.07., https://youtu.be/wxo_ib4WqEM?list=PLKd2de-K0pxnMNhY09DtNeAEfQs7ralw6 (utoljára megtekintve: 2021.11.06.)
24. Marinov Iván: *Kamuhírek az iskolában 1. rész: Hogyan tanítsuk a kamuhírek felismerését az iskolában?* 2017.06.16., https://www.urbanlegends.hu/2017/06/kamuhirek-iskolai-oktatasa/ (utoljára megtekintve: 2021.11.06.)
25. Marinov Iván: *Kamuhírek az iskolában 2. rész: a kritikus gondolkodás oktatása*. 2017.08.30., https://www.urbanlegends.hu/2017/08/kamuhirek-az-iskolaban-2-resz-a-kritikus-gondolkodas-oktatasa/?fbclid=IwAR0soMPfTvS8PLA49blerCcapZMugruOvfUSBpe0FSms9Rvs9Gesfq7WMU4 (utoljára megtekintve: 2021.11.06.)
26. Marinov Iván: *Kamuhírek az iskolában 3. rész: óravázlatok tanároknak*. 2017.10.20., https://www.urbanlegends.hu/2017/10/kamuhirek-az-iskolaban-3-resz-oravazlatok-tanaroknak/?fbclid=IwAR3EydaxTwL_KJ4gQKjPQz4-frudrlMxMgqzrv56zhMozuoOH60w79A-foE (utoljára megtekintve: 2021.11.06.)

27. Marinov Iván: *Kamuhírek az iskolában 4.: íme egy magyar nyelvű program!* 2017.11.08., https://www.urbanlegends.hu/2017/11/kamuhirek-az-iskolaban-4-ime-egy-magyar-nyelvu-program/?fbclid=IwAR0mweK-vJvL9sjy9waINWVnOvL7fv6v8_L0Zz4P_Wh1B-5tMPeeIempxrg (utoljára megtekintve: 2021.11.06.)
28. Laza Bálint, Pintér Dániel Gergő*: Így ismerd fel, és különböztesd meg a valódi szakértőt az álszakértőtől!* 2019.08.26., https://media20.blog.hu/2019/08/26/igy_ismerd_fel_es_kulonboztesd_meg_a_valodi_szakertot_az_alszakertotol?fbclid=IwAR2MjHCOIdAgJqWi6gLaN_WXtkbAuHYVBxS6iL2e_DWOrbtvJV02sszhyQc (utoljára megtekintve: 2021.11.06.)
29. Holló Csaba: *Álprofilok használata az etikus és biztonságos internethasználat tanításában*. In: INFODIDACT 2018 (2018.11.22-24), Informatika Szakmódszertani Konferencia, elektronikus kiadványa, 59-70, Zamárdi, Hungary, április, 2019, ISBN: 978-615-80608-2-0., http://konferenciak.inf.elte.hu/infodidact/InfoDidact18/Manuscripts/HCs.pdf (utoljára megtekintve 2021.11.03.)
30. Nemzeti Kibervédelmi Intézet: *Tájékoztató a sütikről*. https://nki.gov.hu/intezet/tartalom/tajekoztato-a-sutikrol/ (utoljára megtekintve: 2021.11.07.)
31. Kulcsár Bálint: *A digitális lábnyomaink*, 2016.03.03., https://www.adatvedelmirendelet.hu/internet/a-digitalis-labnyomaink/, (utoljára megtekintve: 2021.11.07.)
32. *Adatvédelmi értelmező szótár*. https://www.naih.hu/adatvedelmi-szotar (utoljára megtekintve: 2021.11.14.)
33. Alexin Zoltán: *A személyes adatok védelmének jogi, etikai és informatikai kérdései*. Typotex, 2011, http://publicatio.bibl.u-szeged.hu/1583/ (utoljára megtekintve: 2021.11.09.)
34. Nagy Attila Károly: *Nevesíthető a felhasználó az anonim böngészési adatokból is*. In: Index, 2017.08.04., https://index.hu/tech/2017/08/04/nevesitheto_a_felhasznalo_az_anonim_bongeszesi_adatokbol_is/?fbclid=IwAR2oIfzp64tPDRlCSczUlseJnayN0jrMutJ4wThELE8CxdWtjkTxVnq9ro4 (utoljára megtekintve: 2021.11.07.)
35. L. Sweeney: *Simple Demographics Often Identify People Uniquely*. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000., https://dataprivacylab.org/projects/identifiability/index.html (utoljára megtekintve: 2021.11.07.)
36. Madhumita Murgia: *Hogyan adták el adatbrókerek a személyiségemet*. In: TED, 2017.04., https://www.ted.com/talks/madhumita_murgia_how_data_brokers_sell_your_identity?language=hu (utoljára megtekintve: 2021.11.07.)
37. *Európai adatvédelmi jogi kézikönyv*. 2018, https://op.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1/language-hu/format-PDF/source-111961710 (utoljára megtekintve: 2021.11.09.)
38. Digitális Kutatások Intézete: *Megdöbbentő adatkísérlet*., 2018.10.03., https://www.facebook.com/digitaliskutatasok/videos/140021440286597/ (utoljára megtekintve: 2021.11.08.)
39. Janecskó Kata: *A biztonságérzetünket zúzta szét a Kaleta-ügy. Interjú Gyurkó Szilviával, az UNICEF korábbi gyermekjogi igazgatójával*. In: Index, 2020.07.10., https://index.hu/belfold/2020/07/10/kaleta_gabor_gyermekporno_szabalyozas_itelkezesi_gyakorlat_gyurko_szilvia_interju/ (utoljára megtekintve: 2021.11.08.)
40. *A posztolások veszélyei*. In: Kék Vonal Komputer Klubház Kecskemét, 2014.10.15., https://youtu.be/5ha0E-oJrOw (utoljára megtekintve: 2021.11.08.)
41. *Szexting*. In: Gyerek a neten, https://gyerekaneten.hu/szocikk/Szexting (utoljára megtekintve: 2021.11.08.)
42. Grünfelder Borbála, Holló Csaba: *Az informatikatanár lehetőségei az internetes zaklatás megelőzésében és kezelésében*. In: INFODIDACT 2019 (2019. 11. 21-23), Informatika Szakmódszertani Konferencia, elektronikus kiadványa, 73-86, Zamárdi, Hungary, január, 2020, ISBN: 978-615-80608-3-7., https://people.inf.elte.hu/szlavi/InfoDidact19/Manuscripts/GBHCs.pdf (utoljára megtekintve 2021.11.03.)

43. Horváth Bence: *Az internetes gyűlöletbeszéd nem tartozik a szólásszabadság hatálya alá az Emberi Jogok Európai Bírósága ítélete szerint*. 2017.07.20., https://444.hu/2017/07/20/az-internetes-gyuloletbeszed-nem-tartozik-a-szolasszabadsag-hatalya-ala-az-emberi-jogok-europai-birosaga-itelete-szerint (utoljára megtekintve: 2021.11.10.)
44. MarkMyProfessor, markmyprofossor.com (utoljára megtekintve: 2021.11.10., a megtekintés pillanatában nem elérhető)
45. *Tragédia a West-Balkán szórakozóhelyen*. https://hu.wikipedia.org/wiki/Trag%C3%A9dia_a_West-Balk%C3%A1n_sz%C3%B3rakoz%C3%B3helyen (utoljára megtekintve: 2021.11.08.)
46. *Emlékezzünk a West Balkán áldozataira Facebook csoport*. https://www.facebook.com/tragediawestbalkan/ (utoljára megtekintve: 2021.11.08.)
47. *Diszkótragédia: a közösségi média leszerepelt?* 2011.01.16., https://hvg.hu/itthon/20110116_kozossegi_media_diszkotragedia (utoljára megtekintve: 2021.11.08.)
48. *Előfordulhatna-e egy Sincai-ügy a kolozsvári magyar középiskolákban?* In: Transindex, 2015.03.05., https://eletmod.transindex.ro/?cikk=24990 (utoljára megtekintve: 2021.11.09.)
49. *Hogyan kezelhetjük elhunyt szeretteink online hagyatékát?* Nemzeti Média- és Hírközlési Hatóság, 2019.08.13., https://nmhh.hu/cikk/206320/Hogyan_kezelhetjuk_elhunyt_szeretteink_online_hagyatekat? (utoljára megtekintve: 2021.11.09.)
50. Schleer Tamás: *Digitális illúziónk*. In: TEDxYouth@Budapest, 2016.10.27., https://youtu.be/biBOt61uesE?list=PLDlsemvZx1fJywh1gXT8-tPEPy3B1qgKY (utoljára megtekintve: 2021.11.09.)
51. *Megteremtené az elhunyt családtaggal való időtöltés lehetőségét egy magyar alapítású cég*. HVG, 2020. június. 11., https://hvg.hu/tudomany/20200611_realic_hybri_recall_funkcio_kiterjesztett_valosag_virtualis_valosag_ar_vr (utoljára megtekintve: 2021.11.09.)
52. Bodnár Zsolt: *Virtuális valóságban találkozott újra halott lányával egy koreai nő*. https://qubit.hu/2020/02/09/virtualis-valosagban-talalkozott-ujra-halott-lanyaval-egy-koreai-no (utoljára megtekintve: 2021.11.09.)
53. Karapándzsity Kristóf: *Sors-szinkópa*. https://www.hashtagmagazin.net/elmerengo/sors-szinkopa (utoljára megtekintve: 2021.11.09.)
54. Dr. Kulcsár Zoltán, Útmutató *biztonságos jelszókezeléshez*. 2019.03.22., https://www.xn--adatvdelem-f7a.hu/2019/03/utmutato-biztonsagos-jelszokezeleshez/ (utoljára megtekintve: 2021.11.09.)
55. Major Szabolcs: *Másodpercenként 100 milliárd jelszót fejt meg egy gép: a tiéd sincs biztonságban*. https://computerworld.hu/biztonsag/masodpercenkent-100-milliard-jelszot-fejt-meg-egy-gep-a-tied-sincs-biztonsagban-284833.html (utoljára megtekintve: 2021.11.09.)
56. *Hogyan készíts biztonságos jelszavakat?* 2019. 09. 25., https://hellobiznisz.hu/hogyan-keszits-biztonsagos-jelszavakat/ (utoljára megtekintve: 2021.11.09.)
57. *Védekezz duplán: ez az 5 legjobb app a fiókjaid védelmére*. 2020 01.02., https://pcworld.hu/pcwpro/ketfaktoros-belepes-autentikator-appok-tipp-272545.html (utoljára megtekintve: 2021.11.09.)
58. *Mi az a kétfaktoros azonosítás és hogyan tudom beállítani?* Nexus Learning, https://support.nexiuslearning.com/kb/00023 (utoljára megtekintve: 2021.11.09.)
59. Major Szabolcs: *A Microsoft szerint nem biztonságos a mobilos kétfaktoros azonosítás*. 2020.11.17., https://computerworld.hu/biztonsag/a-microsoft-szerint-nem-biztonsagos-a-mobilos-ketfaktoros-azonositas-287022.html (utoljára megtekintve: 2021.11.09.)
60. Fekete Gábor: *SIMultán átverés: figyelj oda a kártyádra!* 2021.02.04, https://pont-most.hu/gep/simultan-atveres-figyelj-oda-a-kartyadra/ (utoljára megtekintve: 2021.11.09.)
61. *Alapvető információk a biometrikus azonosítás témájáról*. Biometrikus, https://biometrikus.hu/ (utoljára megtekintve: 2021.11.10.)

62. Magyarósi Csaba: *Hogy NE lopják el ONLINE a pénzed?* Karantén Kisokos, https://youtu.be/aEykrr1mjow (utoljára megtekintve: 2021.11.09.)
63. *Kerettanterv Digitális kultúra 5–8. évfolyam*. https://www.oktatas.hu/pub_bin/dload/kozoktatas/kerettanterv/Digitalis_kultura_F.docx (utoljára megtekintve: 2021.11.09.)
64. *Kerettanterv Digitális kultúra 9–11. évfolyam*. https://www.oktatas.hu/pub_bin/ dload/kozoktatas/kerettanterv/Digitalis_kultura_K.docx (utoljára megtekintve: 2021.11.09.)
65. Dr. Richlach Mónika: *Az oktatási célú szabad felhasználás*. Merosus, 2020.04.14., https://merosus.hu/foto-jog/2020/04/az-oktatasi-celu-szabad-felhasznalas/ (utoljára megtekintve: 2021.11.09.)
66. Paál Vince: *Az EU Bírósága az internetes fotók jogszerű felhasználásáról döntött*. Nemzeti Média- és Hírközlési Hatóság Médiatanács Médiatudományi Intézete, https://nmhh.hu/cikk/197636/Az_EU_Birosaga_az_internetes_fotok_jogszeru_felhasznalasarol_dontott (utoljára megtekintve: 2021.11.09.)
67. Ronai András: *Jerusalema kihívás: miért kell engedélyt kérni, mikor kell fizetni, kit kell keresni?* 2021.05.07., https://dalszerzo.hu/2021/05/07/jerusalema-oromtanc-kihivas/ (utoljára megtekintve: 2021.11.09.)
68. *Honnan szerezhetünk jogtisztán zenéket, hangokat, zörejeket?* https://buvosvolgy.hu/tudastar/cikk/Honnan_szerezhetunk_jogtisztan_zeneket_hangokat_zorejeket?fbclid=IwAR1_K1WoCtl6e8_fEsymP-9ZcWXGhVBMz3sX0EeeOrIuGXyHDmVYiFWsnR8 (utoljára megtekintve: 2021.11.09.)
69. *Facebook Hanggyűjtemény*. https://business.facebook.com/creatorstudio/?tab=ct_sound_collection&collection_id=all_pages (utoljára megtekintve: 2021.11.09.)
70. *A szerzői joggal kapcsolatban gyakran ismételt kérdések*. https://euipo.europa.eu/ohimportal/hu/web/observatory/faqs-on-copyright-hu (utoljára megtekintve: 2021.11.09.)