

JOGI FÓRUM PUBLIKÁCIÓ

A COVID19-világjárvány alatti távoktatás egyes adatvédelmi kérdései

Szerző:

Némethné dr. Dancs Tímea

bírósági titkár

Kézirat lezárva: 2025.január 27.

„Olyan lesz a jövő, mint amilyen a ma iskolája.”

(Szent-Györgyi Albert)

1. Bevezetés

A SARS-COV-2 vírus által okozott Covid19 elnevezésű betegséget, közismert nevén a koronavírus, a kínai Wuhan nevű városban azonosították először 2019-ben.¹ Talán a hatalmas földrajzi távolság tette elképzelhetetlenné, hogy egyszer Magyarországon is megjelenjen a betegség. A járvány azonban korábban soha nem látott ütemben kezdett el terjedni és 2020. március 4-én hivatalosan is regisztrálták az első koronavírusos beteget hazánkban. Az orvostudomány képviselői megállapították, hogy a vírus cseppfertőzés útján terjed. Az ember a saját családján kívül több helyen is kapcsolatba lép másokkal, így a munkahelyén, az iskolában, a mindennapi bevásárlást intézve, sportolás közben vagy a hobbijának hódolva csak, hogy a legegyszerűbbeket említsem, amely rohamosan növelte a betegség terjedésének sebességét egy országon belül, a kontinensek közötti akadálymentes utazás pedig azt eredményezte, hogy 2020. márciusára egy világjárvánnyal álltunk szemben. Hamar nyilvánvalóvá vált, hogy a betegség terjedésének megállítása attól várható, ha az emberek minél kevesebbet érintkeznek egymással személyesen. Mindeközben megoldást kellett találni arra, hogy az emberek a mindennapi teendőiket ellássák, hiszen a mindennapi élet fenntartásához szükség volt az emberi munkaerő megtartására. A koronavírus 2020. márciusában kezdődő első hullámának nevezett időszakban a gyermekek szinte tünetmentesen, vagy csak enyhe tünetekkel estek át a betegségen, megnövelve ezzel annak esélyét, hogy észrevétlenül is megfertőzik egymást az oktatási intézményekben. Emiatt az oktatás volt az első terület, ahol biztosítani kellett annak lehetőségét, hogy az oktatás a tanárok és a diákok személyes jelenléte nélkül valósuljon meg. Magyarországon 2020. március 11-én országos veszélyhelyzetet hirdettek ki, amellyel különleges jogrend lépett életbe: a békétől, az állami

¹Forrás: <https://hu.wikipedia.org/wiki/Covid19> utolsó letöltés: 2021.november 7.

működés általános szabályaitól eltérő időszak.² A kormány intézkedései között első lépésként szerepelt az olyan intézmények bezárása vagy működésük biztosítása a lehető legkevesebb számú személyzettel, ahol a mindennapokban nagy számban lépnek kapcsolatba egymással emberek. Ide tartoztak az oktatási intézmények is. Az általános iskolás és középiskolás korú gyermekek személyes jelenlét nélküli oktatásának folyamatos biztosítására tehát az intézményeknek alternatívát kellett kidolgozniuk, és ez volt a feladat a felsőoktatásban is, hiszen ott még több ember találkozik, akik ráadásul az ország különböző helyeiről érkeznek, sőt sok esetben akár külföldről utaznak ide tanulni. Kézenfekvő volt a távoktatás bevezetése minden oktatási intézményben. A távoktatás, mint oktatási forma első fontos jellemzője, hogy a diákok és a tanárok földrajzilag nem egy helyen tartózkodnak. A másik nagyon fontos jellemzője, hogy a fókusz a tanárról a diákra helyeződik át, a hagyományos oktatást ugyanis rendre az egyirányú kommunikáció jellemzi a tanár irányából a diákok felé. A távoktatás során az önálló tanulás a jellemző, ezáltal nő a diák, a hallgató felelőssége, hiszen nagyobb részt rajta múlik, hogyan sajátítja el az iskola által biztosított tananyagot. A távoktatás nem jelent egyet a digitális oktatással. Az internet megjelenése előtt is működött már ez az oktatási forma, akkor még a hallgatók, diákok postai úton kapták meg a tananyagot és csak a vizsgákon jelentek meg személyesen. Az infokommunikációs technológiák (továbbiakban: IKT) fejlődésével a levelezés útján folytatott távoktatás szinte teljesen eltűnt, manapság csak azokban a népelességekben folytatódik, ahol az internethez való hozzáférés problémás vagy egyáltalán nem megoldható.

Jelen tanulmány a Covid19-járvány alatt megvalósult online távoktatást vizsgálja meg adatvédelmi szempontból. A modern korban szinte minden gazdasági és társadalmi területen, valamint a jog, a politika vagy a közigazgatás területén is felértékelődött az infokommunikációs eszközök alkalmazása, a járvány során pedig ezen eszközök használata segítette a távolról végezhető munka lehetőségének biztosítását is. Hazánkban a járvány megjelenésekor az oktatás volt az első olyan terület, ahol a fentiek mintájára bevezették a távoktatást. A Kormány a koronavírus első hullámában az 1102/2020. számú határozatában³ szabályozta az általános iskolai és középiskolai nevelés-oktatás tantermen kívüli, digitális munkarendjét 2020. március

240/2020. (III. 11.) Korm. rendelet a veszélyhelyzet kihirdetéséről Hatálytalan: 2020. június 18-tól

3.Hatályát veszttette: 2020. augusztus 14.

16. napjától.⁴ Ezt úgy határozta meg, hogy kimondta, hogy a tananyag kijelölése, a tanulási folyamat ellenőrzése és támogatása a pedagógusok és a tanulók online kapcsolatában történik úgy, hogy az alkalmas legyen a tanuló tanulmányi követelményeinek teljesítésére. Ennek végrehajtása érdekében módszertani ajánlás kiadására került sor. Az általános és középiskolai oktatás mellett a 41/2020. (III. 11.) Korm. rendeletben⁵ tiltották meg a felsőoktatási intézmények hallgatók általi látogatását. A rendelet azonban kimondta, hogy a látogatási tilalom alatt is biztosítani szükséges a felsőoktatási intézmények működését, ennek kivitelezését pedig az intézményekre bízta. Ebben a helyzetben azonban az egyetemek sem tudtak más döntést hozni, mint azt, hogy az infokommunikációs eszközöket hívják segítségül az oktatás során és a legtöbb hazai egyetem áttért a digitális távoktatásra. A koronavírus járvány harmadik hullámának nevezett időszakban (2021. május) a felsőoktatásban törvényi szintre emelték az online távoktatást, amikor a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény (továbbiakban: Nftv.) rendelkezéseit kiegészítették a zárt rendszerű elektronikus távolléti oktatás fogalmával⁶. Eszerint ez a képzés olyan formáját jelenti, „*amelyben az elméleti képzési ismeretanyag oktatása digitális tananyaggal, továbbá az oktató és hallgató együttműködése az informatikai hálózaton (internet, intranet) keresztül zárt rendszerű távoktatási képzésmenedzsment-rendszerrel valósul meg, amelynek során az oktató, az oktatásszervező és a képzésben részt vevő hallgató vagy személy közös kommunikációs eszköze a számítógép és az informatikai hálózat, továbbá a zárt rendszerű távoktatási képzésmenedzsment-rendszer és a tanulmányi rendszer*”⁷. A törvénymódosítás részletes indoklása szerint a módosítás alapján a jogszabály elvi értelemben különbözteti meg a törvényben már korábban is szereplő távoktatás fogalmát és elkülöníti a személyes érintkezést nem igénylő távolléti oktatás fogalmától.

A fenti folyamat tehát magával hozta az oktatási intézményeknek és a pedagógusoknak a digitális tanulásszervezésre történő átállását. A pedagógusok azon részének, akik már korábban is alkalmazták és szorgalmazták az IKT eszközök alkalmazását az oktatásban, ez óriási lehetőség volt, azon részüknek viszont, akik a hagyományos pedagógia hívei voltak, ez nagy kihívást jelentett. A pedagógusok mellett a diákok és a szülők is nagy kihívás előtt álltak. Sok ezer

4.Holle A. (2020) Oktatási rendszerek az új koronavírus járvány idején. Budapest, Országgyűlés Hivatala.

5Hatályát veszítette:2020. szeptember 1.

62020. évi CXLVIII. törvény a felsőoktatás szabályozására vonatkozó és egyes kapcsolódó törvények módosításáról

7Vö.: Nftv. 108. § 49. pont

szülőnek kellett egyik napról a másikra megoldania kisiskolás gyermeke felügyeletét, emellett pedig az önállóan még tanulni nem tudó gyermekkel együtt kellett tanulni, segíteni a gyermeknek használni a digitális oktatást lehetővé tevő alkalmazásokat, úgy, hogy sok esetben ők is akkor találkoztak vele először. Ennél még nagyobb problémát okozott az, hogy a hátrányos helyzetű településeken élő családok százainál nem volt megfelelő számítógépes eszköz, sem internet - sok esetben áram sem- amivel részesei maradhattak az oktatás folyamatosságának. A Kormány próbált segítséget nyújtani azon tanulóknak, akik nehézségekbe ütköztek az online oktatással kapcsolatban, például azzal, hogy a tantermen kívüli, digitális oktatás elérése érdekében lehetővé tette, hogy az otthoni internet-szolgáltatást ingyenesen vehessék igénybe az általános- és középiskolai diákok családjai, valamint a pedagógusok is. Az előzőekből kiderült, hogy az oktatási intézményeknek nem volt választása abban, hogy áttérnek-e az online távoktatásra, azonban még a távoktatás technikai feltételeinek teljesítésére sem voltak felkészülve az iskolák, nemhogy annak adatvédelmi oldalát ismerték volna.⁸

A tanulmány számos olyan kérdést körbejár, ami valamennyi oktatási szintet érintette, de nagyobb részében az általános és középiskolai oktatás adatvédelmi problémáit vizsgálja, figyelemmel arra, hogy ezen a szinten több kérdés is felmerült a kötelező távoktatás során. Ennek egyik indoka, hogy az érintettek nagy része kiskorú, másik pedig az, hogy az oktatás ezen a szintjén a távoktatás nem volt jellemző oktatási forma, illetve az online tér használata a tanítás során sem volt még gyakori, míg a felsőoktatásban a távoktatás működött és működik is, annak csak a formája változott meg a vírus során. Ezek mellett azonban kitér az egyetemi oktatást érintő kérdések közül is néhányra, hiszen a tisztán online oktatás az egyetemeken is csak a járvány miatti kényszerhelyzetben kezdett el működni, adatvédelmi kérdések pedig ott is felmerültek. A fenti kérdéseket a vonatkozó Európai Uniós és hazai jogszabályokon keresztül próbálja meg a szerző megválaszolni, figyelemmel a nemzetközi és a hazai gyakorlatra is, segítségül hívva a hazai adatvédelmi hatóság állásfoglalásait.

⁸Fekete, T., – Porkoláb, Ádám. (2020). Karanténpedagógia a magyar közoktatásban. Iskolakultúra, 30(9), 96-112.

2. Az online távoktatás adatvédelmi kérdései

2.1. A távoktatásra vonatkozó adatvédelmi jogszabályok

Már a járvány előtti időszakban is megfigyelhető volt az a jelenség, hogy egy természetes személynek egyre kevesebb döntési lehetősége van a tekintetben, hogy részese lesz-e a digitális életnek, elég, ha arra gondolunk, hogy már a legtöbb munkahelyen e-mailen történik a kommunikáció vagy az oktatási intézményekben már digitális naplót használnak. A kötelezően bevezetett online távoktatás pedig egyértelműen korlátozta az iskolaköteles gyermekek, illetve a felsőoktatási intézmények hallgatóinak információs önrendelkezési jogát, hiszen aki nem vett részt a digitális távoktatásban az nagy hátrányt szenvedett. Éppen ezért is vált még fontosabbá az adatvédelem erősítése, a felhasználók ösztönzése a tudatos internethasználatra.

Az adatvédelem területén 2018. május 25. jelentős napnak számított, mivel - a 2016. április 27. napján történt hatályba lépést követő türelmi időszak után - e naptól kezdve kellett alkalmazni az Európai Parlament és Tanács 2016/679 rendeletét a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) azaz az angol elnevezésből⁹ eredően a GDPR-t. A rendelet preambuluma úgy fogalmaz meg a szabályozás fontosságát, ami abban áll, hogy a személyes adatok védelméhez való jog egy mindenkit megillető alapvető jog.¹⁰ Ez nem abszolút jog, annak korlátozását azonban a szükségesség és arányosság elve alapján, minden más alapjoggal összhangban kell értelmezni.¹¹ Az adatvédelmi rendeletet alkalmazni kell minden olyan esetben, ahol személyes adatok részben vagy egészben automatizált módon történő kezelése történik, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelése esetén is, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánunk tenni.¹² A GDPR meghatározza a személyes adat fogalmát, amely szerint „személyes adat az azonosított vagy azonosítható természetes személyre vonatkozó bármely információ”.¹³ Az a természetes személy, aki a személyes adatai alapján azonosítható, az az

⁹General Data Protection Regulation.

¹⁰Lásd GDPR (1) preambulumbekkezdés.

¹¹Lásd GDPR (4) preambulumbekkezdés.

¹²Lásd GDPR 2. Cikk (1) bekezdés.

¹³GDPR 4. Cikk (1) bekezdés.

érintett. A GDPR alapján azonosítható egy természetes személy, „*aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható*”¹⁴A fentiek alapján kétséget kizáróan megállapítható, hogy a diák, hallgató neve és egyéb azonosító adatai, az írásbeli és szóbeli számonkérések tartalma, a tanuló órai hozzászólásai, eredményei vagy a fényképe személyes adatnak minősülnek, ugyanígy a pedagógus által a tanórák keretében elmondottak kapcsán a hangja és a képmása is. Adatkezelési tevékenységnek minősül a személyes adatok gyűjtése, rögzítése, rendszerezése, tagolása, tárolása, átalakítása vagy megváltoztatása, lekérdezése, betekintése, felhasználása, közlése, továbbítása, terjesztése vagy egyéb módon történő hozzáférhetővé tétele, törlése, illetve megsemmisítése, illetve adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése is¹⁵. Nem kérdéses ezután, hogy valamennyi oktatási intézmény tevékenysége során adatkezelést végez, hiszen az ott tanuló diákok nevéről, születési adatairól nyilvántartást vezetnek, a felsőoktatási intézményekben szintén ezen adatok tárolva vannak, egy vizsga alkalmával pedig azonosítani is szükséges a hallgatót, amit fényképes igazolvánnyal vagy a leckekönyvvel tettek meg korábban. Ez alapján tehát megállapíthatjuk, hogy valamennyi oktatási intézmény köteles a GDPR szabályainak megfelelően kezelni a megszerzett személyes adatokat, tehát valamennyi oktatási intézmény, minden adatkezelése az adatvédelmi rendelet hatálya alá tartozik és tartozott a Covid-járvány ideje alatt is. A GDPR mellett a kötelező távoktatás során történő adatkezelésre vonatkozó fontos szabályokat határozott meg az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Infotv.). Ahogyan a jelenleg hatályos Infotv. is, úgy a járvány alatt hatályban lévő is részletesen felsorolta azokat az eseteket, amikor azt a GDPR hatálya alá tartozó adatkezelések esetén alkalmazni kell, ezek tehát kiegészítették a GDPR szabályait.¹⁶ Az alapfokú oktatási intézmények számára a köznevelésről szóló 2011. évi CXC. törvény (továbbiakban: Köznevelési törvény), a felsőoktatási intézmények számára pedig az Nftv. határozott meg speciális adatkezelésre vonatkozó szabályokat, így az oktatási intézmények által kötelezően nyilvántartandó adatok körét is, de az oktatási tevékenység során végzett adatvédelmi tevékenység szabályozására - gondolok itt

¹⁴Infotv. 3.§ 1a. pont.

¹⁵Infotv. 3.§ 10. pont.

¹⁶Vö. Infotv. 2. § (2) és (4) bekezdés a törvény hatályáról

egy írásbeli vizsga anyagának tárolására, megőrzésére, vagy egy vizsgázó személyazonosságának ellenőrzésére - nem tartalmaztak rendelkezéseket, ezért kellett a GDPR, valamint a hazai jogszabályok közül az Infotv. vonatkozó részeit alkalmazni.

2.2. Az adatkezelő az online távoktatásban

A GDPR az adatkezelő meghatározásakor úgy fogalmaz, hogy „*adatkezelő az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza. (...)*”¹⁷ A fenti fogalom meghatározásból megállapíthatjuk, hogy az online oktatás során az adatkezelés célját az oktatási intézmények határozták meg, figyelemmel arra, hogy az oktatás alsóbb szintjeit tekintve ez a cél az iskolai nevelés és oktatás, mint köznevelési alapfeladat ellátása¹⁸, míg az oktatás felsőbb szintjein az Nftv. szerinti felsőoktatás biztosítása. Ki kell emelni, hogy a digitális távoktatás esetén nem a pedagógus, hanem az önálló jogi személyiséggel rendelkező oktatási intézmény tekinthető adatkezelőnek, aki köteles az adatkezelés céljának tükrében a cél eléréséhez szükséges eszközök meghatározására. Az adatkezelő pontos meghatározása azért fontos, mert az ő feladata az adatkezelésről megfelelő tájékoztatás nyújtása és az egyéb adatvédelmi követelményeknek való megfelelés biztosítása, ezek elmulasztásáért felelősségre is az oktatási intézmény vonható. Ezzel szemben a pedagógus használja fel a digitális oktatás során kezelt személyes adatokat az adatkezelés céljától eltérő, tehát a közfeladata ellátásán kívüli bármilyen más célból - így például jogosulatlanul továbbítja harmadik személy részére - magatartása jogellenes adatkezelésnek, bizonyos esetekben bűncselekménynek is minősülhet.¹⁹

2.3. Az adatkezelés alapelvei és azok gyakorlati alkalmazása az online távoktatás során

Az adatkezelési tevékenység során fontos kérdés az adatkezelésnek a jogszabályban meghatározott alapelveknek való megfelelése. Az GDPR 5. cikkében felsorolt alapelvek közül három alapelvet szeretnék kiemelni. Az egyik a GDPR. 5. cikk (1) bekezdés a) pontjában foglalt alapelv, amely szerint „*a személyes adatok kezelését jogszerűen és tisztességesen, valamint*

17Vö. GDPR 4. cikk 7.pont

18Vö. Köznevelési tv. 2.§

19NAIH Tájékoztató a digitális távoktatás adatvédelmi és adatbiztonsági vonatkozásairól ügyszám: NAIH/2020/7127

az érintettek számára átlátható módon kell végezni.” A jogszerű adatkezeléshez elengedhetetlen a megfelelő jogalap meghatározása, mely jogalapokat az általános adatvédelmi rendelet 6. cikk (1) bekezdése taxatív módon sorolja fel. „Ebből fakadóan az adatkezelő az általános adatvédelmi rendelet 6. cikk (1) bekezdés a)-f) pontjában meghatározott jogalapok valamelyikére alapozhatja adatkezelésének jogszerűségét, ezen jogszerűségi feltételek teljesülésének hiányában - pusztán valamely nemzeti jogi rendelkezés - az adatkezelés jogszerűségének alátámasztására nem elégséges, még akkor sem, ha maga az általános adatvédelmi rendelet egyes adatvédelmi jogalapok vonatkozásában kifejezetten megköveteli a nemzeti jogalkotói intézkedést.”²⁰A tisztességesség alapján az adatkezelés a jogszabályokban foglaltak szerint és az érintett érdekeinek szem előtt tartásával kell, hogy történjen. Az átláthatóság azt jelenti, hogy a személyes adatok kezeléséről megfelelő tájékoztatást kell nyújtani az érintett részére, amelyet közérthető és egyszerű nyelvezettel kell megtenni, s a tájékoztatónak könnyen hozzáférhetőnek kell lennie. A GDPR 5. cikk (1) bekezdés b) pontja alapján az adatok kezelése csak meghatározott, egyértelmű és jogszerű célból történhet és tilos az adatoknak a meghatározott és az érintettel közölt célokkal össze nem egyeztethető módon történő kezelése. Ez azt jelenti, hogy a digitális oktatás során csak olyan adatok kezelése lehetséges, ami a tanítás lebonyolítása, mint cél megvalósításához feltétlenül szükséges. Az adattakarékosság elve előírja, hogy a kezelt személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek és a szükségesre kell korlátozódniuk.²¹ Ehhez kapcsolódik egy másik alapelv is, a korlátozott tárolhatóság elve, melynek értelmében az adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé²², tehát online oktatás során az otthoni feladatként meghatározott videó felvétel készítése esetén annak tárolására csak a feladat ellenőrzéséig van szükség.

20NAIH/2019/51/11. számú határozata 14. oldal 3. bekezdés

21Vö. GDPR 5. cikk (1) bekezdés c) pont

22Vö. GDPR 5. cikk (1) bekezdés e) pont

2.4. Az adatkezelés jogalapja

Az adatkezelés során nagyon fontos annak meghatározása, hogy az adatkezelő milyen jogalapon kezeli az érintett személyes adatait, mivel ez teszi jogszerűvé az adatkezelést. Az adatvédelmi rendelet 6. cikke tartalmazza azokat a jogalapokat, amelyek valamelyikének fennállása szükséges ahhoz, hogy egy adatkezelő jogszerűen végezzen adatkezelést. Az oktatási tevékenység, így az online távoktatás során álláspontom szerint két jogalap alkalmazhatósága merülhet fel a személyes adatok kezelésének jogszerűségének igazolására. Egyik a GDPR 6. cikk (1) bekezdés c) pontjában foglalt jogalap, amely szerint az adatkezelés akkor és annyiban jogszerű, ha az az adatkezelő jogi kötelezettségének teljesítéséhez szükséges, tehát az adatkezelést egy jogszabály teszi kötelezővé számára. A másik alkalmazható jogalapot a GDPR 6. cikk (1) bekezdés e) pontja rögzíti, mely szerint az adatkezelés akkor jogszerű, ha az közérdekű feladat végrehajtásához szükséges. A digitális távoktatás esetén az adatkezelés célja az alap- és középfokú oktatási intézményekben - a Köznevelési tv. alapján - az iskolai nevelés és oktatás, mint köznevelési alapfeladat ellátása, a felsőoktatási intézményekben pedig az Nftv. szerinti felsőoktatás biztosítása. Erre tekintettel az előzőekben említett tevékenységek közfeladatnak minősülnek, ezért ezeknek az adatkezeléseknek egyik jogalapjaként a GDPR 6. cikk (1) bekezdés e) pontja szolgálhat. Problémát itt az okozhat, hogy mind a Köznevelési törvény, mind az Nftv. felsorolja azokat az adatköröket, amelyeket az intézményeknek kezelniük kell. Itt tehát nem egyértelmű, hogy az adatok kezelése a GDPR 6. cikk (1) bekezdés c) vagy e) pontján alapul-e, hiszen ebben az esetben az oktatási intézményeknek jogszabály írja elő a kötelezettséget az adatkezelésre, ugyanakkor közfeladat ellátását is szolgálják az adatok, hiszen ezek nélkül nem tudnák ellátni az oktatási tevékenységüket az intézmények. Abban az esetben, ha jogszabály állapítja meg tételesen a kezelendő adatok körét, akkor már a jogalkotó vizsgálat alá vette és mérlegelte, hogy melyek azok az adatok, amelyek feltétlenül szükségesek a közfeladat ellátásához. Ebben az esetben a személyes adatok kezelésének a jogalapja a GDPR 6. cikk (1) bekezdés c) pontja. Ugyanakkor ezek között a személyes adatok között vannak olyan személyes adatok, amelyek nincsenek vagy nem konkrétan vannak meghatározva jogszabályban, de az oktatási feladat ellátásához szükségesek, ezen személyes adatok kezelése így GDPR 6. cikk (1) bekezdés e) pontján alapul. ²³

²³Certicky Mária: A digitális oktatás egyes adatvédelmi kérdései, avagy előrehozta-e a COVID-19 a jövőt? In: Infokommunikáció és Jog, 2020/1. szám, 33-37. o.

2.5. Az érintettek jogai, különös tekintettel az előzetes tájékoztatáshoz való jogra

Az érintetteket megillető legteljesebb jogosultság maga az információs önrendelkezési jog, amely valamennyi érintetti jogot magában foglalja. Ez alapján az érintett jogosult dönteni a személyes adatival kapcsolatban, azokkal ő maga rendelkezhet. Eszerint például adatot szolgáltathat magáról és jogosult ennek a felhasználásáról információt szerezni. *„Az érintetti jogok alapvető rendeltetése, hogy a GDPR 5. cikke szerinti személyes adatok kezelésére vonatkozó, az adatkezelők által betartandó alapelvek az egyes érintetti jogokon keresztül tudnak érvényesülni. Így például az átláthatóság és tisztességes adatkezelés alapelve a tájékoztatás és a hozzáférés jogában, az adattakarékosság és a korlátozott tárolhatóság elve a törléshez, illetve az elfeledtetéshez való jogban, a pontosság alapelve a helyesbítéshez, valamint az adatkezelés korlátozásához való jogban nyilvánul meg.”²⁴*

A GDPR az alábbi érintetti jogokat sorolja fel: a tájékoztatáshoz való jog²⁵, a hozzáféréshez való jog²⁶, a helyesbítéshez való jog, valamint a törléshez és elfeledtetéshez való jog²⁷, az adatkezelés korlátozásához való jog²⁸, az adathordozhatósághoz való jog²⁹, a tiltakozáshoz való jog és az automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást is ³⁰. Ezek közül az online oktatásban valamennyi jognak érvényesülnie kell ahhoz, hogy az adatkezelők által végzett adatkezelés jogszerű legyen, azonban a digitális oktatás során a legfontosabb, hogy az érintettel előzetes tájékoztatáshoz való joga érvényesüljön. Ennek indoka az, hogy amennyiben az érintett nem kap megfelelő tájékoztatást a személyes adatainak kezeléséről, az az összes többi jogosultság érvényesítésétől elzárja őt.

24Bíró János – Kiss Ernő – Tari István – Vass Norber: Jogalapok, érintetti jogok, Szakmai lektor: Dr. Péterfalvi Attila, A kézirat lezárásának dátuma: 2018. szeptember 25. Kiadja: NKE, 2018 Felelős kiadó: Prof. Dr. Kis Norbert Dékán

25GDPR 13-14.cikk

26GDPR 15.cikk

27GDPR 16-17.cikk

28GDPR 18.cikk

29GDPR 20.cikk

30GDPR 21-22.cikk

2.5.1. Az érintett előzetes tájékoztatáshoz való joga

A GDPR 13-14. cikkeiben foglalt előírásnak³¹ megfelelően minden esetben, de álláspontom szerint az online távoktatás keretében, különösen a kiskorú érintettek személyes adatain végzett adatkezelés esetén nagyon fontos, hogy érvényesüljön az érintett jogai közül az előzetes tájékoztatáshoz való jog. Az alapfokú oktatási intézmények esetében, de a középiskolákban is az adatkezeléssel érintett személy kiskorú, így az ő vonatkozásában fontos szerepe van a törvényes képviselőnek, akinek az adatkezelés megkezdésekor meg kell ismernie az adatkezeléssel kapcsolatos tudnivalókat, hiszen a kiskorúak még nem rendelkeznek olyan belátási képességgel, amely alapján a személyes adataik fölötti önrendelkezési jogukat gyakorolni tudják. Felsőoktatási intézmények esetén az érintettek már nagykorú, cselekvőképes személyek, akik maguk gyakorolják az adatkezeléshez kapcsolódó jogukat. A megfelelő tájékoztatás érvényesülésének akkor is jelentősége van, ha az adatkezelés jogalapja nem az érintettől származó hozzájárulás. A GDPR a tájékoztatási kötelezettség körében különbséget tesz aszerint, hogy a személyes adatokat kitől gyűjti az adatkezelő, magától az érintettől vagy mástól. Ha a személyes adatokat az érintettől gyűjti az adatkezelő, akkor az érintettet legkésőbb a személyes adatok megszerzésének időpontjában tájékoztatni kell, amelynek ki kell terjedni az az adatkezelő és - ha van ilyen - az adatkezelő képviselőjének a személyére és elérhetőségeire, illetve, ha az adatkezelőnél kinevezésre került, úgy az adatvédelmi tisztviselő elérhetőségeire is. Nagyon fontos közölni az érintettel a személyes adatok kezelésének célját, valamint az adatkezelés jogalapját. Tájékoztatást kell nyújtani továbbá arról, hogy a személyes adatokat továbbítják-e harmadik személynek, vagy adott esetben harmadik országba vagy nemzetközi szervezet részére. Fontos, hogy az adatkezeléssel érintett ismerje a jogait, tudja azt, hogy az adatkezelő által kezelt adatokhoz bármikor hozzáférhet,³² kérheti ezen adatok helyesbítését³³ vagy törlését³⁴. Ezekről az információkról az adatkezelőknek kötelező átlátható és érthető, valamint könnyen hozzáférhető adatkezelési

³¹Tudniillik a GDPR e két cikke fogalmazza meg az adatkezelő előzetes tájékoztatási kötelezettségét azzal, hogy különbséget tesz az adatkezelések között a szerint, hogy az érintettre vonatkozó személyes adatok az érintettől szerezte-e meg az adatkezelő vagy más forrásból. E két tájékoztatási kötelezettség alapvetően azonos elvek mentén kerültek szabályozásra, utóbbi esetén értelemszerűen annyi többlettájékoztatási kötelezettséggel, hogy az adatkezelőnek meg kell jelölnie a személyes adatok forrását [vö.: GDPR 14. cikk (2) bekezdés f) pont], valamint markáns különbség van a tájékoztatási kötelezettség teljesítésének időpontjaira vonatkozó előírások között [vö.: GDPR 13. cikk (1) bekezdés és 14. cikk (3) bekezdés].

³²Vö.: GDPR 15.cikk

³³Vö.: GDPR 16.cikk

³⁴Vö.: GDPR 17.cikk

tájékoztatót készíteni. Mindezzel a tájékoztatási kötelezettség teljesítése mellett biztosítják az átláthatóság elvének való megfelelést is. Az adatkezelési tájékoztatót az érintett - illetve kiskorú esetén a törvényes képviselője - rendelkezésére kell bocsátani.

2.5.2. A tájékoztatáshoz való jog érvényesülése az online távoktatás során Magyarországon a Covid járvány alatt

Magyarországon a kötelező digitális oktatás során az érintettek tájékoztatáshoz való joga nem minden esetben érvényesült. Egy a szerző által vizsgált 20 tagú, zárt csoport tagjai által megválaszolt, nem reprezentatív felmérés szerint a pandémia idején valamennyi megkérdezett által látogatott oktatási intézményben folyt online távoktatás és szinte minden oktatási intézmény élt azzal a lehetőséggel, hogy videóhívás útján tanórát tartson, csupán egyetlen megkérdezett válaszolt nemmel. A tájékoztatási jog érvényesülése szempontjából az volt a releváns kérdés a felmérésben, hogy a digitális oktatás során a megkérdezettek kaptak-e megfelelő tájékoztatást a fontos adatvédelmi kérdésekről. A válaszadók 50%-a mondta azt, hogy a videóhívások lebonyolítása szempontjából jelentős adatvédelmi kérdésekről kapott valamilyen formában tájékoztatást. A megfelelő tájékoztatás elengedhetetlen, hiszen az érintett csak így tudja megállapítani, hogy az adott adatkezelés milyen hatással lesz a magánszférájára. A megfelelő tájékoztatáson keresztül tudja érvényesíteni az információs önrendelkezési jogát. A kötelező online távoktatás kényszerű helyzetében még fontosabb az olyan garanciák biztosítása, mint a megfelelő tájékoztatás, hiszen ennek elmaradása esetén *„az adatkezelő oldalán olyan „információs erőfölény” alakulhat ki, amelynek felhasználásával az érintett jogai, érdekei sérülhetnek”*³⁵ Bár a felmérést egy kis létszámú és zárt csoport töltötte ki, az semmiképp nem tekinthető reprezentatívnak, ám az megállapítható belőle, hogy a vizsgált oktatási intézmények, mint adatkezelők az esetek felében adták csak meg a megfelelő tájékoztatást az érintettek részére, elvéve ezzel tőlük a GDPR-ban biztosított jogukat.

35A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlása az előzetes tájékoztatás adatvédelmi követelményeiről

3. Az online oktatás adatbiztonsági kérdései

3.1. Az infrastrukturális kérdések

Az online távoktatásra nem csak az oktatási intézmények nem voltak felkészülve, hanem a szülők és a tanulók sem. Elsődleges feladatnak azt tekintette a legtöbb oktatási intézmény, hogy az infrastrukturális feltételeket megteremtse az órák megtartásához, és a távoktatásban részt vevő iskolás korú gyermekek számára is sok esetben ez volt az elsődleges feladat, hiszen bármennyire is szeretett volna egy diák részt venni a tanítási órákon vagy teljesíteni egy iskolai feladatot, ha például egy családban csak egy asztali számítógép vagy egy notebook volt úgy, hogy két iskolás korú gyermeknek kellett volna használnia ugyanabban az időben. A felsőoktatási intézmények hallgatói esetében ilyen probléma ritkábban jelentkezett, hiszen általánosságban elmondható, hogy egy felsőoktatási intézmény hallgatója már beiratkozáskor rendelkezik számítógéppel vagy valamilyen kliens eszközzel és internet eléréssel, hiszen már kivétel nélkül minden intézményben szükséges ezeknek a IKT eszközöknek a megléte az oktatásban való részvételhez elég, ha arra gondolunk, hogy az egyes tantárgyakra való bejelentkezés is interneten keresztül történik. Az infrastruktúra kialakítása után az oktatási intézményeknek ezt követően a megfelelő platformot is meg kellett találnia arra, hogy melyik program alkalmas az élő órák reprodukálására vagy a vizsgák teljesítésére.

3.2. Az online órák és a számonkérések adatvédelmi kérdései a digitális távoktatás során

3.2.1. Az „offline” tanítás és számonkérés adatvédelmi problémái

A kötelező digitális oktatás bevezetésekor nem volt egy megszokott vagy elfogadott módszer a számonkérések lebonyolítására, ennek kiválasztása a pedagógusok szakmai-módszertani szabadságának körébe tartozott és tartozik ma is. Kezdetben inkább a tananyagot tartalmazó írásbeli feladatokat, kép- és videó felvételeket készítettek az oktatók, ezeket küldték meg a diákoknak és hallgatóknak, nem valósult meg a tényleges, élőképpel történő óra tartás. A számonkérés is ehhez hasonlóan „offline” módon valósult meg, tehát otthon elkészített egy feladatot a diák és az arról készült fotót vagy videót elküldte a tanár részére. Ezzel kapcsolatban azonban adatvédelmi szempontból - és gyermekjogi szempontból is - hamar

aggályok merültek fel a kiskorúak vonatkozásában, mégpedig azzal kapcsolatban, hogy a kiskorú tanulók esetén miért nem szükséges a törvényes képviselő hozzájárulása ahhoz, hogy a gyermekről készült videó felvétel megosztásra kerüljön a pedagógussal. Ezzel kapcsolatban több gyermekjogokkal foglalkozó érdekvédelmi szervezet is kérdéssel fordult Nemzeti Adatvédelmi és Információszabadság Hivatalhoz (NAIH). A NAIH válaszával³⁶ segítette az oktatási intézményeket - és a hatósághoz fordulókat - a kérdés megválaszolásával, amelyben kimondta, hogy a diákok által megküldött videó felvételek személyes adatnak tekintendők, figyelembe véve azt, hogy az azon szereplők felismerhetőek és beazonosíthatóak, az adatkezelő pedig nem a pedagógus, hanem az oktatási intézmény, aki az adatkezelés célját meghatározza, az adatkezelés célja pedig nem más, mint az iskolai nevelés és oktatás, mint köznevelési alapfeladat ellátása. Az adatkezelőnek az adatkezelés célján túl pontosan meg kellett határozni az adatkezelés jogalapját is, ami az oktatási intézmények esetében az Infotv. 5.§ (3) bekezdése szerinti kötelező adatkezelésnek minősülő, GDPR 6. cikk e) pontja szerinti közfeladat ellátása volt - ahogyan már az előző bekezdésben is kifejtésre került, erre tekintettel tehát nem volt szükség a szülők hozzájárulására a videó felvétel elküldéséhez. Ha tehát az oktatási intézmény elvégezte a megfelelő mérlegelést és azt állapította meg, hogy csak a tanulók által készített videó felvételekkel igazolható a feladat teljesítése és a pedagógus csak ennek megtekintésével tudta ellenőrizni a munka elvégzését, ezáltal ellátni a nevelési és oktatási feladatát, akkor az adatkezeléshez nem volt szükség a törvényes képviselők hozzájárulására, hiszen az adatok kezelésére a közfeladat ellátása érdekében került sor. Azt kiemelte a NAIH, hogy jogalaptól függetlenül az oktatási intézményeknek, mint adatkezelőknek be kellett tartaniuk a GDPR-ban meghatározott alapelveket, széles körű tájékoztatást kellett nyújtaniuk az adatkezelési tevékenységükről minden érintettnek, ezek mellett a garanciák mellett pedig az ágazatra jellemző etikai szabályok betartásával kellett a tanulók adatait kezelni, hiszen a kiskorúak nincsenek tisztában az adataik kezelésével járó kockázatokkal. Kiemelendő, hogy a pedagógust, a hozzá kerülő személyes adatok tekintetében titoktartási kötelezettség terhelte. A korlátozott tárolhatóság elve alapján a diákok, illetve a szülői felügyeletet gyakorló személy vagy a hallgatók által megküldött vagy feltöltött felvételek megőrzésének időtartama nem lehet korlátlan, azt a feltétlenül szükséges időtartamra kellett szűkíteni. Ez a gyakorlatban azt jelentette, hogy a felvételeket az értékelés megtörténte után a pedagógus haladéktalanul, vissza nem állítható módon törölni volt köteles. „A további

36Vö.: NAIH 2020/2888. számú ügy

megőrzés indokaként az adatkezelő nem hivatkozhat arra, hogy azt egy esetleges későbbi ellenőrzés miatt meg kell tartani, hiszen az iskolai szakfelügyelők sincsenek mindig jelen a gyakorlati órákon".³⁷ A tananyag átadásának és a számonkérésnek ezen formájánál vizsgálni kellett azt, hogy az adatkezelés célját nem lehetséges-e adatkezelést nem igénylő eszközökkel elérni, személyes adatok kezelése esetén pedig minden esetben vizsgálni kellett, hogy létezhet-e hatékony, de az érintettek magánszférájára kevésbé kockázatos megoldás. Erre volt jó megoldás a tanórák élő, valós idejű közvetítése.

3.2.2. Az online órákkal kapcsolatos adatvédelmi kérdések

Ahogy telt az idő a kötelező távoktatás elrendelésétől számítva, egyre több oktatási intézmény kezdett el valódi online órákat tartani. Ez az online oktatási forma megfelelt az adattakarékosság elvének, hiszen nem volt szükséges a hallgatók személyes adatainak tárolása, gyűjtése, elegendő volt, ha csak a nevükkel és bejelentkezéssel azonosítják magukat. Ehhez azonban nagyon fontos volt a megfelelő technológia kiválasztása és olyan alkalmazás használata a számonkérések vagy a kommunikáció során, amelyek a legnagyobb biztonságot nyújtották az adatvédelmi incidensek elkerüléséhez. A GDPR mondja ki, hogy az adatok kezelését úgy kell végezni, hogy a *„megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve*".³⁸ Ennek során az adatkezelőnek kell kiválasztania a megfelelő technikai eszközt, amivel a GDPR-ban megfogalmazott, a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellege és integritása biztosítható. Ez a kötelezettség azonban az adatfeldolgozót is terheli. Az oktatási intézmények számára kiadott tájékoztatójában³⁹ a NAIH is felhívta az iskolák figyelmét a GDPR-ban is megfogalmazott⁴⁰ követelményre, mi szerint adatfeldolgozó igénybevétele esetén az oktatási intézmény kizárólag olyan adatfeldolgozót vehet igénybe, amely megfelelő garanciákat nyújt az adatkezelés GDPR követelményeinek való megfelelését és az érintettek jogainak a védelmét biztosító intézkedések végrehajtására. A járvány idején Magyarországon egy oktatási intézmény sem rendelkezett olyan, saját maga által kifejlesztett zárt rendszerrel, ami a fenti biztonságos

³⁷Vö. NAIH 2020/2888. ügyszámú tájékoztató, 4. oldal V. bekezdés

³⁸GDPR 5. cikk (1) f pont

³⁹A tájékoztató ügyszáma: 2020/7127.

⁴⁰Vö. GDPR 28. cikk (1) bekezdése

kommunikációt lehetővé tenné, emiatt választaniuk kellett a már meglévő videó konferencia megtartására alkalmas platformok közül.

3.2.3. Az online órák lebonyolításához használt videokonferencia rendszerek vizsgálata adatvédelmi szempontból

3.2.3.1. Az adatkezelő és az adatfeldolgozói közötti kapcsolat

Az iskolák több, különböző olyan program közül választhattak az online órák megtartására, ami biztosítja az oktató és a hallgatók vagy diákok egyidejű jelenlétét és élőképek közvetítésével az óra megtartását. Egy a Covid-19-es távoktatást vizsgáló tanulmány⁴¹ és az általam készített - nem reprezentatív- felmérés alapján is állapítható meg, hogy Magyarországon ezek közül a rendszerek közül az oktatási intézmények a legtöbb esetben a Zoom, a Google Hangouts Meet, a Skype, a Microsoft Teams és a Cisco WebEx felületeket használták az online oktatás lebonyolításához. Fontos kérdés, hogy akkor, amikor az adatkezelő, tehát az oktatási intézmény igénybe veszi a tanításhoz a videó konferencia lebonyolítására alkalmas rendszert, akkor ez hogyan befolyásolja az adatkezelői minőségét, a rendszer üzemeltetője adatkezelőként vagy adatfeldolgozóként fog működni. Álláspontom szerint minden olyan esetben, amikor az oktatási intézmény valamilyen szolgáltatót vett igénybe egy online óra megtartására, abban az esetben az oktatási intézmény adatkezelő lett, a videó konferencia lebonyolítását biztosító platform üzemeltetője pedig adatfeldolgozói minőségben szerepelt. Ennek az indoka az, hogy az adatkezelés célját az oktatási intézmény határozta meg, a platformot üzemeltető pedig az iskola nevében, az ő utasítására kezelte a személyes adatokat. Ehhez azonban szükség volt arra, hogy megfelelő jogalapot biztosítsanak az adatkezeléshez, ami lehetett a GDPR 28. cikk (3) bekezdése szerint az adatkezelő és az adatfeldolgozó közötti szerződés vagy más jogi aktus. Az általános adatvédelmi rendelet is megállapítja, hogy a kockázat mértékének megfelelő szintű adatbiztonság megfelelő technikai és szervezési intézkedésekkel való biztosítása nem csak az adatkezelő feladata, hanem egyben az adatfeldolgozó kötelezettsége is.⁴² A jogszabály szerint az adatfeldolgozás során az adatfeldolgozó kizárólag az adatkezelő utasításai és rendelkezései szerint járhat el. Ez ebben a helyzetben, amelyben az oktatási intézmény az adatkezelő azt jelentené, hogy az intézmény határozza meg annak a szolgáltatónak az

⁴¹Fejezetek a Covid-19-es távoktatás digitális tapasztalataiból, Gerhardus Kiadó Szeged, 2020

⁴²Lásd: GDPR 32.cikk (1) bekezdés

adatkezelésre vonatkozó szabályait, amelyiket igénybe vesz az online órák megtartásához. A gyakorlatban azonban ezek a szolgáltatók általános szerződési feltételek keretében határozzák és határozták meg az adatvédelemre vonatkozó rendelkezéseiket. Ez az oktatási intézményre, mint adatkezelőre nézve azért volt problematikus, mert ebben az esetben úgy tűnhet, hogy a szolgáltatók maguk határozták meg az adatfeldolgozás szabályait, nem pedig az adatkezelő⁴³.

3.2.3.2. Adatok külföldre továbbítása

Adatvédelmi szempontból fontos kérdés az, hogy a személyes adatokat továbbítják-e harmadik országba vagy sem. Ennek a jelentősége abban áll, hogy a GDPR biztosítja az Európai Unióban a személyes adatok védelmét és ugyanezt a védelmet kell biztosítani olyan országokban is, ahol nem érvényesül az adatvédelmi rendelet. De mi minősül harmadik országnak? Lényegében az Európai Gazdasági Térség (EGT) tagállamain⁴⁴ kívüli országok tekinthetők, amiből következik, hogy az EU-n belüli adattovábbítás nem minősül harmadik országba (külföldre) történő adattovábbításnak. A GDPR 46. cikkében több lehetőséget is biztosít arra, hogy az adattovábbító megfelelő jogalappal tudja a személyes adatokat harmadik országba továbbítani. Ezek a jogalapok szinte lépcsőzetesen épülnek egymásra, ennek megvizsgálása azonban alapos utánajárást követel meg az adatkezelőtől és az adatfeldolgozótól is, aki a személyes adatot külföldre kívánja továbbítani. Az ő feladatuk annak ellenőrzése, hogy az adattovábbítás olyan országba történik-e, amely a GDPR 45. cikke vagy a korábbi 95/46/EK irányelv alapján hozott megfeleléségi határozatok valamelyikével rendelkezik. Megfeleléségi határozat hiányában az általános adatvédelmi rendelet 46. cikkében felsorolt megfelelő garanciák alapján lehet adatot továbbítani külföldre. Ilyen garancia lehet csak példálózó jelleggel, ha a fogadó országban elfogadtak egy magatartási kódexet vagy van egy tanúsítási mechanizmust a harmadik országbeli adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő garanciákat, ideértve az érintettek jogait illetően is. Ha sem megfeleléségi nyilatkozat, sem garanciák nincsenek, akkor a GDPR biztosítja az eltérést bizonyos feltételek megléte esetén, ilyen feltétel lehet az, ha az

43Certicky Mária: A digitális oktatás egyes adatvédelmi kérdései, avagy előrehozta-e a COVID-19 a jövőt? In: Infokommunikáció és Jog, 2020/1. szám, 33-37. o.

44Az EGT tagállamai: az Európai Uniótag államai, azaz Ausztria, Belgium, Bulgária, Ciprus, Csehország, Dánia, Észtország, Finnország, Franciaország, Görögország, Hollandia, Horvátország, Írország, Lengyelország, Lettország, Litvánia, Luxemburg, Magyarország, Málta, Németország, Olaszország, Portugália, Románia, Spanyolország, Svédország, Szlovákia, Szlovénia, valamint az Európai Gazdasági Térségről szóló megállapodásban részes más állam, Izland, Liechtenstein Norvégia.

érintett hozzájárulását adta a továbbításhoz vagy például, ha az adatok továbbítása az érintett és az adatkezelő közötti szerződés teljesítéséhez szükséges. Ezek megvizsgálása és kiválasztása tehát az adatkezelőt és az adatfeldolgozót is terheli. Amennyiben sikerült megfelelő jogalapot találni az adattovábbításra, ellenőriznie kell, hogy a továbbított adatok védelmének szintje megfelel-e az uniós szinttel. Amennyiben nem, ahhoz az adattovábbítónak kell választania valamilyen, az adatvédelmi rendeletben biztosított eszközt, ami ezt a szinten garantálja. Ez azért is fontos, mert ennek elmulasztásáért felelősségre vonható. Ha azt állapítja meg, hogy egy konkrét adattovábbítás esetén semmilyen intézkedés nem garantálja az uniós szintű védelmet, akkor fel kell függesztenie vagy meg kell szüntetnie az adattovábbítást. Az online oktatás szempontjából ez azért lényeges kérdés, mert az oktatási intézmények által használt videóchat alkalmazás szolgáltatók legtöbbje külföldre továbbítja az online oktatásban részt vevő hallgatók, diákok személyes adatait. Ennek az oka az, hogy a videóchat platformok üzemeltetőinek a szerverei nagyon sok esetben az Európai Uniót kívül helyezkednek el. A kötelező távoktatás során igénybe vett szolgáltatók közül például a Google nem uniós fennhatóságú szervezet, a központja Kaliforniában van és számos szervere is külföldön található. Tájékoztatása szerint amennyiben az Amerikai Egyesült Államokba továbbítja az általa gyűjtött személyes adatokat, akkor az ún. Privacy Shield (EU-USA adatvédelmi pajzs) keretszabályzatainak kikötéseit tartja be. Itt fontos megemlíteni egy, az Európai Unió Bíróságának a pandémia⁴⁵ alatt született és az adatok harmadik országokba történő továbbítására igen jelentős hatást gyakorló ítéletét. Az Egyesült Államokba történő adattovábbítás egyik jogalapja az ún. Adatvédelmi Pajzs (Privacy Shield) volt. Ez egy olyan mechanizmust biztosított, amely a személyes adatok USA-ba történő továbbítása esetére is hivatott volt biztosítani a megfelelő szintű védelmet. Az ún. Schrems II. ügyben⁴⁶ hozott ítéletével a bíróság érvénytelenítette a fenti megfeleléségi határozatot, így személyes adatok a továbbiakban nem továbbíthatók az USA-ba erre a megfeleléségi határozatra alapítottn. Érvényesnek nyilvánította ugyanakkor a személyes adatoknak harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételeket, az ezen alapuló adattovábbítások kapcsán meghatározott a bíróság olyan feltételeket, amelyeket a harmadik országba történő adattovábbításokat megelőzően vizsgálni kell ahhoz, hogy

⁴⁵Nagy embertömegeket érintő, több országra vagy földrészre, sőt akár az egész világra kiterjedő, fertőző betegség okozta járvány.

⁴⁶[C-311/18. számú ügy](#), *Data Protection Commissioner kontra Facebook Ireland Ltd. és Maximillian Schrems*

biztosított legyen a személyes adatok megfelelő védelme. Az ügy előzménye az volt, hogy a felperes azt állította, hogy az USA nem nyújt megfelelő védelmet az oda továbbított adatok vonatkozásában, mert a Facebook az általa kezelt adatait az amerikai hatóságoknak adja át, amelyeket különböző megfigyelési programok keretében használnak fel. Az ítélet nyomán tehát nem kizárt az adatoknak az USA-ba történő továbbítása, de az adatfeldolgozóknak, így jelen esetben a Google-nak is át kell tekinteniük az Adatvédelmi Pajzson, illetve általános adatvédelmi kikötéseken alapuló USA-ba történő adattovábbításaikat és ki kell elemezni, hogy a GDPR 46. cikke alapján mely mechanizmus szolgálhat az adattovábbítás alapjául. A fenti ügy jól mutatja, hogy miben áll annak a veszélye, ha ez érintettek adatait olyan országokba továbbítják, ahol nem az unióban biztosított védelem illeti meg a személyes adatokat. Az érintett elveszítheti a személyes adatai feletti kontrollt, olyan szenzitív információk kerülhetnek más országokba, ahol nem tudja az érintett ellenőrizni, hogy mire használják fel az adatait. Ezért fontos, hogy az adattovábbító garantálja a korábban már kifejtett, adatvédelmi irányelv által biztosított védelem meglétét az adattovábbítás esetén. A NAIH a Tájékoztatójában is jó gyakorlatként említette azt, ha az oktatási intézmények az online oktatás során lehetőség szerint olyan szolgáltatókat alkalmaznak adatfeldolgozóként, amelyek az EGT területén letelepedettek és magukra nézve a GDPR szabályait kötelezőnek ismerik el. A teljes megoldást természetesen erre a kérdésre is az jelentette volna az online oktatásban, ha minden oktatási intézmény rendelkezett volna egy saját zárt rendszerrel az online oktatás lebonyolításához és belföldön található szerverekkel az adatok tárolására.

3.2.3.3. Az online órák személyiségi jogi kérdései

Az élő videó konferencia hívás során megtartott órák számos előnnyel rendelkeztek. Egy részről ez volt az egyetlen olyan módja, ami a legjobban képes volt reprezentálni a tényleges tanórát, a diákok és az oktatók egyidejűleg jelen voltak, kérdéseket tehettek fel, feladatokat oldhattak meg közösen, másfelől ez felelt meg leginkább az adattakarékosság elvének is. Azonban számos adatvédelmi veszélyt is hordozott magában. Az online oktatás során az egyik ilyen veszélyforrás épp a korábban kifejtett adatkezelő igénybevételével függ össze. Az oktatási intézmények által leggyakrabban adatkezelői minőségben igénybe vett ilyen alkalmazás a Zoom volt. Alapvetően nem oktatási célra lett kifejlesztve, de a Covid-19 miatt gyorsan kellett választani az oktatási intézményeknek, emiatt a már meglévő alkalmazások közül válogattak és ez a felület jól alkalmazhatónak bizonyult az online órák megtartására. Az alkalmazás használata adatvédelmi

szempontból azonban számos kockázatokat jelentett, tekintettel az alkalmazást használó diákoktól gyűjtött személyes adatok számára. A 2020. március 18-ai adatvédelmi szabályzata szerint⁴⁷ az alkalmazás a tanulóktól a következő adatokat gyűjtötte: a felhasználó neve és profilképe, illetve más azonosító adatai, a tanuló iskolája, eszközinformációk, hálózatra és internetkapcsolatra vonatkozó adatok és a Zoom platform diák általi használata, beleértve a végrehajtott műveleteket, dátumot és időpontot, gyakoriságot, időtartamot, mennyiséget, minőséget, hálózati kapcsolatot, valamint a bejelentkezésekkel, kattintásokkal, üzenetekkel, névjegyekkel, megtekintett és megosztott tartalommal, hívásokkal, videóhasználattal kapcsolatos teljesítményinformációkat és képernyőmegosztásokat. Nem csak a korábbi, de a 2021. novemberében elérhető adatbiztonsági tájékoztatója szerint is, a Zoom ezeknek az adatkezeléseknek a jogalapját úgy jelölte meg, hogy az „iskolai előfizető” - tehát az oktatási intézmény - adja beleegyezését a szülők és a tanulók nevében. Ez véleményem szerint nem csak az adattakarékosság elvét sértette, de növelte egy esetleges adatvédelmi incidens esetén a károk nagyságát, tekintve azt, hogy minél több adatot kezel egy szervezet, annál nagyobb kárt szenvedhet az érintett magánszférája, ha az adatokhoz illetéktelenek hozzáférnek. Az alapértelmezett **adatvédelem** (*privacy by default*) követelménye szerint *„az adatkezelő megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek.”*⁴⁸ A fenti gyakorlata a Zoom alkalmazásnak mindenképp megsértette ezt a rendeletben foglalt követelményt. A jogellenes adatkezelés lényegét és súlyosságát jól mutatja, hogy az említett Zoom alkalmazás üzemeltetője a Zoom Video Communications nevű vállalat, 25,5 milliárd forintnak megfelelő összeget fizetett ki egy általa vétett adatvédelmi hiba miatt. Kiderült, hogy a Zoom IOS verziója személyes adatokat - az alkalmazás indításának idejét, az eszköz- és helyinformációkat, valamint a telefonhoz tartozó szolgáltatóról szóló információkat - osztott meg a Facebookkal, olyan esetben is, amikor az érintettnek nem volt Facebook fiókja. Ezeket az adatokat célzott hirdetések létrehozására lehet leginkább használni. A digitalizáció korában, az egyik legértékesebb „árucikk” a személyes adat, hiszen egy nagy technológiai vállalat - mint például a Google - bár ingyen kínálja a felhasználók számára a szolgáltatásait, mégis ezekért *„sokszor a legérzékenyebb privát adatokkal fizetnek a felhasználók, hogy aztán - a vállalat - az adatokat*

⁴⁷Lásd: <https://theconversation.com/childrens-privacy-is-at-risk-with-rapid-shifts-to-online-schooling-under-coronavirus-135787> utolsó letöltés:2021.november 6.

⁴⁸Vö. GDPR 25. cikk (2) bekezdés

kielemezze vagy elemeztesse, és az eredmények birtokában, újabb és újabb módszereket találjon ki arra, hogyan tudna azokból még több pénzt csinálni. S mindennek során az ilyen vállalatok olykor gondatlanul járnak el, és felhasználóik beleegyezése nélkül adják át kibogozásra váró adathalmazaitak harmadik félnek.”⁴⁹ A megszerzett személyes adatokból tehát megállapítható egy személy fogyasztói attitűdje, világlátási vagy épp politikai beállítódása, s ezáltal befolyásolható egész élete. A digitális oktatás során ezen túl sérelem érhet az ember magánszféráját is, ami különösen kényes kérdés kiskorú érintettek esetén. Magyarországon is megjelent az a nézet, miszerint, abban az esetben, ha általános és középiskolában az online oktatás ideje alatt - nem csak a számonkérések alatt - folyamatosan bekapcsolva kell tartani a diákoknak a webkamerájukat, azzal sérül a magánszférájuk. A kérdés amiatt volt jelentős, mert sok tanuló azért nem akarta bekapcsolni a kameráját, mert ezáltal láthatóvá vált a lakókörnyezete, ami a többi diáktól származó megjegyzésekből kialakuló bántalmazási helyzetekhez vezetett. A felsőoktatásban ez azért nem jelentős kérdés, mert nem minden órán kötelező a részvétel, ezáltal ott a tanár nem kötelezheti a hallgatókat a webkamera bekapcsolva tartására. A kérdésben a NAIH is állást foglalt⁵⁰ és kifejtette, hogy a köznevelési intézményekben azokon az órákon, ahol a hagyományos oktatás keretein belül is kötelező a részvétel, ott az azon való részvétel ellenőrzése céljából az oktatási intézmény, mint adatkezelő előírhatja a webkamera folyamatos bekapcsolva tartását. Ennek indoka az, hogy a hagyományos oktatásban is folyamatosan látja a pedagógus a diákot, ugyanez történik a webkamera bekapcsolásakor, tehát nagyobb mértékű beavatkozás nem történik a magánszférájába. Az órán való jelenlét ellenőrzésének nincs más, a diákok magánszférájára nézve kevesebb kockázatot jelentő megoldás, a szükségesség-arányosság tesztet elvégezve tehát indokolt a webkamera kötelező bekapcsolása. Az azonban fontos, hogy csak abban az esetben nem okoz nagyobb mértékű beavatkozást a magánszférába, ha csak amiatt kötelező bekapcsolni a kamerát, hogy a jelenlétet ellenőrizze a pedagógus. (Egy feladat teljesítésének ellenőrzésére a korábban már említett videó felvétel megküldése lehet opció.) Tilos ezeket a tanórákat rögzíteni, hiszen az ellentétes az adatkezelés céljával, emellett ennek megsértése számos adatvédelmi, szerzői jogi, illetve büntetőjogi következményt vonhat maga után. A gyermek bántalmazás elleni védelem egyik eszköze lehet, ha az adattakarékosság elvének

⁴⁹<https://www.origo.hu/gazdasag/20190709-mennyit-is-ernek-valojaban-a-szemelyes-adataink.html>

utolsó letöltés 2021. november 4.

⁵⁰Ügyszám: NAIH/2020/8240

megfelelve a videón nem szerepel más személy a tanulón kívül, illetve a lakókörnyezet is a lehető legkisebb mértékben látszik, erre jó megoldás az ún. virtuális háttér alkalmazása.

3.2.3.4. Az online órák adatbiztonsági kérdései

A videokonferencia platformokon keresztül megtartott órák esetén az egyik legfontosabb követelmény volt a korábban már hangsúlyozott integritás és bizalmas jelleg biztosítása, aminek megőrzése az adatbiztonság gyakorlati megvalósításán keresztül történhetett. Ehhez szükséges volt, hogy a beépített és alapértelmezett adatvédelem elveinek megfelelően kerüljön megtervezésre és kialakításra az egész adatkezelési folyamat. A beépített adatvédelem (*privacy by design*) azt jelenti, hogy az *„adatkezelő a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt a rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába”*⁵¹ A gyakorlatban ez azt jelenti, hogy a személyes adatok olyan védelemben részesülnek, hogy nem válnak megismerhetővé illetéktelen személyek számára. Ilyen intézkedés lehet az érintettek részéről például olyan erős jelszó alkalmazása, melyet jelszó generáló programok segítségével készítenek és gyakran változtatnak. Az adatfeldolgozó és az adatkezelők részéről ilyen intézkedés lehet a kétfaktorú azonosítás, illetve, ami az online oktatás estén nagyon fontos a végponttól végpontig terjedő titkosítás⁵² alkalmazása. Az online oktatás során alkalmazott videóchat platformok közül sajnos számos esetben felmerült adatbiztonsági probléma. A Zoom az egyik legnépszerűbb videokonferencia platform volt a koronavírus járvány kirobbanásakor, adatvédelmi szempontból azonban nem volt felkészülve a vírus hatására kialakult távmunka és távoktatással járó felhasználószám növekedésre⁵³. A Zoom

51Vö.: GDPR 25. cikk (1) bekezdés.

52A végponttól végpontig tartó titkosítás a legmagasabb fokú adatvédelmet nyújtja, az adatokat minden eszközön az eszköz egyedi információiból származó kulcs védi, valamint a csak az érintett által ismert eszközjelzőkód

53https://index.hu/techtud/2020/04/16/koronavirus_jarvany_digitalis_tavoktatas_adatvedelem_biztonsag_internet_zoom utolsó megnyitás: 2021.november 7.

tájékoztatása szerint használatakor videóhívás közben megvalósult a végpontok közötti titkosítás, ez azonban félrevezetőnek bizonyult, ami azért veszélyes, mert maga a Zoom hozzáférhetett a konferenciák videó- és hangfelvételeihez, illetve harmadik, illetéktelen személyek is könnyebben megszerezhették ezeket. A Zoom alkalmazásról maguk a készítők is elismerték, hogy jó pár adatvédelmi aggálynak adott okot, ezen túl gyakran fordult elő az ún. zoombombing-nak nevezett jelenség is, amikor rosszindulatú külső személyek hivatlanul csatlakoztak egy-egy videokonferenciához, legtöbb esetben épp az online oktatást zavarták meg oda nem illő tartalmakkal, ami a kiskorú felhasználók esetében igen súlyos veszélyt hordoz magában. Számos adatvédelmi problémát orvosolt azóta a fejlesztő, sajnálatos, hogy ezt az online oktatás során kialakult incidensek után tette meg.

4. Záró gondolatok

A tanulmány elején Szent-Györgyi Alberttől olvasható egy idézet: „*Olyan lesz a jövő, amilyen a ma iskolája*”. Azért választottam ezt az idézetet, mert a dolgozatomban egy olyan folyamatot mutattam meg, ami tulajdonképpen az egész köz- és felsőoktatásra elképesztő hatással lehet. A koronavírus járvány miatt kényszerhelyzetben kezdték alkalmazni az oktatásban az infokommunikációs eszközöket, azonban be kell látnunk, hogy ez a kényszer szülte helyzet tulajdonképpen nem más, mint a jelen kor oktatásának a modernizációja. A korszakunkra jellemző digitális környezetben az online tanulás termékeny talajra talált. Ez a járvány szülte helyzet megmutatta, hogyan lehet a legmodernebb infokommunikációs eszközökkel átlépni a földrajzi akadályokat, modernizálni és még hatékonyabbá tenni az oktatást. Az azonban kiderült, hogy ez a digitalizáció a személyes adatok kezelésére is egyre nagyobb terhet rak. Az internet világában hamar elvesznek a felhasználók, különösen egy váratlan, nem ismert helyzetben, mint amilyen a kötelező távoktatás volt és úgy veszíthetik el a személyes adataik feletti kontrollt, hogy nem is veszik észre. Véleményem szerint a digitális oktatásé lesz a jövő, ehhez azonban szükséges, hogy a személyes adatok védelmével kapcsolatos kérdéseket, feladatokat is megismerje mind az oktatási intézmény, mind a tanulók, diákok és fontos az állami szerepvállalás is a biztonságos online oktatás megvalósításához. Ahogyan a dolgozatban megmutatkozott, az online távoktatás egy eddig ismeretlen, de mára egyre jobban feltérképezett módszer az oktatásban, hatékonyságát és hasznosságát az iskolák egyre jobban

elfogadják, a bemutatott kérdések alapján pedig megállapítható, hogy ennek adatvédelmi kérdéseinek megválaszolása is ugyanolyan fontos, mint az oktatás gyakorlati problémáinak megoldása. Ami pedig az idézetet illeti: az biztos, hogy a jövő a digitalizációé, a kérdés csak az, hogy ez hogyan valósul meg! Reményeim szerint adatvédelmi szempontból is pozitívan!

Irodalomjegyzék

- Bíró János - Kiss Ernő - Tari István - Vass Norbert: Jogalapok, érintetti jogok, Szakmai lektor: Dr. Péterfalvi Attila, A kézirat lezárásának dátuma: 2018. szeptember 25. Kiadja: NKE, 2018.
- 2.Certicky Mária: A digitális oktatás egyes adatvédelmi kérdései, avagy előrehozta-e a COVID-19 a jövőt? Infokommunikáció és Jog, 2020/1. szám, 33-37.
- 3.Fejezetek a Covid-19-es távoktatás digitális tapasztalataiból, Gerhardus Kiadó Szeged,2020. Szerkesztette: Dr. Kozma Gábor
- 4.Fekete, T., - Porkoláb, Ádám. (2020). Karanténpedagógia a magyar közoktatásban. Iskolakultúra, 30(9), 96-112.
- 5.Holle A. (2020) Oktatási rendszerek az új koronavírus járvány idején. Budapest, Országgyűlés Hivatala

Melléklet: A távoktatás adatvédelmi kérdései kérdőív

A kitöltők statisztikai adatai

A válaszadók létszáma: 20 fő

Férfi: 3 fő

Nő: 17 fő

Életkori átlag: 34.5 év

Az eredmények összefoglalása

1. Milyen oktatási intézménybe jár Ön / jár gyermeke (18 év alatti gyermek esetén)?

Általános Iskola 13 65%

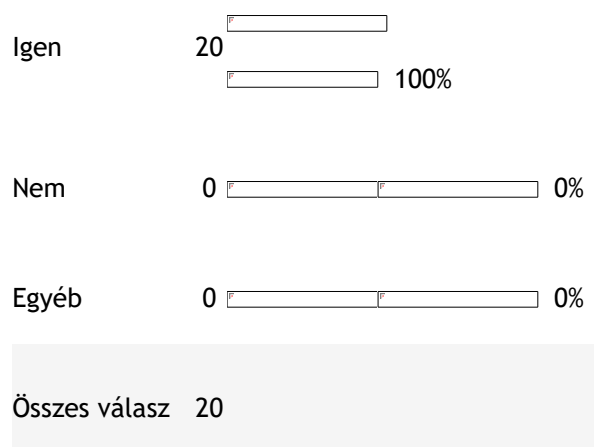
Középiskola 0
 0%

Felsőoktatási intézmény 7 35%

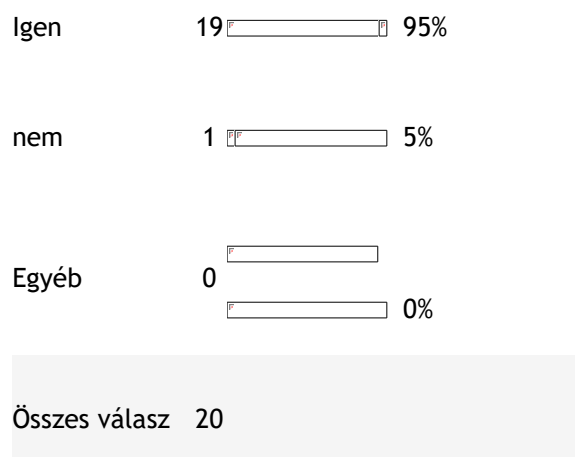
Egyéb 0
 0%

Összes válasz 20

2. A Covid19 járványhelyzetben az oktatási intézmény élt-e a digitális távoktatás lehetőségével?



3. A távoktatás keretein belül az oktatási intézmény oktatói tartottak-e digitális tanórákat?



4. Amennyiben az előző kérdésre igennel válaszolt, úgy milyen csatornát használtak az oktatók ez online órák megtartására? (több válasz is megadható) (több válasz lehetséges)

Skype 4 13.3%

Google Meet 11 36.7%

MS Teams 3 10%

Zoom 10 33.3%

Jitsi Meet 0
 0%

Egyéb 2 6.7%

Összes válasz 30

Egyéb válaszok:

- Webex
- Webex,

5. A digitális oktatás elindulásakor megkapta-e a használt platform adatvédelmi tájékoztatóját?

igen 15 75%

nem 5 25%

Egyéb 0
 0%

Összes válasz 20

6. Kapott-e bármilyen tájékoztatást a digitális oktatás során a videóhívások lebonyolításakor fontos és felmerülő adatvédelmi kérdésekről?

igen	9	<input type="text"/>	45%
nem	10	<input type="text"/>	50%
Egyéb	1	<input type="text"/>	5%

Összes válasz 20

Egyéb válaszok:

- Nem emlékszem