Eszteri Dániel

A deepfake technológia adatvédelmi értékelése a GDPR tükrében

Absztrakt
A fejezet célja a deepfake technológia értékelése a személyes adatok védelméhez fűződő alapvető jog érvényesülése szempontjából. A technológia alkalmazásának adatvédelmi problémáit az Európai Unió általános adatvédelmi rendeletének (GDPR) vonatkozó előírásai alapján elemzem. A fejezet a személyiséglopás és ezzel összefüggésben a valóság manipulálásának történeti előzményeivel kezdődik, majd a deepfake-technológia hátterét abból a szempontból mutatja be, hogy a folyamat egyes részelemei (szoftver tanítása, a deepfake elkészítése, majd annak felhasználása) milyen személyes adatkezelési műveletekkel járnak együtt. E mozzanatok kapcsán az adatkezelői felelősség is szóba kerül. A fejezet a jelenlegi jogérvényesítési lehetőségek és a legújabb, a jelenséget kezelni hivatott jogalkotási irányok felvázolásával zárul. Megállapíthatjuk, hogy a technológia használata kapcsán az érintettek magánszférájára jelentett kockázatok jelenleg nem kezelhetőek hatékonyan a legtöbb esetben, a tartalmakat előállító adatkezelők rendkívül nehéz beazonosíthatósága miatt. Az EU-s jogalkotás jelenlegi irányai azonban előremutató intézkedéseket tartalmaznak, amelyek gyakorlati végrehajthatósága azonban szintén kihívásokat hordoz magában.

Kulcsszavak: személyes adat, adatvédelem, GDPR, gépi tanulás, mesterséges intelligencia, személyiséglopás

Data protection evaluation of deepfake technology in the context of the GDPR

Abstract: The aim of the chapter is to assess deepfake technology in terms of the fundamental right to the protection of personal data. I analyse data protection problems in the use of the technology on the basis of the relevant provisions of the European Union's General Data Protection Regulation (GDPR). The chapter begins with the historical antecedents of personality theft and, in this context, the manipulation of reality. After this, the background of the technology in general will be presented, primarily from the point of view of the personal data processing operations that each part of the process (training the software, preparing the deepfake, and then using it) entails. In connection with these, the responsibility of the data controller is also separated. Finally, the chapter concludes by outlining the current enforcement options and the latest legislative directions to address the phenomenon. According to the findings, the risks posed to the privacy of data subjects associated with the use of this technology are currently not effectively managed in most cases, due to the extremely difficult identification of data controllers producing the illegal content. However, the current directions of EU legislation include forward-looking measures, the practical implementation of which, however, is also challenging.

Keywords: personal data, data protection, GDPR, machine learning, artificial intelligence, identity theft

1. Bevezetés: a személyiséglopás és identitáshamisítás előzményeiről

A tények, információk elferdítése, meghamisítása, majd azok nyilvánosságra hozatala, megtévesztő híresztelése nem újdonság, hanem gyakorlatilag egyidős az emberiséggel. A személyiség meghamisítása, más szerepének felvétele szintén hosszú múltra tekint vissza, már

vallási szövegekben is találunk rá példát. Tóth Dávid (2020: 113) a személyiséglopás büntetőjogi elemzéséről szóló tanulmányában utal a bibliai Jákob és Ézsau történetére: Izsák elsőszülött fia, Ézsau lemondott az őt megillető előjogokról az öccse, Jákob javára egy tál lencséért. Erről azonban az apjuk, Izsák nem tudott. Amikor később Jákob meglátogatta már vak édesapját, hogy megkapja áldását az örökséghez, Ézsau ruháiban és kecskebőrben jelent meg vak apja előtt, hogy Izsák ne vegye észre a csalást (Tóth 2020: 113).

Történelmi adalékot találunk a témához a középkori Angliában, ahol a 15. században uralkodott IV. Edward, akinek a két fia, Edward és Richard nyomtalanul eltűnt. Az uralkodó halála után trónörökös hiányában öccse, III. Richard lett az új király, akit VII. Henrik követett. VII. Henrik uralkodása alatt azonban két trónkövetelő is felbukkant a semmiből. Az egyik, Lambert Simnel, egy közrendű ifjú, a két eltűnt herceg unokaöccsének adta ki magát, Edward Plantagenet néven, miközben az igazi Edward Plantagenet a Towerben raboskodott. A fiatalembert Írországban megkoronázták, mint VI. Edward angol királyt, míg VII. Henrik az igazi herceget szabadon bocsájtotta, így bizonyítva a csalást. Simnel ezek után kegyelmet kapott, majd a királyi udvarban mosogatófiúként, később solymászként szolgált (W1; Szmolenszki 2018: 20). A másik trónkövetelő Perkin Warbeck volt, aki a hatalmon lévő király ellenségeivel Írországban sereget gyűjtött, és kétszer is megpróbált partra szállni, hogy megdöntse a király uralmát. A második akciót követően elfogták és börtönbe vetették. Ennek ellenére Perkin továbbra is a királyi udvarban maradhatott, egészen addig, amíg egy szökési kísérlete után felakasztották (Goble 1999; Szmolenszki 2018: 20).

Évszázadokkal később, az információtechnológia előretörésével a 20. század végén és a 21. század elején a személyiséglopás, ezáltal a valóság meghamisítása teljesen új dimenzióba lépett. Ennek számos oka közül egyik, hogy az emberek saját maguk osztanak meg információkat önmagukról az interneten, többek között fényképeket és videofelvételeket a közösségi oldalakon és más online platformokon. Az interneten ismert emberekről, közszereplőkről is számos kép és videófelvétel kering, akár a napi híreknek és tudósításoknak köszönhetően, amelyek immár digitalizált formában férhetőek hozzá a nagyközönség számára, ezért a vizuális tartalmak feldolgozása (megvágás, retusálás, átdolgozás stb.) számítógépes úton is sokkal egyszerűbb, mint a régebbi technológiával készített felvételeké. Habár a személyiség „ellopására", így a valóság meghamisítására korábban is léteztek különböző technológiák, a valóság eltorzítására, ezáltal egy valós személy cselekedeteinek meghamisítására való képesség a deepfake technológia néhány évvel ezelőtti megjelenésével óriási „minőségi" ugrást eredményezett a személyiséglopás, egyben a tényhamisítás és álhírterjesztés piacán.

Komoly visszhangot váltott ki a médiában a volt amerikai elnökről, Barack Obamáról készült deepfake videó, amelyben az elnök (hamisított mása) ironikusan és vulgáris módon hívja fel a figyelmet a technológia veszélyeire (W2). Szintén hamar felkapták a médiában azt a 2022 márciusában készült deepfake videót, amelyben az ukrán elnök, Volodomir Zelenszkij utasítja az ukrán hadsereget, hogy tegyék le a fegyvert az orosz hadsereg előtt. A videóról hamar kiderült, hogy hamis és ugyancsak deepfake technológiával készült (W3).

A deepfake technológia ugyanis alkalmas arra, hogy olyan audiovizuális tartalmakat hozzanak vele létre, amelyben egy valódi személy olyan dolgokat mond vagy tesz, amit egyébként sosem mondott vagy tett a valóságban (Chesney – Citron 2019: 1753). Az ilyen típusú személyazonossággal való visszaélés alkalmas lehet az emberek és a közvélemény komoly befolyásolására, hiszen a meghamisított felvételen szereplő személy mind az arca, mind a hangja, mind pedig a gesztusai alapján szinte teljesen hasonlít az eredetire. A különbség – néhány nehezen észrevehető vizuális jelen kívül – csupán annyi, hogy az általa előadottak a valóságban az eredeti szereplőtől sosem hangzottak el.

A technológiára építő programok ma már könnyen elérhetők az interneten, alkalmazásuk pedig egyre egyszerűbb, és nem igényel különösebb informatikai tudást. A szórakoztató videótartalmak gyártása mellett a technológia alkalmas arra is, hogy olyan szavakat adjon egy

valós személy szájába, illetve olyan tetteket hajtassanak vele végre a képernyőn, amit egyébként nem mondana vagy tenne, ezáltal sértve meg többek között a személyes adatai védelméhez fűződő jogait (Miskolczi – Szathmáry 2018: 141–142). A technológia mind jó, mind rossz célokra alkalmas lehet. A fejezet célja a technológia értékelése adatvédelmi szempontból az Európai Unió általános adatvédelmi rendeletének (közkeletű angol rövidítése szerint: a GDPR) tükrében (W4). Mielőtt azonban rátérnénk a jelenség adatvédelmi értékelésére, nézzük meg először az annak alapjául szolgáló technológia sajátosságait.

2. A deepfake alapjául szolgáló technológia: gépi tanulás, mélytanulás

A Jan Kietzmann és szerzőtársai által használt fogalom szerint: „a deepfake a gépi tanulás és a mesterséges intelligencia technológiájának felhasználásával olyan vizuális, illetve hangalapú tartalmakat hoz létre, amelyek nagy eséllyel lesznek megtévesztőek" (Kietzmann et al. 2019: 1).

A deepfake alapja a gépi tanuláson alapuló videó- és hangmanipuláció. A gépi tanulás mint a mesterséges intelligencia-fejlesztés egyik ágának lényege, hogy a rendszer saját maga képes a rendelkezésére álló adatokból, információkból, azaz korábbi tapasztalatokból tudást létrehozni. A rendszer példaadatok, minták alapján képes önállóan vagy emberi segítséggel szabályszerűségeket, szabályokat felismerni és meghatározni, majd az elsajátított tudásbázisban felfedezett szabályszerűségek alapján döntéseket hozni. A gépi tanulás során az emberi programozó csak az önálló tanulás kiindulópontjaként használható adatokat ad meg a számítógépnek. Ezek után a gép maga hozza létre és fejleszti tovább azokat az algoritmusokat, amelyekre a döntések – vagy előrejelzések – meghozatalához szüksége van. Az adatokban felfedezett szabályszerűségekből létrehozza az úgynevezett modellt, amely tartalmazza az elsajátított mintázatokat, szabályszerűségeket, majd ezeket alkalmazza az új adatok esetén is. A gép a saját maga által felállított modell alapján hoz immár önálló döntést bármilyen emberi beavatkozás nélkül. Az emberi felhasználó már csak a meghozott döntéssel szembesül a program használata során (Datatilsynet 2018: 7–8).

A deepfake tartalmak létrehozásához gépi tanulási módszereket használnak, annak is egy különleges ágát, amelyet mélytanulásnak (*deep learning*) neveznek. Ez a gépi tanuláshoz képest még szűkebb fogalom. A mélytanulás mesterséges neuronhálózatok alkalmazásán alapszik. Ezeken a mesterséges neuronhálózatokon az emberi neuronok közötti adatátvitel mintájára a számítógépes jelek nem pusztán pozitív és negatív válaszok (tehát 0 és 1) megkülönböztetésére szolgálnak (Hlács 2016).

Az emberi agy működésének alapja a neuronok közötti kapcsolat, azaz a szinapszis. A neuronok a szinapszisokon keresztül küldenek jelet egymásnak, egy neuron pedig párhuzamosan több szinapszist, tehát több kapcsolatot is képes fenntartani másik neuronokkal. A szinapszisok azonban nemcsak a jelek átvitelére képesek, hanem a korábbi kapcsolatok emlékét is meg tudják őrizni. Az agyban gyakrabban használt szinapszisokban a kapcsolatok erősebbek lesznek, ezért van az, hogy egyes gondolatok könnyebben fogalmazódnak meg és jutnak eszünkbe, vagy bizonyos problémát gyorsabban, hatékonyabban tudunk megoldani. A mélytanulás is hasonlóan működik: a többrétegű adatbázisban a számítógép feldolgozó egységei egyrészt végzik a 0 és 1 válaszok megkülönböztetését, továbbá a többi réteg ugyanazon kérdésére adott válaszát is vizsgálják. Így az adott kérdésre minden egyes rétegben létrejön a 0 vagy az 1 válasz, azonban a rétegeket összevetve az adott válasz tényleges értéke súlyozható (Alpaydin 2016: 85–86; Schiff 2020: 16). Az algoritmus itt is az általa beazonosított mintázatok alapján próbálja meg előrejelezni a következő lehetséges értékeket, viszont a mélytanulást végző neuronhálózat többrétegű (általában már tanított) adatbázisból és rájuk épülő tanuló algoritmusokból épül fel. Ennek köszönhetően a rendszer absztrakciós készsége is növekszik a megoldásra váró feladatokkal kapcsolatban, így ez a technológiai megoldás sokkal

összetettebb és gyorsabban fejlődő algoritmusokat, pontosabb válaszokat és magasabb fokú absztrakciót tesz lehetővé az MI számára (Hlács 2016).
A deepfake videós tartalmak készítése általában generatív neurális hálózati architektúrák, legtöbbször úgynevezett generatív ellenséges hálózatok (GAN-ok) betanítását foglalja magában (Chesney – Citron 2019: 1756–1757). A GAN módszert a Google egyik kutatója, Ian Goodfellow és szerzőtársai dolgozták ki 2014-ben (Goodfellow et al. 2014). A GAN két neuronhálózatot kapcsol össze, hogy azok párhuzamosan dolgozzanak. Az egyik hálózat, a „generátor" a rendelkezésre álló adathalmazból kiválogatja azokat a már meglévő, kész képeket, amelyek a célvideón szereplő arc tulajdonságaira (szög, arckifejezés, árnyékolás stb.) a leginkább hasonlítanak. Ezek után a másik hálózat, az úgynevezett „diszkriminátor" elemzi a két adathalmaz hasonlóságait és eltéréseit. Az esetleges eltéréseket a számítógép automatikusan korrigálja, hogy a kép minél jobban hasonlítson az eredeti videón szereplő arc tulajdonságaira (módosítja az arc színeit, mimikáját, a száj, a szemek és az arcizmok mozgását stb.). A diszkriminátor hálózat folyamatosan kommunikál a generátorral, és szükség esetén újabb képeket használ fel a meggyőzőbb eredmény elérésére (Chesney – Citron 2019: 1760–1762; Schiff 2020: 18–19).
A GAN tehát egy valódi többrétegű mélytanuló neuronhálózatra épülő rendszer, amely önmagát is folyamatosan fejleszti, ahogy egyre több adatot (képet) elemez és hoz létre. A GAN képes a saját maga által korábban készített képekből is tanulni, így egyre szofisztikáltabb eredményeket produkál.

3. A deepfake technológia alkalmazásának kapcsolata a személyes adatokkal

A deepfake technológia kapcsolatát a személyes adatokkal két külön szakaszra érdemes bontani: az első a technológiát alkalmazó szoftver tanítása, a második pedig annak alkalmazása. A tanítás során a rendszerbe először nagy mennyiségű adatot táplálnak be, amelyben a tanuló algoritmus megpróbál mintákat, hasonlóságokat keresni. Amennyiben talál ilyen azonosítható mintákat, úgy azokat megjegyzi, és elmenti későbbi használat céljából. A megjegyzett és elmentett minták alapján alkotja meg a rendszer az ún. modellt (Datatilsynet 2018: 7). Amennyiben a tanításra használt adathalmaz személyes adatokból épül fel (ilyenek lehetnek az emberek arcát, mozgását vagy hangját tartalmazó képek és hangok), úgy a tanítás szükségszerűen együtt jár személyes adatok kezelésével is.
A már tanított szoftver alkalmazása mint második lépcső szintén együtt járhat személyes adatok kezelésével, hiszen amennyiben a rendszerbe újabb adatokat töltenek fel, amelyek hasonlóak a tanuláshoz használt adatokhoz, a modell alapján az eldönti, hogy az új adat mely megtanult mintázathoz hasonlít a leginkább, s később ez alapján fogja az elsajátított mintázatok alapján kialakítani az automatikus döntést (Datatilsynet 2018: 7).
A deepfake tartalmak előállítása során egy, a program által létrehozott „szereplő" rendelkezik olyan tulajdonságokkal, amelyek egy létező természetes személytől vagy személyektől származnak. A deepfake videó szereplőjének az arcvonásai, a hangja, de akár a mimikája is az emberi szem számára felismerhetetlenül hasonlíthat arra a természetes személyre, akiről a deepfake videó szereplőjét mintázták. Ezen tartalmak elkészítéséhez és a használt szoftverek működéséhez kimondottan sok személyes adatra van szükség. A deepfake tartalom minősége annál jobb, tehát az azon látható szereplő annál életszerűbb, minél több és minél jobb minőségű adat alapján készült (Klein – Tóth 2018: 67–68).
A tanításhoz használt személyes adatok, a szoftver által a deepfake tartalom előállításához használt személyes adatok és végül a kész tartalom mint személyes adat jogi értékelése adatvédelmi szempontból elkülönül egymástól. A tanítás, a tartalom előállítása és végül maga a tartalom közzététele külön-külön adatkezelési műveletek, és jogszerűségüket ennek

megfelelően érdemes külön vizsgálni (Schiff 2020: 25). A továbbiakban ezen három lépés alapján mutatom be az egyes adatkezelési műveletek adatvédelmi kérdéseit.

4. A deepfake tartalmakat előállító szoftver tanításához használt személyes adatok

A szoftver tanításának adatvédelmi vizsgálata szempontjából szükséges felvázolni néhány alapfogalmat. Az első kérdés az, hogy melyek azok a személyes adatok, amelyek a deepfake tartalmak előállítására használt szoftver tanításakor jelentőséggel bírhatnak.
Ha a GDPR vonatkozó fogalmait keressük, akkor az első mindenképpen a személyes adat fogalma. Eszerint személyes adatnak minősül az azonosított vagy azonosítható természetes személyre – a GDPR szóhasználatával élve: az érintettre – vonatkozó bármely olyan információ, amely alapján ő akár közvetlen, akár közvetett módon azonosítható (GDPR 4. cikk 1. pont). A joggyakorlat is többször foglalkozott már az érintettről készült kép- és hangfelvétel személyes adat jellegével. Ez alapján határozottan elmondható, hogy egy ember arca, képmása személyes adatnak, a képfelvétel készítése, valamint az adatokon elvégzett bármely művelet pedig adatkezelésnek minősül (NAIH 2022: 10). Így a természetes személyekről készült kép- és hangfelvételeknek a szoftverek általi feldolgozása (például az algoritmus tanításának céljára) adatkezelést fog eredményezni.
A GDPR hatálya alá tartozó adatkezelések kapcsán fontos kitétel, hogy a személyes adatok kezelésének részben vagy egészben automatizált módon kell történnie, ahhoz, hogy arra alkalmazni kelljen a rendelet előírásait. A GDPR-t ezen felül azoknak a személyes adatoknak a nem automatizált módon történő kezelésére is alkalmazni kell, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni, bár ezen utóbbi szabály témánk szempontjából kevésbé bír jelentőséggel (GDPR 2. cikk (1) bekezdés).
Mind a gépi tanulás, mind az ennek szűkebb szeletét jelentő és a deepfake technológia alapját adó mélytanulás során létrejövő adatkezeléshez jellemzően sok személyes adatra van szükség. A szoftver megtanítása a feldolgozott személyes adatok, így a kép-, videó- és hangfájlok révén arra, hogy valódinak tűnő tartalmakat tudjon előállítani, így jellemzően sok bemeneti tanító adatot igényel. A felhasználandó adatok mennyiségével a legtöbb esetben egyenesen arányos a létrehozott deepfake videó minősége is, hozzátéve azt is, hogy a legmegfelelőbb adatok előzetes kiválasztása és címkézése is ugyanilyen fontos szempont a hatékony tanítás elérésére (Datatilsynet 2018: 10).
A deepfake tartalmak előállítására alkalmas szoftver tanításához felhasznált személyes adatokért való adatkezelői felelősség szintén fontos problémakör. A GDPR fogalomrendszerében adatkezelőnek minősül 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 (GDPR 4. cikk 7. pont). A deepfake videók előállítására alkalmas szoftver tanítása szempontjából ezért adatkezelőnek azon személyt (akár természetes, akár jogi személyről beszélünk) vagy szervezetet kell tekinteni, aki vagy amely a tanítás alapjául szolgáló adatbázis összeállításának céljait és eszközeit, továbbá ezen adatbázis felhasználásának céljait és eszközeit előzetesen meghatározta. A gyakorlatban ez legtöbbször egy szoftverfejlesztéssel foglalkozó vállalkozást takar, amely abból a célból állít össze személyes adatokból egy tanító adatbázist, hogy azt mélytanuló algoritmusok segítségével elemeztesse egy szoftverrel avégett, hogy a beazonosított mintázatok alapján az később minél élethűbb deepfake videókat tudjon előállítani.
Az adatkezelői minőség tehát az adatkezelés tanítási stádiumában megáll a személyes adatok tanításra való felhasználásának műveleténél. A szoftverfejlesztő adatkezelői felelőssége a tanító adatbázis összeállításánál, a tanítás céljainak meghatározásánál és az ezen célok elérése érdekében megírt tanuló algoritmusok kiválasztásánál vagy megírásánál ér véget. A tanítás és

a szoftverfejlesztés során ezért a fejlesztővállalkozásnak meg kell felelnie a GDPR előírásainak. Ehhez képest magának a konkrét deepfake videónak az elkészítése és ehhez egy megszemélyesíteni kívánt személy személyes adatainak összegyűjtése és felhasználása már elkülönült adatkezelői minőséget fog fő szabály szerint eredményezni.
A teljesség igénye nélkül az alábbiakat szükséges figyelembe venni a tanításkor. A gépi tanuláson alapuló MI fejlesztése során is figyelembe kell venni az olyan, a GDPR-ban is meghatározott alapelveket, mint az adatok kezelésének célhoz kötöttsége, szükségesség-arányossága és a megfelelő adatkezelési jogalap megléte (GDPR 5. cikk).

Különös figyelemmel kell lenni továbbá ezen programoknál a beépített, illetve az alapértelmezett adatvédelem elvére is (GDPR 25. cikk). Az adatok feldolgozása csak átláthatóan és elszámoltatható módon történhet, valamint az érintetti jogok gyakorlása sem korlátozható. Az adattakarékosság elvének érvényesülésére kifejezetten javasolt szintetikus – valós adatokból mesterségesen generált (konkrét személyhez nem köthető) – adatok felhasználása (Datatilsynet 2018: 25). A szintetikus adatok használatával elkerülhető az, hogy a szoftverfejlesztő esetleg megsértse a GDPR vonatkozó előírásait, mivel a konkrét személyhez nem köthető, mesterségesen generált adatokra már nem kell alkalmazni a felhasználásuk során a rendelet előírásait, lévén annak a hatálya csupán a konkrét, élő természetes személyhez köthető adatokra terjed ki (Péterfalvi – Révész – Buzás 2021: 51, 71).

5. A deepfake tartalom elkészítéséhez használt személyes adatok

A konkrét deepfake videók elkészítéséhez a szoftver általános tanításán túl szükség van minden esetben olyan bemeneti adatokra, amelyek elemzése révén a szoftver elő tudja állítani magát a hamisított tartalmat. Egy ismert közéleti szereplőről, például egy ország miniszterelnökéről készítendő deepfake videóhoz a szoftvernek össze kell gyűjtenie olyan fotókat, videókat és hangokat, amelyek valóban az adott alanyról készültek. Ezek elemzése révén a már a tanítás során beazonosított általános mintázatok és a konkrét személyre vonatkozó valódi tartalmak alapján lehet elkészíteni a hamisított felvételt.
A konkrét tartalom tehát úgy készül el, hogy a szoftver a tanítása során megtanulja azt, hogy általánosságban hogyan néznek ki az emberek, és egyes szavak formálása során milyen általános mimikai jelek figyelhetőek meg az arcon. Ezek után a szoftver használata során kiválaszt a felhasználó egy személyt, akiről hamisított felvételt szeretné elkészíteni, ehhez pedig a konkrét személyről készített valódi felvételeket tölt fel a programba. A konkrét személy arcának, hangjának, mimikájának és más testi tulajdonságainak elemzése és az általános mintázatok alapján végül elkészül a konkrét deepfake videó.
Természetesen ehelyütt is érdemes elmondani, hogy a deepfake videó elkészítéséhez a megszemélyesíteni kívánt érintettről felhasznált tartalmak, így képek, videók, hangok is személyes adatnak fognak minősülni a GDPR vonatkozó fogalmai alapján, mivel – ahogy az az előző pontban is kifejtettem – egy ember képmása személyes adatnak, az azokon elvégzett bármely művelet pedig adatkezelésnek minősül (GDPR 4. cikk 1. és 2. pontok). A deepfake videó készítésekor ezért a megszemélyesíteni kívánt valódi személy adatainak kezelése során is meg kell felelni a GDPR előírásainak fő szabály szerint. A személyes adatok ilyen célú felhasználására ezért elvileg legitim céllal és megfelelő jogalappal kell rendelkeznie az azt előállító tartalomkészítőnek.
Ez a gyakorlatban azt jelenti, hogy egy adott személyről egy deepfake videó készítéséhez a videót készítő személynek tudnia kell azt a GDPR 5. cikk (2) bekezdésében foglaltak, azaz az úgynevezett elszámoltathatóság elve alapján igazolni, hogy megfelelő jogalappal rendelkezik a személyes adatok ilyen célú kezeléséhez, továbbá a GDPR egyéb előírásait is betartja az adatkezelés során. Például az ilyen videók készítőjének be kell tudnia azt mutatni a GDPR 7. cikk (1) bekezdése alapján, hogy beszerezte az érintettől a GDPR 6. cikk (1) bekezdés a) pontja

szerinti hozzájárulását egy ilyen célú adatkezeléshez. Tehát az érintettnek hozzá kellene ahhoz járulnia, hogy a személyes adatai felhasználásával deepfake videót fognak róla készíteni. Ezzel kapcsolatban a videó készítőjének pedig előzetesen és megfelelő tartalommal tájékoztatnia kell őt az adatkezelés körülményeiről a GDPR 13. cikkének megfelelően.
Lássuk be, az előzőekben kifejtett adatvédelmi előírásoknak való megfelelés a deepfake videók készítése során az esetek túlnyomó többségében egyáltalán nem tud érvényesülni, hiszen a hamis videóban megszemélyesített személyről legtöbbször lejáratási, megtévesztési céllal készül a felvétel, annak elkészítéséhez pedig nyilvánosan elérhető tartalmakat használnak fel. Ezért nemcsak maga a már elkészült hamis felvétel nyilvánosságra hozatala, hanem annak készítéséhez az eredeti személyes adatok felhasználása is túlnyomórészt jogsértő lesz. Természetesen el lehet képzelni olyan esetet is, amikor valakinek a tudomásával és beleegyezésével, így legitim adatkezelési céllal és jogalappal készül a személyes adatai felhasználásával egy deepfake videó (például oktatási vagy tudatosítási célból), azonban ez valószínűsíthetően az esetek elenyésző hányadát teszi ki.

6. A deepfake videó mint személyes adat

A már elkészült deepfake videó személyes adat jellegével kapcsolatban a legfőbb értelmezési kérdés, hogy tulajdonképpen az abban szereplő „személy” soha nem tanúsította a videón látható magatartást, illetve nem hagyták el a száját az elhangzó szavak, mondatok. Ez esetben tehát egy olyan mesterségesen generált tartalom személyes adat jellegét kellene megállapítani, amely nem az érintettről készült, nem is tőle származik, hiszen magán a videón nem is ő szerepel, hanem egy szintetikus entitás. Kérdés tehát, hogy olyan elkülönült jogi sorsot osztó tartalomnak kell-e tekinteni a deepfake videót, amely nem minősül az utánzott érintett személyes adatának, vagy inkább a testi és más külső jellemzők nagyfokú hasonlósága miatt a tartalom az utánozni kívánt személy személyes adata lesz-e (Schiff 2020: 28).
A GDPR meghatározása alapján a személyes adat fogalmának kulcseleme az, hogy az alapján egy természetes személy azonosítható legyen, akár közvetett, akár közvetlen módon. Azonosíthatóvá pedig egy természetes személy a vele kapcsolatba hozható bármely információ alapján válhat, például ilyen információk lehetnek a testi, fiziológiai vagy szociális azonosságára vonatkozó tényezők (GDPR 4. cikk 1. pont). Ezen fogalom alapján elmondható, hogy nem feltétlenül szükséges az egy természetes személy azonosíthatóságának megállapításához, hogy az információ közvetlenül tőle származzon. Elég az, ha egy konkrét, tehát élő természetes személyre rá lehet ismerni a közölt információk alapján, amelyek testi, fiziológiai jellemzők is lehetnek. Például egy ismert személy jellegzetes hanghordozására, testtartására, arcának és mimikájának jellemzőire vonatkozó információ feldolgozása révén előállított szintetikus deepfake tartalom a GDPR alapján a megszemélyesíteni kívánt érintett személyes adatának fog minősülni. Ilyen módon tehát még egy olyan tulajdonság vagy jellemző is minősülhet személyes adatnak, amely a szemlélőkben azt az érzést kelti, hogy ők ezt a tulajdonságot egy meghatározott élő természetes személyhez tudják kötni. Az információk tehát nemcsak objektívek, hanem akár szubjektívek is lehetnek, és nem szükséges az sem, hogy valósak legyenek. Tehát személyes adatnak minősülhet akár valótlan vagy nem igazolt információ is. Ezért a deepfake videó is a megszemélyesített, így mások által már beazonosítható, tehát egy adott csoport (vagy az egész társadalom) minden más tagjától elkülöníthető természetes személy személyes adata lesz, ezért alkalmazandók rá a GDPR előírásai (Balogh et al. 2019: 48–49). Ez az értelmezés már csak azért is tűnik logikusnak, mivel bizonyos deepfake videók készítése és nyilvánosságra hozatala az azokon keresztül megvalósuló „személyiséglopás” miatt képes súlyosan negatívan befolyásolni az érintett magánszféráját, ezen belül jóhírnevét, társadalmi megítélését, magán- és családi életét, sőt akár hátrányos megkülönböztetés oka vagy indoka is lehet vele szemben, beleértve akár a lehetséges

vagyoni és nem vagyoni károkat is. Az ilyen tartalmak nyilvánosságra hozatala a magánszférára gyakorolt hatásuk miatt olyan alapvető kockázatokat hordoz az egyénre nézve, amelyeket maga a GDPR is külön nevesít a 75-ös preambulumbekezdésében.
Az előző ponthoz hasonlóan tehát a konkrét deepfake videó kapcsán is elmondható, hogy annak kezelésére, így például a nyilvánosságra hozatalára csak akkor kerülhetne sor, ha ehhez jogszerű céllal és jogalappal rendelkezik az azt nyilvánosságra hozó személy. Tehát az ilyen videók nyilvánosságra hozójának is elvileg be kellene tudnia azt mutatni, hogy beszerezte az érintettől annak hozzájárulását egy ilyen célú adatkezeléshez, és őt előzetesen az adatkezelésről tájékoztatta is. Sajnos azonban itt is elmondható, hogy az esetek túlnyomó többségében GDPR ezen előírásai szintén nem tudnak érvényesülni, hiszen a megszemélyesített személyről legtöbbször lejáratási, megtévesztési céllal hozzák nyilvánosságra az elkészült hamis felvételt. Természetesen ilyen esetekben is elképzelhető legitim adatkezelés, szintén oktatási célokból, de az esetek túlnyomó részét nem az ilyen tartalmak teszik ki.

7. Adatvédelmi jogérvényesítési lehetőségek a deepfake tartalmak készítése és nyilvánosságra hozatala kapcsán

A deepfake videó készítése, illetve nyilvánosságra hozatala jogellenesen történik, ha nem rendelkezik az ezt véghez vivő adatkezelő a GDPR szerinti megfelelő, a 6. cikk (1) bekezdése alapján is igazolható jogalappal. Ilyen jogalap lehet az érintett hozzájárulása a személyes adatainak egy vagy több konkrét célból történő kezeléséhez, szerződéskötés teljesítése, az adatkezelőre vonatkozó jogi kötelezettség teljesítése, természetes személy létfontosságú érdekeinek védelme közérdek vagy közhatalmi jogosítvány gyakorlása vagy a jogos érdek.
A GDPR alkalmazásában a megfelelő jogalap megléte önmagában még nem elegendő ahhoz, hogy az adatkezelés jogszerűnek legyen tekinthető, ugyanis bármely olyan tényező, illetve körülmény, amely miatt a személyes adatok kezelése nem felel meg az adatvédelmi rendeletnek, jogellenességet eredményez (Péterfalvi – Révész – Buzás 2021: 181–183). Így például hiába adta az érintett kifejezett hozzájárulását a személyes adatai kezeléséhez, ha egyébként az adatkezelést megelőzően részére nyújtott tájékoztatás nem volt teljes körű, és ezért nem felel meg a GDPR érintetti tájékoztatással kapcsolatos, a 13. cikkben található előírásainak. A rendelet tehát ebben az esetben is jogellenesnek fogja tekinteni az adatkezelést, hiszen abból a logikából indul ki, hogy megfelelő tájékozottság hiányában nem jöhet létre valóban önkéntes hozzájárulás. Amennyiben az érintett tehát nem tudja, hogy pontosan mihez járul hozzá, úgy nem beszélhetünk a hozzájárulására alapított jogszerű adatkezelésről sem.
A személyes adatok kezelésének a jogellenességét az EU-ban az adott tagállam adatvédelmi felügyeleti hatósága és bíróság is megállapíthatja a GDPR 77. és 79. cikkei alapján. A felügyeleti hatóság legtöbbször a jogellenes adatkezelésről az érintett panasza vagy egy a jogsértést észlelő harmadik személy bejelentése alapján értesül, de előfordulhat, hogy a hatóság a sajtóból vagy az internetről értesüljön a visszaélésről. A bíróság szintén az érintett kereseti kérelme alapján szerezhet tudomást a jogsértésről, vagy ha az adatvédelmi felügyeleti hatóság a jogsértést megállapító közigazgatási határozatát a GDPR 78. cikkében foglaltak alapján megtámadják a bíróság előtt.
A probléma a GDPR által biztosított fenti jogorvoslati rendszerrel, hogy a deepfake videókat készítő és közzétevő adatkezelők beazonosítása a legtöbb esetben rendkívül nehéz feladat, legalábbis az adatvédelmi hatóságok közigazgatási eljárásainak keretei között. Ennek oka, hogy a hamis videók készítői általában ügyelnek arra, hogy nehezen legyenek beazonosíthatók az interneten. A tényleges jogsértést elkövető személy mint adatkezelő beazonosítása ezért a büntetőeljárásokban használatos nyomozati eszközöket igényelne.
A hatósági vagy bírósági úton történő jogérvényesítés eszközein túl az érintettnek is lehetősége van, hogy akár közvetlenül az adatkezelőhöz forduljon, és a személyes adatai jogellenesen

kezelése esetén kérje azok törlését a tartalom készítőjétől vagy közzétevőjétől a GDPR 17. cikk (1) bekezdés d) pontja alapján. Természetesen ezen érintetti joggyakorlás kapcsán is el lehet mondani, hogy a legtöbb esetben nem hatékony módszer a deepfake tartalmakkal összefüggő jogsértések orvoslására, mivel az adatkezelőnek nem áll érdekében azok teljesítése, sőt legtöbbször nem is reagálnak ezekre (ha egyáltalán elérhetőek valamilyen címen keresztül). A deepfake kapcsán felmerülő jogsértések kivizsgálása ezért az érintettek rendelkezésére álló, továbbá hatósági és bírósági eszközökkel a legtöbb esetben sajnos egyáltalán nem hatékony.
További megoldás lehet a deepfake készítője, illetve közzétevője ellen büntetőeljárás indítása, mivel a legtöbb esetben az ilyen tartalmak a Büntető Törvénykönyvről szóló 2012. évi C. törvényben foglalt, a 226/A. §-ba ütköző „a becsület csorbítására alkalmas hamis hang- vagy képfelvétel készítésének" vagy a 226/B. § szerinti ilyen felvétel „nyilvánosságra hozatalának" tényállását meríthetik ki. E bűncselekmények speciális elkövetési magatartása a hamis, hamisított vagy valótlan tartalmú hang- vagy képfelvétel készítése, nyilvánosságra hozatala vagy hozzáférhetővé tétele, így azok tárgyába a deepfake videók is beletartozhatnak. Jelen fejezetnek nem képezi szűk értelemben vett tárgyát a deepfake jelenségnek az adatvédelmi mellett a büntetőjogi értékelése is, ezért ennek további elemzésétől a tartalmi keretekre való tekintettel eltekintek.

8. Jogalkotási irányok a deepfake tartalmak által a magánszférára jelentett kockázatok kezelése érdekében

A már elkövetett, deepfake tartalmakkal kapcsolatos konkrét jogsértések elleni érintetti és hatósági fellépés nehézségeit az elmúlt időszakban a jogalkotás is felismerte, és igyekszik hatékonyabb eszközöket biztosítani. Ebben a pontban a deepfake tartalmak elleni küzdelemmel kapcsolatos legújabb európai uniós jogalkotási javaslatokat tekintem át.
Az első jogalkotási javaslat, amely foglalkozik a deepfake technológia szabályozásával, az Európai Bizottság által nyilvánosságra hozott, a mesterséges intelligenciát érintő, ún. MI-rendelet-tervezet (W5), amely valamennyi uniós tagállamban egységesen végrehajtandó jogszabályként szabályozná a mesterséges intelligencia fejlesztését. A tervezet az MI-ként való besorolásra három feltétel együttes teljesülését írja elő. Először is az MI-nek meghatározott technológiákat kell alkalmaznia, másodszor az ember által kijelölt célokat önállóan kell tudnia követni, végül olyan kimeneteleket kell tudnia produkálni, amelyekkel „befolyásolja" a környezetet. Az új kódex tervezete a gépi tanuláson alapuló rendszerekre is kiterjeszti a hatályát (MI-rendelet-tervezet 3. cikk 1. pont és I. melléklet).
A rendelettervezet kockázatalapú megközelítést alkalmaz az MI-k besorolása szempontjából, amely összesen négy nagy kategóriába igyekszik felosztani a rendszereket. Ezek alapján különbséget tesz az elfogadhatatlanul magas kockázatúként besorolt, azaz tiltott rendszerek, a magas kockázatú rendszerek, a korlátozott kockázatú rendszerek és a minimális/kockázat nélküli rendszerek között.
Anélkül, hogy mélyebben elemeznénk az egyes kockázati szinteket, témánk, tehát a deepfake technológia adatvédelmi értékelése kapcsán fontos azt megemlíteni, hogy az MI-rendelet-tervezet kifejezetten utal a szövegében többször is erre a technológiára. A javaslat indokolása kiemeli, hogy célja megbízható kockázati módszertant meghatározni az olyan MI-rendszerek értékelésére, amelyek jelentős kockázatot jelentenek az emberek egészségére és biztonságára vagy alapvető jogaira nézve. Ezeknek az MI-rendszereknek meg kell felelniük a megbízható mesterséges intelligenciára vonatkozó kötelező horizontális követelményeknek, és megfelelőségértékelési eljárások tárgyát kell képezniük, mielőtt forgalomba hoznák őket az uniós piacon. Ezek célja, hogy az MI-rendszerek teljes életciklusa során biztosítsák a biztonságot és az alapvető jogok védelmét biztosító meglévő jogszabályok tiszteletben tartását. A javaslat egyes MI-rendszerek esetében azonban csak minimális átláthatósági

kötelezettségeket javasol. Ide tartoznak különösen a csevegőrobotok vagy a deepfake-tartalmak (MI-rendelet-tervezet indokolása 1.1. pont).
A deepfake tartalmakkal kapcsolatban a rendelettervezet megemlíti, hogy szabályozásukra az általuk jelentett manipulációs kockázatok miatt van szükség, mivel azok erre alkalmas tartalmakat hoznak létre vagy meglévő tartalmakat manipulálnak. Ezért a tervezet szerint, ha az emberek ilyen rendszerekkel érintkeznek, úgy őket előzetesen tájékoztatni kell annak tényéről, hogy deepfake-kel van dolguk. Ezt a rendelettervezet úgy fogalmazza meg, hogy ha az MI-rendszert olyan képek, audio- vagy videótartalmak létrehozására vagy manipulálására használják, amelyek érzékelhetően hasonlítanak hiteles tartalmakra, kötelezővé kell tenni annak előzetes közlését, hogy a tartalom mesterséges módon jött létre, vagy azt manipulálták (MI-rendelet-tervezet 52. cikk (3) bekezdés). Ez lehetővé teszi a személyek számára, hogy megalapozott döntéseket hozzanak, vagy visszalépjenek adott helyzetből.
A rendelettervezet tehát kötelezővé tenné a deepfake tartalmak kapcsán annak előzetes közlését, hogy az ilyen technológiát használva, tehát a „valóság manipulálásával" jött létre. Ennek hiányában a deepfake tartalom valószínűsíthetően jogellenes lesz, így annak létrehozása és nyilvánosságra hozatala nemcsak adatvédelmi, hanem MI-szabályozási szempontból sem lesz jogszerű.
A szabályozás előremutató, azonban a legfőbb kérdés annak hatékonyságával kapcsolatban, hogy vajon hogyan lesz majd képes azt az EU betartatni. Erre a választ szabályozási szempontból azonban nem feltétlenül az MI-rendelet-tervezetben, hanem egy másik, még alkalmazás előtt álló jogszabályban, a Digitális Szolgáltatások Egységes Piacáról szóló rendelettervezetben (*Digital Services Act, DSA*) találjuk (W6).
A DSA kidolgozására azért volt szükség, mivel az online szolgáltatások biztosításával kapcsolatos jelenlegi szabályozás a 2000-ben hatályba lépett, az elektronikus kereskedelemről szóló irányelvben található, amelynek elfogadására immár több mint két évtizede került sor (W7). Az online világ azóta hatalmasat változott, az online platformokon keresztül történő kommunikáció és a határokon átnyúló online kereskedelem a mindennapok részévé vált. A DSA hatálya éppen ezért a legtöbb online elérhető szolgáltatásokat kínáló platformra kiterjed, beleértve az online piactereket, kereskedelmi platformokat, közösségi oldalakat, tartalommegosztó szolgáltatásokat, applikációk letöltését kínáló weblapokat. Ennek oka, hogy ezeket a felületeket gyakran használják illegális tartalmak terjesztésére vagy illegális áruk vagy szolgáltatások online értékesítésére (W8). Néhány nagy szereplő pedig olyan meghatározó – és ez idáig nem vagy nem kielégítően szabályozott – befolyásra tett szert az online piacok és az online információcsere területén, ami komoly nemzetbiztonsági és alkotmányos aggályokat vet fel (lásd a Cambridge Analytica-botrányt; Domokos 2021: 122).

Erre kíván megoldást nyújtani a DSA többek között a jogellenes online tartalmak eltávolítására vonatkozó kötelező szabályok bevezetésével, a szolgáltatók online piacokon történő nyomon követhetőségével, továbbá a tartalommoderáció egységes és általános szabályozásának előírásával és átláthatósági intézkedésekkel (algoritmusok, ajánlórendszerek működése, célzott hirdetések szempontjai, a hirdetők azonosíthatósága). Ezek kapcsán a platformoknak többek között olyan intézkedéseket kell bevezetniük, amelyek kapcsán ki tudják szűrni a manipulatív és hamisított tartalmakat, beleértve a megtévesztő deepfake videókat is (Moyer 2022). Ennek gyakorlati kivitelezése természetesen további kérdéseket vet fel, egyes álláspontok szerint a tartalmak automatikus elemzése és szűrése mellett, az emberi beavatkozást is lehetővé tevő moderálási rendszerek bevezetésére és a panasztétel jogának biztosítására is szükség lesz a DSA vonatkozó rendelkezéseinek való megfelelés érdekében (Frosio – Geiger 2022: 37–38). A DSA-t 2024. január 1-től kellene alkalmazni az Európai Unióban valamennyi, a hatálya alá tartozó szolgáltatónak.

9. Összegzés

Mint az előzőekben láthattuk, a deepfake tartalmak előállítására alkalmas MI-szoftverek tanítása és az ilyen tartalmak előállítása személyes adatok kezelésével jár, azonban ezen adatkezelések jogszerűsége a legtöbb esetben erősen kérdéses. Ezen kívül magának a már kész tartalomnak, tehát a deepfake videónak mint személyes adatnak a felhasználása is számos jogsértő helyzetet eredményezhet a mindennapokban.
A jelenleg hatályos vonatkozó uniós jogszabály, tehát a GDPR szabályai kapcsán felmerülő adatvédelmi aggályokon kívül érdemes azonban egy lépéssel hátrébb lépni és általános társadalmi problémaként tekinteni a deepfake tartalmakra. Az ilyen videók nagy része eleve manipulációs vagy lejáratási céllal készül. A megszemélyesített, szintetikus módon előállított, egyébként egy valós személyre megszólalásig hasonlító szereplő és általa mondott szintén mesterségesen előállított mondatok és tanúsított cselekmények célja a nézők becsapása, manipulálása, a személyiség ellopása és ezen keresztül a valóság meghamisítása. Az ilyen valótlan, az embereket félrevezető tartalmaknak komoly hatásuk lehet az egy-egy társadalmi jelenség kapcsán kialakult közbeszédre és a jelenségre adott társadalmi reakciókra. A meghamisított információk alapján kialakuló közbeszéd és vélemények rossz irányba terelhetik a témáról folyó diskurzust, ami szintén fals, az adott problémát rosszul kezelő reakciókat és megoldásokat szül.
Mindezek miatt nagyon fontos társadalmi kérdés a deepfake tartalmak megfelelő kezelése és a hatékony jogi reakciók kialakítása azokkal kapcsolatban. Láthatjuk, hogy a jelenleg hatályos és alkalmazandó európai uniós adatvédelmi keretrendszer csak tüneti úton képes kezelni a deepfake által jelentett jogsértéseket, és azokra nem tud igazán hatékony reakciót adni, mivel a tartalmat előállító és terjesztő adatkezelő személyének azonosítása nehezen lehetséges az interneten. A kiváltó okokat az adatvédelmi szabályozás így jelenlegi formájában nem képes hatékonyan kezelni. Örvendetes viszont, hogy a legújabb európai uniós jogalkotási kezdeményezések, így az MI-rendelet és a DSA már konkrétabb fellépést fognak lehetővé tenni. A kérdés már csak az, hogy a deepfake tartalmak technikai felderítése és azonosítása hatékonyan megvalósítható-e, és így a szolgáltatók érvényt is tudnak-e megfelelően szerezni a jogi előírásoknak. Remélhetőleg, ha talán nem is teljes körű, de mindenképpen magasabb szintű védelem fog létrejönni az elkövetkező időszakban ezek ellen az alapvetően káros tartalmak ellen.

Szakirodalom

Balogh Gyöngyi – Bíró János – Deák Ferenc – Kovács Melinda – Tömösi Ramóna 2019: *Az adatvédelmi jog alapelvei, fogalmai, szereplői, profilalkotás, a személyes adatok különleges kategóriái, bűnügyi személyes adatok*. Budapest: Nemzeti Közszolgálati Egyetem.

Chesney, Bobby – Citron, Danielle 2019: Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security. *California Law Review* 107/6. https://doi.org/10.15779/Z38RV0D15J [2022. 09. 30.]

Domokos Márton 2021: Globális törésvonalak – a Cambridge Analytica-ügy. In: Szabó Endre Győző (szerk.): *Az Infotörvénytől a GDPR-ig.* Budapest: Ludovika Egyetemi Kiadó. 119–142.

Ethem, Alpaydin 2016: *Machine learning: the new AI*. Cambridge MA: MIT Press Essential Knowledge Series.

Frosio, Giancarlo – Geiger, Christophe 2022: Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime. *European Law Journal* (forthcoming). http://dx.doi.org/10.2139/ssrn.3747756 [2023. 02. 14.]

Goodfellow, Ian J. – Pouget-Abedie, Jean – Mirza, Mehdi – Xu, Bing – Warde-Farley, David – Ozair, Sherjil – Courville, Aaron – Bengio, Yoshua 2014: Generative Adversarial Networks. *Département d'informatique et de recherche opérationnelle, Université de Montréal*. arXiv:1406.2661 [2023. 02. 14.]

Kietzmann, Jan – Lee, Linda W. – McCarthy, Ian P. – Kietzmann, Tim C. 2020: Deepfakes: Trick or treat? *Business Horizons* 63/2. doi:10.1016/j.bushor.2019.11.006 [2022. 09. 30.]

Klein Tamás – Tóth András (szerk.) 2018: *Technológia jog – robotjog – cyberjog* [sic!]. Budapest: Wolters Kluwer.

Miskolczi Barna – Szathmáry Zoltán 2018: *Büntetőjogi kérdések az információk korában*. Budapest: HVG Orac.

Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.) 2021: *Magyarázat a GDPR-ról*. Budapest: Wolters Kluwer.

Schiff Beáta 2020: *A gépi tanulás és MI adatvédelmi kérdései a deepfake technológia vonatkozásában*. Szakdolgozat. Kézirat. Budapest: KRE ÁJK.

Szmolenszki Ildikó 2018: *A személyes adatok büntetőjogi védelme*. Szakdolgozat, kézirat. Budapest: ELTE ÁJK JTI.

Tóth Dávid 2020: Személyiséglopás az interneten. *Büntetőjogi Szemle* 2020/1. https://ujbtk.hu/wp-content/uploads/lapszam/BJSz_202001_113-119o_TothDavid.pdf [2022. 09. 30.]

Források

Datatilsynet 2018: *Artificial intelligence and privacy*. Report, January 2018. https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf [2022. 09. 29.]

Goble, Rachel 1999: The execution of Perkin Warbeck. *History Today*, 1999. november 11. https://www.historytoday.com/rachel-goble/execution-perkin-warbeck [2022. 09. 30.]

Hlács Ferenc 2016: AI: a nem emberi intelligencia már velünk van? 1. rész. *HWSW*, 2016. június 20. https://www.hwsw.hu/hirek/55760/ai-mesterseges-intelligencia-gepi-tanulas-machine-deep-learning.html [2022. 09. 30.]

Moyer, Edward 2022: Amazon, Google, Meta Among Targets of EU Law on Disinformation, Harmful Content. *CNET*, 2022. április 22. https://www.cnet.com/news/politics/amazon-google-meta-among-targets-of-eu-law-on-disinformation-harmful-content/ [2022. 09. 30.]

Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) 2022: NAIH-305-5/2022. számú határozat. https://naih.hu/hatarozatok-vegzesek/file/532-szomszed-kameras-ugy [2022. 09. 30.]

W1 = *Lambert Simnel English pretender*. https://britannica.com/biography/Lambert-Simnel-English-pretender [2022. 09. 30.]

W2 = https://www.youtube.com/watch?v=cQ54GDm1eL0 [2022. 09. 30.]

W3 = https://www.youtube.com/watch?v=enr78tJkTLE [2022. 09. 30.]

W4 = A Európai Parlament és a Tanács (EU) 2016/679. rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:32016R0679 [2022. 09. 30.]

W5 = Az Európai Parlament és a Tanács rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról (javaslat), COM(2021) 206 final, Brüsszel, 2021. április 21. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52021PC0206&from=FR [2022. 09. 30.]
W6 = Az Európai Parlament és a Tanács rendelete a digitális szolgáltatások egységes piacáról (digitális szolgáltatásokról szóló jogszabály) és a 2000/31/EK irányelv módosításáról (javaslat), COM(2020) 825 final, Brüsszel, 2020. december 15. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52020PC0825&from=en [2022. 09. 30.]

W7 = Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem egyes jogi vonatkozásairól (Elektronikus kereskedelemről szóló irányelv). https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:32000L0031 [2022. 09. 30.]

W8 = Európai Bizottság: The Digital Services Act package. https://digital-strategy.ec.europa.eu/hu/node/27 [2022. 09. 30.]

Dr. Eszteri Dániel, PhD
Jogász, a Nemzeti Adatvédelmi és Információszabadság Hatóság osztályvezetője. Az Eötvös Loránd Tudományegyetem Jogi Továbbképző Intézet és a Nemzeti Közszolgálati Egyetem megbízott oktatója adatvédelmi jogból. 2015-ben PhD-fokozatot szerzett a Pécsi Tudományegyetemen a virtuális tulajdonról írt disszertációjával.