9. Modul

A mesterséges intelligencia manipulációja a közösségi médiában

"Azzal érvelni, hogy nem érdekel a **magánélethez való jog**, *mert nincs mit rejtegetned, nem más, mint azt mondani, hogy nem érdekel a* **szólásszabadság**, *mert nincs mit mondanod." - Edward Snowden*

A modulról

Ez a modul két részből áll, és mindkettő a **közösségi médiában történő manipuláció** különböző perspektíváival foglalkozik. A két rész külön-külön, de egymással együtt is használható.

A modul első része **a személyes adatok kezelését járja körbe a közösségi médiaplatformokon**. A diákok saját magatartásukat értékelik, és végig gondoljak adataik nyilvánosságának veszélyeit. Egy további lépésben azt tárgyalják, hogy ezeket az adatokat milyen mértékben használják fel a vállalatok személyre szabott reklámok létrehozására. Végül a modul ezen része foglalkozik az internetes adatok törlésének nehézségével, és megvitatja a lehetőségeket.

A második rész **a "deepfake" jelenséggel** foglalkozik, mint az internetes dezinformáció terjesztésének témaköréből vett résszel. A cél annak tisztázása, hogy mi is az a deepfake, hogyan jön létre, és milyen lehetőségeket és kockázatokat rejt magában. Lehetőség van arra is, hogy a résztvevők maguk is létrehozzanak hamisításokat olyan alkalmazásokkal, mint például a Wombo, és az eredményeket közösen vitassák meg.

Célok

A diákok képesek lesznek:...

- ...Elemezni és értékelni az általuk használt közösségi média csatornákat
- ...Ismerni, átgondolni és mérlegelni a digitális környezet kockázatait és veszélyeit
- ...Védelmi stratégiákat kidolgozni és alkalmazni
- ...Kialakítani az adatok értékének megértését, és megérteni, hogy az interneten található állítólagos ingyenes ajánlatokért adataikkal fizetnek
- ...Elemezni a saját adatsoraikat
- ...Elmagyarázni a deepfake-k mögött álló szándékokat és stratégiákat
- ...Értékelni a tartalomhamisítások formájában megjelenő álhírek demokráciára és társadalomra leselkedő veszélyeit
- ...Felismerni és leírni a tartalomhamisítást, mint a mesterséges intelligencia alapú dezinformáció egy speciális formáját

Időbeosztás - 1. rész: Manipuláció algoritmusokkal

Idő	Tartalom
15 perc	A nyitókérdések megvitatása csoportokban és közösen
15 perc	Elméleti kísérlet + videó
5 perc	A közösségi média adatai
5 perc	Elmélet - Algoritmusok és a GDPR
40 perc	Kutatási feladat - Mutasd meg a fiókodat, és én megmondom, ki vagy
15 perc	Elmélet - Az internet sosem felejt
15 perc	Elmélet - Az internet sosem felejt

Időbeosztás - 2. rész: Tartalomhamisítás

Idő	Tartalom
15 perc	Kvíz - Hamisított vagy valódi?
10 perc	Ötletelés - Mik azok a deepfake-ek?
20 perc	Kutatás - Hogyan működnek a tartalomhamisítások?
10 perc	Hogyan lehet leleplezni a manipulatív tartalomhamisításokat?
20 perc	Feladat - Tartalomhamisítások készítése és értékelés

Bevezetés

Manipuláció az adatokon keresztül a közösségi médiában

Ez a modul egy jól ismert idézettel kezdődik Edward Snowden volt amerikai titkosszolgálati ügynöktől, aki gyorsan nagy feltűnést keltett azzal, hogy nyilvánosságra hozta az Egyesült Államok és Nagy-Britannia megfigyelési stratégiáit. Ez az idézet összefoglalja a modul tanulási céljainak lényegét: **a hangsúly a magánélethez való jogon van a digitális térben, és azon, hogy milyen gondatlanul bánunk a magánadatainkkal ebben a nyilvános térben**. Minden tevékenységünket aprólékosan dokumentálják az interneten, és ennek eredményeképpen részletes profil készül érdeklődési körünkről, fogyasztói magatartásunkról és az általunk fenntartott kapcsolatokról.

Kezdésképp a modul tanításához a diákok csoportokban megvitathatnak egy kérdőívet, és rögzíthetik az eredményeket, hogy a közös megbeszélésen bemutassák azokat (pl. egy poszter vagy egy plakát oldal segítségével).

A következő kérdéseket vitassák meg:

- Milyen alkalmazásokat és weboldalakat használtok rendszeresen?
- Ismeritek a közösségi médiaszolgáltatók (pl. Instagram) valódi nevét?
- Mindenki láthatja a képeiteket a közösségi média profiljaitokon, vagy csak az ismerőseitek?
- Miért vagy aktív a közösségi médiaplatformokon?
- Olvastál már adatvédelmi nyilatkozatot? Érdekel, hogy milyen adatokat gyűjtenek rólad?
- Gugliztál már magadra? Ha igen, meglepett valami? Miért?

Mivel ezek személyes kérdések, a tanulóknak el kell tudni dönteni, hogy **mennyit akarnak felfedni magukról** a csoportos beszélgetések során.

Gyakran **az adatgyűjtés nem magától értetődő**, ami azt jelenti, hogy egyáltalán nem vagy csak kevésbé vagyunk tisztában a digitális térben való tevékenységünk következményeivel.

Példaként a következő forgatókönyvet használhatja az oktató: A tanulóknak el kell képzelniük, hogy minden ember, akivel az utcán találkoznak, azonnal tudja, hol jártak az előbb, hol vették a ruháikat, mit ettek az előbb, vagy mit gugliztak utoljára.

- Hogyan éreznék magukat a diákok?
- Mennyire vannak tudatában annak, hogy milyen információkat tesznek közzé az interneten, és ki fér hozzá?

Vizuális példaként a Tomatolix **video** is le lehet vetíteni a feldolgozás során. Ez a videó egyrészt bemutatja, hogyan lehet megtudnunk, hogy milyen adatokat tárolnak az internetes platformok, másrészt a riporter megpróbálja bemutatni, hogy csak a közösségi média posztok segítségével hogyan tud megkeresni egy valóságos személyt (és ez nagyon rövid idő alatt sikerül is neki). A megfelelő jelenet a videóban 7 percnél kezdődik, és körülbelül 8 percig tart. Ezután, meg lehet kérdezni a diákokat, hogy mit gondolnak erről, és hogy szerintük is lehetséges lenne-e egyszerűen, csak a profiljaik segítségével felkutatni őket. Érdekes lehet többek között a Snapchat "Snap Map" funkciójával, és az ezzel járó lehetőségekkel és kockázatokkal foglalkozni, hiszen itt megjelenik a felhasználó valós tartózkodási helye. Egyrészt megfelelő szűrőket lehet javasolni (pl. egy Bécs-szűrőt, ha Bécsben tartózkodik), mivel a helyinformáció érdekes lehet a barátok számára, másrészt viszont ez a funkció táptalajt kínál a zaklatás számára.

Miután a diákok beszéltek a közösségi médiaplatformokon való felhasználói magatartásukról, egy rövid **kvízjátékot** lehet közösen lejátszani. A diákoknak ki kell találniuk, hogy az olyan platformok, mint az Instagram, a Snapchat és a TikTok milyen adatokat gyűjtenek. A kvíz kitölthető a feladatlap segítségével, vagy a kvíz átvihető egy olyan platformra, mint a Kahoot, vagy a diákok felvetései közvetlenül is megvitathatók.

Továbbá feltehetjük a kérdést, hogy miért gyűjtik ezeket az adatokat? Milyen hasznot húznak belőle? A közösségi médiaplatformok arra **használják az adatainkat, hogy felajánlják azokat a vállalatoknak**, hogy célzott hirdetéseket helyezhessenek el. Mivel az Instagram vagy a TikTok pontosan tudja, hogy Ön nő, 15 és 25 év közötti, és hogy érdekli a sport és a fenntarthatóság, ezért ezután olyan hirdetéseket fognak Önnek mutatni, mint például a bambusz jógamatracok vagy az adalékanyagok nélküli organikus sporttáplálék kiegészítők.

A közösségi médiaplatformok tehát nem elsősorban az embereket akarják összekötni egymással, hanem csak eszközként tekintenek rá. Inkább arról van szó, hogy a személyes adatokat arra használják fel, hogy más cégek hatékony **hirdetéseket helyezhessenek el. Tehát még ha ezek a weboldalak első ránézésre ingyenesek is, passzívan fizetünk**. Fizetünk az időnkért és a figyelmünkért, amelyet a weboldalak arra használnak, hogy adatokat gyűjtsenek rólunk, és azokat a cégek reklámozásra tovább értékesítsék.

A diákoknak most röviden el kell gondolkodniuk, de ellenőrizniük kell az alkalmazásaikat is, hogy milyen adatokat tesznek nyilvánosan közzé (születési dátum, lakóhely, nem, párkapcsolati státusz...), és mennyire érzik komfortosnak, ha ezeket az információkat továbbadják és megosztják, szintén nyilvánosan. Ennek eredményeképpen megállapítható, hogy néhány dolog javítható az adatvédelmi beállítások módosításával. A diákok önállóan kutathatják, hogy mely adatokat lehet és akarják privátra állítani. Közösen megbeszélhetik, hogy milyen lehetőségeik vannak személyes adataik védelmére.

A GDPR és annak jelentése

Azt, hogy az adatvédelem alapvetően mit jelent, országonként eltérő módon határozzák meg. Ez problémákhoz vezethet, mivel az interneten nincsenek országhatárok, és a személyes **adatok gyakran több országon is áthaladnak**, mielőtt célba érnek. Ezért léteznek olyan nemzetközi megállapodások, mint például az "EU-USA adatvédelmi pajzs". Ez a megállapodás az USA és Európa közötti adatcserét szabályozza. Európán belül 2018. május 25. óta hatályos az általános adatvédelmi rendelet (röviden: GDPR), amely a személyes adatok hatóságok és vállalatok általi feldolgozását szabályozza. A GDPR kötelezi a vállalatokat, hogy tájékoztassák a felhasználókat a tárolt adataikról. Ennek elmulasztása esetén magas bírságok szabhatók ki.

> További információk (németül) és izgalmas magyarázó videók a GDPR-ról a következő weboldalon találhatók: **deinedatendeinerechte.de**

Az algoritmusok tudják, mire van szükséged

Ezek a látszólag jól testre szabott hirdetések olyan algoritmusokat használnak, amelyek **a felhasználók böngészési előzményein és mérőszámain alapulnak**. A

hirdetések meghatározott célcsoportok számára hozhatók létre, és így megfelelnek a felhasználók érdeklődési körének és korábban megtekintett tartalmának. Ezek az ajánló algoritmusok azonban teljesen **éleslátó világnézetet** alakíthatnak ki a felhasználók körében, és akár a **felhasználók radikalizálódásához** is vezethetnek.

Ezért fontos, hogy felhasználóként felismerjük az egyoldalú ajánlatok által okozott torzulásokat, és ne bízzunk bennük. Egy másik fontos lépés **az algoritmusok átláthatóvá tétele, etikai irányelvek és a korábban használt algoritmusok elemzése**. Az AlgorithmWatch például egy ilyen követeléseket szorgalmazó civil szervezet lenne.

Tananyag

- Social Media - Introduction.pdf

Hivatkozások

1. (GER) Video: Das weiß das Internet über dich! - Selbstexperiment
2. (GER) Deine Daten Deine Rechte

Mutasd meg a profilod, és megmondom, ki vagy

Az első lépések során a diákok már elgondolkodtak azon, hogy milyen adatokat tesznek közzé nyilvánosan, és mennyire érzik jól magukat ezzel kapcsolatban. Most a profilok ajánlásait, javaslatait és reklámjait kell kiscsoportokban elemezni, és csak ez alapján kell a felhasználó jellemzését megalkotni. Fontos, hogy senkit ne kényszerítsenek semmire, és csak azok a profiljait elemezzék, akik számára ez nem kényelmetlen.

Egy további lépésben a diákok már önállóan kérhetik és elemezhetik a közösségi média fiókjaikban tárolt adatokat. Az adatok lekérdezésének módjára vonatkozó utasítások a függelékben találhatók a gyakrabban használt platformok, az Instagram, a YouTube és a TikTok esetében. Alapvetően az interneten és a platformok GYIK-jaiban is találhatók részletes útmutatások. Az adatok lekérése néhány órától néhány napig is eltarthat. Ezért célszerű az adatokat a foglalkozásokhoz képest legalább egy órával korábban lekérni.

Mit tud rólam az Instagram, a TikTok és társai? Saját adatok elemzése kiscsoportokban (2-4 diák)

A GDPR miatt lehetőséged van arra, hogy az Instagram, Facebook segítségével lekérdezd az összes tárolt adatodat. De vajon tudod, hogy valójában milyen adatokkal rendelkeznek ezek az oldalak rólad?

1. rész - Elemezzétek ki a profilok hirdetéseit, ajánlásait stb.

1. A kiscsoportban válasszatok ki egy vagy több olyan platformot, amelyre be vagytok jelentkezve. Elemezhettek egy profilt közösen, vagy több profilt egymás után. De a csoportban mindig beszélgessetek egymással, és bánjatok egymással tisztelettel! Senkinek sem kell megmutatnia a profilját, ha az illető épp nem akarja!
2. A következőkben próbáljátok meg jellemezni a profilok tulajdonosait a nektek bemutatott tartalom alapján. Kevesebb figyelmet fordítsatok arra, amit az illető maga kedvelt, és inkább arra, amit javasoltak neki.

3. Ehhez görgessetek végig az alkalmazás felületén. Milyen hirdetéseket láttok? Milyen videókat vagy profilokat javasolnak neked?
4. Jegyezd meg azokat a tulajdonságokat, érdeklődési köröket, hobbikat stb., amelyekkel a profil tulajdonosai rendelkeznek.
5. Mennyire hasonlítanak a jellemzések a tényleges profiltulajdonosokra? Mi lepte meg a profiltulajdonosokat? Gondolkodj el azon, hogy miért gondolod úgy, hogy egyes hirdetések vagy javaslatok nem illenek a személyhez, de mégis javasolták azokat.

2. rész - Adatok lekérése

Utasítások az Instagramhoz

1. Menj a saját profilodra.
2. Koppints a fogaskerék ikonra a beállításokhoz. Ott válaszd az Adatvédelem és biztonság menüpontot.
3. Ha lefelé görgetsz, megjelenik az Adatok letöltése szakasz. Koppints a Letöltés kérése lehetőségre.
4. Add meg a fiókodhoz használt e-mail címet.
5. Add meg az Instagram jelszavad.
6. A következő 48 órában meg kell kapnod a jelentést.
7. Töltsd le az adatokat a levélből, és csomagold ki a mappát.
8. Ha az index.html fájlra kattintasz, az Instagram weboldalára jutsz, ahol végigkattinthatod a vállalat birtokában lévő összes információt.

Utasítások a YouTube-hoz

1. Nyisd meg profilod a jobb felső sarokban, és válaszd a "Saját adatok a YouTube-on" lehetőséget.
2. A YouTube-on közvetlenül a weboldal felületén tekintheted meg eredményeidet.

Utasítások a TikTok-hoz

1. A TikTok alkalmazásban koppints a Profilra az alján.
2. Koppints a Menü gombra a tetején.
3. Koppints a Beállítások és adatvédelem lehetőségre.
4. Koppints a Fiók kezelése, majd az Adatok letöltése lehetőségre.

5. A következő 3 napon belül meg kell kapnod a jelentésedet.

3. rész - A jelentések elemzése

Ellenőrizzétek a jelentéseket.

Mi a meglepő? Honnan tudtad, hogy ez az alkalmazás elmenti ezeket az információkat?

Ezek az önvizsgálatok világossá teszik, hogy mennyi adat keletkezik folyamatosan. Egy évtizeddel ezelőttig ez főként PC-ken keresztül történt. Időközben nemcsak az okostelefonok és az azokhoz tartozó alkalmazások generálnak folyamatosan adatokat, hanem a tárgyak internete (IoT) területén az új technológiák, például a viselhető eszközök (pl. pulzusszám és mozgásprofilok mérésére) vagy a kis környezeti mérőállomások (pl. a levegőminőség mérésére) is hihetetlen mennyiségű adatot termelnek. 2020-ban naponta 1 GB adat keletkezett egy felhasználóra vetítve! [1]

Az Instagramra például másodpercenként több mint 1000 fotót töltenek fel, ez körülbelül 100 millió képet jelent naponta! [2]

Tananyag

- Social Media - Introduction.pdf
- Social Media - Worksheet Research.pdf

Hivatkozások

1. Wirtschaftsforum.de: data consumption
2. Instagram Statistics

Az internet sosem felejt!

Ezek az adatok nem tűnnek el csak úgy az internetről. Ráadásul e tartalmak nagy része titkosítatlanul hozzáférhető. Annak bemutatására, hogy a világhálón található adatok, legyenek azok titkosítva vagy titkosítatlanul, örökre kikerülnek az ellenőrzésünk alól, a diákok a **Wayback Machine** segítségével egy kis időutazásra indulhatnak. Felfedezhetik saját iskolai honlapjukat, klubhonlapjaikat vagy blogjaikat. Ezt követően folytassuk **a beszélgetést az internetes archívumok előnyeiről és hátrányairól**, valamint arról, hogy felhasználóként mit lehet tenni, ha kellemetlen tartalmak kerülnek fel az internetre.

Ha magánjellegű tartalom, például meztelen képek kerülnek fel az internetre, senkinek sem kell egyszerűen elfogadnia. Mert még ha a végleges törlés rendkívül nehéz is, akkor is érdemes fellépni ellene! A szerzőkkel a közösségi médiaplatformokon lehet felvenni a kapcsolatot. Ha nem távolítják el a tartalmat, akkor az irányelvek megsértése (meztelenség, erőszak stb.) esetén közvetlenül feljelentést lehet tenni. Egyéb esetekben a megfelelő moderátorokhoz és az oldal üzemeltetőihez lehet fordulni. Más weboldalakkal és blogokkal kapcsolatban is először az oldal tulajdonosaival kell felvenni a kapcsolatot, és kérni őket a tartalom törlésére. Ha a kérésnek nem tesznek eleget, feljelentést lehet tenni a rendőrségen. Ez többek között a "saját képhez való jogra" (UrhG 78. §) vagy a "kiskorúak pornográf ábrázolására" hivatkozhat a 18 év alattiak meztelen képei esetében.[3]

Az alábbi weboldalon további információkhoz juthattok: **www.ombudsstelle.at**

Tananyag

- Social Media - Introduction.pdf
- Social Media - Worksheet.pdf

Hivatkozások

1. saferinternet.at

2. rész Tartalomhamisítás

Az idő szűkössége miatt a modul ezen része elsősorban a videó hamisítványokkal foglalkozik, bár ezek csak egy kis részét teszik ki a digitális dezinformációnak és az álhíreknek. A közösségi médiában történő manipuláció további izgalmas, mélyreható aspektusai lennének például a közösségi média trollok vagy a közösségi robotok működése.

Mik azok a deepfake-ek?

A tartalomhamisítványok **manipulált vagy mesterségesen létrehozott hang- vagy képhordozók, amelyek valódinak tűnnek**. Olyan embereket mutatnak, akik látszólag olyasmit mondanak vagy tesznek, amit soha nem mondanának vagy mondtak volna korábban. A tartalomhamisítványokat mesterséges intelligencia, például gépi tanulás és mélytanulás segítségével hozzák létre.

Köszönhetően a képfeldolgozás és -manipuláció terén megvalósuló új technológiai fejlesztéseknek, a deepfake-ek is egyre hitelesebbnek tűnnek. Egyrészt a számítógépes látás területén olyan **algoritmusokat fejlesztettek ki** és tökéletesítettek, amelyek automatikusan felismerik és feltérképezik az arcszerkezeteket (pl. a szemöldök és az orr helyzetét), ami új technológiákat eredményezett az arcfelismerésben. Másrészt az internet térhódítása - és különösen a képeket és videókat megosztó platformok révén - hihetetlenül **nagy adathalmazt** hozott létre az ehhez felhasználható audiovizuális adatokkal.

A tartalomhamisítás programokban általában két konkrét mesterséges intelligencia-megközelítéssel találkozhatunk: a Generative Adversarial hálózatokkal (GANs) és az automatikus kódolással. A GAN-ok olyan gépi tanulási algoritmusok, amelyek képesek képsorozatokat elemezni, és ezáltal új, hasonló minőségű képeket létrehozni. Az autokódolók ezzel szemben képesek a képekből információt kinyerni az arcszerkezetekről, és ezt az információt felhasználni egy új arckifejezés modellezésére.

Mivel ezekkel a technikákkal valósághűen lehet szimulálni egy személy arckifejezéseit és mozgástípusait, ma már nagyon nehéz megmondani, hogy egy hamisítványt vagy az eredetit nézzük. Azonban nem csak egy meglévő arc arckifejezéseit lehet megváltoztatni: Az arcok kicserélhetők és a semmiből is létrehozhatók.

A meggyőző számítógépes generált képalkotási (CGI) technológiák már évek óta jelen vannak a filmekben és a moziban. A Benjamin Button különös élete például 2009-ben elnyerte a legjobb vizuális effektek Oscar-díját. Brad Pittet, a film főszereplőjét számítógépes manipulációk segítségével fordítottan öregítették (vagyis folyamatosan fiatalították).

A médiamanipuláció és a képfeldolgozás korántsem új jelenség. A tartalomhamisítás lényegét tekintve csak egy sokkal régebbi jelenség technológiai továbbfejlesztése. A közösségi médiaplatformok megjelenése, és a tartalmak (és így a hamis tartalmak, pl. az álhírek) élénk cseréje és megosztása jelentősen megváltoztatta a médiatájképet. Ráadásul az olyan alkalmazások, mint a Snapchat, az Instagram és a TikTok már alacsony küszöbű szűrőket kínálnak az alkalmazásokon belül, amelyekkel arcokat lehet megváltoztatni és videókat szerkeszteni.

Emellett **a vizuális média, különösen a videó**, mint kommunikációs eszköz térhódítása is jelentős. A vizuális médiát az információterjesztés különösen hatékony módjának tekintik. Eddig is köztudott volt, hogy a szövegekben félretájékoztatást helyeznek el, vagy a fényképeket manipulálják, de a videót sokan még mindig erős bizonyítéknak tartották, amelyet nehéz meghamisítani.

Hamis információkat lehet terjeszteni a deepfake-eken keresztül, és egyes felhasználók már nem tudnak különbséget tenni az igazság és a fikció között. Sok ilyen jelentést szándékosan hoznak létre, hogy valamilyen kárt okozzanak. A **tartalomhamisítás terjedése bizonytalanságot kelt az internetfelhasználók körében**: Mi az igazság, és mi a tény? Ebben az esetben melyik médiában lehet még megbízni, és ki manipulálja a tartalmát? A tartalomhamisítás kizárólagos létezése miatt sok felhasználó már nem biztos abban, hogy melyik tartalomban lehet még megbízni. [4]

A tartalomhamisítási technológiák számos célra felhasználhatók, pozitív és negatív hatásokkal egyaránt. A deepfake-ek hasznosak lehetnek például az audiovizuális médiaprodukciók területén (pl. ha hiányzik egy színész), jobban működhetnek az ember-gép interakciók, de olyan területeken is helyet kaphatnak, mint a videokonferenciák, a szatíra és a művészeti projektek vagy a sebészeti arcrekonstrukció. Ugyanakkor számos negatív aspektus is felmerül, mint például a zsarolás, a rágalmazás, a zaklatás, a személyazonosság-lopás, a jó hírnév megsértése, a hírmédia manipulálása, a tudományba, az üzleti életbe és a politikába vetett bizalom elvesztése, a választások manipulálása, a nemzetközi kapcsolatok és a nemzetbiztonság károsítása.

A **deepfake-ek leleplezése** hosszú időt vehet igénybe, ami azt jelenti, hogy látszólag kis videók nagy problémákhoz vezethetnek. Az óra során a tanulóknak önállóan kell példákat találniuk arra, hogy kik használják ezeket a technológiákat, és kinek árthatnak. A példák végigjátszásával képet kaphatnak arról, hogy milyen méreteket ölthet egy manipulatív hamisítás.

Egy lehetséges fiktív példa a tartalomhamisítás hatásaira

Az Instagramra és a Twitterre feltöltöttek egy látszólag valós videót, amelyen egy politikus a kamera előtt vallja be, hogy több millió eurót csalt ki. Ez a videó nem csak a politikus hírnevét rontja, és pszichológiai károkat okoz. Például a politikust vagy a pártot további hamisított vallomásokkal fenyegetve megzsarolhatják. A választók elveszítik a pártba vetett bizalmukat, és a következő választáson már nem fognak rá szavazni. Ez a bizalmatlanság odáig fajulhat, hogy általában már nem bíznak a rendszerben.

> A funk.net videója (az ARD és a ZDF ajánlata) további információkkal szolgál a tartalomhamisítás felismeréséhez: **www.funk.net - Felismeri a hamisítványt?**

Végül közösen megvitatható, hogyan lehet megelőzni a veszélyes deepfake-eket. A lehetséges megközelítések például a következők lennének: ne tegyél fel magadról videókat a világhálóra, kerüld a hangüzeneteket, ne engedd, hogy a nem kívánt tartalmakat rögzítsék, és ragaszkodj a fényképek/videók törléséhez, szigorú törvények alkalmazása a következőkre vonatkozóan: hamisítás, szigorúbb ellenőrzések (különösen a közösségi médiaplatformokon) a terjedés megfékezésére.

Jogi szempontból a mai napig nincsenek konkrét intézkedések vagy törvények. Stratégiák azonban már kidolgozás alatt állnak, mint például az osztrák szövetségi minisztériumok deepfake cselekvési terve. A jogi helyzet konkrét megváltoztatására azonban nincs szükség, hanem a lakosság tudatosítására és a hamisítványok felismerésére szolgáló szoftvereszközök és tényellenőrző platformok használatára. [5]

Tananyag

- Social Media - Deepfakes.pdf

- ✎ Social Media - Worksheet Deepfakes.pdf
- ✎ Social Media - Worksheet Research Deepfakes.pdf

Hivatkozások

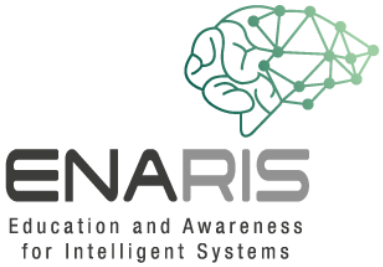
1. saferinternet.at
2. Deepfake Action Plan
3. How to detect deepfakes | Deepfakes explained (english)
4. Fake videos of real people - and how to spot them (english)
5. ganz konkret: Deepfakes gegen Fakten? | Zeit für Politik (german)
6. Deepfakes: Is This Video Even Real? | NYT Opinion (english)
7. How Dangerous are Deepfakes? | Explained (english)
8. Täuschung mit Deepfakes | Odysso - Wissen im SWR (german)

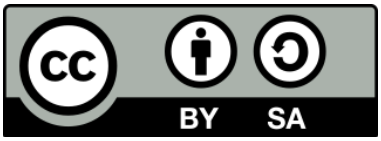
Saját hamisítványt hozunk létre

Az utolsó lépésben a diákok megpróbálhatnak önállóan, alkalmazások segítségével meggyőző hamisítványokat létrehozni. Ehhez hasznos applikáció a Wombo képmanipuláló alkalmazás, amellyel szelfiket lehet énekeltetni. Egy másik lehetséges alkalmazás erre a célra a Reface (megjegyzés: a fizetős Pro módot ki kell X-elni az elején).

Tananyag

- Social Media - Deepfakes.pdf
- Social Media - Worksheet Deepfakes.pdf


ENARIS
Education and Awareness
for Intelligent Systems


BY SA


EUROPEAN UNION


Interreg
Austria-Hungary 2014-2020
European Union – European Regional Development Fund


TU
Graz


mobilis
interaktív kiállítási központ


OESTERREICHISCHE
COMPUTER GESELLSCHAFT
AUSTRIAN
COMPUTER SOCIETY