



Országgyűlési képviselő

Iromány száma: **T/492.**

Benyújtás dátuma: **2026-08-10 15:03**

Parlex azonosító: **N7KFSJVP0001**

Címzett: **Forsthoffer Ágnes, az Országgyűlés elnöke**

Tárgy: **Törvényjavaslat benyújtása**

Benyújtó: **Novák Előd (Mi Hazánk)**

Törvényjavaslat címe: **A mesterséges intelligencia alkalmazásával létrehozott, személyazonosságot manipuláló tartalmakkal való visszaélés szankcionálása érdekében a Büntető Törvénykönyvről szóló 2012. évi C. törvény módosításáról**

Az Alaptörvény 6. cikk (1) bekezdése alapján „**A mesterséges intelligencia alkalmazásával létrehozott, személyazonosságot manipuláló tartalmakkal való visszaélés szankcionálása érdekében a Büntető Törvénykönyvről szóló 2012. évi C. törvény módosításáról**” címmel a mellékelt törvényjavaslatot kívánom benyújtani.

2026. évi törvény

A mesterséges intelligencia alkalmazásával létrehozott, személyazonosságot manipuláló tartalmakkal való visszaélés szankcionálása érdekében a Büntető Törvénykönyvről szóló 2012. évi C. törvény módosításáról

[1] A törvény célja, hogy büntetőjogi választ adjon a generatív mesterséges intelligencia (MI) technológiák gyors fejlődése által teremtett egyes új, súlyos társadalmi veszélyekre.

[2] A törvény bünteti a generatív MI technológia segítségével létrehozott úgynevezett "deepfake" tartalmaknak az érintett személy hozzájárulása nélküli nyilvánosságra hozatalát.

1. §

A Büntető Törvénykönyvről szóló 2012. évi C. törvény a következő alcímmel egészül ki:

„Személyazonosságot manipuláló tartalom nyilvánosságra hozatala

226/C. §

- (1) Aki másról a hozzájárulása nélkül olyan kép- és hangfelvételt tesz hozzáférhetővé,
- a) amelyet mesterséges intelligencia rendszer vagy más hasonló technológia felhasználásával úgy hoztak létre vagy manipuláltak, hogy az erre a személyre érzékelhetően hasonlít, és
 - b) amely megtévesztő módon eredetinek vagy valóságosnak tűnhet,
- vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.
- (2) A büntetés büntett miatt három évig terjedő szabadságvesztés, ha az (1) bekezdésben meghatározott bűncselekményt
- a) nagy nyilvánosság előtt,
 - b) tizennyolcadik életévét be nem töltött személy sérelmére, vagy
 - c) a választás, népszavazás vagy európai polgári kezdeményezés rendjének befolyásolása céljából követik el.”

2. §

Ez a törvény a kihirdetését követő napon lép hatályba.

Általános indokolás

A törvényjavaslat célja, hogy büntetőjogi választ adjon a generatív mesterséges intelligencia (MI) technológiák gyors fejlődése által teremtett egyes új, súlyos társadalmi veszélyekre.

A generatív MI technológián alapuló úgynevezett „deepfake” technológiák lehetővé teszik, hogy bárki, különösebb technikai tudás nélkül valós személyekről megtévesztően élethű videófelveteleket hozzon létre. E tartalmak az érintett személyek, a közbizalom és a demokratikus intézmények ellen fegyverként használhatók, ekként a magán- és a közérdek számára egyaránt súlyos sérelmet okozhatnak.

A hatályos Btk. 226/B. §-a a hamis felvételek nyilvánosságra hozatalát csak akkor szankcionálja, ha a hozzáférhetővé tétel célja a becsület csorbítása. Ez a tényállás nem nyújt védelmet azokkal a manipulált tartalmakkal szemben, amelyek ugyan nem becsületsértőek, de az áldozat engedélye nélkül készültek, és súlyosan sértik az emberi méltósághoz, az önazonossághoz és a képmáshoz fűződő személyiségi jogait. A generatív MI technológia széleskörű elterjedésére válaszul e törvényjavaslat ezt a joghézagot pótolja.

A javaslat illeszkedik az európai jogfejlődés irányába is. Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (a továbbiakban: EU AI Act) - amelynek jogi terminológiájára a törvényjavaslatom is épít - uniós szinten elismeri a deepfake-ekben rejlő megtévesztési kockázatot, és átláthatósági kötelezettségeket ír elő. Míg az EU AI Act az MI-rendszerek fejlesztőivel és telepítőivel szemben állapít meg kötelezettségeket, addig a tagállami büntetőjognak kell fellépnie azzal a felhasználóval szemben, aki a technológiát konkrét személyek sérelmére alkalmazza.

Ezt felismerve több tagállam is lépéseket tett vagy tesz a manipulatív MI-tartalmak büntetőjogi szankcionálására. Franciaország 2024 májusában elfogadott SREN törvénye kifejezetten módosította a francia büntető törvénykönyvet, és szabadságvesztéssel bünteti az engedély nélküli deepfake-ek terjesztését, különös tekintettel a szexuális tartalmúakra. A magyar javaslat ebbe az európai tendenciába illeszkedve biztosítja az emberi méltóság és az alapvető jogok védelmét a digitális korban.

Részletes indokolás

1. §

A bűncselekmény (1) bekezdés szerinti alapesete:

A bűncselekmény elkövetési magatartása a „hozzáférhetővé tétel”, amely a tartalomnak meghatározatlan, nagyobb számú ember számára történő elérhetővé tételét jelenti (pl. feltöltés nyilvános weboldalra, közösségi média platformra). Ebbe nem esnek bele a magáncélú közlések, így egy zárt, néhány fős baráti csoportban (pl. privát üzenetküldő alkalmazásban) megosztott tartalom nem valósítja meg a „hozzáférhetővé tételt”. Ezzel a fogalomhasználattal a Javaslat biztosítja, hogy a magánszférában zajló, alacsony sérelemkockázatú cselekmények (pl. baráti viccelődés) ne minősülhessenek bűncselekménynek, és a büntetőjogi tilalmat azokra az esetekre tartja fenn, ahol a személyiségi jogi sérelem a szélesebb körű megismerhetőség miatt valós és súlyos.

Az (1) bekezdés a) és b) pontja együttesen határozza meg a „manipulált tartalom” fogalmát, átvéve az EU AI Act ezzel kapcsolatos definícióját. A tényállásszerűséghez két feltétel szükséges: 1) a tartalomnak egy valós személyre kell hasonlítani, és 2) megtévesztő jellegűnek kell lennie, azaz alkalmasnak kell lennie arra, hogy egy átlagos személyt a valószínűség látszatával tévedésbe ejtsen.

Az alapeset vétség, amelynek büntetési tétele összhangban van a Btk. hasonló súlyú, személyiségi jogokat sértő bűncselekményeinek büntetési tételével.

A bűncselekmény (2) bekezdés szerinti minősített esetei:

A (2) bekezdés a bűncselekmény súlyosabb, nagyobb társadalmi veszélyességgel bíró eseteit rendeli büntetni, büntetési (és nem vétségi) alakzatban.

A (2) bekezdés a) pontja (nagy nyilvánosság): A „nagy nyilvánosság” fogalmát a Btk. 459. § (1) bek. 22. pontja határozza meg. Amennyiben a hozzáférhetővé tétel ezen minősített módon történik, a cselekmény társadalomra veszélyessége – a sérelem gyors és kontrollálhatatlan terjedése miatt fokozott.

A (2) bekezdés b) pontja (kiskorú sérelmére történő elkövetés): A Javaslat egyik elsődleges célja a gyermekvédelem, hiszen a kiskorúak esetében a deepfake technológia különösen súlyos és maradandó károkat okozhat.

A nemzetközi tapasztalatok azt mutatják, hogy a kiskorúak a deepfake technológiával való

visszaélések kiemelt célpontjai. A deepfake-ek a kiberzaklatás (cyberbullying) új, pusztító formáját jelentik. Gyakori eset például osztálytársakról készült, közösségi médiából gyűjtött képek felhasználása olyan alkalmazásokkal, amelyek hamis meztelen képeket generálnak, és ezeket terjesztik az iskolai közösségben.

Ennél is súlyosabb, amikor a technológiát pl. bűnözők aktívan használják szexuális zsarolásra (sextortion). Az elkövetők a kiskorú áldozatról készült hamis, de élethű pornográf felvétellel kényszerítik az áldozatot pénz fizetésére vagy valódi szexuális tartalmú képek átadására, amely esetben viszont már súlyosabb bűncselekmények megvalósulása is alappal felmerül, mindenesetre ez a visszataszító jelenség a szabályozás indokoltságát kiválóan példázza.

A (2) bekezdés c) pontja (választások befolyásolása): Ez a minősített eset a demokratikus intézmények védelmét szolgálja. A deepfake technológia új, hatékony eszközt ad a választópolgárok jogellenes befolyásolására és a dezinformációs kampányokra. Ezek a támadások nem csupán egy jelölt reputációját sértik, hanem a teljes választási folyamatba vetett közbizalmat és a tájékozott döntéshozatal lehetőségét ássák alá. Ezeknek a jelenségeknek a büntetőjogi tilalmát nem biztosítják teljeskörűen a választás rendjét jelenleg védő tényállások, ezért indokolt ennek a minősített esetnek a külön szabályozása.

2. §

Hatályba léptető rendelkezés.