nem hivatalos fordítás

DIGITÁLIS SZOLGÁLTATÁSOK
EURÓPAI TESTÜLETE

A Digitális Szolgáltatások Európai Testülete és a Bizottság együttműködésében a digitális szolgáltatásokról szóló rendelet 35. cikkének (2) bekezdése alapján készített első jelentés a legjelentősebb és ismétlődő rendszerszintű kockázatokról, valamint a kockázatcsökkentési intézkedésekről

2025. november 18.

DIGITÁLIS SZOLGÁLTATÁSOK
EURÓPAI TESTÜLETE

Tartalomjegyzék

1. A jelentés tárgya

A digitális szolgáltatásokról szóló rendelet (a továbbiakban: „rendelet”) az online közvetítő szolgáltatásokat, platformokat, például az online piactereket[1], a közösségi hálózatokat, az alkalmazásáruházakat, illetve a keresőprogramokat szabályozza. A rendeletben foglalt szabályok felügyeletét és végrehajtását az Európai Bizottság és a tagállami hatóságok, mégpedig a digitális szolgáltatási koordinátorok végzik, amelyek mindegyike együttműködik a Digitális Szolgáltatások Európai Testületében (a továbbiakban: „Testület”).

A rendelet 34. és 35. cikke szerinti kockázatkezelési keret megállapítja az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók legfontosabb kötelezettségeit. E szolgáltatások Unión belüli aktív igénybe vevőinek száma legalább 45 millió. A rendelet 34. cikkének (1) bekezdése megállapítja a szolgáltatók azon kötelezettségét, hogy „*gondosan azonosítaniuk, elemezniük és értékelniük kell a szolgáltatásaik és a kapcsolódó rendszerek – többek között az algoritmikus rendszerek – kialakításából vagy működéséből vagy a szolgáltatásaik használatából eredő rendszerszintű kockázatokat*”. A rendelet 35. cikkének (1) bekezdése előírja, hogy az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak észszerű, arányos és hatékony kockázatcsökkentési intézkedéseket kell hozniuk a kockázatértékeléseikben azonosított rendszerszintű kockázatokhoz igazodva. Ennek során a szolgáltatóknak kiemelt figyelmet kell fordítaniuk az ilyen intézkedések alapvető jogokra gyakorolt hatásaira. A rendelet (90) preambulumbekezdése továbbá kimondja, hogy az online óriásplatformot és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak „*biztosítaniuk kell, hogy kockázatértékelési és -csökkentési megközelítésük a rendelkezésre álló legjobb információkon és tudományos ismereteken alapuljon, és hogy feltételezéseiket a kockázatok által leginkább érintett csoportokkal és az általuk hozott intézkedésekkel teszteljék*”. Ezek a rendelkezések az online óriásplatformot és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatókra alkalmazandóak, de nem alkalmazandóak azokra a platformokra, illetve egyéb közvetítő szolgáltatásokra, amelyek esetében az Unión belüli aktív igénybe vevők havi átlagos száma nem éri el a 45 millió fős küszöbértéket.

1.1. E jelentés háttere

A rendelet 35. cikkének (2) bekezdése megállapítja azt a követelményt, hogy a Testületnek a Bizottsággal együttműködve évente egyszer átfogó jelentést kell közzétennie. A rendelet 35. cikkének (2) bekezdése előírja, hogy azonosítani és értékelni kell az Unión és a tagállamokon belüli legjelentősebb és ismétlődő rendszerszintű kockázatokat, valamint az azok csökkentésére alkalmazott bevált gyakorlatokat.

[1] A rendelet ezekre „*a kereskedőkkel távollévők között kötött szerződések létrehozását lehetővé tevő online platformok*”-ként hivatkozik.

Ez az első jelentés a Testület és a Bizottság kezdeti észrevételeit tartalmazza a kijelölt online óriásplatformok és nagyon népszerű online keresőprogramok által a rendelet végrehajtása terén felmerülő rendszerszintű kockázatokkal és a kapcsolódó kockázatcsökkentési intézkedésekkel kapcsolatban szerzett első tapasztalatok alapján. Ez a jelentés áttekintést nyújt a kijelölt szolgáltatók által a szolgáltatásaik alapján azonosított, valamint az érdekelt felek – például a független kutatók és a civil társadalmi szervezetek – által azonosított legjelentősebb és ismétlődő rendszerszintű kockázatokról, továbbá bizonyos kockázatcsökkentési gyakorlatokról. A kockázatcsökkentés tekintetében ez az első alkalommal kiadott jelentés az alkalmazott vagy javasolt gyakorlatokra helyezi a hangsúlyt. Idővel – és a rendelet gyakorlati végrehajtása során szerzett tapasztalatok alapján – a jelentés jövőbeli kiadásai a rendszerszintű kockázatok csökkentése terén változó bevált gyakorlatok azonosítását is célul tűzik ki.

1.2. A rendelet szerinti kockázatkezelési keret mint az alapvető jogok – többek között a véleménynyilvánítás és a tájékozódás szabadságához való jog – kulcsfontosságú biztosítéka

A rendelet egyik legfontosabb célkitűzése annak biztosítása, hogy az Európai Unió Alapjogi Chartájában (a továbbiakban: „Charta”) rögzített jogok hatékony védelemben részesüljenek online, ahogyan azt a rendelet céljairól szóló 1. cikk konkrétan kimondja. A rendelet 35. cikkének (2) bekezdése szerinti éves jelentések első kiadása ezért lehetőséget teremt annak kiemelésére is, hogy a kockázatkezelési keret a rendelet sarokköve, és ebből kifolyólag az alapvető jogok online védelmére szolgáló eszköz.

Erre tekintettel a Testület és a Bizottság emlékeztet arra, hogy a rendelet 34. cikke (1) bekezdésének b) pontja előírja, hogy az online óriásplatformot és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak gondosan azonosítaniuk, elemezniük és értékelniük kell az alapvető jogok gyakorlását érintő tényleges vagy várható negatív hatásokat.

E jelentés kidolgozása során a Testület és a Bizottság megállapította, hogy a szolgáltatók és civil társadalmi szervezetek online óriásplatformok és nagyon népszerű online keresőprogramok szolgáltatásainak és az azokhoz kapcsolódó rendszereknek a kialakításából vagy működéséből, illetve a szolgáltatásaik igénybevételéből eredő rendszerszintű kockázatokat állapítottak meg, amelyek a véleménynyilvánítás és a tájékozódás szabadságához való alapvető jogot érintették.

- A Testület és a Bizottság emlékeztet arra, hogy a rendelet 35. cikkének (1) bekezdése előírja, hogy az online óriásplatformot vagy a nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak észszerű, arányos és hatékony kockázatcsökkentési intézkedéseket kell bevezetniük, kiemelt figyelmet fordítva az ilyen intézkedéseknek az Alapjogi Charta 11. cikkében rögzített alapvető jogokra – többek között a véleménynyilvánítás és a tájékozódás szabadságához való jogra – gyakorolt hatásaira.

- A Testület és a Bizottság emlékeztet arra is, hogy a rendelet (86) preambulumbekezdése a következőket mondja ki: „Az online óriásplatformot és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak a szükséges eszközök használatával, kellő gondossággal eljárva – az alapvető jogok tiszteletben tartásával – csökkenteniük kell a kockázatértékelésben azonosított rendszerszintű kockázatokat. (...) Az említett szolgáltatóknak különös figyelmet kell fordítaniuk a véleménynyilvánítás szabadságára gyakorolt hatásra.”

A kockázatkezelési kereten túlmenően a rendelet átfogó biztosítékokat tartalmaz a véleménynyilvánítás és a tájékozódás szabadságához való alapvető jog Unión belüli online védelme érdekében.

- ***Fiókok felfüggesztéséhez kapcsolódó panaszkezelési mechanizmus*** A rendelet 20. cikke létrehozta azt a követelményt, hogy a felhasználók számára időben rendelkezésre álló, megkülönböztetéstől mentes, kellő gondosságon alapuló és nem önkényes panaszkezelési mechanizmust kell biztosítani. Ha például egy fiókot felfüggesztenek, a felhasználója jogosult vitatni a döntést, és jogosult arra, hogy választ kapjon az online platform szolgáltatójától.

- ***A tartalommoderálás átláthatósága:*** A rendelet 17. cikke átláthatóságot ír elő a tartalommoderálással kapcsolatos döntésekre vonatkozó kritériumok tekintetében, ideértve az „árnyékletiltási” gyakorlatokat is. Egy fiók letiltásakor például a felhasználóját tájékoztatni kell, és a felhasználó jogosult vitatni a döntést.

- ***Az ajánlórendszereken belüli részrehajlások kezelése:*** A rendelet 27. és 38. cikke az ajánlórendszereken belüli részrehajlások megakadályozását, illetve minimálisra csökkentését célzó új eszközöket vezetett be azáltal, hogy az online óriásplatformot és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatók számára új követelményként előírta, hogy a felhasználók nem profilalkotáson alapuló alternatív lehetőségeket is igénybe vehessenek.

1.3. Jelentéstételi időszak és a rendelet végrehajtási tevékenységeivel való kapcsolat

Ez a jelentés a 2024. február 17. és 2025. február 16. közötti jelentéstételi időszakra vonatkozik. Ez a jelentéstételi időszak egybeesik a rendelet átláthatósági jelentéstételre vonatkozó intézkedései alkalmazási időszakának kezdetével, és attól számított egy évig tart.

Az e jelentésben foglalt megállapítások egyike sem értelmezendő a rendelet 34. vagy 35. cikkének való megfeleléshez tartozó iránymutatásként. Az e jelentésben foglalt megállapítások egyike sem értelmezendő úgy, hogy értékelné kijelölt online óriásplatformoknak és nagyon népszerű online keresőprogramoknak a rendelet 34. vagy 35. cikkének vagy bármely egyéb

rendelkezésének való megfelelését. Ez a jelentés nem sért egyetlen jelenlegi vagy jövőbeli vizsgálatot, végrehajtási intézkedést vagy a rendelet alapján tett hivatalos megállapítást sem.

2. Hogyan készült ez a jelentés?

Az a jelentés az alábbi források alapján készült:

- Az online óriásplatformot és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatók által 2023-ban és 2024-ben a Bizottságnak és a letelepedési helyük szerinti digitális szolgáltatási koordinátoroknak benyújtott kockázatértékelési jelentések közzétett változatai[2]:
    - E jelentés közzétételekor a 2023 áprilisában kijelölt első 17, online óriásplatformot üzemeltető szolgáltató[3] és első 2, nagyon népszerű online keresőprogramot üzemeltető szolgáltató[4] elvégezte a rendelet 34. cikke szerinti első kétéves kockázatértékelését. A rendelet 42. cikke továbbá előírja, hogy ezeket a kockázatértékelési jelentéseket be kell nyújtani a Bizottságnak és a letelepedési helyük szerinti tagállam digitális szolgáltatási koordinátorának, és a nyilvánosság rendelkezésére kell bocsátani. Az ezt követően kijelölt szolgáltatókra[5] már szintén vonatkoznak a 34. cikk szerinti kötelezettségek, és ezek a szolgáltatók – a 42. cikkben előírt követelménynek megfelelően – a Bizottság és a letelepedési helyük szerinti tagállam digitális szolgáltatási koordinátor rendelkezésére bocsátották első jelentésüket, de mivel ezen 35. cikk (2) cikke szerinti jelentés tárgyidőszakában az első kockázatértékelési jelentéseknek a nyilvánosság rendelkezésére bocsátására vonatkozó kötelezettség még nem volt alkalmazandó, azokra ez a 35. cikk (2) bekezdése szerinti jelentés nem terjed ki. A Bizottság 2024 novemberében kérdés-felelet összeállítást tett közzé a rendelet 42. cikke alapján a kockázatértékelési jelentésekről, ellenőrzési jelentésekről és ellenőrzés-végrehajtási jelentésekről, hogy további információkat biztosítson a jelentéstételi és közzétételi kötelezettségekről[6].
- A független ellenőrző szervezetek által a rendelet 37. cikke szerint készített ellenőrzési jelentések közzétett változatai;
    - E jelentés közzétételekor a 2023 áprilisában kijelölt első 17, online óriásplatformot üzemeltető szolgáltató és első 2, nagyon népszerű online keresőprogramot üzemeltető szolgáltató a nyilvánosság rendelkezésére bocsátotta a független ellenőrző szervezetektől kapott ellenőrzési jelentéseket.
- Az online óriásplatformot üzemeltető és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatók által a rendelet szerint készített egyéb átláthatósági jelentések:

[2] Az Európai Bizottság következő weboldalán olyan weboldalakra mutató linkek találhatók, ahol a szolgáltatók a digitális szolgáltatási koordinátoraik kockázatértékelési jelentéseit közzétették: https://digital-strategy.ec.europa.eu/en/policies/dsa-brings-transparency#ecl-inpage-lsets8qr.

[3] Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter (now X), Wikipedia, YouTube, Zalando.

[4] Bing, Google Search.

[5] Pornhub, Shein, Stripchat, Temu, XNXX, XVideos.

[6] „*Q&A on risk assessment reports, audit reports and audit implementation reports under DSA"* (Kérdés-felelet összeállítás a kockázatértékelési jelentésekről, ellenőrzési jelentésekről és ellenőrzés-végrehajtási jelentésekről), elérhető a következő linken: https://digital-strategy.ec.europa.eu/en/faqs/qa-risk-assessment-reports-audit-reports-and-audit-implementation-reports-under-dsa.

- A rendelet 39. cikke szerinti hirdetési adattárak;
- A rendelet 37. cikke szerinti ellenőrzés-végrehajtási jelentések, amelyeket az online óriásplatformot üzemeltető és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatók kötelesek a nyilvánosság rendelkezésére bocsátani a független ellenőrző szervezet ellenőrzési jelentésének beérkezését követő egy hónap elteltével, és amelyekben kötelesek közölni az ellenőrző szervezet ajánlásai nyomán tett intézkedéseket. E jelentés közzétételekor a 2023 áprilisában kijelölt első 17, online óriásplatformot üzemeltető szolgáltató és első 2, nagyon népszerű online keresőprogramot üzemeltető szolgáltató tett közzé ellenőrzés-végrehajtási jelentéseket.
- A rendelet 15. cikke, 24. cikke és 42. cikkének (2) bekezdése szerinti, az online óriásplatformot és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatók által a nyilvánosság rendelkezésére bocsátott átláthatósági jelentések a tartalommoderálásra vonatkozóan.
- A rendelet szerinti átláthatósági adatbázis[7] , amely a 17. cikk szerinti indokolásokat a nyilvánosság rendelkezésére bocsátja. A rendelet előírja az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók számára, hogy tájékoztatniuk kell a szolgáltatásaikat igénybe vevőket a tartalommoderálási döntéseikről, és a döntések okait indokolásokban kell kifejteniük, amelyeket továbbítaniuk kell az átláthatósági adatbázisba. Az adatbázis javítja az átláthatóságot és megkönnyíti a tartalommoderálási döntések vizsgálatát, mivel lehetővé teszi az online platformot üzemeltető szolgáltatók által hozott tartalommoderálási döntések szinte valós időben történő nyomon követését.

- A Bizottság, valamint a digitális szolgáltatási koordinátorok által megrendelt (a mellékletben említett) tanulmányok felhasználásával gyűjtött információk;
- Kutatóintézetek független szakértői és civil társadalmi szervezetek által készített kutatások és tanulmányok, ideértve a fentiekben felsorolt, online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók kockázatértékelési jelentéseire és egyéb átláthatósági jelentéseire adott reakciókat tartalmazó kiadványokat, valamint a Testület és a Bizottság által – felkérésre vagy önkéntes beadványok alapján – civil társadalmi szervezetektől, megbízható bejelentőktől[8] és tagállami hatóságoktól beszerzett információkat (e források felsorolása a mellékletben található).
    - E források közül a Testület és a Bizottság a legjobb elérhető információkra és tudományos ismeretekre hagyatkozott annak meghatározásához, hogy a relevanciájuk és a minőségük miatt mely elemzések és észrevételek járulnának hozzá e jelentés kidolgozásához. A rendelet 35. cikkének (2) bekezdése szerinti, jövőbeli éves jelentésekhez a rendelet 40. cikke szerinti, kutatók

[7] A rendelet szerinti átláthatósági adatbázis a következő linken érhető el: https://transparency.dsa.ec.europa.eu/.
[8] A rendelet 22. cikke szerint a megbízható bejelentőket a tagállamok jelölik ki a következő kritériumok alapján: szakértelem és hozzáértés, függetlenség, kellő gondosság, pontosság és tárgyilagosság.

számára biztosított adathozzáférési mechanizmusok segítségével elért adatokon alapuló további tudományos ismeretek is rendelkezésre állnak majd. Ez a jelentés az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók által bejelentett rendszerszintű kockázatokra és kockázatcsökkentési intézkedésekre helyezi a hangsúlyt. A jelentés figyelembe vette továbbá az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók által nem említett, de kutatóintézetek és civil társadalmi szervezetek független szakértői által megerősített rendszerszintű kockázatokat és kockázatcsökkentési intézkedéseket is.

3. Az azonosított legjelentősebb és ismétlődő rendszerszintű kockázatok

Ez a fejezet a rendelet 34. cikke (1) bekezdésének felépítését követi az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatóktól eredő legjelentősebb és ismétlődő rendszerszintű kockázatok áttekintésekor. Ezek a rendszerszintű kockázatok különböző módon és mértékben konkretizálódhatnak a különböző szolgáltatások esetében, többek között a szolgáltatás típusától és igénybevételétől függően. Az online piactereken felmerülő legjelentősebb és ismétlődő rendszerszintű kockázatok például különböznek a közösségimédia- vagy feltérképezési szolgáltatások legjelentősebb kockázataitól. A jogellenes tartalmakhoz vagy a polgári közbeszédhez kapcsolódó rendszerszintű kockázatok általában valószínűleg más-más módon nyilvánulnak meg az egyes tagállamokban, például regionális vagy nyelvi vonatkozások, vagy a jogellenes tartalom egyes tagállamokban eltérő fogalommeghatározása miatt, míg más rendszerszintű kockázatok, például az interfészek kialakításához kapcsolódó rendszerszintű kockázatok általában valószínűleg azonosak lesznek Unió-szerte.

Az online óriásplatformok és a nagyon népszerű online keresőprogramok idővel változnak, és változik az is, ahogyan a felhasználók kapcsolatot tartanak azokon keresztül és kapcsolódnak azokhoz, továbbá a világ is változik, amelyben azokat használják. A kár kockázata és a ténylegesen bekövetkező kár nem azonos. Ugyanígy különbség van valamely jog megsértése és a tényleges jogsértés között. A rendszerszintű kockázat fennállása azt jelenti, hogy az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak intézkedéseket kell hozniuk e kockázat csökkentésére (a kockázatcsökkentési intézkedésekkel kapcsolatban lásd a jelentés 4. fejezetét). Ez a fejezet a rendszerszintű kockázatokra vonatkozó információkat tartalmaz. Nem nyújt áttekintést azokról a kockázatokról, amelyek bekövetkeztek volna.

Ez a fejezet a rendszerszintű kockázatokon kívül arra vonatkozó példákat is bemutat, hogy a 34. cikk (2) bekezdésében említett egyes kockázati tényezők hogyan befolyásolják a rendszerszintű kockázatokat. Fontos megemlíteni, hogy ezeket a kockázati tényezőket külön-külön és együtt is figyelembe kell venni.

Önmagában az a tény, hogy egy rendszerszintű kockázat ismétlődőnek tekinthető, nem jelenti azt, hogy a kockázat változatlan marad. Emellett – ahogyan a rendelet 35. cikke is említi – relevánsak lehetnek a tagállamokban bekövetkező konkrét fejlemények is. Mindezek a változások befolyásolják a kockázatok felmerülésének és alakulásának módját, és szükségessé teszik a rendszerszintű kockázatokra vonatkozó ismeretek folyamatos frissítését. E tekintetben a rendelet (90) preambulumbekezdése kimondja, hogy az online óriásplatformot és a nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak:

- *„[...] biztosítaniuk kell, hogy kockázatértékelési és -csökkentési megközelítésük a rendelkezésre álló legjobb információkon és tudományos ismereteken alapuljon, és*

hogy feltételezéseiket a kockázatok által leginkább érintett csoportokkal és az általuk hozott intézkedésekkel teszteljék. E célból adott esetben kockázatértékelést kell végezniük, és meg kell tervezniük a kockázatcsökkentési intézkedéseiket a szolgáltatásokat igénybe vevők képviselőinek, a szolgáltatásaik által potenciálisan érintett csoportok képviselőinek, független szakértőknek és civil társadalmi szervezeteknek a bevonásával. Törekedniük kell arra, hogy ezeket a konzultációkat beépítsék a kockázatok értékelésére és a mérséklési intézkedések megtervezésére szolgáló módszertanaikba, beleértve adott esetben a felméréseket, a fókuszcsoportokat, a kerekasztalokat, valamint az egyéb konzultációs és tervezési módszereket. Annak értékelésekor, hogy adott intézkedés észszerű, arányos és hatékony-e, különös figyelmet kell fordítani a véleménynyilvánítás szabadságához való jogra."

Ezen túlmenően a rendelet több rendelkezése lehetővé teszi a rendszerszintű kockázatok folyamatos vizsgálatát. A kockázatértékeléseken túlmenően az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak legalább évente egyszer és az azonosított rendszerszintű kockázatokra valószínűsíthetően kritikus hatással lévő funkciók telepítése előtt gondoskodniuk kell arról, hogy készüljenek a rendelet 37. cikkében említett független megfelelési ellenőrzéseken alapuló ellenőrzési jelentések, ellenőrzés-végrehajtási jelentések, az online platformokon a rendelet 15. és 42. cikke szerint végzett tartalommoderálási gyakorlatokról, valamint a rendelet 40. cikke szerinti adathozzáférési szabályokról szóló átláthatósági jelentések.

Az alábbi szakaszok rendszerszintű kockázatokra vonatkozó példákat ismertető háttérmagyarázatokat tartalmaznak. Ezek csak szemléltetési célt szolgálnak, annak érdekében, hogy az olvasó megismerkedjen arra vonatkozó példákkal, hogy bizonyos rendszerszintű kockázatokat hogyan ismertettek a szolgáltatók vagy civil társadalmi szervezetek. Ezek a háttérmagyarázatok nem minősülnek a szolgáltatók által alkalmazott megközelítés értékelésének. Az idézetek kiválasztása és sorrendje továbbá nem azt jelzi, hogy az általuk szemléltetett kockázatok fontosabbak lennének más kockázatoknál. Hasonlóképpen, az alábbi szakaszokban a kockázati tényezőkről készült háttérmagyarázatok kizárólag szemléltetési céllal szerepelnek, és nem minősülnek az észlelt kockázati tényezők átfogó áttekintésének.

3.1. Jogellenes tartalom

A jogellenes tartalmak terjesztése elleni küzdelemhez való hozzájárulás a rendelet központi célkitűzése, ahogyan azt több preambulumbekezdés megerősíti, többek között a (12) preambulumbekezdés, amely kiemeli a „*biztonságos, kiszámítható és megbízható online környezet*” fontosságát. A rendelet ugyanakkor tartalomsemleges, és nem határozza meg, hogy mi minősül „jogellenes tartalomnak”. Ehelyett a tartalom jogszerűségét a tagállami jog és az uniós jog egyéb rendelkezései határozzák meg. A rendelet 3. cikkének h) pontja kimondja, hogy „*»jogellenes tartalom«: bármely olyan információ, amely önmagában vagy egy tevékenységgel kapcsolatban, beleértve a termékek értékesítését vagy a szolgáltatások nyújtását, nem felel meg az uniós jognak vagy bármely tagállam – az uniós joggal összhangban álló – jogának, függetlenül az adott jog pontos tárgyától vagy jellegétől*”. A rendelet 34. cikke (1) bekezdésének a) pontja előírja, hogy a kijelölt online óriásplatformok és nagyon népszerű online keresőprogramok kockázatértékelésének ki kell terjednie a következőhöz kapcsolódó rendszerszintű kockázatokra: „*jogellenes tartalom terjesztése a szolgáltatásaik használatával*”.

A rendelet (80) preambulumbekezdése a szolgáltatók által értékelendő jogellenes tartalmakra vonatkozó példákat közöl: „*Az első kategóriába tartoznak azok a kockázatok, amelyek jogellenes tartalmak – például gyermekek szexuális bántalmazását ábrázoló anyagok vagy jogellenes gyűlöletbeszéd – terjesztése révén, vagy a szolgáltatásaikkal bűncselekmény elkövetése céljából történő egyéb típusú visszaélések révén valósulnak meg; továbbá ide tartoznak a jogellenes tevékenységek folytatásával – például az uniós vagy nemzeti jog értelmében tiltott termékek vagy szolgáltatások, így többek között a veszélyes vagy hamisított termékek, illetve illegális kereskedelemből származó állatok értékesítésével – összefüggő kockázatok is.*”

Az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók rendeletben foglalt kockázatértékelési és kockázatcsökkentési kötelezettségei egy szélesebb kötelezettségcsoport részét képezik. A rendeletnek a bejelentési és cselekvési mechanizmusokhoz (16. cikk), a megbízható bejelentőkhöz (22. cikk), valamint a jogellenes tartalom elleni fellépésre vonatkozó végzésekhez (9. cikk) kapcsolódó rendelkezései központi jelentőségűek a jogellenes tartalmakra vonatkozó általános végrehajtási ökoszisztéma szempontjából. A jogellenes tartalomhoz kapcsolódó rendszerszintű kockázatok továbbá nemcsak az online óriásplatformok és a nagyon népszerű online keresőprogramok összefüggésében vetődnek fel, hanem más uniós jogszabályokban is, például a terrorista tartalomról szóló rendeletben[9].

A digitális szoláltatásokról szóló rendelet keretében a jogellenes tartalmak terjesztésével szemben végrehajtott fellépéseket össze kell hangolni az alapvető jogokkal, többek között a véleménynyilvánítás és a tájékozódás szabadságához való joggal, amely központi szerepet tölt

[9] Az Európai Parlament és a Tanács (EU) 2021/784 rendelete (2021. április 29.) az online terrorista tartalom terjesztésével szembeni fellépésről, elérhető a következő linken: https://eur-lex.europa.eu/eli/reg/2021/784/oj/hun.

be a rendeletben. E célból a rendelet többek között előírja, hogy minden online platformnak átláthatónak kell lennie és lehetővé kell tennie a tartalommoderálási döntéseik vizsgálatát, például követelményként támasztva azt, hogy a szolgáltatóknak tájékoztatniuk kell a felhasználókat a tartalommoderálási döntéseikről és lehetővé kell tenniük a felhasználók számára, hogy jogorvoslatot kérjenek az adott döntések ellen. A rendelet egyértelmű szabályokat állapít meg az átláthatóság, az elszámoltathatóság, valamint a felhasználók védelme és jogokkal való felruházása tekintetében.

A jogellenes tartalmak – többek között termékek, szolgáltatások és tevékenységek – terjesztéséhez kapcsolódó kockázatokat az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető összes szolgáltató megjegyezte kockázatértékelési jelentésében. Ez a szakasz az ezen összefüggésben azonosított legjelentősebb és ismétlődő rendszerszintű kockázatokat ismerteti.

Ez a szakasz (és a jelentés további része) bizonyos bekezdések elején félkövér és dőlt betűkkel szedett, soron belüli címeket használ. Ezek célja, hogy a rendszerszintű kockázatokat, illetve a kockázatcsökkentési intézkedéseket a könnyebb olvashatóság érdekében alkategóriákba csoportosítsa.

Jogellenes termékek, szolgáltatások és tevékenységek. A jogellenes termékek, szolgáltatások és tevékenységek terjesztéséhez kapcsolódó kockázatokat az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók – különösen az online piacterek (pl. veszélyes, a jogszabályoknak nem megfelelő és/vagy hamisított termékek), a közösségimédia-platformok (pl. erőszakos tevékenységek) és az alkalmazásáruházak (pl. rosszindulatú szoftvert (malware) tartalmazó alkalmazások) – megállapították kockázatértékelési jelentésükben. Egyes szolgáltatók a jogszabályoknak megfelelő, de az ő szerződési feltételeiknek nem megfelelő termékekhez kapcsolódó rendszerszintű kockázatokat, valamint jogellenes termékekhez, szolgáltatásokhoz és tevékenységekhez kapcsolódó rendszerszintű kockázatokat mutattak be.

- ***Jogellenes termékek terjesztése.*** A szolgáltatók, különösen az online piactereket üzemeltető szolgáltatók jogellenes termékek – például az uniós vagy a tagállami jog által tiltott termékek, többek között veszélyes, jogszabályoknak nem megfelelő és/vagy hamisított termékek (például kozmetikumok, játékok vagy elektronikai cikkek, tűzfegyverek, robbanóanyagok, veszélyes vegyi anyagok) – értékesítéséhez és/vagy hirdetéséhez kapcsolódó rendszerszintű kockázatokról számoltak be. Ez negatív hatással van konkrétan a jogellenes termékek felsorolásának kitett felhasználókra, az ilyen termékeket vásárló fogyasztókra, valamint a szellemi tulajdonjogok jogosultjaira. Egyes szolgáltatók azt is megjegyezték, hogy a szolgáltatásaikat esetlegesen visszaélésszerűen veszik igénybe álnevet vagy hamis cégnevet használó kereskedők. Hasonlóképpen, civil társadalmi szervezetek bizonyos gyógyászati és egészségügyi termékek – például vényköteles gyógyszerek, nem engedélyezett pszichoaktív anyagok

és hamisított gyógyszerek – jelenlétét és hozzáférhetőségét jegyezték meg rendszerszintű kockázatként.

- ***Jogellenes szolgáltatások és jogellenes tevékenységek folytatása.*** A szolgáltatók és a civil társadalmi szervezetek szerint előfordulhat, hogy különféle jogellenes szolgáltatásokhoz és tevékenységekhez visszaélésszerűen használnak online platformokat és keresőprogramokat. Az azonosított rendszerszintű kockázatok többek között a következők: jogellenes szexuális szolgáltatások, például (esetlegesen kizsákmányolással vagy emberkereskedelemmel összefüggő) prostitúció; az Unióba való jogosulatlan belépést, az Unión keresztüli áthaladást vagy az Unión belüli tartózkodást lehetővé tevő szolgáltatások; valamint egyéb szolgáltatások, például bűnözői hálózatokba való toborzás, emberrablási, bérgyilkossági ajánlatok vagy engedély nélküli szállásajánlatok biztosítása vagy hirdetése. Egyes szolgáltatók azt is megjegyezték, hogy szolgáltatásaikat esetlegesen visszaélésszerűen veszik igénybe jelentős készpénzösszegek eladása vagy átváltása céljából, valamint tiltott kábítószerek eladása vagy cseréje céljából, vagy kibertámadási szolgáltatások – többek között rosszindulatú szoftverek, adathalászat vagy nem hiteles, megrendelésre történő viselkedés (például robotok, hamis személyazonosság), továbbá személyazonosság-lopás és felhasználói fiókokhoz való jogosulatlan hozzáférés – ajánlása céljából. Az említett további jogellenes tartalmak, amelyek gyakran szorosan kapcsolódnak jogellenes szolgáltatásokhoz, többek között a következők voltak: intim kép- vagy hangfelvételek hozzájárulás nélküli megosztása, hozzájárulás nélküli nemi aktus ábrázolása, jogellenes pornográfia, valamint emberkereskedelemhez vagy szexuális kizsákmányoláshoz kapcsolódó tartalmak. Az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók és a civil társadalmi szervezetek rendszerszintű kockázatként említették az erőszakos vagy kényszerítő tartalmakat is, például a zaklatáshoz, doxoláshoz, szexuális célú csábításhoz és az életveszélyes fenyegetésekhez kapcsolódó tartalmakat.

Gyermekek szexuális bántalmazását ábrázoló anyagok. Az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók többsége és különböző civil társadalmi szervezetek azonosítottak a gyermekek szexuális bántalmazását ábrázoló anyagok terjesztéséhez kapcsolódó rendszerszintű kockázatokat, különösen közösségimédia-platformok és keresőprogramok vonatkozásában. A szolgáltatók konkrétan olyan kockázatokról számoltak be, hogy a felhasználóik ki lehetnek téve a kiskorúakat szexualizáló, a gyermekek bántalmazását, valamint szexuális célú csábítását és szexuális zsarolását magasztaló vagy megkönnyítő jogellenes tartalmaknak. A 3.4. szakasz további részleteket tartalmaz ezekről a rendszerszintű kockázatokról, valamint a kiskorúak védelmét veszélyeztető egyéb rendszerszintű kockázatokról.

Terrorista tartalmak. Az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók és különböző civil társadalmi szervezetek beszámoltak terrorista

tartalmakhoz kapcsolódó rendszerszintű kockázatokról, különösen közösségimédia-platformok és keresőprogramok vonatkozásában. A beszámolók többek között terrorista képanyagok (például újságírási céltól eltérő kontextusban történő) terjesztésével, terroristák méltatásával, magasztalásával, segítésével, támogatásával (például adománygyűjtéssel), toborzásával, radikalizálódásával és képzésével kapcsolatos kockázatokra vonatkoztak. A szolgáltatók megjegyezték, hogy a rendszerszintű kockázatok például jelképeket, zászlókat, szlogeneket, egyenruhákat, gesztusokat, üdvözlési formákat bemutató, illetve erőszakos szélsőséges szervezeteket vagy egyéneket ábrázoló egyéb elemeket bemutató jogellenes tartalmakra terjednek ki. Ebben a kategóriában az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók, valamint a civil társadalmi szervezetek némelyike figyelembe vette a szankcióval sújtott szervezetektől – például kijelölt terrorista csoportoktól – vagy szankcióval sújtott médiaszervezetektől származó tartalmakhoz kapcsolódó rendszerszintű kockázatokat.

Jogellenes gyűlöletbeszéd és gyűlölet által motivált bűncselekményekre való felbujtás. A szolgáltatók – különösen az online óriásplatformok és nagyon népszerű online keresőprogramok szolgáltatói – és a civil társadalmi szervezetek különböző rendszerszintű kockázatokat azonosítottak a jogellenes gyűlöletbeszéd terjesztéséhez és a gyűlölet által motivált bűncselekményekre való felbujtáshoz kapcsolódóan. Ez a jelentés és a digitális szolgáltatásokról szóló rendelet a jogellenes gyűlöletbeszéd fogalmának az alkalmazandó uniós és nemzeti jogszabályokban található meghatározásaira hagyatkozik, mert maga a rendelet nem határozza meg a jogellenesség fogalmát. Az uniós jogi kereten belül a jogellenes gyűlöletbeszéd elsősorban a személyeket vagy csoportokat a védett tulajdonságaik – nevezetesen a faj, bőrszín, vallás, származás, nemzeti vagy etnikai hovatartozás – alapján megcélzó beszédre utal, ahogyan a Tanács 2008/913/IB kerethatározatában[10] szerepel. Egyes szolgáltatók kiemelték, hogy az ilyen jellegű illegális tartalmak az egyének vagy csoportok dehumanizálásához, kirekesztéséhez, szegregációjához vagy rágalmazásához vezethetnek, és ezenkívül a mások által konkrét tulajdonságok alapján kategorizált emberekkel szembeni erőszak fokozódásához vezethetnek. A szolgáltatók szabadon használhatnak további elemeket a saját szerződési feltételeikben és irányelveikben, olyan módon, amely esetleg túlmutathat az uniós és a tagállami jogszabályokban meghatározott jogellenes gyűlöletbeszéd alkalmazási körén. Számos szolgáltató például gyűlöletbeszédként határozza meg az azt kinyilatkoztató tartalmakat is, hogy a bizonyos jellemzőkkel/tulajdonságokkal (például életkor, szexuális irányultság és nemi identitás vagy fogyatékosság) rendelkező egyének vagy csoportok alacsonyabb rendűek vagy bűnözőkhöz, állatokhoz vagy tárgyakhoz hasonlóak.

Szellemi tulajdonjogok megsértése. Bizonyos, online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók, valamint civil társadalmi szervezetek azonosítottak szellemi tulajdonjogokat – például védjegyeket, formatervezésiminta-oltalmi

[10] A Tanács 2008/913/IB kerethatározata (2008. november 28.) a rasszizmus és az idegengyűlölet egyes formái és megnyilvánulásai elleni, büntetőjogi eszközökkel történő küzdelemről, elérhető a következő linken: https://eur-lex.europa.eu/eli/dec_framw/2008/913/oj/hun.

jogokat, szabadalmakat és szerzői jogokat – sértő tartalmakhoz kapcsolódó rendszerszintű kockázatokat, különösen hamisított árukkal, szellemi tulajdonjogi kalózkodás tárgyát képező filmekkel és zenével, valamint jogellenes online közvetítési szolgáltatásokkal összefüggésben. Ezek a rendszerszintű kockázatok különösen az online piactereket, a közösségimédia-szolgáltatásokat és a keresőprogramokat érintik. A példák többek között az áruk és szolgáltatások forrása, eredete, támogatása vagy hovatartozása tekintetében összetéveszthetőség, megtévesztés vagy téves értelmezés előidézése céljából történő jogosulatlan védjegyhasználatra vonatkoztak. A szellemi tulajdonjogok megsértésének kockázatát egyes szolgáltatók, valamint az Európai Unió Szellemi Tulajdoni Hivatalához (EUIPO) tartozó, szellemi tulajdoni jogsértések európai megfigyelőközpontja is elismerte az alkalmazásáruházakban elérhető alkalmazások – például copycat alkalmazások vagy kalóz tartalmakhoz, különösen sporthoz való hozzáférés biztosítására használt alkalmazások – tekintetében. Az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók némelyike zeneművek, audiofájlok, audiovizuális felvételek és más művészeti alkotások, többek között fényképek, festmények, rajzok, valamint más eredeti vizuális alkotások megosztásával járó szerzői jogi jogsértések kockázatait is megjegyezte.

Fogyasztóvédelem. Online piacterek többek között a jogellenes tartalmakkal átfedésben lévő, fogyasztókhoz kapcsolódó különféle rendszerszintű kockázatokról, például jogszabályoknak nem megfelelő termékek értékesítéséről vagy pénzügyi átverésekről számoltak be. A jogellenes tartalmak közvetlenül hatással lehetnek a fogyasztók jogaira és biztonságára. A fogyasztóvédelmet érintő rendszerszintű kockázatokra vonatkozó további információk az alábbi 3.2. szakaszban találhatók.

A jogellenes tartalmakhoz kapcsolódó rendszerszintű kockázatokat érintő kockázati tényezőkre vonatkozó példák:

Interfészek kialakítása és ajánlórendszerek: A szolgáltatók és a civil társadalmi szervezetek megjegyezték, hogy az interfészek kialakítása és a szerződéskötést ösztönző ajánlórendszerek bizonyos jogellenes tartalmakat, valamint olyan jelenségeket motiválhatnak, amelyek esetében a felhasználók a meglévő preferenciáikhoz igazodó jogellenes tartalmaknak lehetnek kitéve.

Hirdetési rendszerek: A szolgáltatók és a civil társadalmi szervezetek hasonló kockázatokat említettek a hirdetési rendszerek tekintetében (például célzott hirdetés miatt).

Tartalommoderálási rendszerek: Az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók általában hivatkoztak a felderítés elkerülését célzó olyan technikákra, mint a kódolt nyelv és a platformon kívüli interakciókhoz és tranzakciókhoz kapcsolódó linkek. A civil társadalmi szervezetek bizonyos nyelvek moderálásának potenciális hiányosságait is megállapították, és kiemelték, hogy a

tartalommoderáláskor fontos a helyi kulturális hivatkozások megértése. A civil társadalmi szervezetek említést tettek a platformszabályzatok és a tartalommoderálási intézkedések biztonsági mentési tartalmak és profilok (azaz duplikált tartalmak és fiókok), valamint más platformokra vagy weboldalakra mutató linkek használatán alapuló kikerülési módszereihez kapcsolódó kockázatokról is. Az audio-, podcast- és élő közvetítési tartalmakat a platformszabályzatok és a tartalommoderálási intézkedések kikerülésére alkalmasként említették, mivel előfordulhat, hogy a tartalommoderálási rendszerek kevésbé fejlettek az audio-formátumok esetében.

A jogellenes tartalmakhoz kapcsolódó rendszerszintű kockázatokat érintő észrevételekre vonatkozó példák:

Zalando, A digitális szolgáltatásokról szóló rendelet szerinti 2024. évi kockázatértékelési jelentés), 6–7. o.: *„A Zalando online platformja ki lehetett téve jogellenes tartalmak terjesztése miatti kockázatnak, magukon a termékeken, a termékeket bemutató, azokat hirdető tartalmakon vagy kommunikációs tartalmakon, valamint vevői értékeléseken keresztül. Ezek a kockázatok többek között, de nem kizárólag a következők voltak: szellemi tulajdonjogok megsértése, a termékekre vonatkozó pontatlan vagy hiányos tájékoztatás, a termékbiztonsággal kapcsolatos helytelen tájékoztatás, valamint a Zalando platformon kínált termékekhez kapcsolódó potenciális környezetvédelmi problémák.”*

AliExpress, A digitális szolgáltatásokról szóló rendelet szerinti 2024. évi kockázatértékelési jelentés, 37. o.: *„Fennáll annak kockázata, hogy a felhasználók visszaélésszerűen használják a platform funkcióit jogszabályoknak nem megfelelő tartalmak közzététele és a felderítés elkerülése céljából. Ez a kulcsszavak és képek felismerésének elkerülésére kép- és szövegmanipulálással tett kísérletekkel történhet. Ezen túlmenően a platform azonnali üzenetküldési vagy csevegési funkcióival való visszaélés keretében robotokat használhattak levélszemét generálásához vagy a felhasználók zaklatásához.”*

X, A digitális szolgáltatásokról szóló rendelet szerinti 2023. évi kockázatértékelési jelentés, 28. o.: *„[E]lőfordulhat, hogy szélsőséges csoportok oly módon játsszák ki az ellenőrzéseket, hogy gyakran kódolt nyelvet használnak és frissítik jelképeiket azzal a céllal, hogy megkerüljék a moderálási erőfeszítéseket, valamint elhomályosítják a kulcsszavakat, vágással vagy színmódosítással manipulálják a képeiket, hogy megkerüljék az ilyen utasításokra támaszkodó automatizált rendszereket”*; A digitális szolgáltatásokról szóló rendelet szerinti 2024. évi kockázatértékelési jelentés, 32. o.: *„Az X szabálysértéshez készített automatizált tartalomfelismerő eszközei szöveges és médiatartalmakon egyaránt működhetnek, és előfordulhat, hogy a felismerések átfedésben vannak vagy nincsenek átfedésben az egyes uniós tagállamok jogellenes gyűlöletbeszédre vonatkozó jogszabályaival.”*

Facebook, A digitális szolgáltatásokról szóló rendelet szerinti 2024. évi kockázatértékelési jelentés, 31. o.: *„A fenyegető szereplők továbbra is keresik a módját, hogy emotikonokkal és elhomályosítással, kódolt nyelv használatával, bizonyos szókapcsolatok kerülésével, vagy más stratégiákkal elkerüljék a felderítést és a jogérvényesítést, ami technológiai kihívássá teheti a potenciális jogsértések felderítését”*; 76. o.: *„Mivel a gyűlöletbeszédhez használt tartalom- és kifejezéstípusok gyakran változnak, a gyűlöletbeszéd következetes felderítése és az azzal szembeni jogérvényesítés továbbra is kihívást jelent. A fenyegető szereplők például továbbra is keresik a felderítés és a jogérvényesítés elkerülésének módjait, például a dolgok konkrét közlése helyett burkoltan fogalmaznak, illetve olyan új tendenciák jelenhetnek meg, mint a regionális nüanszoktól való vitatott függés. Ráadásul a felhasználók gyakran tehetnek közzé gyűlöletbeszéd határesetét jelentő tartalmakat, ami a túlzott jogérvényesítés kezelését kihívássá teszi.”*

3.2. Alapvető jogok

A 34. cikk (1) bekezdésének b) pontja megállapítja, hogy a rendelet szerinti kockázatértékeléseknek ki kell térniük a következőkre: *„az alapvető jogok gyakorlását érintő tényleges vagy várható negatív hatások, különös tekintettel a Charta 1. cikkében foglalt, az emberi méltósághoz való alapvető jogra, a Charta 7. cikkében foglalt, a magán- és a családi élet tiszteletben tartásához való alapvető jogra, a Charta 8. cikkében foglalt, a személyes adatok védelméhez való alapvető jogra, a Charta 11. cikkében foglalt, a véleménynyilvánítás és a tájékozódás szabadságához való alapvető jogra – beleértve a tömegtájékoztatás szabadságát és sokszínűségét –, valamint a Charta 21. cikkében foglalt, a megkülönböztetés tilalmához való alapvető jogra, a Charta 24. cikkében foglalt, a gyermekek jogainak védelméhez való alapvető jogra és a Charta 38. cikkében foglalt, a magas szintű fogyasztóvédelemhez való alapvető jogra”*. Ez a szakasz áttekintést nyújt a 34. cikk (1) bekezdésének b) pontjában felsorolt, kiválasztott alapvető jogokat érintő rendszerszintű kockázatokról, mégpedig az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók kockázatértékelési jelentései és a civil társadalmi szervezetek észrevételei alapján.

A digitális szolgáltatásokról szóló rendelet az alapvető jogokat érintő kockázatok – többek között a véleménynyilvánítás és a tájékozódás szabadságához való jogra kifejtett negatív hatások kockázatai – elleni óvintézkedéseket tartalmaz. A rendelet 35. cikke előírja, hogy az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak észszerű, arányos és hatékony kockázatcsökkentési intézkedéseket kell hozniuk. Ugyanez a cikk azt is előírja, hogy kiemelt figyelmet kell fordítani az ilyen intézkedéseknek az alapvető jogokra – többek között a véleménynyilvánítás és a tájékozódás szabadságához való jogra – gyakorolt hatásaira, ahogyan azt a rendelet (86) preambulumbekezdése hangsúlyozza. A további óvintézkedések a tartalommoderálás átláthatóságára hagyatkoznak, ilyen például az a

követelmény, amely az online platformok szolgáltatói számára előírja, hogy adjanak indokolást a tartalommoderálási döntéseikre, és készítsenek jelentést a tartalommoderálásról a rendelet 15., 16. és 24. cikke alapján. Ezen túlmenően a rendelet 8. cikke szerint az Unió és a tagállamok sem írhatják elő az online platformok számára a polgáraik, illetve az állampolgáraik online viselkedésének módszeres nyomon követését, ami a magán- és a családi élet tiszteletben tartásához, a személyes adatok védelméhez, valamint a véleménynyilvánítás és a tájékozódás szabadságához való alapvető jogot védi.

Az alapvető jogokhoz kapcsolódó rendszerszintű kockázatokat a szolgáltatók és a civil társadalmi szervezetek egyaránt megemlítették. Az érintett alapvető jogok és a kockázatok változóak a különböző platformtípusokon. Az online piactereken az alapvető jogokkal kapcsolatban felmerülő legjelentősebb és ismétlődő rendszerszintű kockázatok például különböznek a közösségimédia- vagy feltérképezési szolgáltatások terén felmerülő kockázatoktól.

A véleménynyilvánítás és a tájékozódás szabadságához való jog.

A digitális szolgáltatásokról szóló rendelet 1. cikke szerint a rendelet célja egy olyan *„biztonságos, kiszámítható és megbízható online környezet”* biztosítása, amelyben az alapvető jogok – többek között a véleménynyilvánítás és a tájékozódás szabadságához való jog – *„hatékony védelmet élveznek”*. A rendelet kockázatkezelési kerete alapján az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók által a Charta 11. cikkében rögzített véleménynyilvánítás és tájékozódás szabadságához való jogot érintő rendszerszintű kockázatok nem konkrét tartalmakra, hanem inkább az adott tartalmak terjesztéséhez vagy moderálásához használt rendszerekre (például ajánlórendszerekre, hirdetési rendszerekre, tartalommoderálási rendszerekre) vonatkoznak. A szolgáltatók – különösen a közösségimedia- és keresőprogram-szolgáltatók – és a civil társadalmi szervezetek által említett rendszerszintű kockázatok többek között a felhasználók online véleménynyilvánítási lehetőségeinek indokolatlan korlátozásai, valamint a természetes és a jogi személyek (köztük a médiaszervezetek) sokféle véleményhez való hozzáférésének hiányával kapcsolatos kockázatok voltak.

A véleménynyilvánítás és a tájékozódás szabadságához való alapvető joghoz kapcsolódó rendszerszintű kockázatokat érintő kockázati tényezőkre vonatkozó példák:

Tartalommoderálási szabályzatok és rendszerek, valamint szerződési feltételek: A szolgáltatók és a civil társadalmi szervezetek egyaránt kiemelték a szabályzatokat nem sértő és jogi tartalmak túlzott moderálásához kapcsolódó kockázatokat. A túlzott moderálás negatívan befolyásolhatja a polgári közbeszédet, és negatív hatásai lehet a véleménynyilvánítás és a tájékozódás szabadságához való alapvető jogra. Ezt a kockázati tényezőt súlyosbíthatják a tartalom- és fiókkorlátozásokhoz kapcsolódó jogorvoslati

mechanizmusok hiányosságai és/vagy a kellő emberi felülvizsgálat nélküli, automatizált tartalommoderálási eszközökre való túlzott hagyatkozás miatti, vagy az automatizált tartalommoderálási eszköz nem megfelelő teljesítménye miatti hiányosságok. A túlzott tartalommoderáláshoz kapcsolódó kockázatok bármely olyan területet érinthetnek, ahol a platformok bármilyen alapon tartalommoderálási döntéseket hoznak. Ezek a kockázatok bárhol felmerülhetnek, függetlenül attól, hogy a tartalommoderálási döntést az online óriásplatform vagy a nagyon népszerű online keresőprogram szerződési feltételeinek végrehajtása indokolja-e. Egyes szolgáltatók és civil társadalmi szervezetek a rendszerek és szabályzatok összefüggésében a véleménynyilvánítás szabadságához való joghoz kapcsolódó rendszerszintű kockázatokat is említettek, amelyek bizonyos tartalomkategóriák nem megfelelő moderálását eredményezik, például a jogellenes gyűlöletbeszéd eltávolításának hiánya esetén, és öncenzúrához vagy más elrettentő hatásokhoz vezetnek. A szerződési feltételek és a szabályzatok módosításai tekintetében a civil társadalmi szervezetek megemlítették, hogy oly módon befolyásolhatják a tartalommoderálási rendszereket, amely a digitális szolgáltatásokról szóló rendelet szerinti rendszerszintű kockázatokat idézhet elő, illetve fokozhatja azokat.

A szolgáltatások szándékos manipulálása: A civil társadalmi szervezetek említettek a tartalomjelentési mechanizmusokkal – megfélemlítés, a jogszerű beszéd elhallgattatása és a gyülekezéstől való elriasztás céljából – (néha összehangolt támadások keretében és egyéb szisztematikus eszközökkel) való visszaéléssel kapcsolatos rendszerszintű kockázatokat.

Ajánlórendszerek: A civil társadalmi szervezetek rámutattak, hogy az ajánlórendszerek befolyásolhatják a valószínűbb és konkrét népességcsoportok számára súlyosabb kockázatokat. Például azt, hogy bizonyos konkrét csoportoktól (fogyatékossággal élő személyektől, vallási vagy etnikai kisebbségektől) származó tartalmak nem feltétlenül ajánlottak, vagy kevésbé ajánlottak, mint más tartalmak. Néhány szolgáltató megjegyezte, hogy az ajánlórendszerekből származó rendszerszintű kockázatok többnyire hasonlóak, függetlenül attól, hogy hol jelennek meg az ajánlások (például honlapon, hírfolyamban).

A véleménynyilvánítás és a tájékozódás szabadságához való alapvető joghoz kapcsolódó rendszerszintű kockázatokat érintő észrevételekre vonatkozó példák:

Wikipedia, A digitális szolgáltatásokról szóló rendelet szerinti 2023–2024. évi kockázatértékelési jelentés): *„A Wikipedián a felhasználók közötti interakciók a megcélzott egyének vagy csoportok (fiatalok; nők; faji, etnikai vagy nyelvi kisebbségek; LMBTIQ+-egyének; fogyatékossággal élő személyek stb.) számára szorongást vagy egyéb lelki bántalmakat okozhattak oly módon, hogy a Wikipedia-projektekben való részvételtől visszariadnak, és a véleménynyilvánítási szabadságuk, valamint a tudás terén érvényesítendő esélyegyenlőséghez való hozzájárulásuk mérséklődik.”*

X, A digitális szolgáltatásokról szóló rendelet szerinti 2024. évi kockázatértékelési jelentés, 42. o.: *„A visszaélés és a zaklatás, a gyűlölködő viselkedés, az erőszakos beszéd és a magánélet megsértése a véleménynyilvánítás szabadságát érintő kockázatokhoz vezethet, olyan károk révén, mint a platformszabályzatok végrehajtásából fakadó cenzúra, valamint a platformon visszaélést és zaklatást tapasztaló felhasználók öncenzúrája.”*

Megkülönböztetésmentesség. A Charta 21. cikkében rögzített megkülönböztetésmentességhez való alapvető jogot érintő rendszerszintű kockázatok említés szintjén szerepeltek az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók – különösen a közösségimédia- és keresőprogram-szolgáltatók – kockázatértékelési jelentéseiben, amelyek kiemelték a diszkriminatív nézeteket esetlegesen erősítő tartalmak széles körben történő terjesztéséből és felerősítéséből fakadó rendszerszintű kockázatokat. A szolgáltatók és a civil társadalmi szervezetek említettek olyan konkrét megkülönböztetési kockázatokat, amelyek konkrét csoportokat – különösen a nemük, faji, etnikai vagy kulturális származásuk, vallásuk vagy meggyőződésük, fogyatékosságuk, életkoruk vagy szexuális irányultságuk alapján – célzó sztereotípiák, diszkriminatív állítások és előítéletek fokozódásából fakadnak.

A megkülönböztetésmentességhez való alapvető joghoz kapcsolódó rendszerszintű kockázatokat érintő kockázati tényezőkre vonatkozó példák:

Hirdetési rendszerek: A szolgáltatók és a civil társadalmi szervezetek a hirdetések megjelenítésének diszkriminatív módon történő megkönnyítését, például az álláshirdetések megjelenítésének kizárólag bizonyos nemű emberekhez célzását említették.

Ajánlórendszerek: A civil társadalmi szervezetek olyan kutatásokat is közzétettek, amelyek arra utaltak, hogy az algoritmikus erősítés egyes csoportok számára kedvező lehet, míg másokat kizár.

A megkülönböztetésmentességhez való alapvető joghoz kapcsolódó rendszerszintű kockázatokat érintő észrevételekre vonatkozó példák:

A **Booking** 2024. évi kockázatértékelési jelentése (18. o.) a következőket említette: *„a tartalommoderálási és diszkrimináció-felderítési rendszereknek valóban lehetnek korlátozásai bizonyos diszkriminatív tartalomtípusok felderítésének nehézségei (például helyi dialektusok vagy jelképek) miatt”*.

A **Google** 2024. évi kockázatértékelési jelentése (133. o.) a következőket említette: *„egy adott alkalmazás vagy szolgáltatás nem minden nyelv, nem minden piac és nem minden korcsoport esetében megfelelő minőségű (...) [vagy] nem működik méltányosan a fogyatékossággal élő felhasználók számára”*.

A **Bing** 2024. évi kockázatértékelési jelentése (110. o.) szerint fennáll *„az a kockázat, hogy a Bing felületén megjelenített hirdetések a célcsoport-kiválasztásuk tekintetében részrehajlóak, ezáltal befolyásolják a védett csoportok kritikus szolgáltatásokhoz való hozzáféréséhez való képességét”*, valamint fennáll *„az a kockázat, hogy a felhasználók a Bing Image Creator alkalmazását vagy a Bing Copilot alkalmazását diszkriminatív vagy gyűlöletkeltő tartalmakhoz használják fel”*.

LinkedIn, 2024. évi kockázatértékelési jelentés, 29. o.: *„Kellő kockázatcsökkentés hiányában diszkriminációhoz és gyűlölethez kapcsolódó kockázatok oly módon nyilvánulhatnak meg a platformon, hogy a tagok gyűlöletbeszédes tartalmakat kísérelnek megosztani a hírfolyamban, az állást hirdetők olyan állást kísérelnek meghirdetni, amely bizonyos fajokat vagy nemeket diszkriminál, vagy a LinkedIn ajánlórendszerei az algoritmusokba beépített részrehajláson alapuló toborzóknak ajánlanak pályázókat.”*

A gyermekek jogai. A Charta 24. cikkében foglalt gyermekek jogait érintő, azonosított rendszerszintű kockázatok elsősorban a gyermekek biztonságára és a kiskorúak védelmére vonatkoztak, amelyeket az alábbi 3.4. szakasz ismertet részletesen.

Fogyasztóvédelem. A 3.1. szakaszban említett, jogellenes tartalmakhoz kapcsolódó, fogyasztóvédelmet érintő rendszerszintű kockázatokon túlmenően az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók beszámoltak más olyan rendszerszintű kockázatokról is, amelyek a Charta 38. cikkében rögzített fogyasztóvédelemhez való joghoz kapcsolódtak. Az online piacterek vonatkozásában ezek például jogszabályoknak nem megfelelő termékekre (például CE-jelölés nélküli termékekre), félrevezető és tisztességtelen kereskedelmi gyakorlatokra, addiktív kialakításra, csalásra, átverésekre, megtévesztő hirdetésre, hamis szerepvállalásra, hamis felhasználói értékelésekre, illetve üzleti vagy termékinformációk félrevezető feltüntetésére vonatkoztak. Ezek a rendszerszintű kockázatok azonban nem korlátozódnak az online piacterekre. Civil társadalmi szervezetek például kiemelték azt a platformokon általánosan felmerülő problémát, hogy online piactereken jogszabályoknak nem megfelelő termékeket terjesztenek az adott termékek közösségi médiában tapasztalt promóciós tendenciái miatt. Ami a pénzügyi átveréseket illeti, egyes közösségimédia- és keresőprogram-szolgáltatók, valamint civil társadalmi szervezetek azonosítottak olyan rendszerszintű kockázatokat, amelyek például a jogellenes vagy magas kockázatú pénzügyi termékek és befektetések – többek között Ponzi-rendszerek, fogadások és kriptovaluták, külföldi ingatlanbefektetések vagy adókedvezmények – széles körű népszerűsítéséhez kapcsolódtak. Civil társadalmi szervezetek említettek más, átveréssel vagy

csalással kapcsolatos rendszerszintű kockázatokat, például étrend-kiegészítőkkel, társkeresési szolgáltatásokkal, jóslási szolgáltatásokkal, lottózással, szerencsejátékokkal, promóciós termékekkel és energiatakarékossággal összefüggésben.

A fogyasztóvédelemhez való alapvető joghoz kapcsolódó rendszerszintű kockázatokat érintő kockázati tényezőkre vonatkozó példák:

Hirdetési rendszerek és a szolgáltatások szándékos manipulálása: A civil társadalmi szervezetek megemlítették, hogy az átverési és csalási kockázatok gyakran megtévesztő hirdetés, valamint nem hiteles felhasználói értékelések következményei, amelyek hatására más felhasználók nem létező termékek vásárlásába vagy nem létező pénzügyi lehetőségekbe fektetnek be.

Bevételszerzési irányelvek: A civil társadalmi szervezetek megjegyezték, hogy a szóban forgó, hirdetéshez kapcsolódó kockázatok tovább fokozódhatnak a tartalmakhoz kapcsolódó, bizonyos bevételszerzési irányelvek miatt, például kattintásvadász tartalmak és hirdetések ösztönzése, valamint a sérülékeny egyének (például idős állampolgárok) megcélzása vagy kényszervásárláshoz vezető játékosítási funkciók bevezetése révén.

Mesterségesintelligencia-rendszerek: Civil társadalmi szervezetek megemlítették, hogy generatív mesterségesintelligencia-rendszereket használtak átverés és csalás megkönnyítése érdekében, például közszereplőknek (tartalomalkotóknak), valamint megbízható médiaforrásoknak és közintézményeknek (például bankoknak) tulajdonított tartalmak generálásával.

A fogyasztóvédelemhez való alapvető joghoz kapcsolódó rendszerszintű kockázatokat érintő észrevételekre vonatkozó példák:

Amazon Store, A digitális szolgáltatásokról szóló rendelet szerinti 2024. évi kockázatértékelési jelentés, 23. o.: *„Rosszindulatú szereplők többféleképpen készítenek hamis értékeléseket, többek között vállalatokat vagy egyéneket vesznek közvetlenül igénybe hamis vagy ösztönzött értékelések létrehozásához; saját termékeik pozitív értékelése, illetve versenytársaik termékeinek sértő értékelése céljából több hamis fiók, sőt személyes fiókok létrehozásához; vevői fiókok átvételével vagy kompromittálásával készített hamis értékelések közzététele céljából, továbbá értékelési ügynököket vesznek igénybe értékelések beszerzéséhez, hogy termékeiket mesterségesen vonzóbbnak tüntessék fel.”*

Pinterest, A digitális szolgáltatásokról szóló rendelet szerinti 2023. évi kockázatértékelési jelentés, 17. o.: *„Sajnos előfordulhat, hogy rosszindulatú szereplők a Pinterest platform*

manipulálására törekednek. Többek között levélszemét-támadások formájában, vagy oly módon, hogy a rosszindulatú szereplők hamis fiókokat használnak, és ezeknek számos megnyilvánulási formája van a platformon. Előfordulhat, hogy levélszemét-küldők arra törekednek, hogy a hirdetéseket vagy más pénzszerzési lehetőségeket megjelenítő spam-weboldalukra mutató linkekre kattintó Pinterest-felhasználók kattintásai révén szerezzenek pénzt. Előfordulhat, hogy más levélszemét-küldők rosszindulatú szoftvereket terjesztenek, azután pedig pénzzé teszik a fertőzött eszközök hálózatát, vagy adathalász linkeket terjesztenek, azután pedig pénzzé teszik az ellopott felhasználói adatokat."

What To Fix, a Digitális Szolgáltatások Európai Testülete és az Európai Bizottság észrevétel-benyújtási felhívására benyújtott beadványok, 1. o.: *„Hatásos pénzügyi ösztönzők biztosításával, valamint nemcsak a tartalmak, hanem a pénzügyi források irányításával vagy az azokhoz való hozzáférés visszatartásával a pénzszerzési rendszereknek még távolabbra mutató következményei lehetnek* [mint a digitális szolgáltatásokról szóló rendelet 34. cikkének (2) bekezdése szerinti kockázati tényezők]*".*

A magán- és a családi élet tiszteletben tartásához való jog és adatvédelem. A szolgáltatók és a civil társadalmi szervezetek a Charta 7. és 8. cikkében rögzített, magán- és családi élet tiszteletben tartásához való alapvető jogot érintő rendszerszintű kockázatokat is említettek. Említettek olyan helyzeteket, amelyekben a felhasználók igénybe vehetik a szolgáltatók szolgáltatásait egymás magán- és családi életének tiszteletben tartásához való jog megsértéséhez, például olyan felügyeleti alkalmazások összefüggésében, amelyeket szülőknek mutatnak be a gyermekeikről való gondoskodás eszközeiként, de amelyeket valójában elsősorban arra használnak, hogy lehetővé tegyék más személyek követését azok hozzájárulása nélkül (ez a kockázat nemi alapú erőszakhoz is vezethet, ahogyan az alábbi 3.4. szakasz tárgyalja). Civil társadalmi szervezetek titkos követéshez és doxoláshoz kapcsolódó rendszerszintű kockázatokat is említettek közösségi média vonatkozásában, például intim képek (például bosszúpornográfia) vagy más személyes adatok (például telefonszám, lakcím, kormány által kiadott személyi azonosító szám, egészségügyi adatok) hozzájárulás nélküli terjesztésére vonatkozó fenyegetések tekintetében.

A magán- és a családi élet tiszteletben tartásához való alapvető joghoz kapcsolódó rendszerszintű kockázatokat érintő kockázati tényezőkre vonatkozó példák:

Ajánlórendszerek és tartalommoderálási rendszerek: Civil társadalmi szervezetek megjegyezték, hogy a szerepvállalásra optimalizált ajánlórendszerek hozzájárulhatnak kizsákmányoló, hozzájárulás nélküli vagy deepfake tartalmak – tartalommoderálás előtti, esetlegesen széles közönség körében történő – terjesztéséhez.

A szolgáltatások szándékos manipulálása: Civil társadalmi szervezetek megjegyezték, hogy az online óriásplatformot vagy nagyon népszerű online keresőprogramot üzemeltető szolgáltatók szolgáltatásainak, különösen a közösségi médiának pszichológiai manipuláció céljára történő igénybevétele hozzájárulhat ahhoz a kockázathoz, hogy rosszindulatú felhasználók megsértik más felhasználók magán- és családi életének tiszteletben tartásához való jogot.

A magán- és a családi élet tiszteletben tartásához való alapvető joghoz kapcsolódó rendszerszintű kockázatokat érintő észrevételekre vonatkozó példák:

Apple App Store, A digitális szolgáltatásokról szóló rendelet szerinti 2023. évi kockázatértékelési jelentés, 39. o.: *„Megfelelő ellenőrzések hiányában a fejlesztők nagy valószínűséggel törekednének arra, hogy az emberi méltósághoz való jogra, valamint a magán- és a családi élet tiszteletben tartásához való jogra tényleges vagy várható negatív hatás kiváltására alkalmas alkalmazásokat tegyenek közzé, és az ilyen kockázatok súlyossága mérsékelttől rendkívül magasig változhatna (például gyermekek szexuális zaklatását ábrázoló anyagok, úgynevezett „bosszúpornográfia”, deepfake-ek stb. esetében).”*

Bing, A digitális szolgáltatásokról szóló rendelet szerinti 2023. évi kockázatértékelési jelentés, 29. o.: *„[A] keresési index segítségével könnyen visszakereshetők az egyénre vonatkozó olyan információk, amelyek a magánszférájukra vonatkoznak, és amelyeket az egyén nem szándékozott nyilvánosan közzétenni, vagy amelyek nyilvános közzétételéhez nem járult hozzá; ilyenek például a hozzájárulás nélküli intim képek (más néven „bosszúpornográfia”), vagy a személyazonosság-lopási kockázatot felvető, rendkívül érzékeny személyes adatok, például hitelkártyaszámok, egészségügyi adatok stb.”*

Google, A digitális szolgáltatásokról szóló rendelet szerinti 2024. évi kockázatértékelési jelentés, 98. o.: *„A Play alkalmazáson keresztül tartalmakhoz hozzáférő felhasználók számára felmerülő egyik legnagyobb kockázat a magánélethez kapcsolódik, ami azt a tényt tükrözi, hogy a Play létezik az alkalmazás-ökoszisztémában, és alkalmazásokat kínál olyan kategóriákban, amelyek valószínűleg személyes adatok használatával járnak (például bankolási vagy kormányzati szolgáltatások).”*

3.3. Polgári közbeszéd, választási folyamatok és közbiztonság

A digitális szolgáltatásokról szóló rendelet 34. cikke (1) bekezdésének c) pontja megállapítja, hogy a rendelet szerinti kockázatértékeléseknek ki kell térniük *„a polgári közbeszédre,*

valamint a választási folyamatokra és a közbiztonságra gyakorolt bármely tényleges vagy várható negatív hatásra”.

Ez a szakasz az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók, valamint a civil társadalmi szervezetek által azonosított rendszerszintű kockázatokat tekinti át nagy vonalakban, amelyek különösen relevánsak, mivel 2024-ben számos tagállamban tartottak választásokat, többek között európai parlamenti választásokat. A rendelet 35. cikkének (1) bekezdése számos példát tartalmaz a rendszerszintű kockázatok csökkentését célzó intézkedésekre. E jelentés 4. fejezete áttekintést nyújt a meglévő és a javasolt kockázatcsökkentési intézkedésekről. A demokratikus folyamatok védelmezésének fontosságát elismerve a Bizottság 2024 áprilisában a digitális szolgáltatásokról szóló rendelet 35. cikkének (3) bekezdése szerinti iránymutatást adott ki *„a választási folyamatok rendszerszintű kockázatainak csökkentéséről”*[11].

Ezek a rendszerszintű kockázatok különféleképpen nyilvánulnak meg a szolgáltatás jellegétől és funkciójától, a szolgáltatás által kiváltott magatartásoktól, valamint a társadalmi háttértől függően. A közösségimédia-platformokon folytatott polgári közbeszéd kihatásai jelentősen eltérnek az online piactereken folytatott polgári közbeszéd kihatásaitól.

A polgári közbeszédre, a választási folyamatokra és a közbiztonságra kifejtett esetleges negatív hatások értékelésekor számos szolgáltató megvizsgálta, hogy hogyan kezeli a félretájékoztatást és a dezinformációt. A félretájékoztatás és a dezinformáció fogalmát a szolgáltatók eltérően határozzák meg. Az európai demokráciára vonatkozó cselekvési terv fogalommeghatározásai szerint a dezinformáció *„olyan hamis vagy félrevezető tartalom, amelyet megtévesztés, illetve gazdasági vagy politikai haszonszerzés szándékával terjesztenek, és amely kárt okozhat a nyilvánosságnak”*, a félretájékoztatás pedig *„olyan hamis vagy félrevezető tartalom, amelyet káros szándék nélkül osztanak meg, ám hatásai ettől még lehetnek károsak”*[12]. Több, online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltató megállapodott a dezinformáció visszaszorítását célzó gyakorlati kódex és/vagy annak jogutódja, a dezinformáció visszaszorítását célzó magatartási kódex[13] alapján arról, hogy kialakítják ezeket a fogalommeghatározásokat. A kódex szerinti „dezinformáció” kifejezést az aláíró felek olyan értelemben használják, hogy magában foglalja a félretájékoztatást, a dezinformációt, a tájékoztatásbefolyásoló műveleteket és az információs térbe való külföldi

[11] A Bizottság közleménye – A Bizottság iránymutatása az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók számára a választási folyamatok rendszerszintű kockázatainak csökkentéséről az (EU) 2022/2065 rendelet 35. cikkének (3) bekezdése alapján, elérhető a következő linken: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52024XC03014&qid=1714466886277.

[12] A Bizottság jelentése az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az Európai Demokráciára vonatkozó cselekvési tervről, elérhető a következő linken: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX%3A52020DC0790.

[13] 2022 A dezinformáció visszaszorítását célzó gyakorlati kódex, elérhető a következő linken: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation. A gyakorlati kódex formája 2025-ben magatartási kódexre változott. A dezinformáció visszaszorítását célzó magatartási kódex, elérhető a következő linken: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

beavatkozást[14]. A dezinformáció és a félretájékoztatás ismertetésekor a jelentés az európai demokráciára vonatkozó cselekvési terv fogalommeghatározásaira hivatkozik. Az alábbiakban vázolt rendszerszintű kockázatok nemcsak egyedi tartalmakra, hanem rendszerekhez és folyamatokhoz is kapcsolódnak: a szolgáltatások kialakításának, üzemeltetésének és széles körű igénybevételének módjához.

A polgári közbeszédhez, a választási folyamatokhoz és a közbiztonsághoz kapcsolódó rendszerszintű kockázatok bemutatásakor több közösségimédia-platform elismerte kockázatértékelési jelentésében, hogy az algoritmikus ajánlórendszereik szerepet játszhatnak a félrevezető narratívák virális terjedésében. A polgári közbeszédre és a választási folyamatokra gyakorolt negatív hatások tekintetében a keresőprogramok például azokra a kockázatokra helyezték a hangsúlyt, hogy a dezinformáció és a félretájékoztatás a rangsorolási mechanizmusok miatt jelenhet meg a keresési találatokban.

A megfelelően működő polgári közbeszédhez mint közjóhoz kapcsolódó rendszerszintű kockázatok szorosan összefüggnek a felhasználók alapvető jogaival, többek között a véleménynyilvánítás és a tájékozódás szabadságához való alapvető joggal (lásd a 3.2. szakaszt).

Polgári közbeszéd. Számos, online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltató beszámolt arról, hogy a polgári közbeszédre kifejtett tényleges és várható negatív hatásokat a dezinformáció és a félretájékoztatás széles körű terjesztése váltja ki, többek között külföldi beavatkozást és információmanipulációt célzó kampányok, valamint összehangolt, hiteltelen magatartás keretében, a platformokon és azokon kívül egyaránt. A szolgáltatók és a civil társadalmi szervezetek a polgári közbeszédet érintő további rendszerszintű kockázatokat neveztek meg, ilyen volt többek között a politikai tartalmak sokszínűségének visszaszorítása vagy hiánya, a polarizáció, az (erőszakos) szélsőséges tartalmaknak a felhasználók radikalizálása céljából történő terjesztése, káros összeesküvés-elméletek, propaganda és tévesen hitelesnek tűnő tartalmak (például széles körben elismert médiaszervezeteknek, közintézményeknek vagy szakmailag lektorált kutatásnak beállított hivatalos források) széles körben történő terjesztése. A szolgáltatók és a civil társadalmi szervezetek szerint ezek a tényezők hozzájárulhatnak a polarizációhoz és ahhoz, hogy az online környezetek károsítják a megfelelően működő polgári közbeszédet és demokratikus folyamatokat.

Szavazási és választási folyamatok. Az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók, valamint a civil társadalmi szervezetek beszámoltak a szavazási és választási folyamatokat érintő, hamis vagy félrevezető tartalmak széles körben történő terjesztéséből fakadó rendszerszintű kockázatokról. Ilyen rendszerszintű kockázat lehet többek között a választások időpontjával, a jelöltek választhatóságával, a választópolgárok regisztrációs folyamatával vagy a demokratikus folyamatok delegitimizációjával kapcsolatos

[14] A dezinformáció visszaszorítását célzó magatartási kódex, Preambulum, I. a. pont.

dezinformáció vagy félretájékoztatás, például választási csalásra, eljárási hibákra, beavatkozásra vagy bizonyos személyek melletti vagy elleni intézményes torzításra vonatkozó, alaptalan állítások megfogalmazásával. Ahogyan e jelentésben másutt is szerepel, a rendelet szerinti kockázatkezelési keretbe tartozó rendszerszintű kockázatok nem egyedi tartalmakra, hanem inkább a szolgáltatás kialakítására, valamint ahhoz kapcsolódó kockázatokra vonatkoznak, hogy a platform rendszerei hogyan teszik lehetővé a felerősítést, például ajánlóalgoritmusokkal vagy hirdetési szolgáltatásokkal. A szolgáltatók és a civil társadalmi szervezetek a generatív mesterséges intelligenciából fakadó rendszerszintű kockázatokra is rávilágítottak, különösen arra, hogy a generatív mesterséges intelligenciát alkalmazó robotok akár helytelen választ is adhatnak választásokkal kapcsolatos kérdésekre, például helytelen választási időpontok vagy a jelöltekre vonatkozó helytelen információk megadásával.

Közszereplők. Több, online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltató és civil társadalmi szervezet beszámolt a közszereplők online környezetekben való ábrázolásához és kezeléséhez kapcsolódó rendszerszintű kockázatokról. Ilyen volt többek között a közhivatalra jelölt személyekkel kapcsolatos dezinformáció, félretájékoztatás és káros összeesküvés-elméletek széles körben történő terjesztése, (a gyakran nőket és kisebbségeket megcélzó) összehangolt zaklatási kampányok, a megszemélyesítés, valamint a félrevezetés céljából tervezett szintetikus média közzététele. A szolgáltatók és a civil társadalmi szervezetek megjegyezték, hogy az ilyen tartalmak jellemző célpontjai többek között politikusok vagy politikai jelöltek, köztisztviselők, kormánytisztviselők, vállalkozásvezetők, újságírók, híres személyek, tudományos szakemberek (különösen a klímaváltozással vagy közegészségüggyel kapcsolatos kérdésekkel foglalkozó szakemberek), valamint civil társadalmi szervezetek képviselői. Gyakran említett példák többek között a következők voltak: hamis ajánlások, helytelen magatartásra vagy bűncselekményekre vonatkozó hamis, káros beismerések, konkrét személyek vagy csoportok elleni hamis támadások, valamint hamisított magánjellegű kommunikáció. A szolgáltatók rámutattak, hogy ezeket a rendszerszintű kockázatokat hogyan befolyásolják időzítéssel, például választások vagy más jelentős demokratikus események közeledtével. Egyes szolgáltatók és civil társadalmi szervezetek aggályokat vetettek fel azzal kapcsolatban, hogy a felhasználók akaratlanul ki vannak téve politikai tartalmaknak, például a tudomásuk vagy a hozzájárulásuk nélkül feliratkoznak politikai szereplők tartalmaira vagy követnek politikai szereplőket.

Válságok és természeti katasztrófák. A szolgáltatók és a civil társadalmi szervezetek beszámoltak – természeti vagy ember okozta – válságok alatti vagy utáni dezinformáció és félretájékoztatás virális terjesztéséhez kapcsolódó rendszerszintű kockázatokról. Ilyen rendszerszintű kockázatok gyakran valós időben jelentkeznek, amikor a tartalmak láthatóságát és hatását felerősítik az ajánlórendszerek és a megnövekedett felhasználói szerepvállalás. A szolgáltatók és a civil társadalmi szervezetek által említett példák többek között az árvizek, földrengések, futótüzek, hurrikánok, földcsuszamlások vagy ipari balesetek, valamint közegészségügyi válságok idején vagy a klímaváltozáshoz hasonló tágabb kérdések összefüggésében tapasztalható hamis vagy félrevezető narratívákra vonatkoztak. A szolgáltatók

és a civil társadalmi szervezetek erőszakos eseményekkel, például lövöldözésekkel, tömeggyilkosságokkal, terrortámadásokkal vagy fegyveres konfliktusokkal összefüggésben is megfigyelték a dezinformáció és a félretájékoztatás virális terjedését. Az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók és a civil társadalmi szervezetek beszámoltak olyan esetekről, amikor hamis állítások, például az alapvető szolgáltatások (például élelmiszer-ellátási láncok, folyóvíz, üzemanyag vagy készpénzkiadó automatákhoz való hozzáférés) összeomlásának közelgő veszélye pánikhoz vagy készletfelhalmozó magatartáshoz vezethet. Ezzel szemben egyes szolgáltatók és civil társadalmi szervezetek megjegyezték, hogy a tagadás (azaz arra vonatkozó hamis állítás, hogy valós válságok nem következtek be) vagy soha meg nem történt események kreálása hozzájárul a hatóságok, a katasztrófa-elhárító szervek és a tudományos intézmények iránti bizalom leépüléséhez.

Közbiztonság. A szolgáltatók és a civil társadalmi szervezetek a társadalmi nyugtalanság összefüggésében is azonosítottak rendszerszintű kockázatokat. Az egyik általánosan említett kockázat régi tartalmak eredeti rendeltetésének megváltoztatását jelentette, ilyen volt például bombázásokról, tömeges lövöldözésekről vagy nagyszabású demonstrációkról készült videófelvételek valós idejű eseményként történő megszerkesztése, a közpánik előidézésének vagy feszültségek szításának nyilvánvaló céljával. A szolgáltatók és egyes civil társadalmi szervezetek a zavargásokat, polgári nyugtalanságot, vagy személyek vagy vagyon – többek között állami vagy közcélú infrastruktúra – elleni bűncselekményeket magasztaló, ösztönző vagy dicsőítő tartalmak terjesztéséhez kapcsolódó rendszerszintű kockázatokat is megállapítottak. A civil társadalmi szervezetek és a szolgáltatók továbbá aggályokat vetettek fel erőszakról vagy annak következményeiről oly módon készült rajzos képek vagy videók szándékos terjesztéséhez kapcsolódó kockázatokra vonatkozóan, hogy azok célja konkrét egyénekkel vagy kisebbségi csoportokkal szembeni ellenséges érzelmek vagy megtorlás hallgatólagos ösztönzése.

A polgári közbeszédhez, a választási folyamatokhoz és a közbiztonsághoz kapcsolódó rendszerszintű kockázatokat érintő kockázati tényezőkre vonatkozó példák

Algoritmikus rendszerek, hirdetési rendszerek, tartalommoderálási rendszerek: A szolgáltatók, valamint a civil társadalmi szervezetek releváns kockázati tényezőkként említették az algoritmikus rendszereket (többek között az ajánlórendszereket és a generatív mesterséges intelligencián alapuló rendszereket), a hirdetési rendszereket, a tartalommoderálási rendszereket, valamint a platformok interfész-kialakítását. Az ajánlórendszerek például felerősíthetik az összeesküvés-elméleteket, a propagandát vagy a tévesen hitelesnek tűnő tartalmakat, különösen akkor, ha ezek a tartalmak hivatalos vagy megbízható forrásokat (például széles körben elismert médiaszervezeteket, közintézményeket vagy szakmailag lektorált kutatásokat) utánoznak. A szolgáltatók és a civil társadalmi szervezetek megjegyezték, hogy ezek a tényezők hozzájárulhatnak a

polarizációhoz és az ellenséges online környezetekhez, ami viszont káros lehet a megfelelően működő polgári közbeszédre és demokratikus folyamatokra. A politikai hirdetéseket a civil társadalmi szervezetek potenciális kockázati tényezőkként említették, amennyiben a hirdetések politikai természete nem átlátható.

A szolgáltatások szándékos manipulálása, virális jelleg, interfész-kialakítás: A civil társadalmi szervezetek a külföldi információmanipulációt és beavatkozást célzó tevékenységeket, valamint más hiteltelen magatartást a polgári közbeszédet, a választási folyamatokat és a közbiztonságot érintő kockázati tényezőkként említették. A szenzációhajhászás, az algoritmusok viralitása, valamint egyes esetekben a nyugtalanság előidézésére tett összehangolt kísérletek a civil társadalmi szervezetek és a szolgáltatók beadványai szerint a közbiztonságot és a polgári közbeszédet érintő rendszerszintű kockázatokat jelenthetnek. Egyes szolgáltatók és civil társadalmi szervezetek kifejtették, hogy például a választási folyamatokkal vagy válságokkal összefüggő dezinformáció és félretájékoztatás áramlása – az ajánlórendszer kialakításától vagy az összehangolt hiteltelen magatartás előfordulásától függően – aránytalanul teheti ki a felhasználókat feszültséget szító narratíváknak, ha az ajánlórendszereket úgy alakították ki, hogy jutalmazza az ilyen tartalmak melletti elköteleződést. A szolgáltatók és a civil társadalmi szervezetek megemlítették, hogy az interfész-kialakítás bizonyos tulajdonságai hozzájárulhatnak az ilyen tartalmak gyors terjedéséhez, ezzel a közbiztonságot és az intézmények iránti bizalmat érintő rendszerszintű kockázatokat okoznak.

A polgári közbeszédhez, a választási folyamatokhoz és a közbiztonsághoz kapcsolódó rendszerszintű kockázatokat érintő észrevételekre vonatkozó példák:

Bing, A digitális szolgáltatásokról szóló rendelet szerinti 2024. évi kockázatértékelési jelentés, 34. o.: *„A [mesterséges intelligencia által] generált tartalmak állandósíthatják a torzítást, hamis vagy félrevezető információkat terjeszthetnek, vagy hozzájárulhatnak visszhangszobák kialakulásához”*, a 116. oldalon pedig említésre kerül *„olyan kockázat, hogy a hírek azokat az alacsony tekintélyű vagy gyenge minőségű hírforrásokat népszerűsítik, amelyek fokozzák a politikai polarizációt és a szűrőbuborékokat”*.

X, A digitális szolgáltatásokról szóló rendelet szerinti 2024. évi kockázatértékelési jelentés, 55. o.: *„[K]ülső események hatására előfordulhat, hogy rosszindulatú szereplők visszaélésszerűen használják az X-et hamis vagy félrevezető információk terjesztésére, valamint összehangolt támadásokat hajtanak végre a közbiztonság ellen. A kockázati környezetet fokozza, hogy visszhangszobák alakulhatnak ki, ahol a felhasználók a meglévő meggyőződéseikhez igazodó információknak lehetnek kitéve, ami megerősítheti a torzításokat, és elfojthatja az egészséges vitát.”*

Snapchat, A digitális szolgáltatásokról szóló rendelet szerinti 2023. évi kockázatértékelési jelentés, 130. o.: *„A személyre szabott tartalmak és az algoritmikus torzítások visszhangszobákba zárhatják a felhasználókat, ezáltal megerősítik a meglévő meggyőződéseiket, emellett polarizált közösségeket alakíthatnak ki, ami gátolja a nyitott párbeszédet.”*

TikTok, A digitális szolgáltatásokról szóló rendelet szerinti 2024. évi kockázatértékelési jelentés, 13. o.: *„A koncentrált tartalom [5. lábjegyzet: Megjegyzendő, hogy ez az 1. éves jelentésben »szűrőbuborék«-ként szerepelt] a civil társadalom széles körben dokumentált, releváns kockázat. Mivel az ajánlórendszereket úgy alakítják ki, hogy a felhasználó érdeklődési körén és korábbi elköteleződésén alapuló tartalmakat kínáljanak, előfordulhat, hogy nem szándékosan, hosszabb időszakokon keresztül leszűkített tartalmakat jelenítenek meg a felhasználók számára.”*

Civil Liberties Union for Europe, a Digitális Szolgáltatások Európai Testülete és az Európai Bizottság észrevétel-benyújtási felhívására benyújtott beadványok: *„Egyre nagyobb aggodalomra ad okot, hogy nem hitelesen veszik igénybe az online óriásplatformokat és a nagyon népszerű online keresőprogramokat olyan esetekben, ha külföldi szereplők vagy belföldi csoportok szándékosan manipulálják a platform rendszereit (például hamis fiókokat vagy robotokat használnak, vagy influenszereket »vásárolnak«) a közvélemény befolyásolása, a választások megzavarása vagy megosztó retorika népszerűsítése céljából. Tanulmányok rámutattak az összehangolt hiteltelen magatartást célzó kampányok elterjedtségére, különösen kritikus jelentőségű politikai események – például népszavazások és választások – idején, amelyek esetében rosszindulatú szereplők a demokratikus folyamatok iránti bizalom megrendítésére és megosztottság elhintésére törekednek”.*

3.4. Nemi alapú erőszak, közegészség, kiskorúak védelme, fizikai és mentális jóllét

A rendelet 34. cikke (1) bekezdésének d) pontja előírja, hogy az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak értékelniük kell a következőt: *„a nemi alapú erőszakkal, a közegészség és a kiskorúak védelmével összefüggő tényleges vagy előre látható negatív hatások, valamint a személyek testi és szellemi jóllétére gyakorolt súlyos negatív következmények”*. Ez a szakasz az e kategóriákban azonosított rendszerszintű kockázatokat ismerteti, melynek során az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók kockázatértékeléseire, valamint a civil társadalmi szervezetek észrevételeire hagyatkozik. Előfordulhat, hogy az e szakaszban ismertetett rendszerszintű kockázatok másként nyilvánulnak meg az egyes szolgáltatások, társadalmi közegek és emberi magatartások esetében. A kiskorúak például más kockázatoknak vannak kitéve, mint a felnőttek.

Nemi alapú erőszak. A 2020–2025 közötti időszakra szóló uniós nemi esélyegyenlőségi stratégia[15] egyik legfontosabb célkitűzése a nemi alapú erőszak megszüntetése. A nőkkel szembeni erőszak és a kapcsolati erőszak elleni küzdelemről szóló irányelv[16] például bűncselekménynek minősíti az intim vagy manipulált anyagok beleegyezés nélküli (többek között mesterséges intelligencia használatával történő) megosztását. A nemi alapú erőszakhoz kapcsolódó rendszerszintű kockázatok ezért a jogellenes tartalmakról szóló, fenti 3.1. szakaszban és a megkülönböztetésmentességről szóló, fenti 3.2. szakaszban említett rendszerszintű kockázatok szempontjából is relevánsak. Az online közvetítő szolgáltatások széles körű igénybevétele hozzájárult a nemi alapú kiberbűnözés megjelenéséhez és felerősödéséhez. Bár minden szerződéstípus esetében azonosítottak nemi alapú erőszakhoz kapcsolódó rendszerszintű kockázatokat, ilyen kockázatokról a közösségimédia-platformok szolgáltatói számoltak be a leggyakrabban. A szolgáltatók és a civil társadalmi szervezetek kiemelték, hogy a nemi alapú erőszak aránytalanul nagy mértékben érinti a nőket és a lányokat, különösen a marginalizált csoportokhoz, többek között az etnikai vagy vallási kisebbségekhez tartozó nőket és lányokat, a fogyatékossággal élőket, valamint az LMBTIQ+-közösségeket[17]. Néhány civil társadalmi szervezet és szolgáltató megjegyezte, hogy az online platformok a marginalizált cscoportokkal szembeni nemi alapú erőszak és egyéb erőszak felerősítésének és normalizálásának kiemelkedő csatornái lehetnek, és hogy az online nőgyűlöletet a „gyűlölet kapuja”-ként emlegetik, amely a megkülönböztetés más formáihoz, többek között az LMBTIQ+-személyek diszkriminálásához is vezethet. A civil társadalmi szervezetek olyan rendszerszintű kockázatokra mutattak rá, mint a nemi alapú, célzott abúzus. Ilyen volt többek között a nemeket célzó zaklatás, a titkos követés, a molesztálás, a szexuális célú csábítás, valamint a nemi alapú gyűlöletre uszítás.

Több szolgáltató és civil társadalmi szervezet megjegyezte, hogy a dehumanizáló beszéd, a kirekesztő narratívák, például a szegregációt és a diszkriminációt népszerűsítő tartalmak, valamint az összehangolt zaklatás ellenséges online környezetek kialakulásához vezethet, amelyek viszont végső soron veszélyeztetik a felhasználók véleménynyilvánításhoz való szabadságát és közbeszédben való részvételét. Néhány közösségimédia-szolgáltató beszámolt konkrét női közszereplők, például politikusok, újságírók és aktivisták konkrét megcélzásáról is, ami szintén aggályokat vet fel az ilyen kockázatok polgári közbeszédre gyakorolt általánosabb hatásával kapcsolatban (lásd a véleménynyilvánítás és a tájékozódás szabadságához való alapvető jogot érintő rendszerszintű kockázatokról szóló 3.2. szakaszt és a polgári közbeszédet érintő rendszerszintű kockázatokról szóló 3.3. szakaszt).

[15] A Bizottság közleménye a Tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Az egyenlőségközpontú Unió: a 2020-2025 közötti időszakra szóló nemi esélyegyenlőségi stratégia, elérhető a következő linken: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52020DC0152

[16] Az az online terrorista tartalom terjesztésével szembeni fellépésről szóló, 2024. május 14-i európai parlamenti és tanácsi irányelv 5. cikke és (19) preambulumbekezdése, elérhető a következő linken: https://eur-lex.europa.eu/eli/dir/2024/1385/oj/hun. 2027. június 14-én lép hatályba.

[17] Ezt az „Egyenlőségközpontú Unió: az LMBTIQ+-személyek egyenlőségéről szóló stratégia (2026–2030)” című közlemény is kiemelte, elérhető a következő linken: https://commission.europa.eu/document/download/b4952371-4308-47ad-b995-02c539b75dda_en?filename=JUST_template_comingsoon_standard.pdf.

A szolgáltatók és a civil társadalmi szervezetek a személyes adatok és kifejezetten szexuális tartalmú anyagok rosszindulatú vagy hozzájárulás nélküli megosztásához kapcsolódó rendszerszintű kockázatokat is azonosítottak. Ezek az anyagok többek között „bosszúpornót", szexuális zsarolást, doxolást ábrázoló és kukkoló tartalmak, például rejtett kamerával készült felvételek és ún. „creepshot"-ok voltak. Több szolgáltató kockázatértékelési jelentése kiemelte a szolgáltatásaiban megjelenített nemi alapú erőszak egyéb eseteit, amelyek különösen nőket és lányokat céloztak meg, többek között az interneten mozdították elő, illetve segítették elő az emberkereskedelmet, a bűncselekménynek minősülő szexuális aktusokat, az erőszakot, a manipulálást, a szexuális erőszakra vonatkozó fenyegetést, valamint a szexualizált fenyegetések és megfélemlítés más formáit (a jogellenes tartalmak terjesztéséből fakadó rendszerszintű kockázatokról szóló 3.1. szakaszt).

A nemi alapú erőszakhoz kapcsolódó rendszerszintű kockázatokat érintő kockázati tényezőkre vonatkozó példák:

Tartalommoderálási rendszerek és ajánlórendszerek: A szolgáltatók gyakran említették, hogy a tartalommoderálási rendszerek és az ajánlórendszerek szerepet játszanak a felhasználók nemi alapú erőszakhoz kapcsolódó tartalmaknak való kitettségének alakításában, valamint az e tartalmak felerősítésében.

Mesterségesintelligencia-rendszerek: A civil társadalmi szervezetek a kifejezetten szexuális tartalmú anyagok – többek között szexuális aktusokat vagy deepfake pornográfiát bemutató anyagok – hozzájárulás nélküli létrehozásának, manipulálásának vagy terjesztésének megkönnyítése céljából mesterséges intelligencia használatával generált tartalmakat egyre nagyobb aggodalomra okot adó problémaként említették, ugyanis ezek aránytalanul nagy mértékben érinthetik a közéleti szerepet vállaló nőket, és gyakran alkalmazhatók tágabb értelemben vett dezinformációt és félretájékoztatást, (szexuális) zaklatást, megfélemlítést vagy hírnévrontást célzó kampányok összefüggésében.

A nemi alapú erőszakhoz kapcsolódó rendszerszintű kockázatokat érintő észrevételekre vonatkozó példák:

Save the Children Denmark, a Digitális Szolgáltatások Európai Testülete és az Európai Bizottság észrevétel-benyújtási felhívására benyújtott beadványok: *„[A] lányokat gyakrabban érik negatív hatások a magánjellegű vagy intim fényképeik vagy videóik megosztásából kifolyólag, mint a fiúkat".*

Google, A digitális szolgáltatásokról szóló rendelet szerinti 2024. évi kockázatértékelési jelentés (55. o.Ö a következő kockázatokat említette: *„Képalapú abúzus, többek között generatív MI-eszközökkel készült tartalmak (többek között a gyermekek szexuális zaklatását ábrázoló anyagok, a hozzájárulás nélküli, kifejezetten szexuális tartalmú képek, valamint a nem önkéntes, szintetikus pornográf képek) és a nemi alapú vagy LMBTIQ+-személyeket célzó zaklatás, gyűlölet és molesztálás”*.

Instagram, A digitális szolgáltatásokról szóló rendelet szerinti 2024. évi kockázatértékelési jelentés, 66. o.: *„Elismerjük továbbá, hogy az LMBTIQ+-közösség, valamint a közszereplők, például a női politikusok – különösen a színes bőrű női politikusok – aránytalanul nagy mértékben molesztálás és zaklatás célpontjai. Ez az LMBTIQ+-közösség és a nők elhallgattatásához, megfélemlítéséhez és/vagy a biztonságuk féltéséhez vezethet”*.

Közegészségügy. A szolgáltatók és a civil társadalmi szervezetek a dezinformáció vagy félretájékoztatás közösségi médián és keresőprogramokon belüli széles körű terjesztéséből fakadó, közegészségügyi vonatkozású rendszerszintű kockázatokat állapítottak meg. Ezek például a védőoltásokra, a jogszerű, de potenciálisan káros anyagokkal és gyakorlatokkal kapcsolatos félrevezető állításokra, a vírusszerűen terjedő káros tendenciák játékosítására, illetve súlyos egészségügyi problémákra, például az ebolára, a HIV-re/AIDS-re vagy a cukorbetegségre vonatkoztak. Az online piacterek szolgáltatói megjegyezték, hogy rendszerszintű kockázatok fakadnak abból, hogy az online piactereiken jogellenes, jogszabályoknak nem megfelelő vagy szabályozatlan egészségügyi termékeket értékesítenek. A példák többek között hamisított vagy nem megfelelő minőségű egészségügyi termékek (például nem tanúsított arcmaszkok) értékesítésére, valamint nem engedélyezett/hasznosítási engedéllyel nem rendelkező orvostechnikai eszközök, étrend-kiegészítők vagy gyógyszerek (például testsúlycsökkentő szerek) értékesítésére vonatkoztak. A szolgáltatók jogszerű, de káros anyagok – például alkohol, dohánytermékek és vényköteles gyógyszerek – és önkárosítással, táplálkozási rendellenességekkel vagy kockázatos egészségpraktikákkal kapcsolatos tartalmak népszerűsítésével összefüggő rendszerszintű kockázatokat is említettek. Bizonyos esetekben a szolgáltatók és a civil társadalmi szervezetek további rendszerszintű kockázatokat azonosítottak a széles körű és összehangolt egészségügyi dezinformációval és félretájékoztatással, valamint a gazdasági vagy politikai célokra használt, manipulált médiával kapcsolatban. A 3.3. szakasz részletesebben vizsgálja a polgári közbeszédet, a választásokat és a közbiztonságot érintő rendszerszintű kockázatokkal összefüggő dezinformációs és félretájékoztatási problémákat.

A közegészségügyhöz kapcsolódó rendszerszintű kockázatokat érintő kockázati tényezőkre vonatkozó példák:

Hirdetési rendszerek és egyéb kockázati tényezők: A szolgáltatók és a civil társadalmi szervezetek a közegészségügyi kockázatok terjesztéséhez és felerősítéséhez kapcsolódó kockázati tényezőket is említettek, például a platform kialakítását, funkcióit és interfészét, tartalommoderálási rendszereit és ajánlórendszereit. Konkrétan a hirdetési rendszerek tekintetében a civil társadalmi szervezetek az átverést vagy nem biztonságos termékeket népszerűsítő influenszer-marketinghez kapcsolódó rendszerszintű kockázatokat említették, amelyek esetében különösen a kiskorúak veszélyeztetettek, mivel nem feltétlenül ismerik fel az influenszerek promóciójának kereskedelmi természetét, még akkor sem, ha van felelősségkizáró nyilatkozat.

A közegészségügyhöz kapcsolódó rendszerszintű kockázatokat érintő észrevételekre vonatkozó példák:

A **Bing** digitális szolgáltatásokról szóló rendelet szerinti 2024. évi kockázatértékelési jelentése (127. o.) megemlítette, hogy létezik olyan *„kockázat, hogy a keresési találatok egészségi állapotra vonatkozó, illetve – az egyén állapota alapján pontatlan, nem biztonságos vagy más módon nem megfelelő vagy nem javallott – kezelésre, védőoltásokra vagy homeopátiás gyógymódokra vonatkozó információkat tartalmaznak”*.

European Fact-Checking Standards Network, a Digitális Szolgáltatások Európai Testülete és az Európai Bizottság észrevétel-benyújtási felhívására benyújtott beadványok: *„Az egészségügyi félretájékoztatás továbbra is jellemző és kifejezetten káros rendszerszintű kockázat az EU egészében, amelyre rengeteg példát szolgáltatnak az online óriásplatformokon keringő, hamis vagy félrevezető tartalmak. Az egészségügyi félretájékoztatás komoly károkat okozhat az egyének számára, de közegészségügyi szükséghelyzetek esetén is”.*

Fundacion Maldita, a Digitális Szolgáltatások Európai Testülete és az Európai Bizottság észrevétel-benyújtási felhívására benyújtott beadványok: *„Az egészségügyi dezinformáció egyik fontos aspektusa, hogy gyakran pénzszerzéshez kapcsolódik. (...) [A] csalárd jóváhagyások arra használják fel az egészségügyi szakemberek érzékelt tekintélyét, hogy potenciálisan káros kezelések vagy kiegészítők vásárlásáról győzzék meg a felhasználókat. (...) Bizonyos tartalmak finoman vagy nyíltan ösztönzik a rendellenes étkezési szokásokat, idealizálják a szélsőséges fogyókúrázást és az egészségtelen testkép-normákat. E demográfiai tényező sérülékenysége miatt ezek a tartalmak súlyos mentális és testi egészségügyi problémákhoz járulhatnak hozzá”.*

A kiskorúak védelme. Az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók többsége – különösen a közösségimédia-platformok és a

keresőprogramok szolgáltatói – és a civil társadalmi szervezetek említettek a kiskorúak védelméhez kapcsolódó rendszerszintű kockázatokat. Ilyen volt többek között a gyermekek szexuális zaklatását ábrázoló anyagok előfordulása és terjesztése, a kiskorúak szexualizálása, a szexuális zsarolás, a szexuális célú csábítás, az internetes zaklatás, az önkárosítás népszerűsítése, a gyermekkereskedelem és a gyermekek kizsákmányolása, valamint felnőttek és kiskorúak közötti egyéb, nem megfelelő interakciók, különösen olyan környezetekben, amelyek lehetővé teszik az anonim vagy magánjellegű interakciókat. A túlzott, megrögzött, függőségszerű közösségimédia-használatot szintén megemlítették a szolgáltatók és a civil társadalmi szervezetek, ahogyan azt a mentális jólléthez kapcsolódó rendszerszintű kockázatokat ismertető alábbi bekezdés részletezi. A civil társadalmi szervezetek az influenszerként működő kiskorúaknak többek között a szüleik vagy a gondviselőik általi, kereskedelmi célú kizsákmányolásra vonatkozó rendszerszintű kockázatokat is megállapítottak. Egyes szolgáltatók és civil társadalmi szervezetek az inkluzivitással kapcsolatos problémákat vetettek fel arra hivatkozva, hogy hiányoznak a különböző nyelveken elérhető minőségi tartalmak, és a tanulási nehézségekkel vagy fogyatékossággal küzdő gyermekek számára nem megfelelően férhetők hozzá. Egyes civil társadalmi szervezetek olyan kockázatokat is említettek, hogy a kiskorúak nem feltétlenül bíznak meg a káros tartalmakhoz kapcsolódó bejelentési mechanizmusokban és/vagy ezek a mechanizmusok nem gyermekbarátak, ami hozzájárulhat ahhoz, hogy a ténylegesnél kevesebb problémát jelentenek be. Bár a civil társadalmi szervezetek a közösségi médiát és a keresőprogramokat emelik ki a kiskorúak védelmét érintő rendszerszintű kockázatokra érzékeny fő platformtípusként, egyes civil társadalmi szervezetek megemlítették, hogy más platformtípusok, például az online piacterek használata is hordozhat kockázatokat, például a félrevezető marketingmódszerek miatt, amelyeket a felnőttek felismerhetnek, de a kiskorúak nem. Ahhoz kapcsolódó rendszerszintű kockázatokat is megállapítottak, hogy a közösségi médiát felhasználják olyan célra, hogy kiskorúakat toborozzanak szervezett bűnözéshez vagy terrorizmushoz[18]. A szolgáltatók továbbá az erőszakos tartalmaknak, a közösségi médiának és élő online közvetítési környezeteknek, (egymás) molesztálásának, zaklatásnak, célzott abúzusnak, titkos követésnek, doxolásnak, gyermekek nem szexuális célú bántalmazásának való kitettséghez kapcsolódó rendszerszintű kockázatokról is beszámoltak. A civil társadalmi szervezetek a közösségi média károkozási kihívásait is rendszerszintű kockázatokként említették.

A kiskorúak védelméhez kapcsolódó rendszerszintű kockázatokat érintő kockázati tényezőkre vonatkozó példák:

[18] Európai Parlament, Állampolgári Jogi, Bel- és Igazságügyi Bizottság (LIBE), 2025. június 4-i meghallgatás: „*Radicalisation online, with a focus on the recruitment of children for organised crime and terrorism"* (Online radikalizálódás, fókuszban a gyermekek szervezett bűnözéshez és terrorizmushoz toborzása), elérhető a következő linken: https://www.europarl.europa.eu/committees/en/online-radicalisation-recruitment-of-chi/product-details/20250516CHE13127. Az Europol hírszerzési értesítése, 2025. február 20.: „*The rise of online cult communities dedicated to extremely violent child abuse"* (A gyermekek elleni rendkívül erőszakos abúzusra szakosodott online kultuszközösségek felemelkedése), elérhető a következő linken: https://www.europol.europa.eu/publications-events/publications/rise-of-online-cult-communities-dedicated-to-extremely-violent-child-abuse.

Ajánlórendszerek: A szolgáltatók és a civil társadalmi szervezetek megjegyezték, hogy az ajánlórendszerek felerősíthetik a káros tartalmak terjesztését (például gyermek felhasználóknak egyre gyakrabban ajánl az algoritmus jogszerű, de potenciálisan problémás tartalmat, és ez a halmozott hatása miatt károssá válhat).

Mesterségesintelligencia-rendszerek: A civil társadalmi szervezetek megemlítették, hogy egyre gyakrabban használnak generatív mesterséges intelligencián alapuló rendszereket arra, hogy egy adott gyermeket ábrázoló bármilyen kép vagy videó alapján szexuális zaklatást ábrázoló anyagokat állítsanak elő, és azokat ezt követően online óriásplatformokon és nagyon népszerű online keresőprogramokon keresztül terjesszék, továbbá olyan rendszerszintű kockázatokat is említettek, amelyek generatív MI-robotokhoz kapcsolódtak (például amelyekkel a gyermekeknek érzelmi kötődésük alakulhat ki, így megzavarhatják a kapcsolati fejlődésüket).

A szolgáltatások szándékos manipulálása: A szolgáltatók kockázatértékelési jelentései aggályokat emeltek ki azzal kapcsolatban, hogy felnőttek kiskorúnak adják ki magukat, hamis profilokat hoznak létre, vagy megosztanak fiókokat gyermekekkel. A szolgáltatók beszámoltak az életkor-hitelesítés tekintetében felmerülő kihívásokról olyan esetekben, amikor a gondviselők félreértik vagy rosszul kezelik az életkor-ellenőrzési folyamatokat, vagy a kiskorúak nem a valós életkoruk megadásával kerülik meg az ellenőrzési vagy becslési intézkedéseket, vagy amikor kiskorúak hamis fiókokat vásárolnak vagy osztanak meg. Hasonlóképpen megjegyezték, hogy kihívások merülnek fel a tartalommoderálás területén, például amikor kódolt nyelvet és emotikonokat használnak a gyorsan változó moderálás kikerülése érdekében (például a „chicken soup”, azaz csirkehúsleves az önkárosításra, a „cheese pizza”, azaz sajtos pizza a gyermekek szexuális zaklatását ábrázoló anyagokra utal). A kockázatértékelési jelentésekben szerepeltek olyan esetek is, hogy gyermekeket eltávolítottak a platformról vagy átirányítottak a platformon kívülre, kevésbé moderált online vagy offline terekbe, ezzel fokozva a kizsákmányolás kockázatait.

A kiskorúak védelméhez kapcsolódó rendszerszintű kockázatokat érintő észrevételekre vonatkozó példák:

A **TikTok** digitális szolgáltatásokról szóló rendelet szerinti 2023. évi kockázatértékelési jelentése (16. o.) megemlítette, hogy a kiskorúak védelme tekintetében fennáll a következő kockázat: *„Magatartási kockázat és kapcsolati kockázat: ha kiskorúak tartalmat hoznak létre vagy tesznek közzé a platformon, vagy elköteleződnek mások által közzétett tartalmak mellett, akkor előfordulhat, hogy nem megfelelő magatartást tanúsítanak, vagy esetleg más felhasználók nem megfelelő magatartásával – például nem megfelelő kommentekkel, molesztálással vagy gyermekek szexuális kizsákmányolásának minősülő magatartással – szembesülnek ”.*

Eurochild, a Digitális Szolgáltatások Európai Testülete és az Európai Bizottság észrevétel-benyújtási felhívására benyújtott beadvány: *„Egyes online óriásplatformok által a jelentésükben megállapított további befolyásoló tényezőt a mesterséges intelligencia, különösen a tartalomgenerátorok jelentik. Annak ellenére, hogy ez még egy fejlődő terület, a káros anyagok mesterséges intelligencián alapuló technológiákkal történő generálása egyre gyakoribb tendencia. Ez különösen veszélyes, amikor gyermekek elleni szexuális abúzushoz – többek között szexuális célú csábításhoz, szexuális zsaroláshoz – és gyermekek szexuális zaklatását ábrázoló anyagok MI-generált létrehozásához használják, nemcsak finomhangolt modellekkel, hanem általános célú MI-rendszerekkel is. Két további aggasztó tendencia jelent meg: (1) MI-generált találatok megerősítenek káros sztereotípiákat, aránytalanul érintik a sérülékeny gyermekeket és (2) a gyermekek érzelmi manipulálása MI-robotokkal és -társakkal”.*

Knight-Georgetown Institute és **Panoptykon Foundation**, a Digitális Szolgáltatások Európai Testülete és az Európai Bizottság észrevétel-benyújtási felhívására benyújtott közös beadvány: *„A platform kialakítása fontos szerepet tölt be a nem kívánt és káros kapcsolatfelvétel kockázatainak előidézésében. Egyes platformok például alapértelmezés szerint lehetővé teszik a felhasználók láthatóságát, és felhasználói fiókokat ajánlanak a hálózatukon kívüli személyeknek, valamint a felhasználók hálózatán kívüli fiókokat ajánlanak nekik. Ezek a kialakítások különös kockázatokat jelentenek a kiskorúak számára annak lehetővé tétele révén, hogy rosszindulatú szereplők megcélozhatják és/vagy összegyűjthetik kiskorúak fiókjait. Kutatások megállapították, hogy a fiókok alapértelmezett láthatóságának kiterjedtsége és a fiókok ajánlása a kialakítás lényeges gyenge pontja a kiskorúakat célzó szexuális zsarolás szempontjából”.*

Fizikai és mentális jóllét.

- ***Fizikai jóllét.*** A fizikai jóllétet érintő rendszerszintű kockázatokat különböző szolgáltatótípusokkal összefüggésben állapítottak meg. A szolgáltatók és a civil társadalmi szervezetek például a közösségi médiában jelentkező rendszerszintű kockázatokat emeltek ki az öngyilkossággal, az önkárosítással, a nem reális testképpel, a táplálkozási rendellenességekkel, a túlzott testsúlyvesztéssel, a táplálkozási rendellenességek elleni helytelen vagy káros felépülési stratégiákkal vagy a megfelelő korlátozások vagy felelősségkizáró nyilatkozatok nélküli droghasználattal kapcsolatban. Az online piacterek ezzel szemben elsősorban a káros árukhoz vagy szolgáltatásokhoz – például az esetlegesen allergiás reakciókat vagy balesetet okozó gyógyhatású termékekhez – kapcsolódó rendszerszintű kockázatokat emeltek ki. A 3.1. és 3.2. szakasz részletesebben vizsgálja az ezekhez kapcsolódó kérdéseket, valamint a jogellenes tartalmak terjesztéséhez és a fogyasztóvédelemhez kapcsolódó rendszerszintű kockázatokat. A szolgáltatók és a civil társadalmi szervezetek az

alkalmazásáruházaktól származó rendszerszintű kockázatokat is megemlítettek olyan alkalmazások kapcsán, amelyek káros magatartásformákat ösztönözhetnek, egészségügyi dezinformációt vagy félretájékoztatást terjeszthetnek, vagy sérülékeny felhasználókat célozhatnak meg megtévesztő tartalmakkal. A kutatók túlzott képernyőidőt a fizikai jóllétet érintő potenciális kockázatokhoz sorolták, ilyen volt például a rövidlátás vagy a szem terhelése. Egyes szolgáltatók és civil társadalmi szervezetek leírták, hogy a felhasználók – különösen a kiskorúak – a túlzott használat következtében hogyan ütemezhetik át az alváshoz és a testmozgáshoz hasonló alapvető tevékenységeket, valamint a személyes társas interakciókat, továbbá leírták azt, hogy ezek a magatartásformák hogyan mutathatnak hasonlóságot a szerencsejáték és a szerhasználat okozta betegségek esetében megfigyelt mechanizmusokkal, potenciális negatív hatásokat fejtve ki a fizikai egészségükre.

- ***Mentális jóllét.*** A szolgáltatók a mentális egészséget és jóllétet érintő rendszerszintű kockázatokat különösen bizonyos tartalomtípusoknak való kitettség, valamint a közösségi média túlzott, megrögzött, függőségszerű használata, valamint az online piactereken tapasztalható kényszervásárlási rendellenességek miatt állapítottak meg. A civil társadalmi szervezetek bizonyos tartalmaknak való kitettséget a mentális egészséget érintő jelentős kockázatként emelték ki, különösen a marginalizált csoportokhoz vagy a kiskorúakhoz hasonló sérülékeny felhasználók esetében. A kockázatértékelési jelentések megállapították, hogy az önkárosításhoz, az öngyilkossághoz és a táplálkozási rendellenességekhez kapcsolódó tartalmak hozzájárulhatnak ahhoz, hogy a káros magatartásformák normalizálódnak vagy ösztönzést kapnak a felhasználókban. Néhány szolgáltató további rendszerszintű kockázatként emelte ki a káros tartalmaknak való tartós kitettséget, ami hosszan tartó lelki gyötrelmet kelthet a felhasználókban, és olyan példákat hoztak fel, mint a célzott zaklatás, az internetes zaklatás, valamint az egyén vagy csoport bizonyos tulajdonságain alapuló inzultusok. Néhány civil társadalmi szervezet megemlítette a közösségi médiában például fegyveres konfliktusokra vonatkozó hírtartalmaknak való jelentős kitettséggel összefüggő szorongás rendszerszintű kockázatait.

A fizikai és mentális jólléthez kapcsolódó rendszerszintű kockázatokat érintő kockázati tényezőkre vonatkozó példák:

Kialakítások, interfészek, jellemzők: A szolgáltatók és a civil társadalmi szervezetek az online óriásplatformok és nagyon népszerű online keresőprogramok kialakításához társuló mentális és fizikai egészségügyi kockázatokat azonosítottak, például a közösségi média túlzott, megrögzött, függőségszerű használatával összefüggésben. Egyesek megjegyezték a platform-kialakítási jellemzőket, például a végtelen görgetést, az automatikus lejátszást, az ideiglenes tartalmakat, az értesítéseket és egyéb, a kényszerhasználati mintázatokkal összefüggő interfész-elemeket, különösen olyan esetekben, amikor a platformok jelentős

felhasználói kontroll nélkül ösztönzik az elköteleződést (például a használat visszaszorítását célzó mechanizmusok). Több civil társadalmi szervezet megemlítette, hogy ezek a jellemzők és kialakítások jelentős függőséget okozhatnak. Más civil társadalmi szervezetek azzal kapcsolatos rendszerszintű kockázatokat jegyeztek meg, hogy a platformokat úgy állítják be, hogy a felhasználók a lehető legtöbb időt töltsenek az alkalmazással, vagy bizonyos módokon figyelemfelkeltésre vagy jóváhagyásra ösztönzik a felhasználókat. Néhány civil társadalmi szervezet például megjegyezte a platformokon elérhető vagy ott hirdetett – különösen kiskorúaknak és sérülékeny egyéneknek szánt – videójátékok szerencsejátékhoz hasonló és függőséget okozó jellemzőit. A civil társadalmi szervezetek a szépségszűrőkhöz hasonló jellemzők esetében említették, hogy hozzájárulnak a felhasználók negatív testképének kialakulásához és a valóságtól elrugaszkodott társadalmi összehasonlítást népszerűsítenek.

Ajánlórendszerek és mesterségesintelligencia-rendszerek: A civil társadalmi szervezetek és a szolgáltatók továbbá megemlítették, hogy ezeket a problémákat súlyosbíthatja az úgynevezett „nyúl ürege hatás”, amellyel konkrét tartalomtípusok ajánlása többször ismétlődik. Néhány civil társadalmi szervezet azt is megemlítette, hogy általában a lakosság számára nem feltétlenül káros, vagy önmagukban nem feltétlenül problémásnak tűnő tartalmak hogyan okozhatnak kockázatokat, ha azokat sérülékeny egyének (például kiskorúak, függőségben vagy betegségben szenvedő személyek) (többször) látják. A civil társadalmi szervezetek a generatív mesterséges intelligenciát alkalmazó robotok által a fizikai és mentális jóllétre jelentett rendszerszintű kockázatokat is megemlítették, például – (táplálkozási rendellenességgel kapcsolatban) különösen gyermekeknek szánt – káros egészségtanácsadás ajánlásával összefüggésben.

A fizikai és mentális jólléthez kapcsolódó rendszerszintű kockázatokat érintő észrevételekre vonatkozó példák:

Snapchat, A digitális szolgáltatásokról szóló rendelet szerinti 2023. évi kockázatértékelési jelentés, 190. o., a „Filter bubble (Szűrőbuborék) címszó alatt: *„Ezért fennáll az a kockázat, hogy biztosítékok hiányában az algoritmus az önmagukban nem feltétlenül káros tartalmakat megtekintő felhasználókat úgy jelöli meg, hogy érdeklődnek az adott tartalmak iránt, valamint az a kockázat, hogy az adott tartalmaknak való, ismétlődő és gyakori kitettség káros lehet”.*

Instagram, A digitális szolgáltatásokról szóló rendelet szerinti 2024. évi kockázatértékelési jelentés, 66. o.: *„A molesztálás és a zaklatás összefügg a digitális szolgáltatásokról szóló rendelet szerinti »polgári közbeszéd és választások«, »nemi alapú erőszak«, valamint »kiskorúak védelme« kockázati területekkel. Ez a problématerület arra a kockázatra utal, hogy a Meta rendszereit felhasználják a felhasználókat degradáló vagy megszégyenítő*

tartalmak népszerűsítése céljával, vagy azzal a céllal, hogy többször kéretlenül felvegyék a kapcsolatot egy adott felhasználóval, például internetes zaklatás, károkozási fenyegetések, tömeges zaklatás és szexuális zaklatás formájában. Elismerjük, hogy a molesztálás és a zaklatás aránytalan hatást gyakorolhat a kiskorúak jóllétére és mentális egészségére".

TikTok, A digitális szolgáltatásokról szóló rendelet szerinti 2024. évi kockázatértékelési jelentés, 50. o.: a „*Risks related to AIGC*" (MI-generált tartalmakhoz kapcsolódó kockázatok) és a „*Well-being impact and social comparison"* (A jóllétre kifejtett hatás és társadalmi összehasonlítás) címszavak alatt: *„Korai kutatások arra utalnak, hogy a fiatalabb felhasználók jóllétét érintő kockázatokat összefüggésbe hozzák MI-generált tartalmakkal, többek között platformon kívüli, MI-generált tartalmak létrehozására szolgáló eszközökkel generált tartalmakkal, különösen az önbecsülés, a testkép és a mentális egészség vonatkozásában".*

A **Google** digitális szolgáltatásokról szóló rendelet szerinti 2024. évi kockázatértékelési jelentése (134. o.) megemlítette, hogy fennáll az a *„[k]ockázat, hogy egy adott szolgáltatás interfésze, kialakítása vagy jellemzői a szolgáltatás kényszerhasználatát ösztönözheti a felhasználók, köztük gyermekek számára".*

Knight-Georgetown Institute és **Panoptykon Foundation**, a Digitális Szolgáltatások Európai Testülete és az Európai Bizottság észrevétel-benyújtási felhívására benyújtott közös beadvány: *„Előfordulhat, hogy a közösségi média ajánlórendszerei a túlzottan személyre szabott élmények nyújtása érdekében magatartási mintázatokra hagyatkoznak. Ezek a mintázatok felfedhetik az egyéni gyenge pontokat, például a függőségeket, a táplálkozási rendellenességeket, a testtel kapcsolatos komplexusokat, a szorongást vagy a depresszív hajlamokat. A felhasználói elköteleződés maximalizálására tervezett ajánlórendszerek szándékosan vagy akaratlanul is kihasználhatják vagy súlyosbíthatják ezeket az egyéni gyenge pontokat. Az egyéntől függően ezek a rendszerek visszacsatolási hurkokat is kialakíthatnak, amelyek a gyenge pontjaiknak megfelelő, szűkebb tartalomválaszték felé terelik a felhasználókat. Ezek a tartalmak önmagukban nem feltétlenül veszélyesek, és elszigetelten tekintve nem feltétlenül elfogadhatók teljes egészében, azonban károssá válnak, ha azokat sérülékeny felhasználók rendszeresen fogyasztják."*

4. A rendszerszintű kockázatok csökkentését célzó gyakorlatok

Ez a fejezet alapvetően a rendelet 35. cikke (1) bekezdésének felépítését követi a szolgáltatók és a civil társadalmi szervezetek által említett kockázatcsökkentési intézkedések főbb kategóriáinak áttekintésekor. E fejezet egyes szakaszai a 35. cikk (1) bekezdésének egy vagy több albekezdésének felel meg, a 35. cikk (1) bekezdésének j) pontja kivételével, amelyre nem tér ki külön szakasz, mert a gyermekek jogaival kapcsolatos kockázatcsökkentési intézkedések az összes többi intézkedésnél szerepelnek.

A 35. cikk (2) bekezdése kimondja, hogy a Testület jelentése a következőket foglalja magában: *„az online óriásplatformot vagy nagyon népszerű online keresőprogramot üzemeltető szolgáltatók által az azonosított rendszerszintű kockázatok csökkentésére alkalmazott bevált gyakorlatok”*. A rendelet végrehajtása – többek között a 34. és 35. cikk végrehajtása – még korai szakaszban van, és a Testület jelentésének első kiadása ezért a jelenlegi gyakorlatok, valamint a szolgáltatók és a civil társadalmi szervezetek által javasolt gyakorlatok bemutatásából áll, nem emel ki egyet sem „bevált” vagy akár feltétlenül „jó” gyakorlatként, és a természetéből adódóan hiányos. Ezenkívül, és ahogyan az 1. fejezetben is szerepel, e jelentés egyetlen megállapítása sem értelmezendő a rendelet 34. vagy 35. cikkének való megfeleléshez tartozó iránymutatásként, és az e jelentésben foglalt megállapítások egyike sem értelmezendő úgy, hogy értékelné kijelölt online óriásplatformoknak és nagyon népszerű online keresőprogramoknak a rendelet 34. vagy 35. cikkének vagy bármely egyéb rendelkezésének való megfelelését. Ez a jelentés nem sért egyetlen jelenlegi vagy jövőbeli vizsgálatot, végrehajtási intézkedést vagy a rendelet szerinti keretrendszer alapján tett hivatalos megállapítást sem.

Az e jelentésben ismertetett gyakorlatokat továbbá nem elszigetelten kell figyelembe venni, hanem inkább konkrét kockázatok csökkentésének biztosítását célzó intézkedések kombinációihoz tartozó lehetséges elemeknek kell tekinteni. Ahogyan az 1. fejezet hangsúlyozza, a szolgáltatóknak kiemelt figyelmet kell fordítaniuk az ilyen intézkedéseknek az alapvető jogokra – többek között a véleménynyilvánítás és a tájékozódás szabadságához való jogra – gyakorolt hatásaira.

Előfordulhat, hogy az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók akár a rendelet hatálybalépése előtt elfogadtak bizonyos kockázatkezelési intézkedéseket, amelyek hozzájárulnak a rendelet szerinti rendszerszintű kockázatok csökkentéséhez, például az üzleti tevékenységük folytatása vagy más alkalmazandó jogszabályoknak való megfelelés keretében. Minden szolgáltatónak vannak például a szolgáltatásaik igénybevételére irányadó részletes és átfogó szerződési feltételei, és a legtöbb, ha nem az összes szolgáltatónak voltak érvényben valamilyen formájú tartalommoderálási intézkedései még a rendelet hatálybalépése előtt. A rendelet által bevezetett egyik újdonság az a követelmény, hogy átfogó jelleggel be kell számolni az elvégzett kockázatértékelésekről és az azokat követően hozott kockázatcsökkentési intézkedésekről, fokozva ezzel a rendszerszintű kockázatok és a csökkentésük átláthatóságát. Az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók a rendelet 35. cikkének (1) bekezdése értelmében a Bizottság felügyelete mellett kötelesek hatékony kockázatcsökkentési intézkedéseket bevezetni, és a 42. cikk (4) bekezdése értelmében kötelesek az intézkedésekről nyilvánosan jelentést tenni, hogy bárki információt szerezhessen azokról. Ez lehetővé teszi az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók elszámoltathatóságát és külső ellenőrzését, ami növeli a szabályozó hatóságok szerepét. A rendszerszintű kockázatok idővel változnak, a rendelet kockázatkezelési kerete ezért előírja a

kockázatértékelési és -csökkentési intézkedések folyamatos megújítását. A szolgáltatóktól elvárt rendszeres kockázatkezelési tevékenységek fényében a Testület által a Bizottsággal együttműködésében a 35. cikk (2) bekezdése szerint készített jelentések lehetővé fogják tenni az éves átláthatósági és számbavételi törekvéseket.

Az e jelentésre való felkészülés során folytatott konzultációk és összegyűjtött információk rávilágítottak arra, hogy annak érdekében, hogy az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók és a civil társadalmi szervezetek a jövőben a legmegfelelőbben azonosíthassák a kockázatcsökkentési lehetőségeket, biztosítaniuk kell, hogy a felhasználók, az érintett csoportok, a civil társadalmi szervezetek és a kutatók képviselői érdemlegesen bekapcsolódjanak a kockázatértékelési jelentések előkészítésébe. A rendelet (90) preambulumbekezdésére vonatkozóan az 1. fejezetben és a 3. fejezet fenti bevezetésében szereplő megjegyzések így szintén relevánsak az észszerű, arányos és hatékony kockázatcsökkentési intézkedések azonosítása szempontjából.

Végezetül ez a jelentés emlékeztet a kiskorúak magas szintű online magánéleti védelmének és biztonságának az (EU) 2022/2065 rendelet 28. cikkének (4) bekezdése értelmében történő biztosítását célzó intézkedésekről szóló bizottsági iránymutatás[19], „az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók számára a választási folyamatok rendszerszintű kockázatainak csökkentéséről az (EU) 2022/2065 rendelet 35. cikkének (3) bekezdése alapján” című bizottsági iránymutatás[20], valamint a dezinformáció visszaszorítását célzó magatartási kódex[21] és a jogellenes online gyűlöletbeszéd felszámolására vonatkozó, felülvizsgált magatartási kódex[22] jelentőségére, de nem részletezi és nem értékeli a szolgáltatók által elfogadott ilyen intézkedések elterjedését. Ez a fejezet az egyéb uniós jogszabályoknak való megfelelés részeként hozott intézkedéseket sem részletezi.

4.1. A szolgáltatások, többek között az online interfészek kialakítása, jellemzői és működése

A rendelet 35. cikke (1) bekezdésének a) pontja a szolgáltatók által bevezetendő, következő kockázatcsökkentési intézkedésekre hivatkozik: *„szolgáltatásaik kialakításának, jellemzőinek vagy működésének módosítása, beleértve online interfészeiket is”*.

Számos szolgáltató ismertetett a jelentésében a rendszerei kialakításából, jellemzőiből vagy interfészeiből fakadó rendszerszintű kockázatok csökkentését célzó intézkedéseket. Néhány, online piacteret üzemeltető szolgáltató például jelezte, hogy a közösségi funkciók és a

[19] A Bizottság közleménye – Iránymutatás a kiskorúak magas szintű online magánéleti védelmének és biztonságának az (EU) 2022/2065 rendelet 28. cikkének (4) bekezdése értelmében történő biztosítását célzó intézkedésekről, elérhető a következő linken: https://eur-lex.europa.eu/eli/C/2025/5519/oj/hun.
[20] Lásd a 11. lábjegyzetet.
[21] Lásd a 13. lábjegyzetet.
[22] A jogellenes online gyűlöletbeszéd felszámolására vonatkozó, 2025. évi felülvizsgált magatartási kódex, elérhető a következő linken: https://digital-strategy.ec.europa.eu/en/library/code-conduct-countering-illegal-hate-speech-online.

felhasználói interakciók (például a felhasználók közötti csevegés) korlátozásával, a felhasználók által generált tartalmak terjesztésének vagy a tartalmak alapértelmezett személyre szabásának korlátozásával csökkenti a rendszerszintű kockázatokat. Bizonyos tartalomkategóriákból – többek között a jogellenes tartalmakból és esetlegesen a rendelet 34. cikke szerinti egyéb kockázatkategóriákba tartozó kategóriák kialakulásához vezető tartalmakból – fakadó rendszerszintű kockázatok csökkentése érdekében a civil társadalmi szervezetek azt javasolták, hogy ösztönzőket, feszültséget kiváltó elemeket, például áramkör-megszakítókat kellene bevezetni, például annak érdekében, hogy a felhasználókat emlékeztessék bizonyos szabályokra a tartalmak közzététele előtt (lásd még az ajánlórendszerekről szóló 4.4. szakaszt). Egyes civil társadalmi szervezetek továbbá azt javasolták, hogy a szolgáltatóknak nem lenne szabad potenciálisan függőséget okozó kialakítási jellemzőket alkalmazniuk, például ki kellene kapcsolniuk az értesítéseket és az alapértelmezett automatikus lejátszást. Több szolgáltató és civil társadalmi szervezet bizonyos típusú (például erőszakot bemutató) káros tartalmaknál alkalmazott kockázatcsökkentési intézkedésként említette a képek és videók elhomályosítását, többek között az elhomályosítás mellett alkalmazott figyelmeztető üzeneteket is (például a felhasználókat azzal a céllal figyelmeztető közvetlen üzeneteket, hogy ne érezzék kényszerítve magukat arra, hogy meztelenséget tartalmazó üzenetekre válaszoljanak, különösen akkor, ha azokat kéretlenül kapták). A szolgáltatók és a civil társadalmi szervezetek megemlítették, hogy előfordul olyan, hogy blokkolnak olyan jellemzőket és egyéb mechanizmusokat, amelyek célja annak megakadályozása, hogy más felhasználók lássák egy-egy felhasználó tartalmait vagy reagáljanak azokra, vagy azon feltételek ellenőrzésének megakadályozása, amelyek szerint mások láthatják egy-egy felhasználó tartalmait vagy reagálhatnak azokra. Egyes civil társadalmi szervezetek és szolgáltatók megemlítették, hogy a szolgáltatók számára fontos, hogy egy-egy felhasználó blokkolása után megőrizzék az információkat, különösen (például zaklatásra irányuló) nyomozások esetén a korábbi beszélgetésekre vonatkozó bizonyítékok megőrzése céljából.

A szolgáltatók – különösen a közösségimédia-platformok szolgáltatói – és a civil társadalmi szervezetek kiemelték a kiskorúak védelmét célzó különböző platformkialakítási döntéseket, illetve alapértelmezett beállításokat. Például többek között a jogszabályban meghatározott korhatárra vonatkozó követelményekhez és az online biztonsági központokban közzétett cikkekhez hasonló figyelemfelkeltési intézkedéseket, az online élő közvetítéseknek és a felnőttek MI-jellemzőkhöz való hozzáférésének korlátozását, az oktatási tartalmak hírfolyamokban való felfedezésének megkönnyítését, tartalombesoroló algoritmusoknak adott tartalmak különböző korcsoportok számára való megfelelősége alapján történő használatát, valamint a potenciálisan káros felhasználókkal való interakciók korlátozása érdekében a kiskorúak fiókjainak alapértelmezetten priváttá tételét emelték ki. A keresőprogram-szolgáltatók többsége megemlítette a kiskorúak számára automatikusan bekapcsolt biztonságos keresési funkciókat a kiskorúak esetében általuk nem megfelelőként besorolt keresési találatok kiszűrése érdekében. Néhány szolgáltató említést tett különböző korcsoportokhoz igazodó (például lefekvésre vagy a tartalom megtekintése közbeni szünet tartására vonatkozó)

emlékeztetőkről. Egyes szolgáltatók továbbá egyedi beállításokat kínáló szülői felügyeleti eszközöket vezettek be annak érdekében, hogy a gondviselők azok segítségével irányítsák a gyermekek online tapasztalatait. Az említett szülői felügyeleti eszközök az alkalmazáshasználathoz tartozó napi limitek beállításának szülők számára való lehetővé tételétől a gyermekeik képernyőidejére vonatkozó értesítésekig, valamint magatartásuk és online kapcsolataik jelentéséig változtak. Egyes esetekben a szolgáltatók említést tettek arról, hogy kiskorúak számára alapértelmezetten letiltják a végtelen görgetési és automatikus lejátszási funkciókat. Egyes civil társadalmi szervezetek azt javasolták, hogy a kiskorúak megfelelőbb védelme érdekében a tervezés által garantált biztonságra vonatkozó megközelítést kellene bevezetni, többek között egyedi címkéket és külön besoroló algoritmusokat kellene használni kiskorúaknak szánt tartalmakhoz. Civil társadalmi szervezetek a kiskorúaknak szánt, többször ajánlott tartalomtípusok azonosítását és korlátozását is megemlítették.

4.2. Szerződési feltételek és azok érvényesítése

A rendelet 35. cikke (1) bekezdésének b) pontja a következő kockázatcsökkentési intézkedések bevezetését említi a szolgáltatók számára:
„szerződési feltételeik módosítása és azok érvényesítése”[23].

Valamennyi szolgáltató beszámolt arról, hogy az újonnan megjelenő és a változó rendszerszintű kockázatok (például deepfake-ek), az új felhasználói tendenciák (például a felhasználók ismétlődő jogsértései), a változó jogi követelmények (például új nemzeti jogi keretek), illetve egyéb fejlemények (például új tervezési jellemzők) kezelése érdekében rendszeresen nyomon követi és frissíti szerződési feltételeit.

A kiskorúak tekintetében egyes szolgáltatók közölték, hogy szerződési feltételeikben bevezettek olyan új rendelkezéseket, amelyek korlátozzák a kiskorúak számára a szolgáltatásaikhoz való hozzáférést, a fiókok regisztrálását vagy a fizetési módszerek használatát. Néhány szolgáltató továbbá azt állította, hogy rendszeres életkor-ellenőrzést végez annak érdekében, hogy biztosítsa szerződési feltételeinek érvényesítését. Néhány szolgáltató közölte, hogy szerződési feltételeinek konkrétabbá és érthetőbbé tétele érdekében azokat példákkal vagy illusztrációkkal javította.

4.3. Tartalommoderálási rendszerek

A rendelet 35. cikke (1) bekezdésének c) pontja a következő kockázatcsökkentési intézkedés bevezetését említi a szolgáltatók számára: *„a tartalommoderálási eljárások módosítása, beleértve a jogellenes tartalmak konkrét típusaira vonatkozó bejelentések feldolgozásának*

[23] A Bizottság létrehozta a digitális szolgáltatások szerződési feltételeinek adatbázisát, amely a következő linken érhető el: https://platform-contracts.digital-strategy.ec.europa.eu/.

gyorsaságát és minőségét, valamint adott esetben a bejelentett tartalom mielőbbi eltávolítását vagy hozzáférhetetlenné tételét – különösen a jogellenes gyűlöletbeszéd vagy az online erőszak esetében –, továbbá a releváns döntéshozatali eljárások és a tartalommoderálásra szánt források módosítása”.

Tartalommoderálási eszközök és módszerek. A szolgáltatók említést tettek (automatizált és emberi értékelést tartalmazó saját) proaktív tartalommoderálási módszerek és (a felhasználói bejelentésekre reflektáló) reaktív módszerek ötvözéséről. A szolgáltatók és a civil társadalmi szervezetek megemlítették a mesterséges intelligencia tartalommoderálás során történő használatát, kiemelve annak előnyeit (például sebesség, reagálási sebesség) és hiányosságait (például a döntések magyarázhatósága tekintetében), valamint azt, hogy önmagában kockázati tényezőt és kockázatcsökkentési intézkedést is jelenthet. A civil társadalmi szervezetek kiemelték, hogy sokféle nyelv lefedése érdekében fontos, hogy legyenek megfelelő erőforrásokkal rendelkező tartalommoderáló csapatok.

A civil társadalmi szervezetek továbbá hangsúlyozták, hogy az emberi moderátoroknak megfelelően képzettnek kell lenniük, és ismerniük kell a helyi környezetet, nyelveket és kultúrákat. Néhány szolgáltató például említett olyan kockázatcsökkentési intézkedéseket, amelyekkel felderíthető, hogy mikor használnak bizonyos emotikonokat jogellenes tevékenységek – például tiltott kábítószerek értékesítése – álcázásának kódolásához. Egyes szolgáltatók említést tettek veszélyes virális tendenciák, például káros kihívások azonosítására szolgáló korai felderítési modellek létrehozásáról. Megemlítették a szólisták használatát (többek között az új szleng kifejezésekhez való alkalmazkodást célzó, kijátszás elleni intézkedéseket és az emotikonok használatát, különösen a kiskorúak által közzétett tartalmakhoz, továbbá a veszélyes kihívásokhoz hasonló új tendenciák azonosítására szolgáló korai felderítési modelleket). Jogellenes tartalmak (például terrorista tartalmak, gyermekek szexuális zaklatását ábrázoló anyagok, szellemi tulajdonjogi jogsértések) esetében az ujjnyomatok, illetve a tartalmi hash-egyezések használatát is kiemelték. Néhány szolgáltató az audio-tartalmak automatizált szöveges átírását és a létrejött szöveg automatizált elemzését is a tartalommoderálás tökéletesítési módjaként említette. Néhány szolgáltató említést tett arról is, hogy bizonyos népszerűségi küszöböt elérő tartalmak esetében emberi értékelést használ. Az életkoron alapuló tartalomszűrők kiskorúak esetében történő használatát szintén megemlítették (például különböző szűrőket használnak a gyaníthatóan 13 év alatti, a 13 és 15 év közötti, illetve a 16 és 18 év közötti felhasználók esetében). A kontextusfüggő szövegmoderálási intézkedéseket szintén megemlítették (például kifejtették a felhasználóknak, hogy bizonyos tartalmak, illetve kommentek miért nem tehetők közzé amiatt, hogy azok a tartalommoderálási szűrőkön esetlegesen megakadnak). A szolgáltatók említést tettek arról is, hogy a különböző formátumok (például szöveg, képek, videók) és felületek (többek között online élő közvetítések) esetében biztosítani kell a következes tartalommoderálást. A szolgáltatók és a civil társadalmi szervezetek kiemelték a független tényellenőrökkel való együttműködést, különösen a dezinformáció visszaszorítását célzó magatartási kódex összefüggésében. Néhány szolgáltató és civil társadalmi szervezet a közösségi értesítések használatát is megemlítette.

Operatív szinten említést tettek annak fontosságáról, hogy szoros kapcsolatnak kell lennie a tartalommoderáló és a jogi munkacsoportok között a határesetek magasabb szintre vitele érdekében, megemlítették továbbá az előítéletek leküzdésével foglalkozó kutatókkal és civil társadalmi szervezetekkel való partnerségeket, a nyelveken belüli helyi árnyalatok, a szleng kifejezések és a kulturális hivatkozások kiszűrését célzó piacspecifikus moderálási folyamatok létrehozását (különösen a gyűlöletbeszéd összefüggésében), valamint az emberi értékelők által a hét minden napján napi 24 órában végzett tartalommoderálás következetes érvényesítésének biztosítását (például az időzónák közötti eltérések kihasználásával). A civil társadalmi szervezetek kiemelték, hogy a platformról platformra terjedő moderálási kihívások előrejelzése érdekében fontos figyelembe venni a platformon kívüli és offline eseményeket. Számos szolgáltató megemlítette, hogy vannak kommunikációs csatornái bűnüldöző hatóságokkal, például a gyermekek szexuális zaklatását ábrázoló anyagokhoz hasonló jogellenes tartalmak tekintetében. Néhány szolgáltató ismertette a belső és külső ellenőrzések, valamint a tartalommoderálási irányelvek és a végrehajtásuk rendszeres felülvizsgálatát, valamint annak értékelését, hogy a rendelet szerinti egyéb jogi kötelezettségek (például az általános adatvédelmi rendelet[24]) hogyan befolyásolhatják a tartalommoderálási gyakorlataikat.

A rendszeresen moderált tartalmakat közzétevő felhasználók számára kiszabott büntetések között a szolgáltatók a bevételszerzés lehetőségének megszüntetésétől a platformról való eltávolításig terjedő eszkalációs mechanizmusokat említettek. Néhány szolgáltató a moderálási döntések meghozatalakor figyelembe veendő tényezők között kiemelte bizonyos felhasználók platformra nem illő magatartását.

Moderálási témakörök. A tartalommoderálás tekintetében leggyakrabban említett témakörök a következők voltak: jogellenes tartalomként és szolgáltatásként felsorolt bármilyen elem, valamint a szerződési feltételeket sértő tartalmak, például az életkornak nem megfelelő tartalmak, becsmérlés, molesztálás és zaklatás, diszkriminatív magatartás, veszélyes szervezetek és bűnözők által közzétett tartalmak, nem hiteles magatartás és a platformok manipulálása.

Több szolgáltató említést tett arról, hogy az egyébként a szerződési feltételeket sértő tartalmak (például erőszak, fegyveres konfliktusok) esetén eltérést alkalmaz a moderáláskor, ha az adott tartalmak különleges – például oktatási, dokumentációs, tudományos, szatirikus vagy művészeti – értéket képviselnek. Néhány szolgáltató a gyermekek biztonságát szolgáló további ellenőrzéseket és kialakítási jellemzőket említett, többek között a szülőknek és a gondviselőknek szánt egyedi szűrőket olyan tartalmak ellenőrzéséhez, amelyeket a gyermekeik esetleg megtekinthetnek.

[24] Az 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), elérhető a következő linken: https://eur-lex.europa.eu/eli/reg/2016/679/oj/hun.

Az online piactereken kínált jogellenes termékek, például szellemi tulajdonjogokat sértő termékek, jogszabályoknak nem megfelelő vagy veszélyes áruk tartalommoderálásával összefüggésben a szolgáltatók olyan automatizált vagy félig automatizált tartalommoderálási gyakorlatokat említettek, mint az eszközök nyomon követése és kiszűrése, a korábban eltávolított termékekhez nagyon hasonló termékek keresztellenőrzése, a megerősítetten nem szabályszerű/jogellenes termékek azonosítására szolgáló rendszerek. A szolgáltatók – többek között harmadik félnek minősülő laboratóriumokkal közösen végzett – saját kezdeményezésű termékmegfelelőségi ellenőrzésekről is említést tettek. Számos kockázatcsökkentési intézkedés irányul a kereskedőkre, ilyenek például a kereskedők uniós termékszabályozási ismereteinek bővítését célzó intézkedések, vagy a jogellenes termékeket értékesítő kereskedők szankcionálásához vagy feketelistára helyezéséhez hasonló, ösztönző kezdeményezések. A hamisított és a szellemi tulajdonjogokat sértő termékek esetében egyes platformok, például online piacterek említették, hogy szellemi tulajdonjogok vagy márkák védelmét célzó programok keretében együttműködést folytatnak a jogosultakkal hamis listák mögé rejtett hamisított termékek, valamint más visszaéléstípusok azonosítása érdekében. Néhány, online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltató továbbá arról számolt be, hogy speciális eszközöket kínálnak a márkák számára a jogaik kezeléséhez és védelméhez, többek között platformok közötti keresést, képblokkolást, valamint csoportos jogérvényesítési intézkedéseket.

A civil társadalmi szervezetek a szankcionált jogalanyoktól származó tartalmak tekintetében olyan intézkedéseket javasoltak, mint a földrajzi blokkolás, a pénzszerzési lehetőségek megszüntetése, az árnyékletiltás vagy a szankcionált jogalanyok tartalmait terjesztő felhasználók és fiókok nyílt letiltása. Ebben az összefüggésben a civil társadalmi szervezetek azt javasolták, hogy az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók rendszeresen vizsgálják felül a szankciólistákat.

4.4. Algoritmikus rendszerek, ideértve az ajánlórendszereket is

A rendelet 35. cikke (1) bekezdésének d) pontja a következő kockázatcsökkentési intézkedések bevezetését említi a szolgáltatók számára:
„algoritmikus rendszereik, köztük ajánlórendszereik tesztelése és módosítása”.

Tartalomajánlások. A szolgáltatók és a civil társadalmi szervezetek beszámoltak annak előfordulásáról, hogy az ajánlórendszerek visszaminősíthetnek káros vagy potenciálisan káros tartalmakat, például jogellenes tartalmakat, nem hiteles tartalmakat, a szerződési feltételeket sorozatosan megsértőktől származó tartalmakat vagy dezinformációs tartalmakat. A szolgáltatók és a civil társadalmi szervezetek néhány esetben megemlítették a tartalomterjesztés esetleges korlátozását, például kiskorúak által létrehozott tartalmak, vagy bizonyos szintű népszerűséget elért, de emberi felülvizsgálaton még át nem esett tartalmak esetében. A

szolgáltatók hasonlóképpen megjegyezték, hogy a nagyon kockázatos témákkal kapcsolatos tartalmak vagy a kritikus időszakokban – például választások, vagy természeti katasztrófákhoz vagy közegészségügyi válságokhoz hasonló válságok idején – közzétett tartalmak terjesztési korlátozások alá eshetnek. Néhány szolgáltató beszámolt arról, hogy észlelt offline koordinációból vagy más platformokról kiinduló incidensekből fakadó átgyűrűző hatást, például virális trendeket, és információs szalaghirdetéseket vagy az oldalt teljesen eltakaró hirdetést (interstitial) használt az ilyen tartalmak terjedésének korlátozása érdekében.

A rendszerek kialakítása. Néhány szolgáltató azt közölte, hogy algoritmikus rendszereit úgy alakította ki, hogy azok változatos, ne leszűkített és ismétlődő tartalmakat ajánljanak, és a potenciális ajánlásokhoz kiválogatott tartalmi elemeket megbízható forrásokból és elismert szakértőktől szerzi be. Egyes szolgáltatók azt állították, hogy az ajánlórendszereik nemcsak a megtekintési időre, hanem a tartalom minőségére is optimalizálva vannak. A szolgáltatók és a civil társadalmi szervezetek megjegyezték, hogy az ajánlórendszerek és a tartalommoderálási rendszerek nemcsak kockázati tényezőknek, hanem kockázatcsökkentési intézkedéseknek is minősülhetnek, amennyiben mérvadó tartalmakat népszerűsíthetnek. Bizonyos civil társadalmi szervezetek javaslatot tettek olyan funkciók bevezetésére, amelyek előmozdítják a marginalizált vélemények és tartalmak láthatóságát. Civil társadalmi szervezetek és egyes szolgáltatók is megemlítették az olyan ajánlórendszerek előnyeit, amelyek alapvetően nem a felhasználói elköteleződésen alapulnak; például egyes civil társadalmi szervezetek említettek olyan lehetséges kockázatcsökkentési intézkedéseket, mint a „bridging” (azaz a konstruktív párbeszédet vagy pozitív érzelmeket népszerűsítő tartalmakra vonatkozó ajánlások hangsúlyossá tétele). Néhány civil társadalmi szervezet felvetette azt, hogy bizonyos szolgáltatók pénzszerzési irányelvei az ajánlások révén felerősíthetik a káros tartalmak terjesztését, valamint azt, hogy az adott irányelvek átláthatóságának fokozása kockázatcsökkentési intézkedés szerepét töltheti be.

Felhasználói választások. Néhány szolgáltató kifejtette, hogy lehetővé teszi a felhasználók számára, hogy visszaállítsák ajánlási profiljukat, új felhasználót utánozzanak, illetve lehetővé teszi számukra, hogy kikapcsolják az ajánlórendszereket vagy leiratkozzanak azokról. Néhány szolgáltató megemlítette, hogy lehetővé teszi a felhasználók számára, hogy megadják, ha „nem érdeklődnek” egy-egy konkrét tartalom iránt, ezzel jelezve a rendszereknek, hogy csökkentsék a hasonló tartalmaknak való kitettségüket. Ezenfelül néhány szolgáltató közölte, hogy lehetővé teszi a felhasználók számára a tartalommegjelenítéshez vagy -szűréshez tartozó kulcsszavak kiválasztását. Bizonyos szolgáltatók ismertették azt is, hogy olyan értesítéseket használnak, amelyek segítségével a felhasználók megérthetik, hogy bizonyos tartalmakat miért ajánlanak nekik. Egyes civil társadalmi szervezetek megemlítették, hogy az ajánlásként preferált tartalomtípusokat konkrétan megnevező, felhasználóknak szánt eszközök hozzájárulhatnak bizonyos kockázatok csökkentéséhez, például a hosszú vagy rövid tartalomformákhoz kapcsolódó felhasználói preferenciákra irányuló felmérések, valamint a „kemény leállások” aktiválása bizonyos tartalomtípusok megjelenítésének megakadályozása érdekében.

A kiskorúak tekintetében néhány szolgáltató kifejtette, hogy kiegészítő óvintézkedéseket vezetett be, például a potenciális ismerősök vagy kapcsolatok ajánlásához, vagy az életkoruknak megfelelőbb tartalmak megjelenítéséhez. Civil társadalmi szervezetek azt javasolták, hogy alapértelmezetten korlátozni kell az ismeretlen felhasználókkal való interakciókat, például az idegenek kiskorúakkal való, közvetlen üzenetekben kezdeményezett kapcsolatfelvételének korlátozása érdekében. A kiskorúak ellenőrzött fiókjai esetében néhány civil társadalmi szervezet külön ajánlóalgoritmusok kifejlesztését javasolta, amelyek az életkornak megfelelő tartalmakat részesítik előnyben.

4.5. Hirdetési rendszerek

A rendelet 35. cikke (1) bekezdésének e) pontja a következő kockázatcsökkentési intézkedések bevezetését említi a szolgáltatók számára: *„hirdetési rendszereik módosítása és az általuk kínált szolgáltatásokkal kapcsolatban a hirdetések megjelenítésének korlátozására vagy kiigazítására irányuló célzott intézkedések elfogadása”*.

A szolgáltatók a hirdetési rendszereikhez kapcsolódó kockázatcsökkentési intézkedésként például a következőket említették: a hirdetők ellenőrzési folyamata (például csak ellenőrzött civil társadalmi szervezetek tehetnek közzé bizonyos érzékeny témákra, például fegyveres konfliktusokra vonatkozó hirdetéseket), a hirdetések előzetes szűrése azok közzététele előtt (többek között külön ellenőrzések az esetlegesen átverést, csalást, jogellenes tartalmakat és szolgáltatásokat vagy egészségügyi dezinformációt, valamint alkoholhoz és dohánytermékekhez hasonló termékeket népszerűsítő hirdetések esetében). Néhány szolgáltató megemlítette, hogy nézettségi minimumokat használ a hirdetési rendszerekhez, hogy ne alkalmazzon túlzottan leszűkített célcsoport-kiválasztást. Egyes szolgáltatók említést tettek a választásokhoz hasonló érzékeny témákra vonatkozó, mesterséges intelligencia által generált tartalmakat bemutató hirdetések betiltásáról, valamint a hirdetők arra vonatkozó saját nyilatkozatairól, hogy egy-egy hirdetés létrehozása során mesterséges intelligenciát alkalmaztak.

A hirdetési irányelvek megsértéséért kiszabott büntetések tekintetében a szolgáltatók megemlítették, hogy a hirdetést eltávolítják a platformról. Civil társadalmi szervezetek megemlítették azt is, hogy az influenszerek képzésben és tájékoztatásban részesülnek a hirdetési tárgyú jogszabályok megsértésének kockázataival kapcsolatban, többek között azt is felvetették, hogy egyes tagállamokban képzési tanúsítvány is szerezhető a hirdetési tevékenységet szabályozó hatóságoktól. Számos szolgáltató azt állította, hogy a személyes adatok alapján nem teszi lehetővé a kiskorúaknak szánt közvetlen hirdetést, és lehetőségeket biztosít a kiskorúaknak arra, hogy kikapcsolják a személyre szabott ajánlásokat. A digitális szolgáltatásokról szóló jelentés hangsúlyának megőrzése érdekében itt nem térünk ki más,

hirdetési vonatkozású uniós jogszabályokban – például a politikai reklámtevékenység átláthatóságáról és célzott folytatásáról rendeletben[25] – rögzített szabályokra.

4.6. A kockázatok észlelése, valamint a szolgáltatások visszaélésszerű igénybevételéhez, a tartalmak és a fiókok hitelességéhez kapcsolódó kihívások

A rendelet 35. cikke (1) bekezdésének f) pontja a következő kockázatcsökkentési intézkedések bevezetését említi a szolgáltatók számára: *„a belső folyamataik, erőforrásaik, a tesztelés, a dokumentáció megerősítése vagy a tevékenységeik felügyelete, különös tekintettel a rendszerszintű kockázatok észlelésére”*.

A rendelet 35. cikke (1) bekezdésének k) pontja a következő kockázatcsökkentési intézkedések bevezetését említi a szolgáltatók számára: *„annak biztosítása, hogy valamely információ, amely olyan generált vagy manipulált kép, audio- vagy videotartalom lehet, amely számottevően hasonlít létező személyekre, tárgyakra, helyekre vagy más entitásokra vagy eseményekre, és az eredetiség vagy a hitelesség hamis látszatát kelti valaki számára, megjelenítésekor jól látható jelzések révén megkülönböztethető legyen online interfészeiken, továbbá egy könnyen használható funkció biztosítása, amely lehetővé teszi a szolgáltatás igénybe vevői számára az ilyen információ megjelölését”*.

A kockázatok felderítésére szolgáló eszközök és módszerek. A szolgáltatók és a civil társadalmi szervezetek számos kockázatcsökkentési intézkedést említettek a szolgáltatásaik visszaélésszerű igénybevételéhez, valamint a tartalmak (pl. deepfake-ek) és a fiókok (például robotok) hitelességére vonatkozó problémákhoz kapcsolódó rendszerszintű kockázatok felderítésére. Néhány szolgáltató például megemlítette, hogy tartalmi, viselkedési és technikai jelzésekre hagyatkozik a nem hiteles viselkedés (például ember esetében valószínűtlennek tűnő sebességű tartalommegosztási mintázatok) felderítéséhez. Bizonyos esetekben ezeket úgy írták le, hogy mesterséges intelligenciát vetnek be a mesterséges intelligencia által létrehozott tartalmak felderítéséhez (továbbá irányelveket hoznak létre annak megakadályozására, hogy mesterséges intelligenciát használjanak mások, többek között közszereplők megszemélyesítésére, valamint orvosi vagy jogi tanácsadás generálására). Néhány szolgáltató kifejtette, hogy nyilvántartást vezet a hamis vagy kompromittált fiókokról, és intézkedéseket hozott létre annak megakadályozására, hogy letiltott felhasználók más álnév alatt vagy közvetítőkön keresztül újra csatlakozzanak a platformhoz. Ugyanígy megjegyezték, hogy harmadik feleket vesznek igénybe, illetve nyílt forráskódú hash-eket és kulcsszóadatbázisokat használnak a közelgő fenyegetésekre vonatkozó jelzésekhez. Néhány civil társadalmi szervezet azt javasolta, hogy a hamis állítások gyors és méretezhető módon történő azonosítása, valamint a tényellenőrök munkájának megkönnyítése érdekében MI-alapú rendszerek megfeleltethetnék a tartalmakat adatbázisokkal és megbízható hírforrásokkal. Bizonyos szolgáltatók ismertettek

[25] Az Európai Parlament és a Tanács (EU) 2024/900 rendelete (2024. március 13.) a politikai reklámtevékenység átláthatóságáról és célzott folytatásáról, elérhető a következő linken: https://eur- lex.europa.eu/eli/reg/2024/900/oj/hun.

olyan intézkedéseket, amelyek az átirányítás (azaz a szerződési feltételek érvényesítésének megkerülése érdekében a platformon kívülre vezető tartalmak) megakadályozását célozták.

Néhány szolgáltató és civil társadalmi szervezet kockázatcsökkentési intézkedésként említette az új funkciók és tervezési elemek fokozatos bevezetését, többek között kívülálló/kontrollcsoportok (azaz olyan felhasználói csoportok, amelyek számára az új funkciók vagy tervezési elemek nem azonnal elérhetők) (akár hosszabb ideig történő) igénybevételével, amelyek összehasonlítási alapként szolgálnak a többi felhasználóhoz képest, és amelyek segítségével elkülöníthetők és azonosíthatók a potenciális új kockázatok, például amikor A/B új funkciókat tesztel.

Működési kockázatok felderítése. Néhány szolgáltató leírta, hogy – a helyi fenyegetések körének megértése érdekében – nyelvi képességekkel rendelkező fenyegetés-felderítő munkacsoportokat hoz létre (amelyek többek között a külföldi információmanipulációval és beavatkozással kapcsolatos szakértelemmel, valamint különböző feladatkörökkel, például jogi, bizalmi és biztonsági, kiberhírszerzési, pénzügyi és pénzmosás elleni feladatkörökkel rendelkeznek). Ebben az összefüggésben egyes szolgáltatók úgynevezett „red team" megközelítéseket említettek. Említést tettek a civil társadalmi szervezetekkel létesített közvetlen kommunikációs csatornák fontosságáról is, valamint arról, hogy utólagos elemzést végeznek olyan jelentős események után, mint a választások vagy a válságok, illetve levonják azokból a tanulságokat, és rendszeres fenyegetési jelentéseket tesznek közzé a platformok manipulálásáról. Néhány civil társadalmi szervezet azt javasolta, hogy közvetlen együttműködést kell folytatni az érintett közösségekkel, és be kell vonni őket az azonosított kockázatok szempontjából megfelelő kockázatcsökkentési intézkedések felkutatásába.

Fiókellenőrzés. A szolgáltatók és a civil társadalmi szervezetek azt is megemlítették, hogy az alkalmazásáruházat esetében a fiókellenőrzésnek fontos szerepe van a platformok manipulálásának megakadályozásában, ezen belül fontos a kétfaktoros hitelesítés, a 13 év alatti felhasználók fiókjainak törlése, valamint például az „ismerd a fejlesztődet" programok. A szolgáltatók megjegyezték, hogy erőforrásokat rendelnek (csoportosítanak át) a szerződési feltételeik nyomon követéséhez és érvényesítéséhez, például a rosszindulatú szereplők általi kijátszás vagy összehangolt támadások megakadályozását célzó mechanizmusokat vezetnek be. Ebben az összefüggésben néhány szolgáltató, különösen online piacterek kifejtették, hogy egyes esetekben kétfaktoros hitelesítést követelnek meg harmadik felektől a szolgáltatásaik igénybevételéhez és/vagy tartalmak közzétételéhez.

4.7. Megbízható bejelentők

A rendelet 35. cikke (1) bekezdésének g) pontja a következő kockázatcsökkentési intézkedések bevezetését említi a szolgáltatók számára: *„a 22. cikk szerinti megbízható bejelentőkkel való*

együttműködés kezdeményezése vagy módosítása, valamint a 21. cikk szerinti, peren kívüli vitarendezési testületek határozatainak végrehajtása”.

Néhány szolgáltató megemlítette, hogy összegyűjti a megbízható bejelentők jelentéseit, a megbízható bejelentőket bevonja a termékbiztonság fejlesztését célzó folyamataiba és termékfrissítéseibe, áttekintőtáblákat hoz létre a megbízható bejelentők számára az értesítéseik állapotának nyomon követése érdekében, partnerségeket létesít civil társadalmi szervezetekkel és hatóságokkal, hogy a megbízható bejelentőkhöz hasonló szerepet töltsenek be és jelentsék például a jogellenes tartalmakat.

4.8. Magatartási kódexek

A rendelet 35. cikke (1) bekezdésének h) pontja a következő kockázatcsökkentési intézkedések bevezetését említi a szolgáltatók számára: *„az egyéb online platformot vagy online keresőprogramot üzemeltető szolgáltatókkal való együttműködés kezdeményezése vagy módosítása a 45. cikkben említett magatartási kódexeknek, illetve a 48. cikkben említett válságkezelési protokolloknak megfelelően”*.

A rendelet különleges szerepet szán a magatartási kódexeknek a rendszerszintű kockázatok csökkentését célzó ágazati bevált gyakorlatok bemutatásához. Az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatókat egymással való együttműködésre ösztönzi, többek között magatartási kódexekhez csatlakozással. Néhány szolgáltató hivatkozott magatartási kódexekre, például a jogellenes online gyűlöletbeszéd felszámolására vonatkozó magatartási kódexre és a dezinformáció visszaszorítását célzó magatartási kódexre (korábban: a dezinformáció visszaszorítását célzó gyakorlati kódex), valamint az azokban említett kockázatcsökkentési intézkedésekre. Említést tettek továbbá a civil társadalmi szervezetekkel, a tényellenőrökkel, más platformokkal és hatóságokkal a dezinformáció és félretájékoztatás tartalmáról és a választásokról folytatott információcserére szolgáló gyorsreagálási rendszerek létrehozásáról. Ahogyan a Bizottságnak a dezinformáció visszaszorítását célzó gyakorlati kódex értékeléséről szóló véleményében szerepel: *„a dezinformáció visszaszorítását célzó gyakorlati kódex jelentős és érdemi referencia lehet a digitális szolgáltatásokról szóló rendeletnek való megfeleléshez azon online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók számára, amelyek támogatják annak kötelezettségvállalásait és eleget tesznek azoknak”*[26]. A kódex értéke különösen abban rejlik, hogy számos érdekelt fél (köztük az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatók, civil társadalmi szervezetek, a hirdetési ágazat) által önként elfogadott kötelezettségvállalások és intézkedések átfogó gyűjteménye, amely megállapítja a dezinformáció terjedéséhez kapcsolódó kockázatok

[26] A Bizottság véleménye (2025. február 13.) a dezinformáció visszaszorítását célzó gyakorlati kódexnek a 2022/2065 rendelet 45. cikke szerinti értékeléséről, C(2025) 1008 final, elérhető a következő linken: https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation.

csökkentését célzó ágazati bevált gyakorlatokat. Ezért a kódex a kockázatcsökkentési intézkedések fontos forrása.

4.9. Tudatosságnövelés

A rendelet 35. cikke (1) bekezdésének i) pontja a következő kockázatcsökkentési intézkedések bevezetését említi a szolgáltatók számára: *„tudatosság növelésére irányuló intézkedések meghozatala és online interfészük módosítása annak érdekében, hogy a szolgáltatásukat igénybe vevőket több információval lássák el”*.

A szolgáltatók megemlítették, hogy a tudatosság javítása és a felhasználók rendszerszintű kockázatokkal kapcsolatos részletesebb tájékoztatása érdekében ismeretterjesztő vagy tájékoztató bizottságokat hoztak létre a választásokra vagy válságeseményekre vonatkozó mérvadó információkhoz, létrehoztak továbbá médiatudatossággal kapcsolatos kampányokat, jólléti témájú segítő oldalakat felhasználók és tartalomalkotók számára (például a molesztáláshoz és zaklatáshoz kapcsolódó mentális jólléti forrásokat), valamint a magánélet tiszteletben tartásával és a biztonsággal kapcsolatos oldalakat, felhasználói segítségnyújtó vonalakat, valamint szülőknek és gondviselőknek szánt útmutatókat alakítottak ki. A szolgáltatók más intézkedéseket is említettek, például tartalmak kommentelése vagy feltöltése előtt mérlegelendő, felhasználóknak és tartalomalkotóknak szánt információkat tartalmazó szalaghirdetések, egy-egy fiók ellenőrzéséről vagy tartalmak tényellenőrzéséről tájékoztató címkék megjelenítését. Néhány civil társadalmi szervezet a közösségi média túlzott használatának rendszerszintű kockázatainak tudatosítását célzó intézkedéseket javasolt, különösen kiskorúak és újonc felhasználók számára vagy új funkciók bevezetését követően.

5. Kitekintés

Ez a digitális szolgáltatásokról szóló rendelet 35. cikkének (2) bekezdésében említett éves jelentés első kiadása. A jövőben kiadandó további jelentések – idővel – hosszú távú perspektívát biztosítanak azzal kapcsolatban, hogy melyek az évről évre legjelentősebb és ismétlődő rendszerszintű kockázatok. A szolgáltatókkal szemben meghozott jogérvényesítési intézkedéseket is alapul fogják venni. A digitális szolgáltatásokról szóló rendelet, beleértve annak 34. és 35 cikkét is, még a végrehajtásának korai szakaszában van. A jövőben kiadandó jelentésekhez felhasználható lesz az érdekelt felek – köztük a kutatók, valamint a civil társadalmi szervezeteket képviselők – fejlődő szakértelme is. A rendelet egyéb rendelkezéseinek, például a 40. cikk szerinti adathozzáférési mechanizmusoknak a végrehajtása és érvényesítése terén bekövetkező fejlemények, és különösen az említett adathozzáférésnek köszönhető kutatási eredmények hozzá fognak járulni ahhoz a gazdag információs bázishoz, amelyek segítségével még jobban megérthetők a rendszerszintű kockázatok, valamint a rendelet 34. és 35. cikke szerinti kockázatcsökkentési intézkedések.

Melléklet: Független szakértőktől és civil társadalmi szervezetektől származó források és tanulmányok

Az alábbi listák nyilvános forrásokat, független szakértőktől és civil társadalmi szervezetektől származó tanulmányokat, valamint a Testület és a Bizottság által – felkérésre vagy önkéntes beadványok alapján – civil társadalmi szervezetektől, megbízható bejelentőktől és tagállami hatóságoktól beszerzett információkat tartalmaznak.

Azon független szakértők és civil társadalmi szervezetek felsorolása, amelyek 2025 áprilisában információt szolgáltattak ehhez a jelentéshez a Testületnek és a Bizottságnak:

- 5rights
- 7amleh
- A Jewish Contribution to an Inclusive Europe (CEJI)
- Addiction France
- Agence France Presse (AFP)
- AlgorithmWatch
- Alliance4Europe
- Austrian Fund for the Documentation of Religiously Motivated Political Extremism
- BodyWhys
- Center For Digital Paedagogik (CFDP)
- Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE)
- Civil Liberties Union for Europe (Liberties)
- Comunicare
- Conseil Représentatif des Institutions Juives de France (Crif)
- Deutsches Kinderhilfswerk (DKHW)
- Digitale Chancen
- Digitalt Ansvar
- E-enfance
- EU Disinfo Lab
- Eurochild
- European Fact-Checking Standards Network (EFCSN)
- European Partnership for Democracy (EPD)
- Foundation Diaspora in Action for Human Rights and Democracy (formerly Foundation The London Story)
- Freepressunlimited
- Fundación Maldita
- Fundación Secretariado Gitano
- Global Witness
- HateAid
- In IUSTITIA
- Integrity Institute
- International Lesbian, Gay, Bisexual, Trans and Intersex Association (ILGA)

- International Network Against Cyber Hate (INACH)
- Knight-Georgetown Institute
- Medierådet for Børn og Unges
- Österreichisches Institut für angewandte Telekommunikation (OIAT)
- Panoptykon Foundation
- Pointdecontact
- Rathenau
- Red Barnet (Save the Children Denmark)
- Reporter Sans Frontières
- Reset Tech
- Savati Copiii (Save the Children Romania)
- Social Media Exchange (SMEX)
- SOS Racisme
- The Foreign Policy Centre
- Verbraucherzentrale Bundesverband
- WhatToFix

Független szakértők és civil társadalmi szervezetek azon egyéb forrásainak listája, amelyeket a Testület és a Bizottság e jelentéséhez figyelembe vettek (fordított időrendi sorrendben):

Szerző / Szervezet	Angol cím	Dátum	Link
Open Evidence, PPMI, Spark Legal	DSA study on systemic risks and their mitigation (EC-CNECT/2024/OP/0032) *(a Bizottság által többek között e jelentés alátámasztása érdekében megrendelt tanulmány, amelyet nem önálló publikációnak szántak)*	2025. július	n/a
Marie-Therese Sekwenz, Rita Gsenger, Scott Dahlgren, Ben Wagner	Doing Audits Right? The Role of Sampling and Legal Content Analysis in Systemic Risk Assessments and Independent Audits in the Digital Services Act	2025. május	Link
Science Feedback, Who Targets Me	Online misinformation pays. Why? Taking stock of a broad range of evidence	2025. április	Link
Stanford University	Stanford Youth Safety and Digital Wellbeing Report, 2025	2025. április	Link
Gianclaudio Malgieri, Cristiana Santos	Assessing the (severity of) impacts on fundamental rights	2025. április	Link
Deloitte, Zentrum für Psychosoziale Medizin des Universitätsklinikums	Societal impacts of digital services with a view to addiction risks *(a német digitális szolgáltatási koordinátor által megrendelt tanulmány)*	2025. március	Link

Hamburg-Eppendorf (UKE)			
Knight-Georgetown Institute, Panoptykon Foundation	Better Feeds: Algorithms That Put People First	2025. március	Link
Civil Liberties Union for Europe, European Partnership for Democracy	Beyond Disinformation: How DSA Risk Assessments Ignore Democracy's Real Threats	2025. március	Link
DSA Civil Society Coordination Group	Initial Analysis on the first round of risk assessment reports under the EU Digital Services Act	2025. március	Link
Civil Liberties Union for Europe, European Partnership for Democracy	Civic Discourse and Electoral Processes in the Risk Assessment and Mitigation Measures Reports under the Digital Services Act	2025. március	Link
Alexander von Humboldt Institut für Internet und Gesellschaft	"Societal impact of systemic risks" *(a német digitális szolgáltatási koordinátor által megrendelt tanulmány)*	2025. március	Link
Global Counsel	Online safety: the next wave of regulation	2025. március	Link
Centro de Estudios en Libertad de Expresión y Acceso a la Información	Are Risks the New Rights? The Perils of Risk-based Approaches to Speech Regulation	2025. március	Link
Mateus Correia de Carvalho	It will be what we want it to be: Socitechnical and contested systemic risk at the core of the EU's regulation of platforms' AI systems	2025. március	Link
Ahnul Ha, Yun Jeong Lee, Marvin Lee, *et al.*	Digital Screen Time and Myopia: A systematic review and dose-response meta-analysis	2025. február	Link
Integrity Institute	Global Transparency Audit	2025. február	Link
Integrity Institute	Risk assessment guidance and initial analysis	2025. február	Link
Integrity Institute	Risk dimensions and mitigation effectiveness	2025. február	Link
David Sullivan	Systemic Risk Assessments Hold Clues for EU Platform Enforcement	2025. február	Link
Amnesty International	Meta's new content policies risk fuelling more mass violence and genocide	2025. február	Link

Center for Democracy and Technology	EU Tech Policy Brief: January 2025	2025. február	Link
Electronic Frontier Foundation	Systemic Risk Reporting: A System in Crisis?	2025. január	Link
Knight-Georgetown Institute	Advancing Platform accountability: The promise and perils of the DSA RAs	2025. január	Link
Institute for Strategic Dialogue	"Identification, assessment and management of systemic risks in the context of the Digital Services Act" *(a német digitális szolgáltatási koordinátor által megrendelt tanulmány)*	2025. január	Link
Tim Bernard	Reading the Systemic Risk Assessments for Major Speech Platforms: Notes and Observations	2024. december	Link
Merve Sambel Aykutlu, Hasan Cem Aykutlu *et al.*	Digital media use and its effects on digital eye strain and sleep quality in adolescents: a new emerging epidemic?	2024. december	Link
Mark Scott	5 Things to Know about the Digital Services Act's First Risk Assessments and Audits	2024. december	Link
DSA Observatory	DSA risk assessment reports: a guide to the first rollout and what's next	2024. december	Link
Centre on Regulation in Europe (CERRE)	Evaluating systemic risk management under the DSA	2024. december	Link
Sally Broughton Micova, Bryn Enstone	What to Do with the Long-Awaited DSA Systemic Risk Assessments	2024. november	Link
Center for Democracy and Technology *et al.*	Joint Civil Society Statement on Meaningful Transparency of Risk Assessments under the Digital Services Act	2024. november	Link
AlgorithmWatch	Researching Systemic Risks under the Digital Services Act	2024. július	Link
Centre on Regulation in Europe (CERRE)	Cross-Cutting issues for DSA systemic risk management: an agenda for cooperation	2024. július	Link
Institute for Strategic Dialogue	Identifying sock-puppets on Wikipedia: a semantic clustering approach	2024. április	Link
Crossover.social	"Up next", biased politics? YouTube recommendations and political bias in the Finnish Presidential elections 2024	2024. március	Link
Electronic Frontier Foundation, Article 19	Disinformation and Elections: EFF and ARTICLE 19 Submit Key Recommendations to EU Commission	2024. március	Link
Panoptykon Foundation	Joint-Submission on the Commission's Guidelines for Providers of Very Large Online Platforms and Very Large	2024. március	Link

	Online Search Engines on the Mitigation of Systemic Risks for Electoral Processes		
Panoptykon Foundation	Safe by default: Moving away from engagement-based rankings towards safe, rights-respecting, and human centric recommender systems	2024. március	Link
AlgorithmWatch	Ensuring legitimacy in stakeholder engagement: the ‘5 Es’ framework	2024. február	Link
Civil Liberties Union for Europe, European Partnership for Democracy	Identifying, analysing, assessing and mitigating potential negative effects on civic discourse and electoral processes: a minimum menu of risks very large online platforms should take heed of	2024. január	Link
Verbraucherzentrale Bundesverband	100 days of the Digital Services Act: consumer protection on online platforms still insufficient	2023. december	Link
AI Forensics	An analysis of Microsoft’s copilot in Swiss and Bavarian elections	2023. november	Link
AI Forensics, Amnesty International	TikTok’s role in youth mental health	2023. november	Link, link
Joan Barata, Jordi Calvet-Bademunt	The European Commission’s Approach to DSA Systemic Risk is Concerning for Freedom of Expression	2023. október	Link
AI Forensics	Amazon’s risky recommendations	2023. október	Link
Access Now, European Center for Not-for-Profit Law	Towards meaningful fundamental rights impact assessments under the DSA	2023. szeptember	Link
Irish Council for Civil Liberties, Panoptykon Foundation, People vs BigTech and al.	Fixing Recommender Systems	2023. augusztus	Link
AlgorithmWatch	Making sense of the DSA: How to define platforms’ systemic risks to democracy	2023. augusztus	Link
David Sullivan, Jason Pielemeier	Unpacking “Systemic Risk” Under the EU’s Digital Service Act	2023. július	Link
Centre on Regulation in Europe (CERRE)	Elements for effective systemic risk assessment under the DSA	2023. július	Link
Alessandro Mantelero	Fundamental rights impact assessments in the DSA	2022. november	Link
Amnesty International	What the EU’s Digital Services Act means for human rights and harmful Big Tech business models	2022. február	Link