2024/2659

2024.10.16.

A BIZOTTSÁG (EU) 2024/2659 AJÁNLÁSA

(2024. október 11.)

a kibertér-megfigyelési termékek kivitelére vonatkozó, az (EU) 2021/821 európai parlamenti és tanácsi rendelet 5. cikke szerinti iránymutatásokról

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 292. cikkére,

mivel:

(1) Az (EU) 2021/821 európai parlamenti és tanácsi rendelet ([1]) létrehozza a kettős felhasználású termékek kivitelére, az azokkal végzett brókertevékenységre, az azokkal kapcsolatos technikai segítségnyújtásra, valamint azok tranzitjára és transzferjére vonatkozó uniós ellenőrzési rendszert.

(2) Az (EU) 2021/821 rendelet kitér annak kockázatára, hogy a kibertér-megfigyelési termékeket belső elnyomással és/vagy az emberi jogok és a nemzetközi humanitárius jog súlyos megsértésével összefüggésben használják fel.

(3) Az (EU) 2021/821 rendelet 5. cikkének (2) bekezdése és 26. cikkének (1) bekezdése értelmében a Bizottság és a Tanács iránymutatásokat nyújt az exportőrök számára a fel nem sorolt kibertér-megfigyelési termékeket illetően, mivel biztosítani kell az uniós exportellenőrzési rendszer hatékonyságát a kiberbiztonsággal összefüggésben, valamint az (EU) 2021/821 rendelet végrehajtásának következetességét.

(4) Ezen ajánlás és az ahhoz csatolt iránymutatások célja, hogy támogassák az exportőröket a fel nem sorolt kibertér-megfigyelési termékek ellenőrzésének alkalmazásában, beleértve többek között az ilyen termékek kivitelével kapcsolatos kockázatokat értékelő, kellő gondosságra vonatkozó intézkedéseket.

(5) Az ajánláshoz csatolt iránymutatások széles körű konzultáció tárgyát képezték a megfigyelési technológiákkal foglalkozó szakértői csoportban 2022-ben és 2023-ban, és figyelembe veszik a 2023 második negyedévében tartott nyilvános konzultáció ([2]) során beérkezett észrevételeket.

(6) Emlékeztetni kell arra, hogy az ajánlás és a csatolt iránymutatások nem kötelező érvényűek. Ezért továbbra is az exportőrök feladata, hogy biztosítsák az (EU) 2021/821 rendeletben foglalt kötelezettségeik teljesítését, a Bizottságnak pedig biztosítania kell, hogy ezen ajánlás a jövőben is releváns maradjon,

([1]) Az Európai Parlament és a Tanács (EU) 2021/821 rendelete (2021. május 20.) a kettős felhasználású termékek kivitelére, az azokkal végzett brókertevékenységre, az azokkal kapcsolatos technikai segítségnyújtásra, valamint azok tranzitjára és transzferjére vonatkozó uniós ellenőrzési rendszer kialakításáról (HL L 206., 2021.6.11., 1. o., ELI: http://data.europa.eu/eli/reg/2021/821/oj).

([2]) https://policy.trade.ec.europa.eu/consultations/guidelines-export-cyber-surveillance-items-under-article-5-regulation-eu-no-2021821_en.

ELFOGADTA EZT AZ AJÁNLÁST:

A Bizottság ajánlja, hogy a tagállamok illetékes hatóságai és az exportőrök az (EU) 2021/821 rendelet 5. cikkének (2) bekezdése szerinti kötelezettségeik teljesítése érdekében vegyék figyelembe az ezen ajánlás mellékletében foglalt iránymutatásokat.

Kelt Brüsszelben, 2024. október 11-én.

a Bizottság részéről
Valdis DOMBROVSKIS
ügyvezető alelnök

MELLÉKLET

TARTALOMJEGYZÉK

oldal

Bevezetés ... 4

1. Vonatkozó jogi rendelkezések, fogalommeghatározások és kulcsfogalmak ... 4

1.1. A vonatkozó jogi rendelkezések áttekintése ... 4

1.2. Főbb fogalommeghatározások ... 5

1.2.1. „Kifejezetten arra tervezett” ... 5

1.2.2. „Megfigyelés” ... 6

1.2.3. „Természetes személyek” ... 6

1.2.4. „Adatok nyomon követése, kinyerése, gyűjtése, elemzése” ... 6

1.2.5. „Információs és telekommunikációs rendszerekből” ... 7

1.2.6. „Tudomás” és „valamilyen célra szánt” ... 7

1.3. Belső elnyomás, az emberi jogok és a nemzetközi humanitárius jog súlyos megsértése ... 7

1.3.1. Belső elnyomás ... 8

1.3.2. Az emberi jogok súlyos megsértése ... 8

1.3.3. A nemzetközi humanitárius jog súlyos megsértése ... 9

2. Műszaki hatály ... 9

2.1. Felsorolt kibertér-megfigyelési termékek ... 9

2.2. Potenciális fel nem sorolt kibertér-megfigyelési termékek ... 9

2.2.1. Arc- és érzelemfelismerési technológia ... 10

2.2.2. Helymeghatározó eszközök ... 10

2.2.3. Videokamerás megfigyelési rendszerek ... 10

3. Kellő gondosságra vonatkozó intézkedések ... 10

Az (EU) 2021/821 rendelet 5. cikkének (2) bekezdésében meghatározott követelmények ... 12

4. Függelék ... 12

Az (EU) 2021/821 rendelet I. melléklete által ellenőrzés alá vont, ott felsorolt kibertér-megfigyelési termékek ... 12

Telekommunikációs szolgáltatások lehallgatására szolgáló rendszerek (5A001.f) ... 12

Internetalapú megfigyelési rendszerek (5A001.j) ... 13

„Támadószoftver” (4A005, 4D004, valamint a 4E001.a. és 4E001.c. pont szerinti kapcsolódó ellenőrzések) ... 13

Kommunikációfigyelő szoftver (5D001.e) ... 14

Rejtjelelemzéshez használt termékek (5A004.a) ... 14

Kriminalisztikai/nyomozó eszközök (5A004.b, 5D002.a.3.b és 5D002.c.3.b) ... 14

BEVEZETÉS

Az (EU) 2021/821 rendelettel (a továbbiakban: a rendelet) létrehozott uniós exportellenőrzési keret célja annak biztosítása, hogy az Unió és tagállamai eleget tegyenek – többek között a regionális békére, biztonságra és stabilitásra, valamint az emberi jogok és a nemzetközi humanitárius jog tiszteletben tartására vonatkozó – nemzetközi kötelezettségeiknek és kötelezettségvállalásaiknak. Ezért az Unió és tagállamai végrehajtották a többoldalú exportellenőrzési rendszerek keretében hozott határozatokat, és azoknak megfelelően aktualizálták a rendelet I. mellékletében szereplő uniós ellenőrzési jegyzéket ([1]). Ráadásul a tagállamok illetékes hatóságai már a rendelet 5. cikkének alkalmazásba lépése előtt is ellenőrizték egyes felsorolt, megfigyelésre felhasználható termékek ([2]) kivitelét, figyelembe véve azt, hogy bizonyos különleges körülmények között fennáll a visszaélés kockázata. Rendkívül súlyos körülmények esetén az Unió szankciókat vezetett be egyes megfigyelési eszközök kivitelének korlátozására ([3]).

A rendelet tükrözi az Unió kötelezettségvállalását az iránt, hogy hatékonyan kezelje a kibertér-megfigyelési termékek belső elnyomással és/vagy az emberi jogok és a nemzetközi humanitárius jog súlyos megsértésével összefüggésben történő felhasználásának kockázatát. Konkrétan a rendelet új rendelkezéseket vezet be a fel nem sorolt kibertér-megfigyelési termékek kivitelének ellenőrzésére vonatkozóan, beleértve azt a kötelezettséget is, hogy az exportőröknek értesíteniük kell a hatáskörrel rendelkező hatóságot, ha a kellő gondosságra vonatkozó intézkedésekből fakadó ténymegállapításaik szerint tudomásuk van arról, hogy az általuk exportálni tervezett, fel nem sorolt kibertér-megfigyelési termékeket részben vagy egészben belső elnyomással és/vagy az emberi jogok és a nemzetközi humanitárius jog súlyos megsértésével összefüggésben lévő felhasználási célokra szánják. A rendelet felszólítja továbbá a Bizottságot és a Tanácsot, hogy nyújtsanak iránymutatásokat az exportőrök számára, ezzel támogatva a fel nem sorolt kibertér-megfigyelési termékekre vonatkozó új ellenőrzések hatékony végrehajtását.

A jelen iránymutatások ezért támogatni kívánják az exportőröket a fel nem sorolt kibertér-megfigyelési termékekre vonatkozó ellenőrzések alkalmazásában, beleértve többek között azokat a kellő gondosságra vonatkozó intézkedéseket, amelyek értékelik az e termékek végfelhasználóknak történő kivitelével és végfelhasználásával kapcsolatos kockázatokat a rendelet új rendelkezései szerint.

1. VONATKOZÓ JOGI RENDELKEZÉSEK, FOGALOMMEGHATÁROZÁSOK ÉS KULCSFOGALMAK

1.1. A vonatkozó jogi rendelkezések áttekintése

A rendelet új rendelkezéseket vezet be, amelyek kifejezetten előírják a rendelet I. mellékletében fel nem sorolt azon kibertér-megfigyelési termékek kivitelének ellenőrzését, amelyeket részben vagy egészben belső elnyomással és/vagy az emberi jogok és a nemzetközi humanitárius jog súlyos megsértésével összefüggésben lévő felhasználási célokra szánnak vagy szánhatnak. A vonatkozó preambulumbekezdések és cikkek a következők:

a) (8) preambulumbekezdés: „Annak a kockázatnak a kezelése érdekében, hogy egyes, az Unió vámterületéről exportált, fel nem sorolt kibertér-megfigyelési termékekkel visszaéljenek olyan személyek, akik az emberi jogokat vagy a nemzetközi humanitárius jogot súlyosan sértő cselekmények irányításában vagy végrehajtásában részt vállaltak vagy azért felelősek, indokolt az ilyen termékek exportjának ellenőrzése. A kapcsolódó kockázatok különösen azokra az

([1]) Lásd különösen a telekommunikációs szolgáltatások lehallgatására szolgáló rendszerekkel (5A001.f.), az internetalapú megfigyelési rendszerekkel (5A001.j.), a támadószoftverekkel (4A005., 4D004. és a 4E001.a. és 4E001.c. pont szerinti kapcsolódó ellenőrzések), valamint a bűnüldözési szervek általi nyomon követésre tervezett szoftverekkel (5D001.e.) kapcsolatos ellenőrzéseket. Lásd továbbá az egyes kriminalisztikai/nyomozó eszközökre (5A004.b., 5D002.a.3.b. és 5D002.c.3.b.) vonatkozó – eseti értékelés alapján végzett – ellenőrzéseket.

([2]) Különösen az információbiztonsági rendszerek.

([3]) Lásd: a Tanács 765/2006/EK rendelete (2006. május 18.) a belarusz helyzetre és Belarusznak az Ukrajna elleni orosz agresszióban való részvételére tekintettel hozott korlátozó intézkedésekről (HL L 134., 2006.5.20., 1. o., ELI: http://data.europa.eu/eli/reg/2006/765/oj); a Tanács 359/2011/EU rendelete (2011. április 12.) az iráni helyzetre tekintettel egyes személyekkel, szervezetekkel és szervekkel szemben hozott korlátozó intézkedésekről (HL L 100., 2011.4.14., 1. o., ELI: http://data.europa.eu/eli/reg/2011/359/oj); a Tanács 36/2012/EU rendelete (2012. január 18.) a szíriai helyzetre tekintettel korlátozó intézkedések meghozataláról és a 442/2011/EU rendelet hatályon kívül helyezéséről (HL L 16., 2012.1.19., 1. o., ELI: http://data.europa.eu/eli/reg/2012/36/oj); a Tanács 401/2013/EU rendelete (2013. május 2.) a mianmari/burmai helyzetre tekintettel hozott korlátozó intézkedésekről és a 194/2008/EK rendelet hatályon kívül helyezéséről (HL L 121., 2013.5.3., 1. o., ELI: http://data.europa.eu/eli/reg/2013/401/oj); és a Tanács (EU) 2017/2063 rendelete (2017. november 13.) a venezuelai helyzetre tekintettel hozott korlátozó intézkedésekről (HL L 295., 2017.11.14., 21. o., ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

esetekre vonatkoznak, amikor a kibertér-megfigyelési termékeket kifejezetten abból a célból tervezték, hogy lehetővé tegyék az információs és távközlési rendszerekbe való behatolást vagy az azokra vonatkozó mélyreható adatcsomag-elemzést annak érdekében, hogy az e rendszerekből származó adatok – többek között biometrikus adatok – nyomon követése, kinyerése, gyűjtése vagy elemzése révén természetes személyeket figyelhessenek meg. A kizárólag kereskedelmi célokra, például számlázással, marketinggel, minőséggel kapcsolatos szolgáltatásokkal, felhasználói elégedettséggel vagy hálózatbiztonsággal összefüggésben használt termékek általában úgy tekinthetők, hogy nem hordoznak ilyen kockázatot.";

b) (9) preambulumbekezdés: „A fel nem sorolt kibertér-megfigyelési termékek kivitelére irányuló hatékony ellenőrzés megerősítése érdekében alapvető fontosságú a mindenre kiterjedő (catch-all) ellenőrzések alkalmazásának további harmonizálása ezen a területen. E célból a tagállamok elkötelezettek az ilyen ellenőrzések támogatása mellett, egyrészt azáltal, hogy megosztják egymással és a Bizottsággal az információkat, különösen a kibertér-megfigyelési termékek technológiai fejlesztései tekintetében, másrészt azáltal, hogy az uniós szintű információcsere előmozdítása érdekében az ilyen ellenőrzések lefolytatása során éberséget tanúsítanak.";

c) 2. cikk, 20. pont, amely a következőképpen határozza meg a kibertér-megfigyelési termékek fogalmát: „olyan kettős felhasználású termékek, amelyeket kifejezetten arra terveztek, hogy lehetővé tegyék természetes személyek megfigyelését információs és telekommunikációs rendszerekből származó adatok nyomon követése, kinyerése, gyűjtése vagy elemzése révén;"

d) az 5. cikk bevezeti a fel nem sorolt kibertér-megfigyelési termékek kivitelének engedélykötelezettségét, amennyiben a hatáskörrel rendelkező hatóság az exportőrt tájékoztatta arról, hogy a szóban forgó termékeket részben vagy egészben belső elnyomással és/vagy a nemzetközi emberi jogok és a nemzetközi humanitárius jog súlyos megsértésével összefüggésben lévő felhasználási célokra szánják vagy szánhatják (5. cikk (1) bekezdés). Arra kötelezi továbbá az exportőröket, hogy értesítsék a hatáskörrel rendelkező hatóságot, ha a kellő gondosságra vonatkozó intézkedésekből fakadó ténymegállapításaik szerint tudomásuk van arról, hogy a termékeket részben vagy egészben a belső elnyomással és/vagy az emberi jogok és a nemzetközi humanitárius jog súlyos megsértésével összefüggésben lévő felhasználási célokra szánják (5. cikk (2) bekezdés). A hatáskörrel rendelkező hatóság eldönti, hogy az érintett kivitelt engedélykötelessé teszi-e; valamint

e) az 5. cikk (2) bekezdése előírja továbbá, hogy „[a] Bizottság és a Tanács a 26. cikk (1) bekezdésében említettek szerint iránymutatásokkal vagy ajánlásokkal szolgál az exportőrök számára".

1.2. **Főbb fogalommeghatározások**

A rendelet külön preambulumbekezdésekben és rendelkezésekben pontosítja a fel nem sorolt kibertér-megfigyelési termékek kivitelének ellenőrzése szempontjából releváns konkrét fogalmakat, amelyeket az exportőröknek fontos világosan megérteniük a kellő gondosság teljesítése és az ellenőrzések hatékony végrehajtása érdekében. Kiemelten fontos a 2. cikk 20. pontja, amely a következő pontos meghatározást adja a „kibertér-megfigyelési termékek" fogalmáról: „*olyan kettős felhasználású termékek, amelyeket kifejezetten arra terveztek, hogy lehetővé tegyék természetes személyek megfigyelését információs és telekommunikációs rendszerekből származó adatok nyomon követése, kinyerése, gyűjtése vagy elemzése révén*".

Ezen iránymutatások alkalmazásában pontosítani kell a fenti fogalommeghatározás egyes vonatkozásait.

1.2.1. *„Kifejezetten arra tervezett"*

Egy terméket megfigyelésre terveztek, ha műszaki jellemzői alkalmasak természetes személyek megfigyelésére, és azt objektíve lehetővé teszik. Ezért a „kifejezetten arra tervezett" kifejezés azt jelenti, hogy a természetes személyek megfigyelésének kellett lennie az elsődleges célnak a termék fejlesztésekor és tervezésekor. Ez a kifejezés azonban nem követeli meg, hogy a terméket kizárólag természetes személyek megfigyelésére lehessen használni.

Amint azt a rendelet (8) preambulumbekezdése egyértelművé teszi, a kizárólag kereskedelmi célokra, például számlázással, marketinggel, minőséggel kapcsolatos szolgáltatásokkal, felhasználói elégedettséggel vagy hálózatbiztonsággal összefüggésben használt termékeket nem kifejezetten a természetes személyek megfigyelésére tervezték, és ezért nem tartoznak a kibertér-megfigyelési termékek fogalommeghatározása alá. Például, még ha az ágazatban működő operációs rendszerek felügyeletére vagy a felhasználók forgalmának nyomon követésére szolgáló termékek megfigyelési célokra is felhasználhatók, ezek a termékek nem minősülnek a fogalommeghatározás alá tartozó kibertér-megfigyelési termékeknek, mivel azokat nem kifejezetten a természetes személyek megfigyelésére tervezték.

1.2.2. *„Megfigyelés”*

A termékek mindenekelőtt akkor tesznek lehetővé megfigyelést, ha a megfigyelés nem nyilvánvalóan észlelhető az érintett természetes személy számára. Ez az eset, ha az érintett személyeknek nincs tudomásuk kibertér-megfigyelési termékek jelenlétéről és/vagy tevékenységéről, és ezért nincs lehetőségük arra, hogy kivonják magukat a megfigyelés alól, vagy legalábbis ennek megfelelően módosítsák viselkedésüket. Még akkor is, ha a megfigyelést nyilvános térben telepített vagy működő eszközök segítségével végzik, az adatok gyűjtése – bizonyos esetekben – relevánsnak tekinthető a megfigyelés fennállásának szempontjából, főleg ha az összegyűjtött adatok eltéríthetők, értékelhetők vagy feldolgozhatók olyan egyéb célokra, amelyről az érintett természetes személynek nincs tudomása. Más szóval, ha egy természetes személy objektíve nem számíthat arra, hogy megfigyelés alatt áll, akkor az a rendelet 2. cikkének 20. pontja szerint megfigyelésnek tekinthető.

1.2.3. *„Természetes személyek”*

A „természetes személy” kifejezés élő emberre utal, valamely jogi személlyel vagy szervezettel szemben, amelyek ezért nem tartoznak a rendelkezések hatálya alá. A fogalom nem terjed ki a tárgyak, helyszínek vagy gépek megfigyelésére.

1.2.4. *„Adatok nyomon követése, kinyerése, gyűjtése, elemzése”*

Az Oxford English Dictionary szerint a nyomon követés, kinyerés, gyűjtés és elemzés kifejezések nyelvi jelentése a következő:

— „nyomon követés”: felügyelet, megfigyelés, lehallgatás,

— „kinyerés”: kivonás,

— „gyűjtés”: összegyűjtés, felhalmozás,

— „elemzés”: valami (összetett) dolog elemeinek megkülönböztetése vagy meghatározása az adott dolog struktúrájának vagy jellegének megállapítása és ezáltal annak magyarázata vagy megértése érdekében; értelmezés céljából végzett alapos és módszeres vizsgálat; kritikai vagy számítási elemzésnek való alávetés.

Ezek a kifejezések arra utalnak, hogy a megfigyelésre használt termékeknek pontos technikai adatkezelési képességekkel kell rendelkezniük az adatok nyomon követése, gyűjtése, kinyerése vagy elemzése céljából. Ilyenek például a következő termékek:

a) Az információs és telekommunikációs rendszerekből ([4]) származó adatok (például az ilyen rendszerben továbbított adatok fájlméretének vagy csomagforgalmának) nyomon követésére használt termékek.

b) Az információs és telekommunikációs rendszerekből adatokat behatolással és kinyeréssel kivonó termékek (például támadószoftver).

c) Olyan termékek, amelyek lehetővé teszik az információs és telekommunikációs rendszerekből kivont adatok elemzését, beleértve azokat is, amelyek képesek az e rendszerekben tárolt kameraképek feldolgozására (például az arcfelismerő rendszerek részeként használt bizonyos típusú adatelemzési technológiák).

A pusztán az információs rendszerek nyomon követésére vagy a lakosság videokamerákon keresztül történő megfigyelésére használt olyan eszközök, amelyek lehetővé teszik a beszélgetések, az adatcserék, a mozgások és az egyéni viselkedések rögzítését, nem minősülnének a rendelet fogalommeghatározása alá tartozó kibertér-megfigyelési termékeknek, mivel nem kifejezetten erre a célra tervezték őket, és más technológiákkal, például mesterséges intelligenciával vagy nagy adathalmazokra épülő technológiával együtt kell működniük. A teljes rendszer azonban (amely más technológiákkal, például mesterséges intelligenciával vagy nagy adathalmazokra épülő technológiával együtt működik) potenciálisan lehet kibertér-megfigyelési termék a rendelet 2. cikkének 20. pontjában szereplő fogalommeghatározás szerint.

Fontos megjegyezni, hogy a szemléltetés céljából bemutatott hasznos példák nem határolják le a kibertér-megfigyelési termékek meghatározását és hatályát, mivel az 5. cikk célja az, hogy lehetővé tegye a fel nem sorolt termékek hatékony exportellenőrzését.

([4]) A fogalommeghatározást lásd az 1.2.5. pontban.

Amint azt a fogalommeghatározásban a „vagy” kötőszó használata is bizonyítja, a felsorolt technikai képességek alternatívának tekintendők, és nem szükséges, hogy egy adott termék az adatok nyomon követésére, kinyerésére, gyűjtésére vagy elemzésére irányuló ezen összes technikai képességgel rendelkezzen. Más szóval egy terméknek elegendő az említett technikai képességek egyikével rendelkeznie ahhoz, hogy a kibertér-megfigyelési terméknek a 2. cikk 20. pontjában szereplő fogalommeghatározása alá tartozzon.

1.2.5. *„Információs és telekommunikációs rendszerekből”*

Ezek a kifejezések olyan rendszerekre utalnak, amelyek elektronikusan feldolgozzák az információkat, például programozás/kódolás, a PC-rendszer (hardver) műveletei és más információadminisztráció, beleértve a szoftvertechnológiát, a webtechnológiát, a számítógépes technológiát, a tárolási technológiát stb., valamint egyes olyan rendszerekre, amelyek távolról továbbítják az információkat, például a hangokat, jeleket, szövegeket, egyéb jeleket, képeket vezetékes és vezeték nélküli csatornákon, optikai szálakon vagy rádió- és egyéb elektromágneses rendszeren keresztül. E két fogalom együtt az információ-továbbító vagy -feldolgozó rendszerek széles skáláját foglalja magában. Meg kell jegyezni, hogy a kifejezés rendszerekre, nem pedig berendezésekre vonatkozik.

1.2.6. *„Tudomás” és „valamilyen célra szánt”*

A rendelet 5. cikkének (2) bekezdése értelmében az exportőrnek értesítenie kell a hatáskörrel rendelkező hatóságot, ha *„tudomása van arról, hogy [a] kibertér-megfigyelési termékeket […] belső elnyomással és/vagy a[z] […] emberi jogok és a nemzetközi humanitárius jog súlyos megsértésével összefüggésben lévő felhasználási célokra szánják*”.

A „tudomása van” kifejezés nem új jogi fogalom, hanem már használatban van a rendelet 4., 6., 7. és 8. cikke szerinti, végfelhasználással kapcsolatos engedélyezési követelményekkel (úgynevezett mindenre kiterjedő, „catch-all” ellenőrzésekkel) összefüggésben. A „tudomása van” arra utal, hogy az exportőr tud a visszaélés szándékáról. Az ilyen kockázat puszta lehetősége nem elegendő a „tudomás” megállapításához. A „tudomás” kifejezés azonban nem azonosítható a passzivitással: szükségessé teszi, hogy az exportőr lépéseket tegyen annak érdekében, hogy elegendő és megfelelő tudást szerezzen be a kivitellel kapcsolatos kockázatok értékeléséhez és a rendeletnek való megfelelés biztosításához.

Az, hogy jelek utalnak arra, hogy a terméket bizonyára egy releváns, érzékeny végfelhasználásra „szánják”, azzal jár, hogy az exportőrnek eseti alapon, az adott eset sajátos körülményeinek fényében értékelnie kell a végfelhasználást. Ezzel szemben egy elméleti kockázat, amely nem az ügy ténybeli értékelésén alapulva jelzi, hogy a termékeket az emberi jogokat sértő módon használhatják fel, nem lenne elegendő utalás arra, hogy a termékeket az 5. cikk szerinti konkrét visszaélésre „szánják”.

1.3. **Belső elnyomás, az emberi jogok és a nemzetközi humanitárius jog súlyos megsértése**

A rendeletnek az engedély elbírálásához kapcsolódó megfontolásokat meghatározó 15. cikke értelmében a tagállamoknak figyelembe kell venniük minden vonatkozó szempontot, beleértve a 2008/944/KKBP tanácsi közös álláspont hatálya alá tartozókat is ([5]).

A rendelet 5. cikke kiterjeszti az ellenőrzéseket a fel nem sorolt kibertér-megfigyelési termékek kivitelére, figyelembe véve annak kockázatát, hogy azokat belső elnyomással és/vagy az emberi jogok és a nemzetközi humanitárius jog súlyos megsértésével összefüggésben használják fel. A 2008/944/KKBP közös álláspont és az e közös állásponthoz kapcsolódó felhasználói útmutató ([6]) hasznos iránymutatással szolgál e tekintetben.

([5]) A Tanács 2008/944/KKBP közös álláspontja (2008. december 8.) a katonai technológia és felszerelések kivitelének ellenőrzésére vonatkozó közös szabályok meghatározásáról, HL L 335., 2008.12.13., 99. o., ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Lásd a katonai technológia és felszerelések kivitelének ellenőrzésére vonatkozó közös szabályok meghatározásáról szóló 2008/944/KKBP tanácsi közös álláspont felhasználói útmutatóját, https://www.consilium.europa.eu/media/40659/st12189-en19.pdf.

1.3.1. *Belső elnyomás*

A 2008/944/KKBP közös álláspont 2. cikkének (2) bekezdése szerint a „belső elnyomás körébe tartozik, többek között, a kínzás és más kegyetlen, embertelen és megalázó bánásmód vagy büntetés, a gyorsított eljárásban foganatosított vagy önkényes kivégzések, az eltűnések, az önkényes őrizetbe vétel és más, a vonatkozó nemzetközi emberi jogi okmányokban, ideértve az Emberi Jogok Egyetemes Nyilatkozatában és a Polgári és Politikai Jogok Nemzetközi Egyezségokmányában meghatározott, emberi jogokat és alapvető szabadságjogokat súlyosan sértő cselekmények". A 2008/944/KKBP közös állásponthoz készült felhasználói útmutató iránymutatást nyújt az exportőr általi értékelés során figyelembe veendő elemekre vonatkozóan, beleértve „a tervek szerinti végfelhasználóról az emberi jogok tiszteletben tartása tekintetében, a fogadó országról pedig általában rendelkezésre álló jelenlegi és múltbeli információkat".

1.3.2. *Az emberi jogok súlyos megsértése*

A fel nem sorolt kibertér-megfigyelési termékekkel való visszaélés negatív hatással lehet az emberi jogok széles körére, és közvetlenül sértheti a magánélethez és az adatvédelemhez való jogot. Az önkényes vagy jogellenes megfigyelés más emberi jogokat is sérthet, például a véleménynyilvánítás, az egyesülés és a gyülekezés szabadságát, a vallás vagy meggyőződés szabadságát, valamint az egyenlő bánásmódhoz vagy a megkülönböztetés tilalmához való jogot, illetve a szabad, egyenlő és titkos választásokhoz való jogot. Bizonyos esetekben a természetes személyek – például emberijog-védők, aktivisták, politikai személyiségek, kiszolgáltatott helyzetben lévő lakosság és újságírók – megfigyelése, többek között a velük kapcsolatos információk nyomon követése vagy gyűjtése megfélemlítéshez, elnyomáshoz, önkényes fogva tartáshoz, kínzáshoz vagy akár bírósági eljárás nélküli kivégzéshez vezethet. Ezért az exportőröknek értékeléseikben figyelembe kell venniük e szempontokat is, amelyek összefüggésben állnak az emberi jogok súlyos megsértésével.

A nemzetközi gyakorlat azt mutatja, hogy az emberi jogok korlátozásának „megfelelőnek" kell lennie, és összhangban kell állnia a nemzetközi emberi jogi normákkal. A gyakorlatban ez azt jelenti, hogy megfelelő biztosítékok állnak rendelkezésre annak biztosítására, hogy a korlátozásokat a jogok lényeges tartalmának megőrzése mellett törvény írja elő. Az arányosság elvére figyelemmel korlátozásukra csak akkor kerülhet sor, ha az szükséges és ténylegesen jogszerű célt szolgál – például a nemzetbiztonságot vagy a közbiztonságot, a közrendet, a népegészség védelmét vagy mások jogainak és szabadságainak védelmét.

A kibertér-megfigyelési termékek magukban foglalhatnak bűnüldözési célú jogszerű és szabályozott eszközöket is, például olyanokat, amelyek a – többek között a terrorizmus elleni küzdelem területén elkövetett – bűncselekmények megelőzésével, nyomozásával, felderítésével vagy büntetőeljárás alá vonásával, illetve a büntetőjogi szankciók végrehajtásával összefüggésben alkalmazhatók. Ugyanakkor a kibertér-megfigyelési termékekkel vissza is lehet élni az emberi jogok és a nemzetközi humanitárius jog súlyos megsértése céljából, amikor azokat elnyomó rezsimek vagy magán végfelhasználók számára és/vagy konfliktus sújtotta területekre exportálják.

Ez szükségessé teszi az adott eset körülményeinek egyedi értékelését, beleértve a vonatkozó rendeletek alkalmazását is, ha például az ENSZ, az Unió vagy az Európa Tanács illetékes szervei súlyos emberi jogi jogsértésekről számolnak be. Az emberi jogok megsértésének „súlyosságát" jelezheti például az, hogy az ENSZ illetékes szervei, az Unió vagy az Európa Tanács által közzétett információkban elismerik ezeknek a jogsértéseknek a fennállását. Ez nem feltétlenül szükséges az említett szervek általi kifejezett elismeréshez, de lényeges tényező a teljesülendő kritériumok szempontjából.

Az 5. cikk feltételei értelmében az emberi jogok megsértésének „súlyosnak" kell lennie. Az esetleges emberi jogi jogsértések „súlyosnak" minősítéséhez hasznos iránymutatás található a 2008/944/KKBP közös állásponthoz készült felhasználói útmutatóban. Ezen útmutató szerint a jogsértés jellege és következményei a meghatározók. Az emberi jogok rendszeres és/vagy széles körű megsértése rendszerint súlyosnak minősül; ugyanakkor a nem rendszeres vagy nem széles körben elterjedt jogsértések is tekinthetők „súlyosnak" – például akkor, ha a beavatkozás az érintett személyek szempontjából súlyosnak minősül.

A 2008/944/KKBP közös állásponthoz készült felhasználói útmutató II. melléklete tartalmazza a főbb nemzetközi és regionális emberi jogi eszközök nem kimerítő felsorolását, beleértve a Polgári és Politikai Jogokról Szóló Nemzetközi Egyezményokmányt (ICCPR), a kínzás és más kegyetlen, embertelen vagy megalázó büntetések vagy bánásmódok elleni egyezményt, az emberi jogok európai egyezményét (a továbbiakban: az egyezmény) és az Alapjogi Chartát (a továbbiakban: Charta), amelyek fontos iránymutatással szolgálhatnak a kritériumok értelmezéséhez és alkalmazásához az alapos emberi jogi értékelések alátámasztására. Ezen eszközök és azok kiegészítő jegyzőkönyvei képviselik a fő nemzetközi normákat és előírásokat az emberi jogok és az alapvető szabadságok területén.

1.3.3. *A nemzetközi humanitárius jog súlyos megsértése*

A nemzetközi humanitárius jog (más néven a genfi jog vagy a fegyveres konfliktusok joga) számos nemzetközi szerződés – legfőképpen a hágai rendeletek, a genfi egyezmények és azok 1977. évi két kiegészítő jegyzőkönyve – révén jött létre, és meghatározza azokat a szabályokat, amelyek a fegyveres konfliktusok idején az ellenségeskedésben nem vagy már nem részt vevő személyek (például polgári személyek, sebesültek, betegek vagy foglyul ejtett harcosok) védelmét szolgálják, és a hadviselők számára korlátozásokat írnak elő a hadviselési eszközök és módszerek tekintetében (hágai jog).

A fel nem sorolt kibertér-megfigyelési termékek használatának meg kell felelnie a nemzetközi humanitárius jognak, amikor azokat fegyveres konfliktus keretében hadviselési eszközként és módszerként alkalmazzák. Ilyen körülmények között a rendelet értelmében megfontolás tárgyát képezi a nemzetközi humanitárius jog súlyos megsértésének kockázata, és azt – az emberi jogok súlyos megsértése tekintetében – a termékek konkrét esetben tervezett végfelhasználásának fényében kell értékelni. A 2008/944/KKBP közös álláspontho kapcsolódó felhasználói útmutató iránymutatást nyújt a figyelembe veendő elemekről, amelyek magukban foglalják annak vizsgálatát, hogy a fogadó fél a múltban és jelenleg tiszteletben tartotta/tartja-e a nemzetközi humanitárius jogot, továbbá a fogadó fél hivatalos kötelezettségvállalások útján kifejezett szándékainak vizsgálatát, valamint a fogadó fél annak biztosítására vonatkozó képességének vizsgálatát, hogy az átadott felszerelést vagy technológiát a nemzetközi humanitárius joggal összeegyeztethető módon használják fel, és azt ne használják fel eltérő célra vagy ne adhassák át más olyan felhasználóknak, amelyek azt esetleg e jog súlyos megsértésére használhatják fel.

Az 5. cikk értelmében a nemzetközi humanitárius jog megsértésének „súlyosnak” kell lennie. Iránymutatás található a 2008/944/KKBP közös álláspontho készült felhasználói útmutatóban, amely elismeri, hogy „a nemzetközi humanitárius jog megsértésének elszigetelt esetei nem feltétlenül jellemzik a fogadó országnak a nemzetközi humanitárius joggal kapcsolatos magatartását”, „komoly aggodalomra adhat okot azonban az, ha a jogsértések meghatározott minta szerinti ismétlődése fedezhető fel, vagy a fogadó ország nem tett megfelelő lépéseket a jogsértések büntetésére”. A Vöröskereszt Nemzetközi Bizottsága (ICRC) iránymutatásokat adott ki a nemzetközi humanitárius jog megsértésének exportellenőrzési célú értékelésére vonatkozóan. A Vöröskereszt Nemzetközi Bizottsága szerint „a nemzetközi humanitárius jog megsértése súlyos, ha védett személyeket (például polgári személyeket, hadifoglyokat, sebesülteket és betegeket) vagy tárgyakat (például polgári létesítményeket vagy infrastruktúrát) veszélyeztet, vagy fontos egyetemes értékeket sért”. A háborús bűncselekmények például a nemzetközi humanitárius jog súlyos megsértésének minősülnek. A Vöröskereszt Nemzetközi Bizottsága továbbá a 2008/944/KKBP közös álláspontho kapcsolódó felhasználói útmutatóban szereplőkhöz hasonló tényezőket említ, ideértve a nemzetközi humanitárius jog szabályainak alkalmazására vonatkozó hivatalos kötelezettségvállalásokat, a nemzetközi humanitárius jog megsértésével kapcsolatos elszámoltathatóságot biztosító megfelelő intézkedéseket, a nemzetközi humanitárius joggal kapcsolatos képzést a katonaság számára, valamint a gyermekek fegyveres erőkbe való toborzásának tilalmát.

2. **MŰSZAKI HATÁLY**

2.1. **Felsorolt kibertér-megfigyelési termékek**

Ezen iránymutatások függeléke tájékoztatást nyújt a rendelet I. mellékletében felsorolt kibertér-megfigyelési termékekről, hogy segítse az exportőröket a potenciális fel nem sorolt kibertér-megfigyelési termékek azonosításában.

2.2. **Potenciális fel nem sorolt kibertér-megfigyelési termékek**

Bár fogalmilag lehetetlen kimerítő jelleggel felsorolni azokat a termékeket, amelyek az 5. cikk értelmében „fel nem sorolt termékként” ellenőrizhetők, a következő termékek alkalmasak lehetnek megfigyelésre, és különös éberségre adhatnak okot a rendelet értelmében.

Amint azt a rendelet (8) preambulumbekezdése egyértelművé teszi, a kizárólag kereskedelmi célokra, például számlázással, marketinggel, minőséggel kapcsolatos szolgáltatásokkal, felhasználói elégedettséggel vagy hálózatbiztonsággal összefüggésben használt termékek általában úgy tekinthetők, hogy nem hordoznak visszaélési kockázatot az emberi jogok vagy a nemzetközi humanitárius jog súlyos megsértése terén, ezért általában nem tartoznak az 5. cikk szerinti ellenőrzés hatálya alá. E termékek közül sok rendelkezik olyan információbiztonsági (rejtjelezési vagy akár rejtjelfejtési) funkciókkal, amelyek megfelelnek a rendelet I. mellékletében foglalt ellenőrzési szöveg szerinti 5. kategória 2. részében meghatározott ellenőrzési paramétereknek. A biztonsági hálózati berendezésekre – beleértve az útválasztókat, kapcsolókat vagy reléket, ahol az információbiztonsági funkció a kizárólag közzétett vagy kereskedelmi kriptográfiai szabványokat alkalmazó „működési, adminisztrációs vagy karbantartási” feladatokra korlátozódik – szintén nem terjed ki a „kibertér-megfigyelési termékek” fogalommeghatározása, bár az exportőröknek ébernek kell lenniük, mivel több ízben is voltak bejelentések az ilyen termékek emberi jogok megsértése céljából történő felhasználásával összefüggő visszaélésekről.

2.2.1. *Arc- és érzelemfelismerési technológia*

Az arc- és érzelemfelismerési technológiák a kibertér-megfigyelésen kívül többféle célra is szolgálnak – például azonosításra vagy hitelesítésre –, és nem tartoznának automatikusan a fogalommeghatározás hatálya alá. Bizonyos körülmények között azonban az arc- és érzelemfelismerési technológiák a rendelet 2. cikke 20. pontjának hatálya alá tartozhatnak.

A tárolt videofelvételek nyomon követésére vagy elemzésére használható arc- és érzelemfelismerési technológiák a kibertér-megfigyelési termék fogalommeghatározásának hatálya alá tartozhatnak. Azonban még ha a fent említett kritériumok teljesülnek is, gondosan meg kell vizsgálni, hogy a szoftvert kifejezetten megfigyelésre tervezték-e.

2.2.2. *Helymeghatározó eszközök*

A helymeghatározó eszközök lehetővé teszik az eszköz fizikai helyének időbeli nyomon követését, és a bűnüldöző és hírszerző ügynökségek egy ideje már alkalmaznak bizonyos helymeghatározó technológiákat. A célzott és tömeges megfigyeléssel kapcsolatos potenciáljuk jelentősen fejlődött, mivel a nyomkövetési technológiák fejlettebbé váltak – ideértve a műholdas helymeghatározást, a cellás toronyalapú helymeghatározást, a Wifi- és a Bluetooth-vevőket –, és mivel széles körben elterjedtek az olyan „nyomkövető eszközök”, mint az okostelefonok és más elektronikus eszközök (például a gépjárművek fedélzeti rendszerei).

A bűnüldöző és hírszerző ügynökségek helymeghatározó eszközöket használnak például a nyomozás során történő bizonyítékgyűjtésre vagy a gyanúsítottak nyomon követésére, de a vállalatok kereskedelmi célokból is alkalmazzák ezeket, például a bevásárlóutcák összesített mozgási mintáiról való jelentéstétel, a helyszínen kívül dolgozó alkalmazottak nyomon követése vagy a helyalapú hirdetések céljából.

2.2.3. *Videokamerás megfigyelési rendszerek*

Annak érdekében, hogy segítsék az exportőröket a lehetséges kibertér-megfigyelés azonosításában, hasznos tisztázni, hogy mely termékek nem tartoznának a fogalommeghatározás hatálya alá. Ebben az értelemben például a nyilvános tereken emberek filmezésére használt videokamerás rendszerek és kamerák – beleértve a nagy felbontású kamerákat is – nem tartoznak a kibertér-megfigyelési termékek fogalommeghatározása alá, mivel nem követnek nyomon és nem gyűjtenek információs és telekommunikációs rendszerekből származó adatokat.

3. KELLŐ GONDOSSÁGRA VONATKOZÓ INTÉZKEDÉSEK

A rendelet (7) preambulumbekezdése szerint „Döntő fontosságú, hogy az exportőrök […] hozzájáruljanak a kereskedelmi ellenőrzések általános céljához. Annak érdekében, hogy e rendelettel összhangban járhassanak el, az e rendelet által érintett ügyletekkel kapcsolatos kockázatok értékelését belső megfelelési program részeként ügyletátvilágítási intézkedések révén – vagyis az átvilágítás elve alapján – kell elvégezni”.

A 2. cikk 21. pontja a következőképpen definiálja a belső megfelelési programot: „az exportőrök által az e rendelet rendelkezéseinek és célkitűzéseinek, valamint az e rendelet alapján végrehajtott engedélyek feltételeinek való megfelelés elősegítése céljából elfogadott, folyamatban lévő, hatékony, megfelelő és arányos politikák és eljárások, ideértve többek között a termékek végfelhasználók számára történő kivitelével és végfelhasználásával kapcsolatos kockázatok értékelését szolgáló, a kellő gondosságra vonatkozó intézkedéseket is”.

Az (EU) 2019/1318 bizottsági ajánlás ([7]) keretrendszerrel szolgál a kettős felhasználású termékek kereskedelmének ellenőrzésével kapcsolatos kockázatok exportőrök általi azonosításának, kezelésének és csökkentésének megkönnyítéséhez és a vonatkozó uniós és nemzeti jogszabályoknak való megfelelés biztosításához.

Ezek az iránymutatások támogathatják az exportőröket az ügyletátvilágítási intézkedések – más néven a kellő gondosság elve – belső megfelelési program részeként történő végrehajtásában.

Az (EU) 2021/821 rendelet 5. cikkének (2) bekezdése értelmében a fel nem sorolt kibertér-megfigyelési termékek exportőrei ügyletátvilágítási intézkedések révén kötelesek kellő gondosságra vonatkozó intézkedéseket végrehajtani, azaz lépéseket tenni a termékek besorolását és az ügyleti kockázat értékelését illetően. A gyakorlatban ez azt jelenti, hogy az exportőröktől a következők vizsgálatát várják el:

([7]) A Bizottság (EU) 2019/1318 ajánlása (2019. július 30.) a kettős felhasználású termékek kereskedelmének a 428/2009/EK rendelet szerinti ellenőrzésére vonatkozó belső megfelelési programokról (HL L 205., 2019.8.5., 15. o., ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **Annak vizsgálata, hogy az exportálni tervezett, fel nem sorolt termék lehet-e olyan „kibertér-megfigyelési termék”, amelyet kifejezetten arra terveztek, hogy információs és telekommunikációs rendszerekből származó adatok nyomon követése, kinyerése, gyűjtése vagy elemzése révén lehetővé tegye természetes személyek megfigyelését.**

Ez a lépés az adott terméknek a kibertér-megfigyelési termékekre vonatkozó rendelkezések szerinti meghatározását foglalja magában. Ennek részét képezi a termékek műszaki jellemzőinek vizsgálata egyfelől a felsorolt termékekre vonatkozóan a rendelet I. mellékletében meghatározott műszaki paraméterek alapján, másfelől a fel nem sorolt termékekre vonatkozóan a kibertér-megfigyelési termékek fogalommeghatározásában szereplő konkrét kifejezések és fogalmak, továbbá a termék ezt követő besorolása (áruk, technológia vagy szoftver) fényében.

3.2. **Az adott termék képességeinek vizsgálata annak megállapítása érdekében, hogy rendelkezik-e potenciállal ahhoz, hogy külföldi végfelhasználók belső elnyomással és/vagy az emberi jogok és a nemzetközi humanitárius jog súlyos megsértésével kapcsolatban visszaéljenek vele.**

Az exportőröknek értékelést kell végezniük annak megállapítása érdekében, hogy a termékkel vissza lehet-e élni belső elnyomás, az emberi jogok megsértése vagy az azokkal való visszaélés céljából, ideértve az élethez való jogot, a kínzás, az embertelen és megalázó bánásmód tilalmát, a magánélethez való jogot, a szólásszabadságot, az egyesülés és a gyülekezés szabadságát, a vallás és meggyőződés szabadságát, az egyenlő bánásmódhoz vagy a megkülönböztetés tilalmához való jogot, illetve a szabad, egyenlő és titkos választásokhoz való jogot.

Ez magában foglalja annak értékelését is, hogy a termék felhasználható-e olyan rendszer alkatrészeként vagy alkotóelemeként, amely ugyanezeket a jogsértéseket és/vagy visszaéléseket eredményezheti.

Az exportőröknek értékelésük során figyelembe kell venniük az úgynevezett figyelmeztető jelzéseket, amelyek jelzik, ha valamely ügyletet arra utaló rendellenes körülmények öveznek, hogy a kivitelt nem megfelelő végfelhasználásra, végfelhasználónak vagy rendeltetési helyre szánhatják.

Figyelmeztető jelzések:

a) a termék forgalmazásához használt információk szerint a termék potenciálisan megfigyelésre is alkalmazható;

b) arra utaló információk, hogy egy hasonló termékkel visszaélést követtek el belső elnyomással és/vagy az emberi jogok és a nemzetközi humanitárius jog súlyos megsértésével kapcsolatban (lásd az 1.3. szakaszt);

c) arra utaló információk, hogy a terméket jogellenesen használták fel valamely tagállam ellen irányuló megfigyelési tevékenységekben vagy egy uniós polgár jogellenes megfigyelésével összefüggésben;

d) arra utaló információk, hogy az ügyletben szereplő egyes termékek felhasználhatók olyan rendszer létrehozására, testre szabására vagy konfigurálására, amellyel az ismeretek szerint már visszaéltek belső elnyomással és/vagy az emberi jogok és a nemzetközi humanitárius jog súlyos megsértésével kapcsolatban (lásd az 1.3. szakaszt);

e) a termék vagy egy hasonló termék szerepel a rendelet 5. cikke (6) bekezdésének megfelelően az *Európai Unió Hivatalos Lapjának* C sorozatában közzétett listán.

3.3. **A hatáskörrel rendelkező hatóságok támogatása érdekében az ügyletben részt vevő érdekelt felek felülvizsgálata (ideértve a végfelhasználókat és a címzetteket, például a forgalmazókat és a viszonteladókat).**

Az exportőröknek a hatáskörrel rendelkező hatóságok támogatása érdekében és a lehetőségekhez mérten teljesíteniük kell a következőket:

a) az ügylet előtt és alatt a végfelhasználási nyilatkozatok alapján felül kell vizsgálniuk, hogy a címzettek és/vagy a végfelhasználók hogyan kívánják használni a terméket vagy a szolgáltatást;

b) tisztában kell lenniük a termékek rendeltetési helyén fennálló helyzettel, különösen az emberi jogok általános helyzetével, mivel az fontos mutatója annak, hogy a kivitellel összefüggésben fennáll-e az emberi jogok és a nemzetközi humanitárius jog súlyos megsértésének a kockázata;

c) az alább felsorolt figyelmeztető jelzések alapján felül kell vizsgálniuk annak kockázatait, hogy a terméket vagy a szolgáltatást egy másik jogosulatlan végfelhasználónak adják át.

Figyelmeztető jelzések:

a) a végfelhasználó nyilvánvaló kapcsolatban áll egy olyan külföldi kormánnyal, amely a múltban már elkövetett belső elnyomást és/vagy súlyosan megsértette az emberi jogokat és a nemzetközi humanitárius jogot;

b) a végfelhasználó strukturálisan a fegyveres erők vagy más olyan csoport része, amely a múltban belső elnyomással járó intézkedéseket és/vagy az emberi jogok és a nemzetközi humanitárius jog súlyos megsértését magában foglaló fegyveres konfliktusban vett részt;

c) a végfelhasználó korábban kibertér-megfigyelési termékeket exportált olyan országokba, ahol az ilyen termékek használata belső elnyomást és/vagy az emberi jogok és a nemzetközi humanitárius jog súlyos megsértését eredményezte.

3.4. **A kellő gondosságra vonatkozó intézkedésekből fakadó ténymegállapítások felhasználása a lehetséges jövőbeli kedvezőtlen hatások megelőzésére és enyhítésére irányuló tervek kidolgozása során.**

Az exportőröknek a kellő gondosságra vonatkozó intézkedéseikből fakadó ténymegállapítások alapján meg kell szüntetniük az emberi jogokkal kapcsolatos kedvezőtlen hatásokat okozó vagy azokhoz hozzájáruló tevékenységeket, valamint korrekciós intézkedési tervet kell kidolgozniuk és végrehajtaniuk. Ezek az intézkedések a következők lehetnek:

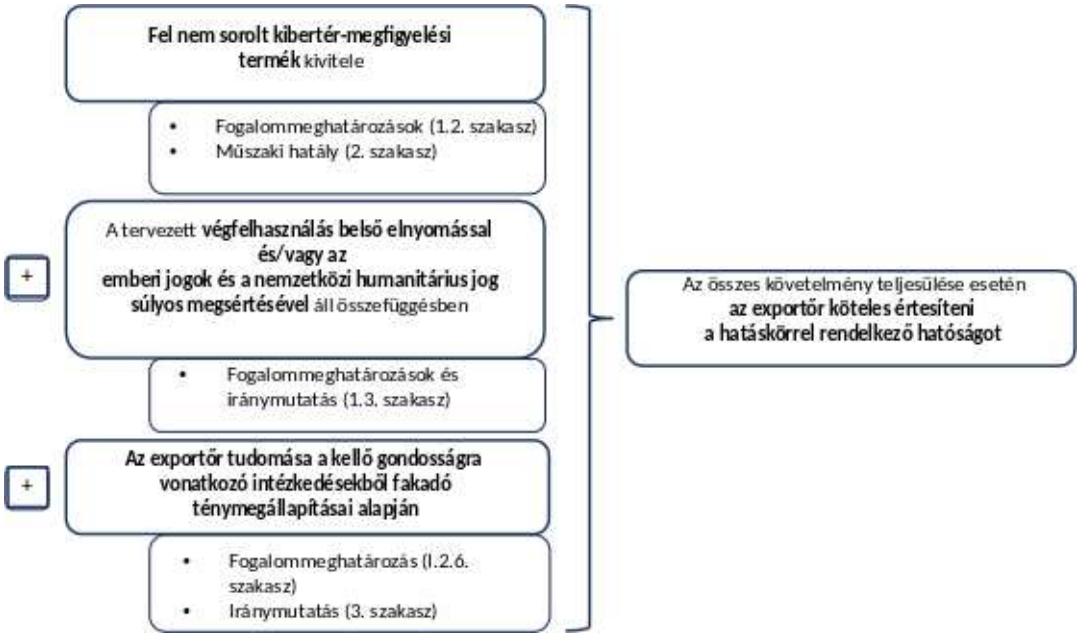
a) a vállalkozás szabályzatainak aktualizálása arra vonatkozó iránymutatás nyújtása érdekében, hogy a jövőben hogyan kerülhetők el és kezelhetők a kedvezőtlen hatások, továbbá végrehajtásuk biztosítása;

b) a kockázatértékelés megállapításai alapján az irányítási rendszerek aktualizálása és megerősítése az információk jobb nyomon követése és a kockázatoknak a kedvezőtlen hatások bekövetkezése előtti jelzése érdekében;

c) információk gyűjtése az ágazatot érintő kedvezőtlen hatások magas szintű kockázatainak megértése érdekében;

d) a tagállamok hatáskörrel rendelkező hatóságainak értesítése a kellő gondosságra vonatkozó intézkedésekből fakadó ténymegállapításokról az egyes termékekre, végfelhasználókra és rendeltetési helyekre vonatkozó információáramlás előmozdítása érdekében.

Az (EU) 2021/821 rendelet 5. Cikkének (2) bekezdésében meghatározott követelmények



4. **FÜGGELÉK**

Az (EU) 2021/821 rendelet I. Melléklete által ellenőrzés alá vont, felsorolt kibertér-megfigyelési termékek

— **Telekommunikációs szolgáltatások lehallgatására szolgáló rendszerek (5A001.f.)**

A legtöbb országban, beleértve a tagállamokat is, a kommunikáció titkosságát törvény védi, de a kommunikáció kormányzati hatóságok általi rejtett elektronikus megfigyelése a jogszabályokkal összhangban engedélyezhető (úgynevezett jogszerű lehallgatás). A digitális kor azonban bevezette a lehallgatási technológiák tömeges használatának lehetőségét. A líbiai rezsim által alkalmazott lehallgatási eszközök rávilágítottak e technológiák tömeges bevezetésének lehetőségére, és ösztönözték a telekommunikációs szolgáltatások lehallgatására szolgáló rendszerek exportellenőrzésének 2012-ben történő bevezetését.

Ez az ellenőrzés a kommunikáció (hang vagy adatok) tartalmának kinyerésére tervezett berendezésekre, valamint a vezeték nélküli kommunikáción keresztül továbbított előfizetői azonosítókra vagy más metaadatokra, valamint a rádiófrekvencia-monitoring berendezésekre vonatkozik. Ez az ellenőrzés vonatkozik például az IMSI-t (nemzetközi mobil-előfizetői azonosító) gyűjtő berendezésekre, amelyek lehallgatják a mobiltelefon-forgalmat és nyomon követik a mobiltelefon-használók mozgását, vagy az IMSI-számokat telefonról kinyerni képes hamis Wifi-hotspotokat létrehozó berendezésekre, valamint a kifejezetten a telekommunikációs rendszerek „mély csomagvizsgálatának" lehetővé tételére tervezett bizonyos típusú termékekre. A mobil telekommunikációs szolgáltatásokat zavaró berendezések nem tartoznak a kibertér-megfigyelési termékek körébe, mivel nem gyűjtenek adatokat.

Bár az általános célú technológia felhasználható ilyen rendszerek építésére, azok tömeges lehallgatási képessége meghatározott alkatrészekre és alkotóelemekre fog támaszkodni – ideértve például a specifikus szoftvert, a fejlett vagy alkalmazásspecifikus integrált áramköröket (például FGPA-k, ASIC-ek) – a másodpercenként feldolgozható adatcsomagok vagy kommunikációs munkamenetek számának növelése érdekében.

— **Internetalapú megfigyelési rendszerek (5A001.j.)**

Bár ma már számos internetalapú kommunikációt jellemzően alapértelmezés szerint titkosítanak, a kommunikációra vonatkozó forgalmi adatok (metaadatok) – például az IP-címek, valamint az adatcsere gyakorisága és mérete – továbbra is felhasználhatók a személyek és a doménnevek közötti kapcsolatok azonosítására. A kormányok jogszerűen – és bírósági felügyelet mellett – jogszerű célokra használhatják ezeket a rendszereket, például azon személyek azonosítására, akik bűnözői vagy terrorista tartalmakkal összefüggő doméneket látogatnak meg. Az internetes forgalom etnikai, vallási, politikai vagy társadalmi jellemzésen alapuló nyomon követése és elemzése azonban egy ország átfogó emberi és társadalmi feltérképezéséhez vezethet a lakosság ellenőrzése és elnyomása, valamint más célok, például a politikai disszidensek azonosítása céljából. Az emberi jogokkal és a belső elnyomással kapcsolatban felmerülő kérdések mellett ezek a termékek hozzájárulhatnak a biztonsági és katonai képességek megerősítéséhez is.

Az 5A001.j. szerinti ellenőrzés azokra az internetalapú vezérlőrendszerekre vonatkozik, amelyek „szolgáltatói szintű IP-hálózaton (például nemzeti szintű IP gerinchálózaton)" működnek a továbbított metaadat-tartalmak (hang, videó, üzenetek, csatolmányok) elemzése, kinyerése és indexálása céljából „erős szelektorok" alapján, és feltérképezik az emberek kapcsolati hálózatát. Ezek olyan termékek, amelyek „megfigyelést" végeznek, mivel a célszemélyeknek nincs tudomásuk a kommunikáció lehallgatásáról. Ezzel szemben az ellenőrzések nem olyan rendszerekre irányulnak, amelyekben fennáll egy felhasználó vagy előfizető tevékenysége vagy egy vele folytatott interakció, és például nem vonatkoznak a közösségi hálózatokra vagy a kereskedelmi keresőprogramokra. Ezenkívül az ellenőrzések az internetszolgáltató törzshálózatából származó adatokat feldolgozó rendszerekre vonatkoznak, és nem alkalmazandók azokra a közösségi hálózatokra vagy kereskedelmi keresőmotorokra, amelyek a felhasználók által megadott adatokat kezelik.

— **„Támadószoftver" (4A005., 4D004., valamint a 4E001.a. és 4E001.c. pont szerinti kapcsolódó ellenőrzések)**

A támadószoftver lehetővé teszi kezelője számára, hogy rejtett módon távoli hozzáférést szerezzen egy elektronikus eszközhöz, például okostelefonhoz, laptophoz, szerverhez vagy a dolgok internetéhez használt eszközhöz, megszerezze az eszközön tárolt adatokat, lehallgatást végezzen az eszközbe beépített vagy ahhoz csatlakoztatott kamerán vagy mikrofonon keresztül, valamint az eszközt lépőkőként használja az eszközhöz kapcsolódó berendezések vagy felhasználói kapcsolatok elleni támadások végrehajtásához („harmadik fél eszközein keresztül történő feltörés"). Bár a támadószoftvereknek léteznek jogszerű felhasználási módjai ([8]), például az informatikai részlegek távoli támogatására használt „távhozzáférési szoftver" esetében, a megfigyelés leplezett jellege és az esetlegesen gyűjtött információk nagysága, a magánélethez és a személyes adatok védelméhez való jog megsértésének magas kockázatát hordozza magában, és súlyosan alááshatja a véleménynyilvánítás szabadságához való jogot.

([8]) Az egyértelműség érdekében megjegyzendő, hogy a kettős felhasználású termékekről szóló rendelet I. melléklete által ellenőrzött, felsorolt kibertér-megfigyelési termékek harmadik országokba történő kiviteléhez engedélyre lenne szükség, függetlenül attól, hogy a termék használata jogszerű-e.

A 4A005. és a fent említett kapcsolódó pontok szerinti ellenőrzés magában foglalja a kifejezetten „támadószoftverek” előállításához, irányításához és vezérléséhez vagy célba juttatásához tervezett vagy módosított szoftvereket, valamint rendszereket, berendezéseket, alkotóelemeket és kapcsolódó technológiákat, de nem vonatkozik magára a rendelet I. mellékletében meghatározott „támadószoftverekre”. Ezek a kibereszközök azon esetleges zavarokra és károkra tekintettel tartoznak ellenőrzés alá, amelyeket sikeres használat és végrehajtás esetén okozhatnak, de az ellenőrzésnek nem célja az, hogy befolyásolja például a kiberbiztonsági kutatók és ágazat tevékenységét, hiszen nekik meg kell osztaniuk a támadószoftverekkel kapcsolatos információkat annak érdekében, hogy javításokat dolgozhassanak ki termékeikre, és azoknak a sebezhetőség nyilvánosságra hozatala előtt rendelkezésre kell állniuk.

— **Kommunikációfigyelő szoftver (5D001.e.)**

Ez a szoftver arra szolgál, hogy az engedéllyel rendelkező bűnüldöző hatóságok nyomon kövessék és elemezzék a hírközlési szolgáltatótól kért célzott lehallgatási intézkedések révén gyűjtött adatokat. Ez a szoftver lehetővé teszi a kommunikációs tartalom vagy metaadatok „erős szelektorokon” alapuló keresését, a jogszerű lehallgatásra szolgáló interfész használatával, valamint a kapcsolati hálózat feltérképezését vagy a megcélzott személyek mozgásának a keresések eredményei alapján történő nyomon követését. Ez a szoftver „megfigyelésre” szolgál, mivel a kommunikáció lehallgatásából gyűjtött adatokat használja fel anélkül, hogy arról a személyek tudomást szereznének. Ezenkívül „elemzi” a „telekommunikációs rendszereken” keresztül gyűjtött adatokat. A szoftver a kormányzati hatóságnál van telepítve (például bűnüldözési megfigyelő létesítménynél), és az ellenőrzés nem vonatkozik a jogszerű lehallgatási megfelelési rendszerekre (például a jogszerű lehallgatási irányítási rendszerekre és közvetítő eszközökre), amelyeket kereskedelmileg fejlesztettek ki és telepítenek a hírközlési szolgáltató terében (például a kommunikációs hálózatba integráltak), és amelyeket a szolgáltató üzemeltet és tart fenn. Amint azt az ellenőrzési szöveg egyértelművé teszi, az ellenőrzések nem vonatkoznak a kifejezetten kereskedelmi célokra tervezett vagy átalakított „szoftverekre”, mint például a számlázás, a hálózati szolgáltatásminőség (QoS), a felhasználói élmény (QoE), a közvetítő eszközök, vagy a mobil fizetés vagy banki felhasználás.

— **Rejtjelelemzéshez használt termékek (5A004.a.)**

Ez az ellenőrzés olyan termékekre alkalmazandó, amelyeket a rejtjelezési mechanizmusok hatálytalanítására terveztek a célból, hogy bizalmas változókhoz vagy érzékeny adatokhoz – ideértve a tiszta szövegeket, jelszavakat vagy rejtjelezési kódokat – jussanak. A rejtjelezést a továbbítás alatt álló és használaton kívüli adatok bizalmas jellegének védelme érdekében használják. A rejtjelelemzést e bizalmas jelleg hatálytalanítására használják, ezért ez a technológia „lehetővé teszi” a megfigyelést az információs és telekommunikációs rendszerekből származó adatok nyomon követése, kinyerése, gyűjtése vagy elemzése révén.

— **Kriminalisztikai/nyomozó eszközök (5A004.b., 5D002.a.3.b. és 5D002.c.3.b.)**

A kriminalisztikai/nyomozó eszközöket arra tervezték, hogy nyers adatokat nyerjenek ki egy (például számítástechnikai vagy kommunikációs) eszközből az adatok manipulálása vagy megrongálása nélkül, hogy azok igazságügyi célokra, azaz bűnügyi nyomozásban vagy bíróságon felhasználhatók legyenek. Ezek a termékek kijátsszák az eszköz általi „hitelesítést” vagy engedély-ellenőrzést, hogy a nyers adatok kinyerhetők legyenek az eszközből. Ezeket a termékeket a kormány és a bűnüldöző szervek, valamint a katonai erők is használják a lefoglalt eszközökből származó adatok kinyerésére és elemzésére. Bár rendelkeznek jogszerű felhasználási módokkal, visszaélhetnek velük, és így kockázatot jelentenek az érzékeny vagy kereskedelmi adatokra nézve.

Azok a kriminalisztikai/nyomozó eszközök azonban, amelyeket nem „kifejezetten” megfigyelésre terveztek, nem tartoznak a kibertér-megfigyelési termékek 2. cikk 20. pontjában szereplő fogalommeghatározása alá. Az 5A004.b. és a fent említett kapcsolódó pontokban szereplő ellenőrzési szöveg nem rögzíti azokat a kriminalisztikai/nyomozó eszközöket, amelyek csak felhasználói adatokat nyernek ki, vagy amelyek esetében az adatok az eszközön nem védettek. Az ellenőrzések ugyanakkor nem vonatkoznak a gyártó gyártó- vagy vizsgálóberendezéseire, a rendszeradminisztrátor-eszközökre vagy a kizárólag a kiskereskedelemben használt termékekre, például a mobiltelefon-feloldó termékekre. Ezért az ilyen típusú technológiák sokféleségére tekintettel az ellenőrzések alkalmazása az egyes termékek eseti értékelésétől függ.

Végezetül figyelembe kell venni, hogy a rendelet I. mellékletében más olyan, megfigyeléssel kapcsolatos termékek is szerepelnek, amelyek nem tartoznak a kibertér-megfigyelési termékek fogalommeghatározásába, mint például a kommunikáció vagy a rendszerek megrongálására vagy zavarására tervezett, mobil telekommunikációs szolgáltatások zavarására szolgáló berendezések (5A001.f.), a rendszert módosító támadószoftverek (4D004.) és a lézeres akusztikai érzékelő berendezések (6A005.g.), amelyek audioadatokat gyűjtenek lézerrel, vagy lehetővé teszik a beszélgetések távolról történő meghallgatását (úgynevezett „lézermikrofon”). Hasonlóképpen, a felsorolt UAV-k megfigyelési célokra történő használata sem vonná ezeket a termékeket a kibertér-megfigyelési termékek fogalommeghatározása alá.