

(Az Európai Unióról szóló szerződés VI. címe alapján elfogadott jogi aktusok)

A TANÁCS 2005/222/IB KERETHATÁROZATA

(2005. február 24.)

az információs rendszerek elleni támadásokról

AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unióról szóló szerződésre és különösen annak 29. cikkére, 30. cikke (1) bekezdésének a) pontjára, 31. cikke (1) bekezdésének e) pontjára valamint 34. cikke (2) bekezdésének b) pontjára,

tekintettel a Bizottság javaslatára,

tekintettel az Európai Parlament véleményére⁽¹⁾,

mivel:

- (1) E kerethatározat célja a tagállamok igazságügyi és egyéb hatóságai – beleértve a rendőrséget és egyéb bűnüldözési szakszolgálatokat – közötti együttműködés javítása a tagállamok büntető jogszabályainak az információs rendszerek elleni támadások terén történő közelítése révén.
- (2) Bizonyítékok állnak rendelkezésre az információs rendszerek elleni támadásokról, különösen a szervezett bűnözésből eredő fenyegetések eredményeképpen, és egyre nagyobb aggodalmat okoz a tagállamok kritikus infrastruktúrájának részét képező információs rendszerek elleni terrortámadások lehetősége. Ez veszélyezteti a biztonságosabb információs társadalom, valamint a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség megvalósítását, ezért az Európai Unió szintjén kell fellépni ellene.
- (3) Az e fenyegetések elleni hatékony fellépéshez átfogó megközelítésre van szükség a hálózat- és információbiztonság tekintetében – amint azt az eEurópa cselekvési terv, a Bizottság „Hálózat- és információbiztonság: megközelítési javaslat egy európai politikára” című közleménye és a hálózat- és információbiztonság terén alkalmazandó közös megközelítésről és különös intézkedésekről szóló, 2002. január 28-i tanácsi állásfoglalás⁽²⁾.
- (4) Az Európai Parlament 2001. szeptember 5-i állásfoglalása kiemelte az információbiztonsághoz kapcsolódó problémák fokozottabb megismertetésének és a gyakorlati segítségnyújtásnak a szükségességét is.

(5) A tagállami jogszabályokban az e területre vonatkozó szabályozottság mértékében és módjában fennálló jelentős különbségek akadályozhatják a szervezett bűnözés és a terrorizmus elleni küzdelmet, és megnehezíthetik a hatékony rendőrségi és igazságügyi együttműködést az információs rendszerek elleni támadások területén. A modern információs rendszerek transznacionális és határok nélküli jellegéből adódóan az ilyen rendszerek elleni támadások gyakran szintén határokon átnyúló természetűek, így hangsúlyozottan sürgős szükség van a büntető jogszabályok e területen történő közelítését célzó további intézkedésekre.

(6) A Tanács és a Bizottság cselekvési terve az Amszterdami Szerződés a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségre vonatkozó rendelkezéseinek⁽³⁾ lehető legjobb végrehajtásáról, az 1999. október 15–16-i tamperei Európai Tanács, a 2000. június 19–20-i santa maria da feira-i Európai Tanács, a Bizottság „eredménytáblája” és az Európai Parlament 2000. május 19-i állásfoglalása rámutat, illetve felhív a csúcstechnológiával kapcsolatos bűnözés elleni jogalkotói fellépés szükségességére, beleértve a fogalmak, tényállási elemek és szankciók közös meghatározását is.

(7) A nemzetközi szervezetek által végzett munkát, különösen az Európa Tanács által a büntető jogszabályok közelítése terén, valamint a G-8 által a csúcstechnológiával kapcsolatos bűnözés területén történő transznacionális együttműködéssel kapcsolatban végzett munkát, ki kell egészíteni az Európai Unión belül e téren kialakítandó közös szemlélettel. E felhívás további kidolgozásra került a Bizottságnak a „Biztonságosabb információs társadalom megteremtése az információs infrastruktúrák biztonságának javítása és a számítógépes bűncselekmények elleni küzdelem révén” című, a Tanácshoz, az Európai Parlamenthez, a Gazdasági és Szociális Bizottsághoz és a Régiók Bizottságához címzett közleményében.

(8) Az információs rendszerek elleni támadásokhoz kapcsolódó bűncselekmények területén való lehető legnagyobb mértékű rendőrségi és igazságügyi együttműködés, valamint a szervezett bűnözés és a terrorizmus elleni küzdelemhez való hozzájárulás érdekében közelíteni kell egymáshoz a büntető jogszabályokat az információs rendszerek elleni támadások területén.

⁽¹⁾ HL C 300. E, 2003.12.11., 26. o.

⁽²⁾ HL C 43., 2002.2.16., 2. o.

⁽³⁾ HL C 19., 1999.1.23., 1. o.

- (9) Az Európa Tanácsnak az egyének személyes adataik gépi feldolgozása során való védelméről szóló, 1981. január 28-i egyezményét az összes tagállam megerősítette. Az e kerethatározat végrehajtásával összefüggésben feldolgozott személyes adatokat az említett egyezmény elveinek megfelelő védelemben kell részesíteni.
- (10) A kerethatározat alkalmazása során a tagállamok következetes szemléletének biztosítása érdekében fontos a közös meghatározások kialakítása e téren, különösen az információs rendszerek és a számítógépes adatok vonatkozásában.
- (11) A bűncselekmények tényállási elemeivel kapcsolatos közös szemléletet kell kialakítani az információs rendszerhez való jogsértő hozzáférés, valamint a rendszerekbe, illetve adatokba való jogsértő beavatkozás egységesen meghatározott bűncselekményeiről való rendelkezés révén.
- (12) A számítógépes bűncselekmények elleni küzdelem érdekében minden tagállamnak biztosítani kell a hatékony igazságügyi együttműködést a 2., 3., 4. és 5. cikkben említett elkövetési magatartástípusokkal elkövetett bűncselekmények tekintetében.
- (13) A büntetőjogi túlszabályozást – különösen az enyhébb esetekben –, továbbá a jogosultak és engedéllyel rendelkező személyek büntetőjogi felelősségre vonását el kell kerülni.
- (14) Szükséges, hogy a tagállamok szankciókat állapítsanak meg az információs rendszerek elleni támadásokra. A megállapított szankcióknak hatékonynak, arányosnak és visszatartó erejűnek kell lenniük.
- (15) Helyénvaló súlyosabb büntetéseket megállapítani, amennyiben az információs rendszer elleni támadást valamely bünszervezet keretén belül követték el, az Európai Unió tagállamaiban a bünszervezetben való részvétel bűncselekménnyé nyilvánításáról szóló, 1998. december 21-i 98/733/IB együttes fellépés⁽¹⁾ meghatározása szerint. Szintén helyénvaló a súlyosabb büntetések megállapítása, amennyiben az ilyen támadás súlyos kárt vagy alapvető érdeksérelmet okozott.
- (16) Az információs rendszerek elleni támadásokkal szemben történő hatékony fellépés érdekében a tagállamok közötti együttműködés céljaira is meg kell hozni a szükséges

intézkedéseket. Ennélfogva, az információcsera céljaira a tagállamoknak célszerű igénybe venni a csúcstechnológiához kapcsolódó bűnözés elleni küzdelem érdekében 24 órás szolgálatot biztosító kapcsolattartókról szóló, 2001. június 25-i tanácsi ajánlásban⁽²⁾ említett operatív kapcsolattartók meglévő hálózatát.

- (17) Mivel e kerethatározat célkitűzéseit – vagyis annak biztosítását, hogy az információs rendszerek elleni támadásokat minden tagállamban hatékony, arányos és visszatartó erejű szankciókkal büntessék, valamint a lehetséges nehézségek kiküszöbölése révén javítsák és ösztönözzék az igazságügyi együttműködést – a tagállamok nem tudják megfelelően megvalósítani, mivel a szabályoknak egységesnek és összeegyeztethetőnek kell lenniük, és ezért az Unió szintjén jobban megvalósíthatóak, az EK-Szerződés 5. cikkében meghatározott szubszidiaritás elvével összhangban az Unió intézkedéseket hozhat. Az említett cikkben meghatározott arányosság elvének megfelelően e kerethatározat nem haladja meg az említett célok eléréséhez szükséges mértéket.
- (18) E kerethatározat tiszteletben tartja az alapvető jogokat, és betartja az Európai Unióról szóló szerződés 6. cikkében elismert és az Európai Unió alapjogi chartájában, nevezetesen annak II. és VI. fejezetében kifejezésre juttatott alapelveket,

ELFOGADTA EZT A KERETHATÁROZATOT:

1. cikk

Fogalommeghatározások

E kerethatározat alkalmazásában a következő fogalommeghatározásokat kell alkalmazni:

- a) „Információs rendszer”: minden olyan eszköz vagy összekapcsolt vagy kapcsolódó eszközökből álló eszközcsoport, amelyek közül egy vagy több valamely program alapján automatikus adatfeldolgozást hajt végre számítógépes adatokon, valamint a működése, használata, védelme és karbantartása céljából általa tárolt, feldolgozott, helyreállított vagy továbbított számítógépes adatokon.
- b) „Számítógépes adatok”: tények, információk vagy fogalmak megjelenítése olyan formában, amely alkalmassá teszi azokat egy információs rendszer általi feldolgozásra, beleértve azon programokat is, amelyek alkalmasak valamely funkciónak egy információs rendszer általi elvégzésére.
- c) „Jogi személy”: bármely jogalany, amely az alkalmazandó nemzeti jog szerint ilyen jogállással bír, kivéve az államokat, illetve az állami hatáskört gyakorló közjogi szervezeteket, valamint a nemzetközi közjogi szervezeteket.

⁽¹⁾ HL L 351., 1998.12.29., 1. o.

⁽²⁾ HL C 187., 2001.7.3., 5. o.

d) „Jogosulatlanul”: olyan módon történő hozzáférés vagy beavatkozás a rendszerbe, amelyet a rendszernek vagy a rendszer részének tulajdonosa vagy egyéb jogosultja nem engedélyezett, vagy amelyet a nemzeti jogszabályok nem tesznek lehetővé.

2. cikk

Információs rendszerekhez való jogsértő hozzáférés

(1) Minden tagállam meghozza a szükséges intézkedéseket annak érdekében, hogy a valamely információs rendszerhez vagy annak egy részéhez való szándékos jogosulatlan hozzáférés legalább a jelentősebb esetekben bűncselekménynek minősüljön.

(2) Minden tagállam határozhat úgy, hogy az (1) bekezdésben említett magatartás csak akkor minősüljön bűncselekménynek, ha azt valamely biztonsági intézkedés megsértése által követték el.

3. cikk

Rendszerbe való jogsértő beavatkozás

Minden tagállam meghozza a szükséges intézkedéseket annak érdekében, hogy valamely információs rendszer működésének számítógépes adatok bevitel, továbbítása, megromlása, törlése, minőségi rontása, megváltoztatása, elrejtése vagy hozzáférhetetlenné tétele révén történő szándékos és súlyos akadályozása vagy megszakítása, amennyiben azt jogosulatlanul követték el, legalább a jelentősebb esetekben bűncselekménynek minősüljön.

4. cikk

Adatokba való jogsértő beavatkozás

Minden tagállam meghozza a szükséges intézkedéseket annak érdekében, hogy a valamely információs rendszer számítógépes adatainak szándékos törlése, megromlása, minőségi rontása, megváltoztatása, elrejtése vagy hozzáférhetetlenné tétele legalább a jelentősebb esetekben bűncselekménynek minősüljön.

5. cikk

Felbujtás, bűnrészesség, bűnpártolás és kísérlet

(1) Minden tagállam biztosítja, hogy a 2., 3. és 4. cikkben említett bármely bűncselekményre való felbujtás, az abban való bűnrészesség, valamint bűnpártolás bűncselekménynek minősüljön.

(2) Minden tagállam biztosítja, hogy a 2., 3. és 4. cikkben említett bűncselekmények elkövetésére irányuló kísérlet bűncselekménynek minősüljön.

(3) Minden tagállam határozhat úgy, hogy a 2. cikkben említett bűncselekmények esetében nem alkalmazza a (2) bekezdést.

6. cikk

Szankciók

(1) Minden tagállam meghozza a szükséges intézkedéseket annak érdekében, hogy a 2., 3., 4. és 5. cikkben említett bűncselekményeket hatékony, arányos és visszatartó erejű büntetőjogi szankciókkal sújtsák.

(2) Minden tagállam meghozza a szükséges intézkedéseket annak érdekében, hogy a 3. és 4. cikkben említett bűncselekmények maximálisan legalább 1 évtől 3 évig terjedő szabadságvesztéssel legyenek büntetendők.

7. cikk

Súlyosbító körülmények

(1) Minden tagállam meghozza a szükséges intézkedéseket annak érdekében, hogy a 2. cikk (2) bekezdésében említett bűncselekmény, valamint a 3. és 4. cikkben említett bűncselekmény maximálisan legalább 2 évtől 5 évig terjedő szabadságvesztéssel legyen büntetendő, amennyiben azokat a 98/733/IB együttes fellépés meghatározása szerint bűnszervezetben követték el, az ott említett büntetési tételtől eltekintve.

(2) A tagállamok meghozhatják az (1) bekezdésben említett intézkedéseket is, amennyiben a bűncselekmény súlyos kárt vagy alapvető érdeksérelmet okozott.

8. cikk

A jogi személyek felelőssége

(1) Minden tagállam meghozza a szükséges intézkedéseket annak biztosítása érdekében, hogy a jogi személyek felelősségre vonhatók legyenek a 2., 3., 4. és 5. cikkben említett azon cselekményekért, amelyeket akár saját nevükben eljárva, akár a jogi személy valamely szervének tagjaként eljárva olyan személy követett el a jogi személy javára, aki a jogi személyen belül vezető tisztséget tölt be, amely a következők egyikén alapul:

a) a jogi személy képviselőjének joga; vagy

b) a jogi személy nevében történő döntéshozatal joga; vagy

c) a jogi személyen belüli ellenőrzés joga.

(2) Az (1) bekezdésben meghatározott eseteken túlmenően a tagállamok gondoskodnak arról, hogy a jogi személy felelősségre vonható legyen akkor is, amennyiben az (1) bekezdésben említett személy által gyakorolt felügyelet vagy ellenőrzés hiánya tette lehetővé, hogy egy neki alárendelt személy az adott jogi személy javára a 2., 3., 4. és 5. cikkben említett valamely bűncselekményt elkövesse.

(3) A jogi személynek az (1) és (2) bekezdés alapján fennálló felelőssége nem zárja ki a büntetőeljárás azok ellen a természetes személyek ellen, akik a 2., 3., 4. és 5. cikkben említett bűncselekmények valamelyikét tettesként, felbujtóként vagy bűnsegédként követik el.

9. cikk

A jogi személyekkel szemben alkalmazható szankciók

(1) Minden tagállam megteszi a szükséges intézkedéseket annak érdekében, hogy a 8. cikk (1) bekezdése alapján felelősséggel tartozó jogi személy hatékony, arányos és visszatartó erejű szankciókkal legyen sújtható, beleértve a büntetőjogi és nem büntetőjogi pénzbírságokat és egyéb szankciókat is, mint például:

- a) kizárás az állami kedvezményekből és támogatásokból;
- b) kereskedelmi tevékenység folytatásától való átmeneti vagy végleges eltiltás;
- c) bírósági felügyelet alá helyezés; vagy
- d) bíróság által elrendelt felszámolás.

(2) Minden tagállam meghozza a szükséges intézkedéseket annak érdekében, hogy a 8. cikk (2) bekezdése értelmében felelősséggel tartozó jogi személyt hatékony, arányos és visszatartó erejű szankciókkal vagy intézkedésekkel legyen sújtható.

10. cikk

Joghatóság

(1) Minden tagállam megállapítja joghatóságát a 2., 3., 4. és 5. cikkben említett bűncselekmények tekintetében, amennyiben a bűncselekményt:

- a) egészben vagy részben a területén követték el; vagy
- b) az elkövető az adott tagállam állampolgára; vagy
- c) olyan jogi személy javára követték el, amelynek tevékenysége végzésének központja a tagállam területén található.

(2) Az (1) bekezdés a) pontja szerinti joghatóság megállapításakor minden tagállam biztosítja, hogy a joghatóság kiterjedjen azokra az esetekre, amelyekben

- a) az elkövető a bűncselekmény elkövetésekor fizikailag jelen van az adott állam területén, függetlenül attól, hogy a bűncselekmény a területén található információs rendszer ellen irányul-e; vagy
- b) a bűncselekmény a területén található információs rendszer ellen irányul, függetlenül attól, hogy az elkövető a bűncselekmény elkövetésekor fizikailag jelen van-e az adott állam területén.

(3) Minden olyan tagállam, amely nemzeti joga alapján nem adja ki vagy nem adja át a saját állampolgárát, megteszi a szükséges intézkedéseket joghatóság megállapítására és – adott esetben – a büntetőeljárás lefolytatására a 2., 3., 4. és 5. cikkben említett bűncselekményekre vonatkozóan, amennyiben a bűncselekményt a saját állampolgára a területén kívül követte el.

(4) Amennyiben a bűncselekmény egynél több tagállam joghatósága alá tartozik és az érintett tagállamok bármelyike ugyanazon tények alapján jogszerűen büntetőeljárás indíthat, akkor azzal a céllal, hogy amennyiben lehetséges, az eljárásokat egy tagállam folytassa le, az érintett tagállamoknak együtt kell működniük annak eldöntésében, hogy melyikük fog eljárást indítani az elkövető ellen. E célból a tagállamok bármely, az Európai Unión belül létrehozott szervhez vagy mechanizmushoz folyamodhatnak az igazságügyi hatóságaik közötti együttműködés megkönnyítése és intézkedéseik összehangolása érdekében. A megadott sorrendben az alábbi tényezők vehetők figyelembe:

- az az illetékes tagállam, amelynek területén a bűncselekményeket az (1) bekezdés a) pontja és a (2) bekezdés szerint elkövették,
- az az illetékes tagállam, amelynek az elkövető az állampolgára,
- az az illetékes tagállam, amelynek területén az elkövetőt megtalálták.

(5) A tagállamok határozhatnak úgy, hogy nem alkalmazzák vagy csak egyedi esetekben vagy különleges körülmények fennállása esetén alkalmazzák az (1) bekezdés b) és c) pontjában a joghatóságra vonatkozóan meghatározott szabályokat.

(6) A tagállamok tájékoztatják a Tanács Főtitkárságát és a Bizottságot, amennyiben az (5) bekezdés alkalmazásáról határoznak, és adott esetben közlik, hogy a határozatot mely egyedi esetekben vagy különleges körülmények között alkalmazzák.

11. cikk

Információcsere

(1) A tagállamok biztosítják, hogy a 2., 3., 4. és 5. cikkben említett bűncselekményekre vonatkozó információk cseréjének céljára és az adatvédelmi szabályokkal összhangban, a meglévő, a hét minden napjának huszonnégy órájában rendelkezésre álló operatív kapcsolattartási hálózatot igénybe veszik.

(2) Az általa az információs rendszerek elleni támadásokhoz kapcsolódó bűncselekményekre vonatkozó információ cseréjére kijelölt kapcsolattartóról minden tagállam tájékoztatja a Tanács Főtitkárságát és a Bizottságot. A Főtitkárság továbbítja ezt az információt a többi tagállamhoz.

12. cikk

Végrehajtás

(1) A tagállamok megteszik a szükséges intézkedéseket annak érdekében, hogy e kerethatározatnak rendelkezéseinek 2007. március 16-án megfeleljenek.

(2) A tagállamok 2007. március 16-án eljuttatják a Tanács Főtitkárságának és a Bizottságnak azoknak a rendelkezéseknek a szövegét, amelyekkel az e kerethatározatban előírt kötelezettségeket nemzeti jogukba átültetik. Az e tájékoztatás alapján elkészített jelentés és a Bizottság által készített írásbeli jelentés alapján a Tanács 2007. szeptember 16-án megvizsgálja, hogy a tagállamok mennyiben felelnek meg e kerethatározat rendelkezéseinek.

13. cikk

Hatálybalépés

Ez a kerethatározat az *Európai Unió Hivatalos Lapjában* való kihirdetésének napján lép hatályba.

Kelt Brüsszelben, 2005. február 24-én.

a Tanács részéről
az elnök
N. SCHMIT