# Az Európai Gazdasági és Szociális Bizottság véleménye – A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Az 5G biztonságos kiépítése az EU-ban –Az uniós eszköztár alkalmazása

*[COM(2020) 50 final]*

(2020/C 429/37)

Előadó: **Alberto MAZZOLA**

Társelőadó: **Dumitru FORNEA**



| | |
|---|---|
| Felkérés: | Európai Bizottság, 2020.3.9. |
| Jogalap: | az Európai Unió működéséről szóló szerződés 304. cikke |
| Illetékes szekció: | „Közlekedés, energia, infrastruktúra és információs társadalom” szekció |
| Elfogadás a szekcióülésen: | 2020.9.3. |
| Elfogadás a plenáris ülésen: | 2020.9.16. |
| Plenáris ülés száma: | 554. |
| A szavazás eredménye: (mellette/ellene/tartózkodott) | 217/0/2 |



## 1. **Következtetések és ajánlások**

1.1. Az EGSZB üdvözli a tagállamok és az Európai Bizottság arra irányuló kezdeményezését, hogy ellenőrizzék az 5G ökoszisztéma bevezetésének biztonságosságával kapcsolatos stratégiai, technikai és kulcsfontosságú intézkedéscsomag következtetéseiben javasolt intézkedések sorozatának tagállamok általi végrehajtását.

1.2. Az EGSZB úgy véli, hogy – az 5G alkalmazások növekvő bonyolultsága és sokszínűsége fényében – (az Európai Bizottság a következő kapcsolódási célokat tűzte ki 2025-re: az iskoláknak, egyetemeknek, kutatóközpontoknak, kórházaknak, kulcsfontosságú közszolgáltatóknak és a nagy digitális intenzitást igénylő vállalkozásoknak hozzáférést kell biztosítani a másodpercenkénti egy gigabites internetes adatletöltési/-feltöltési sebességhez; a városi és a vidéki háztartásoknak biztosítani kell a másodpercenként legalább 100 megabites letöltési sebességet; míg a városi területeknek, a főbb utaknak és vasútvonalaknak folyamatos 5G lefedettséggel kell rendelkezniük),az 5G ökoszisztémának, valamint az Európai Bizottság hatáskörébe tartozó, az 5G hálózatok kiberbiztonságát és a változatos 5G értékláncnak a védelmét garantáló intézkedéseknek, a műszaki szabványosításnak és tanúsításnak, a közvetlen külföldi befektetéseknek, a piacvédelemnek és a versenynek, a közszolgáltatási kötelezettségeknek, a beszerzéseknek és az informatikai diplomáciának a szóban forgó ellenőrzése meg kell, hogy feleljen a geopolitikai, az infrastruktúrára és az adatokra vonatkozó biztonsági előírásoknak, valamint az egészségbiztonságnak, az EUMSZ 168. cikke (1) bekezdésének megfelelően is.

1.3. Az EGSZB szerint fontos, hogy az európai 5G ökoszisztéma biztosítsa az integritást, a titoktartást, a vezetési és üzemeltetési felelősséget, a biztonságot, az ellátás helyettesíthetőségét, a hardveres és a szoftveres alkatrészek interoperabilitását, a közös műszaki és szabályozási szabványokat, a szolgáltatás folytonosságát, az adatáramlás folytonosságának megbízhatóságát és az adatvédelmet, minden terület lefedettségét még a ritkán lakott területeken is, a felhasználó mint a digitális piac aktív alanya felé történő kommunikáció egyértelműségét, valamint az ICNIRP irányelveinek dinamikus betartását a lakosság egészségének védelme érdekében, a sugárzás lehető legnagyobb mértékű csökkentése mellett. Ennek megfelelően az ICNIRP (Nemzetközi Nemionizáló Sugárvédelmi Bizottság) frissítette az 1998. évi iránymutatások rádiófrekvenciás elektromágneses mezőkre vonatkozó részét. Ez a dokumentum bemutatja ezeket a felülvizsgált irányelveket, amelyek védelmet nyújtanak az emberek számára a 100 kHz-től 300 GHz-ig terjedő, elektromágneses mezőknek való kitettséggel szemben. Health Phys. 118(5):483–524; 2020- MARCH 2020. Az ICNIRP (2020) számos változtatást hajtott végre annak biztosítása érdekében, hogy az olyan új technológiák, mint az 5G, a jelenlegi várakozásainktól függetlenül ne tudjanak kárt okozni.

1.4. Az EGSZB arra kéri az Európai Bizottságot, hogy szigorúan kövesse nyomon az 5G kiépítésének és tényleges felhasználásának előrehaladását, és sürgeti a tagállamokat, hogy gyorsítsák fel a folyamatot és biztosítsák a felelősségteljes végrehajtást, figyelembe véve a biztonság és a védelem minden szempontját, ideértve az 5G technológiáknak a lakosság egészségére és az élő ökoszisztémákra gyakorolt hatásával kapcsolatos szempontokat, a társadalmi-gazdasági hatásokat, a versenyképességre, az oktatásra és a képzésre gyakorolt hatásokat, illetve az alapvető jogok tiszteletben tartásának garantálását.

1.5. Az EGSZB arra kéri az EU-t, hogy töltsön be globális vezető szerepet az 5G mobiltechnológia következő generációjában, amelyet olyan biztonságos digitális infrastruktúrával látnak el, amely Európa új, korszerű ipari stratégiájának szilárd építőeleme az új mobil összeköttetések radikális megváltoztatásán keresztül, valamint óriási dinamikus potenciállal rendelkezik, és képes növelni a termelékenységet, a gazdaságot és bővíteni a polgárok számára nyújtott szolgáltatásokat.

1.6. Az EGSZB különösen fontosnak tartja a beszállítók kockázati profiljának értékelését és az összehangolt uniós kockázatértékelésben kritikusként és érzékenyként meghatározott kulcsfontosságú eszközök tekintetében megfelelő korlátozások – többek között a hatékony kockázatcsökkentéshez és a kötelezettségek meghatározásához szükséges kizárások – alkalmazását a magas kockázatúnak tekintett beszállítók esetében.

1.7. Az EGSZB véleménye szerint elengedhetetlen, hogy Európa középtávon ezen a területen az autonómiára és az önellátásra összpontosítson azáltal, hogy erőteljesen támogatja a kutatást, illetve számos európai vállalatot. Az EGSZB fontosnak tartja a digitális K+I-re fordított közösségi források növelését, valamint az üzemeltetők és a beszállítók új műszaki biztonsági funkciókra fordított beruházásainak támogatását, amellyel párhuzamosan a piacnak fel kell tudnia ismerni és jutalmaznia kell mindazon kezdeményezéseket, amelyek célja a rendszerek biztonságának és ellenálló képességének növelése.

1.8. Fontos garantálni a biztonságot az összes tagállam számára, többek között a kutatóközpontok fenntartása révén az EU számos területén: az EGSZB emellett megismétli arra vonatkozó javaslatát, hogy minden országnak legalább két beszállítója legyen, amelyek közül legalább az egyik európai, és amely képes garantálni az adatok politikai biztonságát és az egészségügyi követelmények betartását.

1.9. Az EGSZB szerint a nemzeti szabályozó hatóságok hatáskörével és a távközlési szolgáltatók szerepével kapcsolatos megfelelő intézkedések mellett nagyobb hangsúlyt kell fektetni a felhasználók, a polgárok és az érintett civil társadalmi szervezetek rendelkezésére álló, korlátozott és nem hatékony eszközökre, hogy elősegítsük a fogyasztói szerepvállalást, és kiépítsük arra való képességüket, hogy proaktív szereplőkké váljanak a piacon.

1.10. Az Európai Bizottságnak, az EP-nek, a Tanácsnak, valamint a tagállamok kormányainak és parlamentjeinek demokratikus keretet kell biztosítaniuk a konzultációhoz, ahol tudományos vagy technológiai kérdéseket, jogi garanciákat és az érintett intézményeknek a civil társadalom kérdéseire adott válaszait ismertethetik a nyilvánossággal.

1.11. Az EGSZB az európai technológiai diplomácia megerősítését javasolja annak érdekében, hogy az EU kiegyensúlyozottabb, kölcsönös feltételeket biztosíthasson a kereskedelem és a beruházások számára, különös tekintettel a piacra jutásra, a támogatásokra, a közbeszerzésre, a technológiaátadásra, az ipari tulajdonra, valamint a szociális és környezetvédelmi normákra.

## 2. **Bevezetés**

2.1. Az 5G hálózatok biztonsága stratégiai jelentőségű kérdés a polgárok és a vállalatok, az egész egységes piac és az EU technológiai szuverenitása számára. Az Európai Bizottság már 2013-ban elindította az EU kiemelt kezdeményezését az 5G köz- és magánszféra partnerségének (5G PPP) létrehozásával az 5G technológiával kapcsolatos kutatás és innováció felgyorsítása érdekében.

2.2. Mivel a várható bevételek összege 2025-re a becslések szerint meghaladja az 100 milliárd EUR-t, nyilvánvaló, hogy az 5G technológia kulcsfontosságú szerepet tölt be Európa globális versenyképessége szempontjából, és kiberbiztonsága alapvetően fontos az Unió stratégiai autonómiájának biztosításához.

2.3. Az 5G hálózatok a jelenlegi negyedik generációs (4G) hálózati technológiákon és száloptikás infrastruktúrán alapulnak, egyúttal új szolgáltatási kapacitásokat és központi infrastruktúrát biztosítanak, illetve kulcsfontosságú tényezőnek számítanak az uniós gazdaság nagy része számára, mivel a belső piac működéséhez, valamint olyan létfontosságú gazdasági és társadalmi funkciók, mint például az energia, a közlekedés, a banki és az egészségügyi szolgáltatások, valamint a mezőgazdasági és ipari termelési, forgalmazási és fogyasztási rendszerek fenntartásához és kezeléséhez szükséges alapvető szolgáltatások széles skálájának gerincét képezik.

2.4. Az 5G hálózatok központi szerepe az uniós gazdaság és társadalom digitális átalakulásának elérésében, a digitális ökoszisztéma alapját képező infrastruktúrák összekapcsoltsága és transznacionális jellege, valamint az érintett fenyegetések határokon átnyúló jellege azt jelenti, hogy az 5G hálózatokat érintő bármely jelentős sebezhetőség és/vagy kiberbiztonsági esemény az Unió egészét érintené. Ezért olyan intézkedéseket kell hozni, amelyek az 5G hálózatok magas szintű kiberbiztonságának alapját képezik.

2.5. 2016-ban az Európai Bizottság – egy kezdeményezéskomplexum keretében, amely „Az összekapcsoltság a versenyképes digitális egységes piac szolgálatában: Úton a gigabitalapú európai információs társadalom felé” című közleménytől ([1]) ([2]) kezdve magában foglalja többek között az elektronikus hírközlés szabályozási keretének ([3]) és az Európai Elektronikus Hírközlési Szabályozók Testületének (BEREC) feladatainak ([4]) reformját, az IKT digitális egységes piac érdekében történő szabványosításának prioritásait ([5]), valamint az internetes kapcsolat helyi közösségekben való elősegítésére irányuló intézkedéseket ([6]) – elfogadta az EU 5G-vel kapcsolatos cselekvési tervét ([7]), amellyel kapcsolatban az EGSZB pozitívan nyilatkozott ([8]). Ennek a cselekvési tervnek a célja, hogy fokozza az EU erőfeszítéseit az 5G infrastruktúrának és szolgáltatásoknak a digitális egységes piacon való bevezetése érdekében. Ehhez ütemtervet állapít meg az EU 5G infrastruktúrájába történő állami és magánbefektetésekhez, illetve megfogalmaz egy célkitűzést is az 5G kereskedelmi hálózatok 2020 során megvalósuló elindítására vonatkozóan.

2.6. Az Európai Bizottság ajánlásában ([9]) szereplő fogalommeghatározás szerint „5 G hálózatok”: „a mobil és vezeték nélküli kommunikációs technológiákkal kapcsolatos releváns hálózati infrastrukturális elemek összessége, amelyeket olyan kiváló teljesítményjellemzőkkel rendelkező konnektivitási szolgáltatásokban és hozzáadott értéket képviselő szolgáltatásokban alkalmaznak, mint a nagyon nagy adatátviteli sebesség és kapacitás, az alacsony válaszidő, a nagy fokú megbízhatóság vagy az összekapcsolt eszközök nagy számának támogatása”.

2.7. Az ajánlás szerint az Európai Bizottság támogatni fogja az EU 5G kiberbiztonsági megközelítésének végrehajtását, és a tagállamok kérésének megfelelően törekszik az 5G infrastruktúra és az ellátási lánc biztonságának garantálására, adott esetben a rendelkezésére álló összes alábbi eszköz felhasználásával:

— távközlési, multimédiás és kiberbiztonsági szabályok,

— uniós szintű szabványosítás és tanúsítási koordináció,

— a közvetlen külföldi befektetések ellenőrzési keretrendszere az európai 5G ellátási lánc védelme érdekében,

— piacvédelmi eszközök,

— versenyszabályok,

— közbeszerzések, biztosítva a biztonsági szempontok megfelelő figyelembevételét,

— uniós finanszírozási programok, biztosítva, hogy a kedvezményezettek megfeleljenek a vonatkozó biztonsági követelményeknek.

2.8. 2019 júliusában a tagállamok bemutatták a nemzeti kockázatértékeléseik eredményeit a kiberbiztonsági irányelv ([10]) által megkövetelt (az egyes tagállamok képviselőiből álló) együttműködési csoportnak, az Európai Bizottság-nak és az ENISA-nak, a fő tevékenységekkel, a fenyegetésekkel és a sebezhetőségekkel kapcsolatos információkkal az 5G infrastruktúrára és a fő kockázati forgatókönyvekre vonatkozó ISO/IEC 27005 szabvány szerint, ismertetve azokat a lehetséges módszereket, amelyek révén a fenyegető szereplők kihasználhatják egy tevékenység bizonyos sebezhetőségét: ezek a nemzeti értékelések képezték a későbbi összehangolt értékelés és a lehetséges kockázatcsökkentő intézkedések közös „eszközkészletének” alapját.

2.9. 2019 októberében a Kiberbiztonsági Együttműködési Csoport az Európai Bizottság és az ENISA támogatásával jelentést tett közzé az ötödik generációs 5G hálózatok kiberbiztonsági kockázatainak uniós szintű összehangolt értékeléséről, amely számos fontos biztonsági kihívást azonosított a szoftverek, alkalmazások és szolgáltatások kulcsfontosságú technológiai újításaival, a szolgáltatóknak az 5G hálózatok létrehozásában és használatában betöltött szerepével, valamint az egyes beszállítóktól való függés mértékével kapcsolatban:

— támadásoknak való fokozott kitettség, illetve az ilyen támadások elkövetői potenciális hozzáférési pontjai számának növekedése,

— fokozott érzékenység az 5G hálózatok új architekturális jellemzői és funkcionalitása iránt,

— a fenyegetést jelentő szereplők által kihasználható támadási útvonalak számának növekedésével párhuzamosan a mobilhálózat-üzemeltetők beszállítóktól való függésével kapcsolatos kockázatok,

---

([1]) Az EUMSZ 168. cikkének (1) bekezdése: „Az Unió fellépése, amely kiegészíti a nemzeti politikákat …”.
([2]) COM(2016) 587.
([3]) COM(2016) 590.
([4]) COM(2016) 591.
([5]) COM(2016) 176.
([6]) COM(2016) 589.
([7]) COM(2016) 588.
([8]) HL C 125., 2017.4.21., 74. o.
([9]) Az Európai Bizottság (EU) 2019/534 ajánlása (2019. március 26.) az *5G hálózatok kiberbiztonságáról* (HL L 88., 2019.3 29., 42. o.).
([10]) Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19., 1. o.).

— az egyes beszállítók kockázati profiljának relevanciája az esetleges EU-n kívüli interferenciák szempontjából,

— a beszállítóktól való nagy fokú függésből fakadó megnövekedett kockázatok, amelyek a kereskedelmi vagy egyéb feszültségek okozta lehetséges beszállítási zavarokból fakadhatnak,

— a hálózatok rendelkezésre állását és integritását fenyegető veszélyek a biztonság, a titoktartás és a magánélet védelme terén.

2.10. Mindezek a kihívások új biztonsági paradigmát hoznak létre, amely megköveteli az ágazatra és annak ökoszisztémájára alkalmazandó jelenlegi politikai és biztonsági keret felülvizsgálatát, valamint rákényszeríti a tagállamokat, hogy tegyék meg a szükséges kockázatcsökkentő intézkedéseket.

2.11. Az ENISA 2019. november 21-én jelentést tett közzé az *5G hálózatokkal kapcsolatos fenyegetettségre* vonatkozóan, amelyben értékelte a mobil távközlési hálózatok ötödik generációjára leselkedő veszélyeket, valamint szerepeltette az uniós tagállamok jelentését.

2.12. 2020. január 29-én a Kiberbiztonsági Együttműködési Csoport közzétette a „*Cybersecurity of 5G networks – EU toolbox of risk mitigating measures*" (Az 5G hálózatok kiberbiztonsága – az EU kockázatcsökkentő eszközkészlete) ([11]) című javaslatcsomagját az 5G hálózatok legfontosabb kiberbiztonsági kockázatainak mérséklése céljából, amelyben iránymutatásokat ad azoknak az intézkedéseknek a kiválasztására, amelyeknek prioritást kell élvezniük a nemzeti és uniós szintű mérséklési tervekben. Ugyanezen a napon az Európai Bizottság közleményt fogadott el az eszköztár támogatásáról ([12]), amely e vélemény tárgyát képezi.

2.13. Az 5G hálózati infrastruktúra fő szereplői:

— polgárok, fogyasztók, az 5G végfelhasználói,

— mobilhálózat-üzemeltetők: olyan szervezetek, amelyek mobilhálózati szolgáltatásokat nyújtanak a felhasználók számára, hálózatuk harmadik felek segítségével történő kezelése útján,

— mobilhálózat-szolgáltatók: olyan szervezetek, amelyek szolgáltatásokat vagy infrastruktúrákat nyújtanak a mobilhálózat-üzemeltetők számára hálózataik kiépítése és/vagy kezelése céljából. Ebbe a kategóriába a következők tartoznak: telekommunikációs készülékek gyártói; harmadik fél beszállítók, például felhőinfrastruktúra-szolgáltatók, rendszerintegrátorok, biztonsági és karbantartási vállalkozók, átviteli berendezések gyártói,

— csatlakoztatott készülékek gyártói és kapcsolódó szolgáltatók: olyan szervezetek, amelyek 5G hálózatokra csatlakoztatható termékeket vagy szolgáltatásokat (például okostelefonok, csatlakoztatott járművek, e-egészségügy) és az ehhez kapcsolódó, az 5G vezérlési tervben tárolt szolgáltatási összetevőket kínálnak, a szolgáltatásalapú architektúra vagy a Mobile Edge Computing fogalommeghatározása szerint,

— egyéb érdekelt felek, többek között szolgáltatók és tartalomszolgáltatók.

Mindezek az érdekelt felek fontos érdekeltek a biztonságot illetően, mind az 5G hálózatok kiberbiztonságához való hozzájárulás, mind pedig potenciális belépési pontként vagy támadási felületként. Ezért fontos felmérni az 5G ökoszisztémán belüli helyzetükkel kapcsolatos kockázatokat.

2.14. A fenyegetések legfontosabb hagyományos kategóriái a titoktartást, az integritást és a rendelkezésre állást sértik. Konkrétan megállapítható, hogy az 5G hálózatokat célzó fenyegetési forgatókönyvek egy része különösen a következőkre vonatkozik:

— a helyi vagy globális 5G hálózat megszakadása (rendelkezésre állás),

— az adatforgalom kémlelése az 5G hálózati infrastruktúrában (titoktartás),

— az adatforgalom módosítása vagy átirányítása az 5G hálózati infrastruktúrában (integritás és/vagy titoktartás),

— egyéb digitális infrastruktúrák vagy információs rendszerek megsemmisítése vagy megváltoztatása az 5G hálózatokon keresztül (integritás és/vagy rendelkezésre állás).

2.15. Az államok vagy államok által támogatott szereplők által jelentett veszélyeket rendkívüli jelentőségűnek tekintik, mivel azok ténylegesen a legsúlyosabb és legvalószínűbb fenyegetést képviselik, ugyanis motivációik, szándékaik és mindenekelőtt képességeik révén képesek lehetnek tartós és kifinomult támadásokat folytatni az 5G hálózatok biztonságosságának veszélyeztetése érdekében.

([11]) https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5 g-networks-eu-toolbox-risk-mitigating-measures

([12]) https://ec.europa.eu/digital-single-market/en/news/secure-5 g-deployment-eu-implementing-eu-toolbox-communication-commission

Habár ezeknek a sebezhetőségeknek a nagy része nem csak az 5G hálózatokra jellemző, számuk és jelentőségük valószínűleg növekszik az 5G bevezetésével, mivel ez a technológia meglehetősen összetett, és a gazdaságok és társadalmak a jövőben nagyobb mértékben támaszkodnak majd erre az infrastruktúrára.

2.16. Különösen mivel az 5G hálózatok nagyrészt szoftveralapúak lesznek, a főbb biztonsági hibák, amelyek például a berendezésgyártók nem megfelelő szoftverfejlesztési folyamataiból fakadnak, megkönnyíthetik a szereplők számára, hogy szándékosan kiskapukat rejtsenek el a termékekben, és megnehezítsék azok felismerését. Ez megnövelheti annak az esélyét, hogy az ezekkel történő visszaéléseknek különösen súlyos és kiterjedt negatív hatásai legyenek. Míg a 4G kiberbiztonsági problémáit még nem sikerült teljes mértékben megoldani, az 5G problémák exponenciálisan növekedhetnek.

2.17. Vannak tehát olyan folyamat- vagy konfigurációs biztonsági rések, amelyeket figyelembe kell venni:

— az 5G hálózatok védelmére, megfigyelésére és karbantartására szakosodott és képzett személyzet hiánya,

— hiányosságok a megfelelő belső biztonsági ellenőrzésben, a felügyeleti gyakorlatban, a biztonsági irányítási rendszerekben és a kockázatkezelési gyakorlatban,

— nem megfelelő biztonsági vagy működési karbantartási eljárások, mint például a szoftverfrissítés/a javításkezelés az 5G hálózatokban,

— a 3GPP szabványok figyelmen kívül hagyása vagy helytelen végrehajtása,

— a hálózati tervezés vagy architektúra hiányosságai, ideértve a hatékony vészhelyzeti és folytonossági mechanizmusok hiányát, a nem megfelelő vagy helytelen konfigurációt, például a virtualizálásban, valamint az adminisztrációs vagy hozzáférési jogokban,

— a hálózati elemek helyi és távoli elérésének nem megfelelő kritériumai,

— a biztonsági követelmények elégtelensége a beszerzési folyamatban: ez a sebezhetőség a beszállítók kiválasztásának nem megfelelő stratégiáiban vagy a biztonság más szempontokkal szembeni prioritásának hiányában jelentkezhet.

2.18. Az egyes szállítók kockázati profilját több tényező alapján kell értékelni, amelyek többek között a következők: annak lehetősége, hogy a beszállítót egy EU-n kívüli ország beavatkozása veszélyezteti, amelyet elősegítenek a beszállító és az adott harmadik ország kormánya közötti szoros kapcsolatok; harmadik országbeli jogszabályok, különösen akkor, ha ott nincsenek jogalkotási vagy demokratikus fékek és ellensúlyok, ahol ennek következtében a vállalat EU-ban működő leányvállalatai elriaszthatók az uniós jogszabályok betartásától, vagy ha az EU és a szóban forgó harmadik ország között nincs biztonsági vagy adatvédelmi megállapodás; a beszállító vállalati tulajdonjogának jellemzői; a harmadik ország azon képessége, hogy bármilyen nyomást gyakoroljon, a berendezés előállítási helyének vonatkozásában is; a beszállítói kiberbiztonsági gyakorlatok általános minősége, ideértve az ellátási lánc feletti ellenőrzés mértékét és azt, hogy megfelelő prioritásként kezelik-e a biztonsági gyakorlatokat.

2.19. A tagállamok megállapodtak arról, hogy intézkedéseket hoznak a már azonosított kockázatokra és a lehetséges jövőbeli kockázatokra való megfelelő és arányos reagálás biztosításának érdekében. Különösen vállalták annak biztosítását, hogy képesek lesznek korlátozni, tiltani és/vagy előírni az 5G hálózati berendezések szállítására, terjesztésére és üzemeltetésére vonatkozó kockázatalapú megközelítésnek megfelelő konkrét követelményeket és feltételeket.

2.20. Ezt szem előtt tartva a tagállamoknak biztosítaniuk kell az alábbiakat:

— a mobilhálózat-üzemeltetők biztonsági követelményeinek szigorítása, például szigorú hozzáférés-ellenőrzés, a biztonságos működésre és ellenőrzésre vonatkozó szabályok, bizonyos funkciók kiszervezésének korlátozásai,

— a beszállítók kockázati profiljának objektív és világos kritériumok alapján történő értékelése; következésképpen az összehangolt uniós kockázatértékelésben kritikusként és érzékenyként meghatározott kulcsfontosságú eszközök tekintetében, az arányosság és a jogbiztonság elve alapján, megfelelő korlátozások – többek között a hatékony kockázatcsökkentéshez szükséges kizárások – alkalmazása a magas kockázatúnak tekintett beszállítók esetében,

— globálisan elismert és végrehajtott, konszenzuson alapuló biztonsági normák és bevált gyakorlatok bevezetése,

— az egyes üzemeltetők által meghatározott megfelelő többszörös értékesítési stratégia, hogy elkerüljék vagy korlátozzák az egyetlen beszállítótól vagy hasonló kockázati profilú beszállítóktól való nagyobb mértékű függőséget,

— a hozzáférés és a kezelés szigorú ellenőrzése, a hálózat biztonságos működtetése és ellenőrzése az 5G hálózat elemeinek és/vagy folyamatainak tanúsítása során. E stratégiának a tagállamok és az üzemeltetők által végzett kockázatelemzésen kell alapulnia, hogy a több forgalmazóra kiterjedő stratégia választása ne növelje az üzemeltető hálózatának kockázati szintjét,

— a beszállítók megfelelő szintű egyensúlya nemzeti szinten és a magas kockázatúnak ítélt beszállítóktól való függőség elkerülése, a berendezések fokozottabb interoperabilitásának előmozdítása révén,

— diverzifikált és fenntartható 5G ellátási lánc fenntartása a hosszú távú függőség elkerülése érdekében, teljes mértékben kihasználva az EU közvetlen külföldi befektetéseinek ellenőrzésére szolgáló eszközöket, a piacvédelmi eszközöket, a versenyszabályokat és az EU beszerzésekre vonatkozó szabályait,

— az EU belső képességeinek erősítése az 5G és az 5G utáni technológiák terén a vonatkozó uniós programok és finanszírozások felhasználásával; tagállamok közötti koordináció a szabványosításban a „tesztelési" és „ellenőrzési" képességek megerősítésével; konkrét biztonsági célok elérése; releváns uniós tanúsítási rendszerek kifejlesztése az informatikai biztonsági jogszabályok alapján, valamint az interoperabilitás elősegítése.

2.21. Amint az Európai Bizottság többször hangsúlyozta, az európai belső piac nyitott és az is marad mindazok számára, akik Európába tartanak, mindaddig, amíg mindenki tiszteletben tartja az objektív kritériumokon alapuló egyértelmű és szigorú szabályokat.

2.22. A Tanács 2020. június 6-án hangsúlyozta a digitális szuverenitás és együttműködés megerősítésének fontosságát az EU-ban, valamint a szinergiák létrehozását olyan uniós programokon keresztül, mint például az Európai Hálózatfinanszírozási Eszköz és a Digitális Európa program, a digitális készségek és az adatgazdaság fejlesztése, a mesterséges intelligencia és az informatikai biztonság fontossága, valamint a digitalizáció által a zöld megállapodás céljainak elérésében betöltött aktív szerep mellett.

## 3. **Az Európai Bizottság közleménye**

3.1. A kiberbiztonsági kommunikációs csoport 5G biztonsági eszközkészletére válaszul az Európai Bizottság:

— a tagállamok kérésének megfelelően az 5G infrastruktúra és az ellátási lánc biztonságának biztosítása érdekében jár el, adott esetben a rendelkezésére álló valamennyi eszköz felhasználásával,

— felhívja a tagállamokat és az intézményeket, hogy biztosítsák a hatékony kockázatcsökkentési stratégiák végrehajtását, és fogadjanak el további uniós szintű koordinációs intézkedéseket az 5G kiberbiztonságának összehangolt megközelítése érdekében,

— felhívja a tagállamokat, hogy hajtsák végre az eszközcsomag következtetéseiben javasolt intézkedéscsomagot, és készítsenek közös jelentést azok végrehajtásáról, miközben a Kiberbiztonsági Együttműködési Csoport folytatja az eszközcsomag végrehajtásának támogatását,

— a hatáskörébe tartozó területeken intézkedéseket ír elő az 5G hálózatok és a változatos 5G értéklánc kiberbiztonságának, a műszaki szabványosításnak és a tanúsításnak, a közvetlen külföldi befektetéseknek, a piacvédelemnek és a versenynek, a beszerzéseknek és az informatikai diplomáciának, valamint a saját – különösen a K+I, a kohézió és a fejlesztés területét felölelő – programjainak és alapjainak támogatása érdekében.

## 4. **Általános megjegyzések**

4.1. Az EGSZB meg van győződve arról, hogy az új 5G technológiák képesek átalakítani a világgal való kölcsönhatás módját, lehetőséget kínálva új alkalmazások, üzleti modellek, új életmód, intelligens gyárak, magasabb termelékenység és az állampolgárok számára kínált új minőségi szolgáltatások számára. Potenciálisan megnyithatják az ajtót a forradalmi technológiák, mint például az automatizált autók, illetve a fejlett gyártási és elosztó rendszerek előtt, valamint lehetővé teszik több ezer összekapcsolt eszköz használatát, amelyeknek a dolgok internetéhez tartozva mindennapi világunk részeivé kell válniuk. Az EGSZB azonban azt szeretné, hogy az Európai Bizottság erősítse meg az 5G hatás- és megvalósíthatósági tanulmányait, valamint költség-haszon elemzéseit a 4G technológia vagy az optikai távközlés használatához képest. Az EGSZB alapvető fontosságúnak tartja, hogy az 5G a jobb körforgásos erőforrás-gazdálkodás elérésére és az energiával kapcsolatos jelentős szén-dioxid-lábnyom csökkentésére irányuljon. Az EGSZB szerint kezelni kell a társadalmi strukturális változásokat, méghozzá egy méltányos és gördülékeny átmenet elősegítésével és a készséghiány problémájának kezelésével, hogy jobban fizetett, rugalmas, magas képzettséget igénylő munkahelyek jöjjenek létre.

4.2. A három veszélyforrás – az ellenőrizhetetlen világjárványok, az elégtelen gazdaságpolitikai arzenál és a geopolitikai „fekete hattyúk" – tartós válságba taszíthatja a világgazdaságot, hatására pedig szűkülhet vagy összeomolhat a pénzügyi piac. Ugyanakkor az európai társadalom valamennyi alkotóeleme egyre inkább tudatában van annak, hogy a fenntartható gazdasági fejlődés **és a folyamatban lévő digitális forradalom érdekében – amelynek az 5G képviseli az egyik fő eszközét** – olyan módszereket kell alkalmazni, amelyek egyszerre biztosítják a technológiai szuverenitását, a magasabb termelékenységet és a rendelkezésre álló erőforrások hatékonyabb felhasználását a megfelelő jogi-szabályozási és gazdasági-pénzügyi keret támogatásával.

4.3. Az EGSZB sürgeti az uniós intézményeket és a tagállamokat, hogy valósítsák meg a digitális egységes piacot, ideértve az 5G szolgáltatások integrálásának és felhasználásának kapacitásépítését az európai iparágak versenyképességének védelme és javítása érdekében: felszólítja az Európai Bizottságot, hogy szigorúan kövesse nyomon a az 5G telepítése és valós felhasználása terén elért eredményeket, és felhívja a tagállamokat, hogy gyorsítsák tovább a folyamatot, figyelembe véve a biztonság és védelem minden szempontját, ideértve az 5G technológiáknak a népesség egészségére és az élő ökoszisztémákra gyakorolt hatásait, a társadalmi-gazdasági, a versenyképességre, illetve a oktatás és képzés terén kifejtett hatásait, továbbá az olyan alapvető jogok tiszteletben tartásának garantálását, mint például a tulajdonhoz vagy a magánélethez való jog és a személyes adatok biztonsága.

4.4. Az EGSZB arra kéri az EU-t, hogy töltsön be globális vezető szerepet az 5G mobiltechnológia következő generációjában, amelyet olyan biztonságos digitális infrastruktúrával látnak el, amely Európa új, korszerű ipari stratégiájának szilárd építőeleme az új mobil összeköttetések radikális megváltoztatásán keresztül, valamint hatalmas dinamikus potenciállal rendelkezik, és képes növelni a termelékenységet, a gazdaságot és bővíteni a polgárok számára nyújtott szolgáltatásokat, fokozni jólétüket, illetve az éghajlat és a környezet védelmét, miközben az EU-t az 5G forradalom élvonalába helyezi.

4.5. Tekintettel arra, hogy a kiberbiztonság és a nemzetbiztonság két elválaszthatatlanul összekapcsolódó fogalom, az EGSZB úgy véli, hogy az uniós tagországok nemzetbiztonságával kapcsolatos döntéseket az EU kontextusában kell meghozni, a nem műszaki jellegű vizsgálatokat pedig objektíven kell alkalmazni, olyan, egész Európára kiterjedő kockázatértékelési kritériumok alapján, amelyek egy kiszámítható és harmonizált európai szabályozási környezet biztosításához szükségesek, és amelyek garantálják a teljes interoperabilitást.

4.6. Az EGSZB úgy véli, hogy az információ minősége és a kommunikáció formái – az úgynevezett kontextushatás vagy a releváns helyzet –, továbbá az észlelhetőség jelentősen befolyásolják a befogadók viselkedési lehetőségeit. A fogyasztói szerepvállalás ösztönzésének célja tehát a fogyasztók oktatására és képességeinek megerősítésére szolgáló olyan eszközök azonosítása, amelyek aktív szereplővé teszik őket a digitális piacon. Az EGSZB elismeri, hogy a tudományos közösség túlnyomó többségének konszenzusára alapozva naprakész és helytálló információkat kell szolgáltatni az állampolgároknak az 5G előnyeiről és kockázatairól, jelezve azokat a szempontokat, amelyekben ez a konszenzus bizonytalan.

4.7. Az EGSZB meggyőződése, hogy az európai digitális piachoz való hozzáférésnek továbbra is megkülönböztetés nélkül szabadnak kell maradnia minden vállalkozás számára, a határozott és egyértelmű szabályok, szabványok, értékelési és biztonsági kritériumok európai keretének tiszteletben tartása mellett, amelyek középpontjában az európai technológiai szuverenitás helyreállítása és újraindítása áll.

4.8. Habár az öt legfontosabb infrastrukturális szolgáltató között két európai, két kínai és egy koreai beszállító található ([13]), és egyetlen nagyobb európai vállalat sem szerepel az elsők között az 5G eszközök és lapkakészletek gyártása terén; az EGSZB meg van győződve arról, hogy garantálni kell a több beszállítóval való együttműködést, amelyek közül legalább egynek európai tulajdonban kell lennie, és hogy biztosítani kell a hardver- és szoftverkomponensek átjárhatóságának és teljes körű működtethetőségének keretét, a maradéktalan európai technológiai szuverenitás biztosítása érdekében, erős nemzetközi együttműködés és a piacok nyitottsága, hozzáférhetősége és működése teljes körű kölcsönössége keretében. Ez a diverzitás mindaddig alkalmazható, amíg a szolgáltatások interoperabilitása lehetséges, és a kiberbiztonsági kockázatok a sokféleség miatt nem növekednek.

4.9. Az EGSZB véleménye szerint elengedhetetlen, hogy Európa középtávon ezen a területen az autonómiára és az önellátásra összpontosítson azáltal, hogy erőteljesen támogatja a kutatást és sok európai vállalatot. Az EGSZB üdvözli az 5G technológia bevezetésével járó biztonsági és védelmi kockázatok kezelése céljából a tagállamok által elfogadott, az európai értékelésben már azonosított intézkedéscsomagot. Úgy véli azonban, hogy az uniós szinten javasolt, a nem ionizáló sugárzás elleni védelemmel foglalkozó nemzetközi bizottság (ICNIRP) által frissített iránymutatásain alapuló és az Egészségügyi Világszervezet (WHO) által elismert, elektromágneses terekre vonatkozó szigorú és biztonságos expozíciós határértékeket az 5G-re tervezett valamennyi frekvenciasávra alkalmazni kell ([14]): az ICNIRP-határértékek az elővigyázatosság elvén alapulnak, mivel ezek ötvenszer alacsonyabbak a rendelkezésre álló tudományos bizonyítékok alapján megállapított közegészségügyi hatásszinteknél.

([13]) Jelenleg az Ericsson, a Nokia, a Huawei, a ZTE és a Samsung az öt globális beszállító.
([14]) EP – E-003040/2019 Stella Kyriakides válasza az Európai Bizottság nevében (2020. 01. 17.).

4.10. Az EGSZB mindazonáltal megjegyzi, hogy az ICNIRP-t nem ismeri el az egész tudományos közösség, és egyes tudósok az észszerűen elérhető legalacsonyabb szint elvének megfelelően sokkal szigorúbb lakossági expozíciós határértékeket támogatnak. Az 5G kommunikációs infrastruktúra kiegészítésére javasolható megoldások között szerepel a rögzített adatátviteli összeköttetések használata a meglévő nem rádiós technológiákkal (Ethernet kábelek, száloptika stb.) olyan helyzetekben, amikor azok használata rögzített (pl. ATM-ek, bankfiókok, ipari robotok, távvezérelt orvosi robotok stb.), vagy nagy adatfelhasználók (digitális szolgáltatók, vállalatok/vállalkozások stb.), illetve rögzített, nem hordozható helyeken elhelyezkedő dolgok internete esetén (intelligens otthon, okos város, közüzemi érzékelők stb.).

4.11. Az Európai Bizottságnak, az EP-nek, a Tanácsnak, valamint a tagállamok kormányainak és parlamentjeinek demokratikus keretet kell biztosítaniuk a konzultációhoz, ahol tudományos vagy technológiai kérdéseket, jogi garanciákat és az érintett intézményeknek a civil társadalom kérdéseire adott válaszait ismertethetik a nyilvánossággal.

4.12. Az EGSZB szerint a nemzeti szabályozó hatóságok hatáskörén és a távközlési szolgáltatók szerepén alapuló megfelelő intézkedések mellett nagyobb hangsúlyt kell fektetni a felhasználók, a polgárok és az érintett civil társadalmi szervezetek eszközeire, amelyek korlátozottak és nem hatékonyak.

4.13. Az EGSZB elismeri ([15]) az elektromágneses túlérzékenység (EHS) problémájának létezését, és kifejezte ezzel kapcsolatos aggodalmait, ugyanakkor biztatónak tartja, hogy további mélyreható kutatások folynak a probléma és annak okai megértése érdekében. Sürgeti továbbá az Európai Bizottságot, hogy folytassa és frissítse az e területen folytatott munkát.

4.14. Az EGSZB alapvető fontosságúnak tartja az 5G távközlési és alkalmazásszolgáltatók hitelességét, mivel az internetes információkezelés az összesített adatszolgáltatás alapját képezi, ahol a felhasználók az adatokat technológiai, jogi és pénzügyi mechanizmusok révén, objektumok, gépek és algoritmusok közvetlen összekapcsolásával gyűjtik össze és dolgozzák fel.

4.15. Az EGSZB az adatok feletti rendelkezési joggal kapcsolatos koncepciók helyett a magánszemélyek és a jogi személyek adatokkal kapcsolatos jogainak meghatározására való áttérést javasolta ([16]). A fogyasztóknak ellenőrizniük kell a csatlakoztatott eszközök által előállított adatokat annak érdekében, hogy garantálják a fogyasztók magánéletének védelmét a hozzáférhetőség, az átjárhatóság és az adatátvitel során, biztosítva ugyanakkor a megfelelő adatvédelmet és a titoktartást, a tisztességes versenyt és a fogyasztók rendelkezésére álló szélesebb választékot.

4.16. Az általános adatvédelmi rendeletet (GDPR) illetően egyértelműen meg kell határozni az alkalmazási lehetőségeket a gépek és tárgyak összekapcsolhatóságának fényében az egységes alkalmazás, valamint a magas szintű adat- és fogyasztóvédelem megvalósítása céljából, továbbá felül kell vizsgálni a polgári jogi felelősségre vonatkozó szabályokat, hogy ezeket alkalmazni lehessen azokra a helyzetekre, ahol egyre inkább szoftverek döntenek, a teljes körű biztonság keretén belül.

4.17. Az EGSZB elengedhetetlennek tartja, hogy a tagállamok betartsák az EU eszközkészletében szereplő stratégiai és technikai ajánlásokat, és elkerüljék olyan speciális nemzeti megközelítések kidolgozását, mint például a kiegészítő tesztek és tanúsítások, amelyek a piac széttöredezettségéhez vezethetnek, késleltethetik a technológiák bevezetését, és inkoherenciát okozhatnak a piacokon, ami azzal a kockázattal is jár, hogy veszélyeztetik a tesztelési és tanúsítási rendszerekbe vetett bizalmat.

4.18. Az EGSZB véleménye szerint alapvető fontosságú – az Európa által is egyre inkább támogatott – globális szabványok, valamint a megosztott és elismert bevált gyakorlatok használata a veszélyek hatékony kezelése, a méretgazdaságosság, a széttöredezettség elkerülése és az európai rendszerek interoperabilitásának garantálása érdekében. A műszaki szabványokról folytatott megbeszélésekre szükség van ahhoz, hogy biztosítsák a vállalatok számára, hogy ismét versenyezhessenek és részt vehessenek ezekben az alapvető tevékenységekben, amelyek lehetővé teszik az olyan fejlett technológiák, mint például az 5G és a mesterséges intelligencia bevezetését valamennyi piacon.

4.19. Az EGSZB különösen fontosnak tartja a beszállítók kockázati profiljának értékelését és az összehangolt uniós kockázatértékelésben kritikusként és érzékenyként meghatározott kulcsfontosságú eszközök tekintetében megfelelő korlátozások – többek között a hatékony kockázatcsökkentéshez szükséges kizárások – alkalmazását a magas kockázatúnak tekintett beszállítók esetében.

4.20. Az EGSZB fontosnak tartja az üzemeltetők és a beszállítók új műszaki biztonsági funkciókra fordított beruházásainak támogatását, amelyek mellett a piacnak képesnek kell lennie felismerni és jutalmazni mindazon kezdeményezéseket, amelyek célja a rendszerek biztonságának és ellenálló képességének növelése. A biztonságba történő beruházások jobb láthatósága új elemekkel bővítheti a piaci jutalmazást.

([15]) HL C 242., 2015.7.2., 31. o.
([16]) HL C 353., 2019.10.18., 79. o.

4.21. Az EGSZB határozottan támogatja az ipari fejlesztés és az 5G bevezetésének támogatására irányuló közös beavatkozásokat: a lehetséges kudarcok vagy az 5G értéklánc piaci hiányosságainak vizsgálatát, amelynek célja, hogy igazolják a célzott beavatkozásokat a következő hosszú távú költségvetés vagy az 5G kiberbiztonsággal (biztonság és védelem) kapcsolatos esetleges közös európai érdekű projekt keretében.

4.22. Az EGSZB hangsúlyozza, hogy bár a digitális infrastruktúra ellenállónak és erősnek bizonyult a Covid19-válság idején, további beruházásokra van szükség az 5G infrastruktúrába annak érdekében, hogy áthidalhatóvá váljon a továbbra is fennálló digitális szakadék, amely korlátozhatja az állampolgárok hozzáférését az e-egészségügyhöz, az e-tanuláshoz és a távoli munkavégzéshez.

4.23. A technológiai diplomácia szempontjából az EGSZB elengedhetetlennek tartja, hogy az EU kiegyensúlyozottabb, kölcsönös feltételeket biztosítson a kereskedelem és a beruházások számára, különös tekintettel a vállalkozások piacra jutására, a támogatásokra, a közbeszerzésre, a technológiaátadásra, az ipari tulajdonra, valamint a szociális és környezetvédelmi normákra (főként mivel „alternatív irányítási modelleket támogató rendszerszintű versenytársak" vannak), miközben ösztönzi a teljes versenyt és a technikai innovációt a piacon.

4.24. Az EGSZB határozottan támogatja a változatos és fenntartható 5G ellátási lánc fenntartásának szükségességét a hosszú távú függőség elkerülése érdekében, több beszállító jelenlétének biztosítását a helyettesíthetőség és interoperabilitás keretei között, és még inkább támogatja az 5G és az 5G utáni európai kapacitási és technológiai szuverenitási programokat és kezdeményezéseket a 2021–2027 közötti pénzügyi kereten belül.

4.25. A 2020. május 27-én elfogadott európai helyreállítási tervvel kapcsolatban a 2020 Digital Economy and Society Index (a 2020. évi digitális gazdaság és társadalom indexe, DESI) nyújt tájékoztatást az európai szemeszter digitális ajánlásait alátámasztó országspecifikus elemzésekkel kapcsolatban. Ez elősegíti a tagállamok számára, hogy megcélozzák és rangsorolják reform- és beruházási igényeiket, ezáltal megkönnyítve az 560 milliárd eurós helyreállítási és ellenálló képességet javító eszközhöz való hozzáférést. Az eszköz forrásokat biztosít a tagállamok számára gazdaságaik ellenállóbbá tételéhez, valamint annak biztosításához, hogy a beruházások és a reformok támogassák a zöld és a digitális átmenetet. Mivel a világjárvány jelentős hatással bírt a DESI-nek mind az öt dimenziójára, az 5G-re vonatkozó 2020. évi következtetéseket az Európai Bizottság és a tagállamok által a válság kezelésére és a fellendülés támogatására tett számos intézkedéssel összefüggésben kell értelmezni.

Kelt Brüsszelben, 2020. szeptember 16-án.

*az Európai Gazdasági és Szociális Bizottság*
*elnöke*
Luca JAHIER