Stanovisko Európskeho hospodárskeho a sociálneho výboru – Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov – Bezpečné zavádzanie 5G v EÚ – Vykonávanie súboru nástrojov

[COM(2020) 50 final]

(2020/C 429/37)

Spravodajca: **Alberto MAZZOLA**

Pomocný spravodajca: **Dumitru FORNEA**

Konzultácia	Európska komisia, 9. 3. 2020
Právny základ	článok 304 Zmluvy o fungovaní Európskej únie
Príslušná sekcia	sekcia pre dopravu, energetiku, infraštruktúru a informačnú spoločnosť
Prijaté v sekcii	3. 9. 2020
Prijaté v pléne	16. 9. 2020
Plenárne zasadnutie č.	554
Výsledok hlasovania	217/0/2
(za/proti/zdržalo sa)	

1. **Závery a odporúčania**

1.1. EHSV víta iniciatívu členských štátov a Európskej komisie (EK) zameranú na kontrolu toho, ako členské štáty vykonávajú súbor opatrení odporúčaných v záveroch súboru nástrojov strategických, technických a kľúčových opatrení v oblasti bezpečnosti zavádzania ekosystému 5G.

1.2. EHSV sa domnieva, že vzhľadom na rastúcu zložitosť a rozmanitosť aplikácií 5G (EK stanovila pre rok 2025 tieto ciele pripojiteľnosti: školy, univerzity, výskumné centrá, nemocnice, hlavní poskytovatelia verejných služieb a digitálne náročné podniky by mali mať prístup s rýchlosťou sťahovania z internetu/nahrávania na internet jeden gigabit dát za sekundu; mestské a vidiecke domácnosti by mali mať prístup s rýchlosťou sťahovania najmenej 100 megabitov za sekundu; mestské oblasti, hlavné cesty a železnice by mali mať nepretržité pokrytie 5G), táto kontrola ekosystému 5G, ako aj opatrení v rámci právomoci EK na zaručenie kybernetickej bezpečnosti sietí 5G a rôznorodého hodnotového reťazca 5G, technickej normalizácie a certifikácie, priamych zahraničných investícií a ochrany obchodu a hospodárskej súťaže, záväzkov vyplývajúcich zo služieb vo verejnom záujme, verejného obstarávania a kybernetickej diplomacie, sa musí týkať geopolitickej bezpečnosti (*security*), infraštruktúry a údajov a ochrany zdravia (*safety*), a to aj podľa článku 168 ods. 1 ZFEÚ.

1.3. Podľa EHSV je dôležité, aby európsky ekosystém 5G zabezpečoval integritu, dôvernosť, zodpovednosť za správu a prevádzku, bezpečnosť, zameniteľnosť dodávok, interoperabilitu hardvérových a softvérových komponentov, spoločné technické a regulačné normy, kontinuitu služieb, spoľahlivosť toku údajov a ich ochranu, pokrytie vo všetkých oblastiach vrátane riedko osídlených oblastí, jasnosť komunikácie s používateľom ako aktívnym subjektom na digitálnom trhu, dynamické dodržiavanie usmernení ICNIRP na ochranu zdravia obyvateľstva, pričom treba čo najviac znížiť žiarenie. V súlade s tým ICNIRP aktualizovala v usmerneniach z roku 1998 časť o rádiofrekvenčných elektromagnetických poliach. Revidované usmernenia, ktoré poskytujú ľuďom ochranu pred vystavením elektromagnetickým poliam v rozsahu 100 až 300 GHz obsahuje dokument: Health Phys. 118(5), s. 483 – 524, marec 2020. ICNIRP urobila v roku 2020 niekoľko zmien aby sa zabezpečilo, že nové technológie, ako je 5G, nebudú spôsobovať škody, a to bez ohľadu na naše súčasné očakávania.

1.4. EHSV žiada Európsku komisiu, aby prísne monitorovala pokrok v šírení a skutočnom využívaní 5G a vyzýva členské štáty, aby tento proces ďalej urýchľovali a zaručili zodpovedné vykonávanie a zohľadňovali pri tom všetky aspekty bezpečnosti a ochrany vrátane aspektov týkajúcich sa vplyvu technológií 5G na zdravie obyvateľstva a živé ekosystémy, sociálno-ekonomického vplyvu a vplyvu na hospodársku súťaž, vplyvu na vzdelávanie a odbornú prípravu a záruky dodržiavania základných práv.

1.5. EHSV žiada, aby EÚ bola globálnou jednotkou, pokiaľ ide o budúcu generáciu mobilných technológií 5G so zabezpečenou digitálnou infraštruktúrou ako pevným stavebným kameňom novej modernej priemyselnej stratégie Európy prostredníctvom radikálnej zmeny mobilného pripojenia a obrovského dynamického potenciálu zvýšenia produktivity a rastu hospodárstva a objemu služieb pre občanov.

1.6. EHSV sa predovšetkým domnieva, že je nevyhnutné zaručiť posúdenie rizikového profilu dodávateľov a uplatniť príslušné obmedzenia na dodávateľov považovaných za vysoko rizikových vrátane vylúčení potrebných na účinné zmenšenie rizík a vymedzenie záväzkov pre kľúčové aktíva vymedzené ako kriticky dôležité a citlivé v rámci koordinovaného hodnotenia rizika na úrovni EÚ.

1.7. EHSV sa domnieva, že je nevyhnutné, aby sa Európa v strednodobom horizonte zamerala na samostatnosť a sebestačnosť v tejto oblasti prostredníctvom výraznej podpory výskumu a plurality európskych podnikov. EHSV sa domnieva, že je dôležité zvýšiť financovanie digitálneho výskumu a inovácií zo zdrojov EÚ a podporovať investície prevádzkovateľov a dodávateľov do nových technických bezpečnostných prvkov, investície, ktoré musia ísť ruka v ruke so schopnosťou trhu uznávať a odmeňovať všetky iniciatívy zamerané na zvýšenie bezpečnosti a odolnosti systémov.

1.8. Je dôležité zaručiť bezpečnosť všetkým členským štátom aj prostredníctvom zachovania výskumných centier na viacerých územiach EÚ: EHSV tiež trvá na tom, aby existovali aspoň dvaja dodávatelia pre každú krajinu, z ktorej aspoň jeden bude európsky, ktorý môže zaručiť politickú bezpečnosť údajov a dodržiavanie zdravotných požiadaviek.

1.9. Podľa EHSV by sa mal klásť väčší dôraz na nástroje pre používateľov, občanov a príslušné organizácie občianskej spoločnosti, ktoré sú obmedzené a nedostatočne efektívne, a to nad rámec kladenia dôrazu na vhodné opatrenia týkajúce sa právomoci národných regulačných orgánov a úlohy telekomunikačných operátorov s cieľom posilniť postavenie spotrebiteľov zlepšením ich schopností stať sa aktívnym subjektom na trhu.

1.10. Komisia, EP, Rada a vlády a parlamenty členských štátov musia zabezpečiť demokratický konzultačný rámec, v ktorom sa môžu verejnosti prezentovať vedecké alebo technologické témy, právne záruky a odpovede príslušných inštitúcií na otázky občianskej spoločnosti.

1.11. EHSV odporúča posilniť európsku technologickú diplomaciu, aby EÚ zabezpečila vyváženejšie a recipročné podmienky obchodu a investovania, najmä pokiaľ ide o prístup podnikov na trh, dotácie, verejné obstarávanie, transfery technológií, priemyselné vlastníctvo a sociálne a environmentálne normy.

2. **Úvod**

2.1. Bezpečnosť sietí 5G má strategický význam pre občanov, podniky, celý jednotný trh a technologickú suverenitu EÚ. Už v roku 2013 Komisia spustila hlavnú iniciatívu EÚ vytvorením verejno-súkromného partnerstva v oblasti 5G s cieľom urýchliť výskum a inovácie technológií 5G.

2.2. Keďže celosvetové výnosy z technológie 5G sa na rok 2025 odhadujú na viac ako 100 miliárd EUR, táto technológia predstavuje pre Európu zásadnú výhodu v globálnej hospodárskej súťaži, a preto je kybernetická bezpečnosť nevyhnutná na zaručenie strategickej autonómie EÚ.

2.3. Siete 5G sú založené na súčasnej 4. generácii sieťových technológií (4G) a infraštruktúre optických sietí, poskytujú nové kapacity služby a stávajú sa ústrednou infraštruktúrou, ako aj faktorom, ktorý veľkej časti hospodárstva EÚ umožňuje vytvoriť štruktúru nesúcu širokú škálu základných služieb pre fungovanie vnútorného trhu a udržiavanie a riadenie životne dôležitých hospodárskych a sociálnych funkcií, ako je energetika, doprava, bankové a zdravotnícke služby a poľnohospodárske a priemyselné systémy výroby, distribúcie a spotreby.

2.4. Vzhľadom na ústrednú úlohu sietí 5G pri uskutočňovaní digitálnej transformácie hospodárstva a spoločnosti EÚ, na vzájomne prepojený a nadnárodný charakter infraštruktúry, z ktorej vychádza digitálny ekosystém, a na cezhraničný charakter hrozieb, prípadne významných zraniteľných miest a/alebo incidentov v oblasti kybernetickej bezpečnosti týkajúcich sa sietí 5G vyskytujúcich sa v jednom členskom štáte by ovplyvnili EÚ ako celok. Z tohto dôvodu by sa mali stanoviť opatrenia, ktoré budú základom vysokej úrovne spoločnej kybernetickej bezpečnosti 5G sietí.

2.5. V roku 2016 Európska komisia – ako súčasť súboru iniciatív v nadväznosti na oznámenie o pripojení pre konkurencieschopný jednotný digitálny trh ([1]), ([2]), ktorý zahŕňa reformu regulačného rámca pre elektronické komunikácie ([3]) a funkcie Orgánu európskych regulátorov pre elektronické komunikácie (BEREC) ([4]), priority v oblasti normalizácie IKT pre jednotný digitálny trh ([5]) a opatrenia na podporu internetového pripojenia v miestnych spoločenstvách ([6]) – prijala akčný plán EÚ pre 5G ([7]), ku ktorému EHSV vydal pozitívne stanovisko ([8]), s cieľom zvýšiť úsilie EÚ o zavedenie infraštruktúry a služieb 5G na jednotnom digitálnom trhu s plánom pre verejné a súkromné investície do infraštruktúry 5G v EÚ a cieľom do roku 2020, ktorým je zavedenie komerčných sietí 5G.

2.6. Podľa vymedzenia uvedeného v odporúčaní Komisie ([9]) „siete 5G“ znamenajú „súbory všetkých príslušných prvkov sieťovej infraštruktúry pre mobilné a bezdrôtové komunikačné technológie používané na pripojenie a služby s pridanou hodnotou s pokročilými výkonnostnými charakteristikami, ako sú veľmi vysoká rýchlosť a kapacita prenosu dát, malé oneskorenie komunikácie, ultravysoká spoľahlivosť či podpora veľkého počtu pripojených zariadení“.

2.7. V odporúčaní sa uvádza, že EK bude podporovať vykonávanie prístupu EÚ ku kybernetickej bezpečnosti 5G a tak, ako to požadujú členské štáty sa bude sa snažiť zaručiť bezpečnosť infraštruktúry 5G a dodávateľského reťazca, prípadne s využitím všetkých dostupných nástrojov:

— pravidlá pre telekomunikácie, multimédiá a kybernetickú bezpečnosť,

— koordinácia normalizácie a certifikácie na úrovni EÚ,

— rámec kontroly priamych zahraničných investícií na ochranu európskeho dodávateľského reťazca 5G,

— nástroje na ochranu obchodu,

— pravidlá hospodárskej súťaže,

— verejné obstarávanie, pričom sa zabezpečí, aby sa náležite zohľadnili aspekty bezpečnosti,

— programy financovania EÚ, ktorými sa zabezpečí, aby príjemcovia dodržiavali príslušné bezpečnostné požiadavky.

2.8. V júli 2019 predložili členské štáty výsledky svojich hodnotení rizika skupine pre spoluprácu zriadenej na základe smernice o NIS ([10]) (zloženej zo zástupcov každého členského štátu), Komisii a Agentúre EÚ pre kybernetickú bezpečnosť (ENISA), spolu s informáciami o hlavných činnostiach, hrozbách a zraniteľných miestach podľa normy ISO/IEC 27005 týkajúcimi sa infraštruktúry 5G a hlavných scenárov rizika a opísali možné spôsoby, akými by mohli subjekty, ktoré predstavujú hrozbu, využiť určitú zraniteľnosť niektorých činností: tieto národné hodnotenia boli základom následného koordinovaného hodnotenia a spoločného „súboru nástrojov“ k možný opatreniam na zmiernenie rizika.

2.9. V októbri 2019 skupina pre spoluprácu NIS s podporou Komisie a agentúry ENISA predložila správu o koordinovanom hodnotení rizika pre kybernetickú bezpečnosť v sieťach 5G piatej generácie v rámci celej EÚ, v ktorej sa určilo niekoľko dôležitých bezpečnostných výziev súvisiacich s kľúčovými technologickými inováciami softvéru, aplikácií a služieb a s úlohou dodávateľov pri vytváraní a využívaní sietí 5G a stupňom závislosti od jednotlivých dodávateľov:

— zvýšená miera vystavenia sa útokom a zvýšenie počtu potenciálnych prístupových bodov pre páchateľov týchto útokov,

— zvýšená citlivosť na nové charakteristiky architektúry a funkčných vlastností sietí 5G,

— riziká súvisiace so závislosťou prevádzkovateľov mobilných sietí od dodávateľov, so zvýšením počtu možností útokov využiteľných útočníkmi,

---

([1]) Článok 168 ods. 1 ZFEÚ „Činnosti Únie, ktoré dopĺňajú vnútroštátne politiky […]“.
([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]) Ú. v. EÚ C 125, 21.4.2017, s. 74.
([9]) Odporúčanie (EÚ) 2019/534 z 26. marca 2019, *Kybernetická bezpečnosť sietí 5G* (Ú. v. EÚ L 88, 29.3.2019, s. 42).
([10]) Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚL 194, 19.7.2016, s. 1).

— relevantnosť rizikového profilu jednotlivých dodávateľov pre možné zasahovanie mimo EÚ,

— zvýšené riziká vyplývajúce z veľkej závislosti od dodávateľov v súvislosti s možným prerušením dodávok pre obchodné napätie alebo inú príčinu,

— ohrozenia dostupnosti a integrity sietí, pokiaľ ide o bezpečnosť, dôvernosť a ochranu súkromia.

2.10. Všetky tieto výzvy si vyžadujú nový bezpečnostný model, čiže prehodnotenie súčasného politického a bezpečnostného rámca uplatniteľného na toto odvetvie a jeho ekosystém a od členských štátov sa očakáva, že prijmú potrebné zmierňovacie opatrenia.

2.11. Agentúra ENISA 21. novembra 2019 uverejnila správu s názvom „Prehľad hrozieb pre siete 5G“, v ktorej hodnotila hrozby súvisiace s piatou generáciou mobilných telekomunikačných sietí a integrovala do nej správu členských štátov EÚ.

2.12. Skupina pre spoluprácu NIS uverejnila 29. januára 2020 dokument s názvom *Cybersecurity of 5G networks – EU toolbox of risk mitigating measures* ([11]) s možným spoločným súborom opatrení schopných zmierniť hlavné riziká kybernetickej bezpečnosti sietí 5G a poskytnúť usmernenia na výber opatrení, ktoré by mali byť prioritou vo zmierňovacích plánov členských štátov aj EÚ. V ten istý deň Komisia prijala oznámenie podporujúce súbor nástrojov ([12]), ktorý je predmetom tohto stanoviska.

2.13. Hlavnými účastníkmi sieťovej infraštruktúry 5G sú:

— občania, spotrebitelia a koncoví používatelia 5G,

— prevádzkovatelia mobilných sietí: subjekty, ktoré poskytujú služby mobilných sietí používateľom a spravujú svoju sieť s pomocou tretích strán

— dodávatelia prevádzkovateľov mobilných sietí: subjekty, ktoré poskytujú služby alebo infraštruktúru prevádzkovateľom mobilných sietí s cieľom vybudovať a/alebo spravovať ich siete. Táto kategória zahŕňa: výrobcov telekomunikačných zariadení; iných dodávateľov tretích strán, napríklad dodávateľov cloudovej infraštruktúry, integrátorov systémov, dodávateľov v oblasti bezpečnosti a údržby, výrobcov prenosových zariadení,

— výrobcovia pripojených zariadení a poskytovatelia súvisiacich služieb: subjekty, ktoré poskytujú predmety alebo služby, ktoré sa budú pripájať k sieťam 5G (napr. smartfóny, pripojené vozidlá, elektronické zdravotníctvo), a súvisiace komponenty služieb zahrnutých do plánu kontroly 5G, ktorý je vymedzený v architektúre založenej na službách alebo *Mobile Edge Computing*,

— ostatné zainteresované subjekty vrátane poskytovateľov služieb a obsahu.

Všetky tieto zainteresované subjekty majú veľký vplyv v oblasti bezpečnosti, a to tak z hľadiska prispievania ku kybernetickej bezpečnosti sietí 5G, ako aj z hľadiska potenciálnych vstupných bodov alebo vektorov, pokiaľ ide o útoky. Preto je dôležité posúdiť riziká spojené s ich postavením v ekosystéme 5G.

2.14. Hlavné tradičné kategórie hrozieb súvisia s narušením dôvernosti, integrity a dostupnosti. Konkrétnejšie sa zistilo, že niekoľko scenárov hrozieb zameraných na siete 5G sa týka najmä:

— prerušenia miestnej alebo globálnej siete 5G (dostupnosť),

— špionáže dátového prenosu v sieťovej infraštruktúre 5G (dôvernosť),

— úpravy alebo presmerovania dátového prenosu v sieťovej infraštruktúre 5G (integrita a/alebo dôvernosť),

— zničenia alebo zmeny iných digitálnych infraštruktúr alebo informačných systémov prostredníctvom sietí 5G (integrita a/alebo dostupnosť).

2.15. Hrozby, ktoré predstavujú štáty alebo štátom podporovaní útočníci, sa považujú za mimoriadne relevantné v tom, že skutočne predstavujú najzávažnejších a najpravdepodobnejších útočníkov, pretože môžu mať motivácie, úmysly a predovšetkým schopnosť viesť pretrvávajúce a sofistikované bezpečnostné útoky na 5G siete.

([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.

Aj keď mnohé z týchto zraniteľných miest nie sú špecifické pre siete 5G, ich počet a význam sa s 5G pravdepodobne zvýši v dôsledku vyššej úrovne zložitosti technológie a budúceho väčšieho využívania tejto infraštruktúry hospodárstvami a spoločnosťami.

2.16. Najmä vzhľadom na to, že siete 5G sa budú zväčša zakladať na softvéri, hlavné bezpečnostné nedostatky, napríklad tie, ktoré sú výsledkom zlých procesov vývoja softvéru u výrobcov zariadení, by mohli útočníkom uľahčiť zámerné vkladanie zadných dvierok do výrobkov a sťažiť ich odhalenie. To môže zväčšiť možnosť, že ich využívanie bude mať obzvlášť závažný a rozšírený negatívny vplyv. Ešte sa úplne nevyriešili problémy s kybernetickou bezpečnosťou 4G a problémy s 5G môžu rásť exponenciálne.

2.17. Existujú aj zraniteľné miesta týkajúce sa procesu alebo konfigurácie:

— nedostatok špecializovaného a školeného personálu na ochranu, monitorovanie a údržbu sietí 5G,

— nedostatok primeraných vnútorných bezpečnostných kontrol, monitorovacích postupov, systémov riadenia bezpečnosti a nedostatky v postupoch riadenia rizík,

— neprimeranosť postupov bezpečnosti alebo prevádzkovej údržby, ako je aktualizácia softvéru/riadenie opráv v sieťach 5G,

— nedodržiavanie noriem 3GPP alebo nesprávne uplatňovanie noriem,

— nedostatky v návrhu alebo architektúre siete vrátane chýbajúcich účinných núdzových mechanizmov a mechanizmov na zabezpečenie kontinuity, neprimeranej alebo nesprávnej konfigurácie, napríklad pri virtualizácii alebo v súvislosti s právami na administráciu alebo prístup,

— neprimerané kritériá pre miestny a diaľkový prístup k sieťovým komponentom,

— nedostatočné bezpečnostné požiadavky pri dodávkach: toto zraniteľné miesto môže mať formu neprimeraných stratégií výberu dodávateľov alebo nedostatočného uprednostňovania bezpečnosti pred inými aspektmi.

2.18. Rizikové profily jednotlivých dodávateľov sa musia posudzovať na základe rôznych faktorov, najmä: možnosti, že na dodávateľa bude pôsobiť zasahovanie z krajiny mimo EÚ uľahčené silnými väzbami medzi dodávateľom a vládou konkrétnej tretej krajiny; právnych predpisov tretích krajín, najmä ak neexistujú legislatívne alebo demokratické kontroly a rovnováhy a ak v dôsledku toho dcérske spoločnosti pôsobiace v EÚ môžu byť odrádzané od dodržiavania právnych predpisov EÚ, alebo ak neexistujú dohody o bezpečnosti alebo ochrane údajov medzi EÚ a príslušnou treťou krajinou; charakteristík podnikového vlastníctva dodávateľa; schopnosti tretej krajiny vyvíjať akýkoľvek tlak, aj vo vzťahu k miestu výroby zariadenia; všeobecnej kvality výrobkov a postupov kybernetickej bezpečnosti dodávateľov vrátane stupňa kontroly nad vlastným dodávateľským reťazcom a primeranej priority bezpečnostných postupov.

2.19. Členské štáty sa dohodli na zabezpečení zavedenia opatrení na vhodnú a primeranú reakciu na už identifikované riziká a možné budúce riziká. Súhlasili najmä s tým, že zabezpečia, aby v súlade s prístupom založeným na hodnotení rizík boli schopné stanovovať obmedzenia, zákazy a/alebo osobitné požiadavky a podmienky pre dodávku, distribúciu a prevádzku sieťových zariadení 5G.

2.20. V tejto súvislosti by členské štáty mali:

— posilniť bezpečnostné požiadavky na prevádzkovateľov mobilných sietí, ako sú prísne kontroly prístupu, pravidlá bezpečnej prevádzky a monitorovania, obmedzenia outsourcingu špecifických funkcií,

— posúdiť rizikový profil dodávateľov na základe objektívnych a jasných kritérií; v dôsledku toho v súlade so zásadami proporcionality a právnej istoty uplatňovať príslušné obmedzenia pre dodávateľov, ktorí sa považujú za vysokorizikových – vrátane potrebných vylúčení v záujme účinného zmiernenia rizík – v prípade kľúčových aktív vymedzených v koordinovanom posúdení rizík na úrovni EÚ ako kritické a citlivé,

— schváliť celosvetovo uznávané a vykonávané bezpečnostné normy a osvedčené postupy založené na konsenze,

— zabezpečiť, aby mal každý prevádzkovateľ primeranú stratégiu viacerých dodávateľov s cieľom zabrániť akejkoľvek veľkej závislosti od jedného dodávateľa (alebo dodávateľov s podobným rizikovým profilom) alebo ju obmedziť,

— zaručiť dôslednú kontrolu prístupu a bezpečné riadenie, prevádzku a monitorovanie siete pri používaní certifikácie komponentov a/alebo procesov siete 5G. Táto stratégia musí byť založená na posúdení rizika vykonanom členskými štátmi a prevádzkovateľmi, aby voľba stratégie viacerých dodávateľov nezvýšila úroveň rizika pre sieť prevádzkovateľa,

— zaručiť primeranú rovnováhu dodávateľov na štátnej úrovni a predchádzať závislosti od dodávateľov považovaných za vysoko rizikových, a to aj podporovaním väčšej interoperability zariadení,

— udržiavať rôznorodý a udržateľný dodávateľský reťazec 5G s cieľom vyhnúť sa dlhodobej závislosti a plne využívať nástroje EÚ na kontrolu priamych zahraničných investícií, nástroje na ochranu obchodu, pravidlá hospodárskej súťaže, pravidlá verejného obstarávania EÚ,

— posilniť vnútorné kapacity EÚ v oblasti technológií 5G a technológií ďalších generácií využitím príslušných programov a financovania EÚ, koordináciu medzi členskými štátmi v oblasti normalizácie posilnením kapacít „testovania“ a „auditu“ s cieľom dosiahnuť konkrétne bezpečnostné ciele a rozvíjať príslušné systémy certifikácie EÚ podľa zákona o kybernetickej bezpečnosti a podporu interoperability.

2.21. Ako opakovane zdôrazňuje Európska komisia, európsky vnútorný trh je a zostáva otvorený pre každého, kto chce prísť do Európy, pokiaľ každý rešpektuje jasné a náročné pravidlá založené na objektívnych kritériách.

2.22. Rada 6. júna 2020 zdôraznila význam posilnenia digitálnej suverenity a spolupráce v EÚ, ako aj vytvorenia synergií prostredníctvom programov EÚ, ako je Nástroj na prepájanie Európy a program Digitálna Európa, spolu s rozvojom digitálnych zručností, rozvojom dátového hospodárstva, významom umelej inteligencie a kybernetickej bezpečnosti s aktívnou úlohou digitálneho systému pri dosahovaní cieľov zelenej dohody.

3. **Oznámenie Komisie**

3.1. V reakcii na súbor bezpečnostných nástrojov 5G komunikačnej skupiny NIS Európska komisia:

— usiluje sa zaručiť bezpečnosť infraštruktúry 5G a dodávateľského reťazca, podľa potreby pomocou všetkých nástrojov, ktoré má k dispozícii, ako o to požiadali členské štáty,

— vyzýva členské štáty a inštitúcie, aby zabezpečili vykonávanie účinných stratégií na zmiernenie rizika a prijali ďalšie koordinačné opatrenia na úrovni EÚ na zosúladený prístup ku kybernetickej bezpečnosti 5G,

— vyzýva členské štáty, aby pokračovali vo vykonávaní súboru opatrení odporúčaných v záveroch k súboru nástrojov a pripravili spoločnú správu o ich vykonávaní, zatiaľ čo skupina pre spoluprácu NIS bude naďalej pracovať na podpore vykonávania súboru nástrojov,

— v oblastiach svojej pôsobnosti poskytuje opatrenia na zaručenie kybernetickej bezpečnosti sietí 5G a rôznorodého hodnotového reťazca 5G, technickej normalizácie a certifikácie, priamych zahraničných investícií a ochrany obchodu a hospodárskej súťaže, verejného obstarávania a kybernetickej diplomacie, ako aj vlastných programov a fondov, najmä na výskum a inovácie, súdržnosť a rozvoj.

4. **Všeobecné pripomienky**

4.1. EHSV je presvedčený, že nové technológie 5G dokážu zmeniť spôsob našej interakcie so svetom a ponúkajú príležitosti pre nové aplikácie, obchodné modely, nový životný štýl, inteligentné továrne, vyššiu produktivitu a nové kvalitné služby pre občanov. Zároveň potenciálne otvárajú dvere revolučným technológiám, ako sú automatizované automobily a moderné výrobné a distribučné systémy, a umožňujú vzájomné prepojenie tisícov zariadení, ktoré by mali vstúpiť do nášho každodenného sveta ako súčasť internetu vecí (IoT). EHSV však očakáva, že EK posilní štúdie vplyvu a realizovateľnosti a analýzu nákladov a prínosov 5G v porovnaní s používaním technológie 4G alebo optických telekomunikačných sietí. EHSV sa domnieva, že je nevyhnutné, aby sa technológia 5G zamerala na dosiahnutie lepšieho obehového využívania zdrojov a na zníženie veľkej energetickej uhlíkovej stopy. EHSV zdôrazňuje, že je dôležité, aby sa spoločenské štrukturálne zmeny riešili podporovaním spravodlivej a hladkej transformácie a riešením nedostatku kvalifikovanej pracovnej sily s cieľom dosiahnuť lepšie odmeňované, flexibilné a vysokokvalifikované pracovné miesta.

4.2. Trojité riziko nekontrolovaných pandémií, nepostačujúcich nástrojov hospodárskej politiky a úplne nepredvídateľných geopolitických udalostí, by mohlo celosvetové hospodárstvo vohnať do trvalého poklesu a spôsobiť kolapsy finančného trhu a jeho opúšťanie, a to práve v čase, keď si všetky zložky európskej spoločnosti čoraz viac uvedomujú, že udržateľný hospodársky rozvoj a **pokračujúca digitálna revolúcia – v rámci ktorej 5G predstavuje jeden z hlavných nástrojov** – si vyžadujú prístup, ktorý zohľadňuje súčasne technologické aspekty, rast produktivity a efektívnejšie využívanie dostupných zdrojov s podporou primeraného právneho, regulačného a hospodárskeho a finančného rámca.

4.3. EHSV vyzýva inštitúcie EÚ a členské štáty, aby dokončili jednotný digitálny trh vrátane budovania kapacít na integráciu a využívanie služieb 5G na ochranu a zlepšenie konkurencieschopnosti európskych priemyselných odvetví: vyzýva Európsku komisiu, aby prísne monitorovala pokrok pri šírení a skutočnom využívaní 5G a vyzýva členské štáty, aby ďalej zrýchľovali tento proces, pričom zohľadnia všetky aspekty bezpečnosti a ochrany vrátane aspektov týkajúcich sa vplyvu technológií 5G na zdravie obyvateľstva a živé ekosystémy, sociálno-ekonomického vplyvu a vplyv na hospodársku súťaž, vplyvu na vzdelávanie a odbornú prípravu, záruky dodržiavania základných práv, ako je majetkové právo alebo právo na súkromie a bezpečnosť osobných údajov.

4.4. EHSV žiada, aby EÚ bola globálnou jednotkou v rámci budúcej generácie mobilných technológií 5G so zabezpečenou digitálnou infraštruktúrou ako pevným stavebným kameňom novej modernej priemyselnej stratégie Európy prostredníctvom radikálnej zmeny mobilného pripojenia a obrovského dynamického potenciálu zvýšenia produktivity a rastu hospodárstva a objemu služieb pre občanov, ich blahobytu a ochrany klímy a životného prostredia tým, že sa EÚ postaví na čelo revolúcie 5G.

4.5. Vzhľadom na to, že kybernetická bezpečnosť a národná bezpečnosť sú dva neoddeliteľne spojené aspekty, EHSV sa domnieva, že každé rozhodnutie o národnej bezpečnosti členského štátu EÚ musí byť prijaté v kontexte EÚ a netechnické hodnotenia sa musia uplatňovať objektívne na základe kritérií hodnotenia rizík definovaných na európskej úrovni, ktoré sú potrebné na zabezpečenie predvídateľného a harmonizovaného regulačného prostredia v celej Európe zaručujúceho úplnú interoperabilitu.

4.6. EHSV sa nazdáva, že kvalita informácií a spôsoby komunikácie – tzv. rámcový efekt, efekt kontextu alebo postavenia – významne ovplyvňujú možnosti správania príjemcov. Cieľ posilnenia postavenia spotrebiteľov sa preto premieta do identifikácie nástrojov na vzdelávanie spotrebiteľa a zväčšenie jeho schopností, čím sa z neho stáva aktívny hráč na digitálnom trhu. EHSV uznáva potrebu poskytnúť občanom aktuálne a správne informácie o prínosoch a rizikách 5G na základe konsenzu drvivej väčšiny vedeckej obce a uviesť aspekty, v ktorých je tento konsenzus neistý.

4.7. EHSV je presvedčený, že prístup na európsky digitálny trh musí zostať voľný pre každý podnik bez diskriminácie, ale len v rámci rešpektovania európskeho rámca pevných a jasných pravidiel, noriem a hodnotiacich a bezpečnostných kritérií, pre ktoré je stredobodom európskej stratégie obnova európskej technologickej suverenity, ktorá je jej vlastnou.

4.8. Hoci medzi päť najväčších poskytovateľov infraštruktúry patria dvaja európski dodávatelia, dvaja čínski a jeden kórejský ([13]), žiadna významná európska spoločnosť nepatrí medzi najväčšie, ktoré vyrábajú zariadenia 5G a čipové sady; EHSV je presvedčený, že musí byť zaručený väčší počet dodávateľov, z ktorých aspoň jeden je vo vlastníctve európskej materskej spoločnosti a že je potrebné zaručiť rámec interoperability a úplnej zameniteľnosti hardvérových a softvérových komponentov, aby sa zabezpečila aj úplná európska technologická suverenita v rámci silnej medzinárodnej spolupráce a úplnej reciprocity otvorenosti, prístupnosti a pôsobenia na trhoch. Takáto diverzifikácia sa môže uplatňovať, pokiaľ je interoperabilita služieb možná a riziká v oblasti kybernetickej bezpečnosti sa v dôsledku rozmanitosti nezvyšujú.

4.9. EHSV sa domnieva, že je nevyhnutné, aby sa Európa v strednodobom horizonte zamerala na samostatnosť a sebestačnosť v tejto oblasti prostredníctvom výraznej podpory výskumu a plurality európskych podnikov. EHSV víta súbor opatrení dohodnutých členskými štátmi na riešenie bezpečnostných rizík (*security and safety*) spojených so zavedením technológie 5G, ktoré už boli identifikované v rámci európskeho hodnotenia. Domnieva sa však, že prísne a bezpečné limity vystavenia pôsobeniu elektromagnetických polí, ktoré sa odporúčajú na úrovni EÚ a sú založené na aktualizovaných údajoch Medzinárodnej komisie pre ochranu pred neionizujúcim žiarením (ICNIRP), ktorú uznala Svetová zdravotnícka organizácia (WHO), by sa mali uplatňovať na všetky frekvenčné pásma predpokladané pre 5G ([14]): limity ICNIRP sú založené na zásade predbežnej opatrnosti, pretože sú 50-krát nižšie ako úrovne účinku na zdravie verejnosti stanovené na základe dostupných vedeckých dôkazov.

([13]) V súčasnosti pôsobí na trhu 5 globálnych dodávateľov: Ericsson, Nokia, Huawei, ZTE, Samsung.

([14]) Odpoveď, ktorú poskytla pani Kyriakides v mene Európskej komisie, Európsky parlament, E-003040/2019, 17. 1. 2020.

4.10. EHSV však konštatuje, že nie celá vedecká obec uznáva ICNIRP, pričom niektorí vedci presadzujú pre obyvateľstvo oveľa prísnejšie expozičné limity podľa zásady „na čo najnižšej rozumne dosiahnuteľnej úrovni“ (ALARA). Medzi riešenia, ktoré by sa mohli navrhnúť na doplnenie komunikačnej infraštruktúry 5G, patrí používanie pevných dátových pripojení súčasnými nerádiovými technológiami (eternetové káble, optické káble atď.) pri pevných zariadeniach (napr. bankomaty, POS terminály, priemyselné roboty, diaľkovo ovládané medicínske roboty atď.) a tam, kde pôsobia používatelia prenosov rozsiahlych dát (poskytovatelia digitálnych služieb, spoločnosti/ podniky atď.); internet vecí v pevných, nemobilných lokalitách (inteligentná domácnosť, inteligentné mesto, snímače na verejných zariadeniach atď.).

4.11. Komisia, EP, Rada a vlády a parlamenty členských štátov musia zabezpečiť demokratický konzultačný rámec, v ktorom sa môžu verejnosti prezentovať vedecké alebo technologické témy, právne záruky a odpovede príslušných inštitúcií na otázky občianskej spoločnosti.

4.12. Podľa EHSV by sa mal klásť väčší dôraz na nástroje pre používateľov, občanov a príslušné organizácie občianskej spoločnosti, ktoré sú obmedzené a nedostatočne efektívne, a to nad rámec kladenia dôrazu na vhodné opatrenia týkajúce sa právomoci národných regulačných orgánov a úlohy telekomunikačných operátorov.

4.13. EHSV uznal ([15]) existenciu problému elektromagnetickej precitlivenosti (EHS) a zdôraznil svoje obavy, pričom považuje za povzbudzujúce konštatovanie, že prebieha ďalší dôkladný výskum s cieľom porozumieť problému a jeho príčinám, a naliehavo žiada Európsku komisiu, aby pokračovala vo svojej práci v tejto oblasti a aktualizovala ju.

4.14. Podľa názoru EHSV je dôveryhodnosť poskytovateľov telekomunikačných a aplikačných služieb 5G nevyhnutná, pretože riadenie informácií na internete je základom služieb v oblasti agregovaných údajov, ktoré používatelia zhromažďujú a spracúvajú prostredníctvom technologických, právnych a fiškálnych mechanizmov, a uvádzajú tak predmety, stroje a algoritmy do priameho vzájomného vzťahu.

4.15. EHSV navrhol ([16]) prechod od koncepcie vlastníctva údajov k definícii práv na údaje pre jednotlivcov a právnické osoby. Spotrebitelia by mali mať kontrolu nad údajmi vytvorenými pripojenými zariadeniami, aby sa zaručilo súkromie spotrebiteľa s prístupnosťou, interoperabilitou a prenosom údajov, pričom by sa mala zabezpečiť primeraná ochrana a dôvernosť údajov, spravodlivá hospodárska súťaž a širší výber spotrebiteľov.

4.16. Všeobecné nariadenie o ochrane údajov (GDPR) by sa malo doplniť o jasné vykonávacie usmernenia, aby sa dosiahlo jednotné uplatňovanie a vysoká úroveň ochrany údajov a spotrebiteľov vzhľadom na vzájomnú prepojenosť strojov a predmetov a prehodnotili sa pravidlá občianskoprávnej zodpovednosti a poisťovania produktov a prispôsobili sa situácii, v ktorej bude softvér čoraz častejšie robiť rozhodnutia pri zaručení úplnej bezpečnosti.

4.17. EHSV sa domnieva, že je nevyhnutné, aby sa členské štáty riadili strategickými a technickými odporúčaniami obsiahnutými v súbore nástrojov EÚ a vyhýbali sa vypracovaniu osobitných vlastných prístupov, ako sú dodatočné testy a certifikácie, ktoré by spôsobili fragmentáciu trhu, oneskorenia pri zavádzaní technológií a nezrovnalosti medzi trhmi, s rizikom narušenia dôvery v systémy testovania a certifikácie.

4.18. EHSV sa domnieva, že je nevyhnutné využívať globálne normy so zvýšenou európskou podporou a spoločné a uznávané najlepšie postupy, aby sa umožnilo účinné zvládanie hrozieb, dosiahli sa úspory z rozsahu, zabránilo sa fragmentácii a zaručila sa interoperabilita európskych systémov. Diskusie o technických normách sú nevyhnutným vysvetlením, ktoré umožní spoločnostiam opäť súťažiť a viesť v týchto základných činnostiach, ktoré umožňujú implementáciu moderných technológií, ako je 5G a umelá inteligencia, na všetkých trhoch.

4.19. EHSV sa predovšetkým domnieva, že je nevyhnutné zaručiť posúdenie rizikového profilu dodávateľov a uplatniť príslušné obmedzenia na dodávateľov považovaných za vysoko rizikových vrátane vylúčení potrebných na účinné zmenšenie rizík pre kľúčové aktíva vymedzené ako kriticky dôležité a citlivé v rámci koordinovaného hodnotenia rizika na úrovni EÚ.

4.20. EHSV sa domnieva, že je dôležité zvýšiť investície prevádzkovateľov a dodávateľov do nových technických bezpečnostných prvkov, ktoré musia ísť ruka v ruke so schopnosťou trhu uznať a odmeňovať všetky iniciatívy zamerané na zväčšenie bezpečnosti a odolnosti systémov. Väčšia viditeľnosť investícií do bezpečnosti by mohla priniesť nové prvky trhovej odmeny.

([15]) Ú. v. EÚ C 242, 2.7.2015, s. 31.
([16]) Ú. v. EÚ C 353, 18.10.2019, s. 79.

4.21. EHSV dôrazne podporuje spoločné intervencie na podporu priemyselného rozvoja a zavádzania 5G: vyhodnotenie možných nedostatkov alebo zlyhaní trhu v rámci hodnotového reťazca 5G, ktoré by odôvodňovali cielené intervencie v rámci nasledujúceho dlhodobého rozpočtu alebo možné dôležité projekty spoločného európskeho záujmu v oblasti kybernetickej bezpečnosti 5G (*security and safety*).

4.22. EHSV zdôrazňuje, že hoci sa digitálna infraštruktúra počas krízy COVID-19 ukázala ako odolná a spoľahlivá, na prekonanie existujúcej digitálnej priepasti sú potrebné ďalšie investície do infraštruktúry 5G, čo môže obmedziť prístup občanov k elektronickému zdravotníctvu, elektronickému učeniu a telepráci.

4.23. Pokiaľ ide o technologickú diplomaciu, EHSV považuje za nevyhnutné, aby EÚ zabezpečila vyváženejšie a recipročné podmienky obchodu a investovania, najmä pokiaľ ide o prístup podnikov na trh, dotácie, verejné obstarávanie, transfery technológií, priemyselné vlastníctvo a sociálne a environmentálne normy, najmä za prítomnosti „systémových súperov propagujúcich alternatívne modely riadenia, a zároveň podporovala plnú hospodársku súťaž a technické inovácie na trhu.

4.24. EHSV dôrazne podporuje potrebu zachovať rôznorodý a udržateľný dodávateľský reťazec 5G, aby sa predišlo dlhodobej závislosti, a to tým, že sa zabezpečí prítomnosť viacerých dodávateľov v rámci zameniteľnosti a interoperability, a aby sa v rámci finančného rámca na roky 2021 – 2027 ďalej posilňovali programy a iniciatívy zamerané na budovanie kapacít a európsku suverenitu v oblasti technológií 5G a technológií ďalších generácií.

4.25. V kontexte plánu obnovy pre Európu prijatého 27. mája 2020 sa index digitálnej ekonomiky a spoločnosti (DESI) v roku 2020 použije ako informácia pre analýzu jednotlivých krajín na podporu digitálnych odporúčaní v rámci európskeho semestra. To pomôže členským štátom zamerať sa na ich potreby reforiem a investícií a dať im prioritu, čím sa uľahčí prístup k mechanizmu na podporu obnovy a odolnosti vo výške 560 miliárd EUR. Tento mechanizmus poskytne členským štátom finančné prostriedky na zvýšenie odolnosti ich hospodárstiev a zabezpečí, aby investície a reformy podporili ekologickú a digitálnu transformáciu. Keďže pandémia mala významný vplyv na každú z piatich dimenzií DESI, závery z roku 2020 týkajúce sa 5G by sa mali interpretovať v spojení s mnohými opatreniami prijatými Komisiou a členskými štátmi na zvládnutie krízy a podporu obnovy.

V Bruseli 16. septembra 2020

Predseda
Európskeho hospodárskeho a sociálneho výboru
Luca JAHIER