Stanovisko Evropského hospodářského a sociálního výboru ke Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Bezpečné zavádění sítí 5G v EU – Implementace souboru opatření EU

[COM(2020) 50 final]

(2020/C 429/37)

Zpravodaj: **Alberto MAZZOLA**

Spoluzpravodaj: **Dumitru FORNEA**

Konzultace	Evropská komise, 9. 3. 2020
Právní základ	článek 304 Smlouvy o fungování Evropské unie
Odpovědná sekce	Doprava, energetika, infrastruktura a informační společnost
Přijato v sekci	3. 9. 2020
Přijato na plenárním zasedání	16. 9. 2020
Plenární zasedání č.	554
Výsledek hlasování	217/0/2
(pro/proti/zdrželi se hlasování)	

1. **Závěry a doporučení**

1.1 EHSV vítá iniciativu členských států a Evropské komise zaměřenou na kontrolu toho, jak členské státy provádějí opatření doporučená v závěrech souboru strategických, technických a klíčových opatření v oblasti bezpečnosti při zavádění ekosystému 5G.

1.2 EHSV se domnívá, že vzhledem k rostoucí složitosti a rozmanitosti aplikací 5G (Evropská komise stanovila pro rok 2025 tyto cíle v oblasti možností připojení: školy, univerzity, výzkumná střediska, nemocnice, hlavní poskytovatelé veřejných služeb a digitálně intenzivní podniky by měly mít přístup k rychlosti stahování/odesílání dat přes internet ve výši 1 gigabit za sekundu; městské a venkovské domácnosti by měly mít přístup k připojení s rychlostí stahování alespoň 100 megabitů za sekundu; městské oblasti, hlavní silnice a železnice by měly mít nepřetržité pokrytí 5G) se tato kontrola ekosystému 5G, jakož i opatření v pravomoci Komise k zajištění kybernetické bezpečnosti sítí 5G a diverzifikovaného hodnotového řetězce 5G, technické normalizace a certifikace, přímých zahraničních investic a ochrany obchodu a hospodářské soutěže, závazků veřejné služby, zadávání veřejných zakázek a diplomacie v oblasti IT musí týkat geopolitické bezpečnosti infrastruktury a údajů a ochrany zdraví, a to mj. podle čl. 168 odst. 1 SFEU.

1.3 Podle EHSV je důležité, aby evropský ekosystém 5G zajišťoval integritu, důvěrnost, odpovědnost za řízení a provoz, bezpečnost, zastupitelnost dodávek, interoperabilitu hardwarových a softwarových součástí, společné technické a regulační normy, kontinuitu služeb, spolehlivost toku údajů a jejich ochranu, pokrytí ve všech oblastech včetně řídce osídlených oblastí, jasnost komunikace s uživatelem jako aktivním subjektem na digitálním trhu a dynamické dodržování pokynů ICNIRP pro ochranu zdraví obyvatelstva. Zároveň je nutné omezit v co největší míře záření. ICNIRP tedy aktualizovala část pokynů z roku 1998 týkající se rádiové frekvence EMF. V tomto dokumentu jsou uvedeny tyto revidované pokyny, které zajišťují ochranu člověka před expozicí frekvencím 100 kHz až 300 GHz. Health Phys. 118(5):483–524; 2020- březen 2020. ICNIRP (2020) provedla řadu změn s cílem zajistit, aby nové technologie, jako je 5G, nemohly způsobit škodu bez ohledu na naše současná očekávání.

1.4 EHSV vyzývá Evropskou komisi, aby důsledně sledovala pokrok při zavádění a skutečném využívání sítí 5G, a vyzývá členské státy, aby tento proces dále urychlily a zajistily odpovědné provádění při zohlednění všech aspektů bezpečnosti a ochrany, včetně aspektů týkajících se dopadu technologií 5G na zdraví obyvatel a na živé ekosystémy, socioekonomického dopadu, dopadu na hospodářskou soutěž, dopadu na vzdělávání a odbornou přípravu, a dále také při zohlednění záruk ohledně dodržování základních práv.

1.5 EHSV žádá, aby byla EU světovým lídrem příští generace mobilních technologií 5G s bezpečnou digitální infrastrukturou jako pevným základním prvkem nové moderní průmyslové strategie Evropy prostřednictvím radikální změny mobilního připojení a s obrovským dynamickým potenciálem pro zvýšení produktivity a pro růst ekonomiky a objemu služeb pro občany.

1.6 EHSV se zejména domnívá, že je nezbytné zaručit posouzení rizikového profilu dodavatelů a uplatnit příslušná omezení vůči dodavatelům považovaným za vysoce rizikové, včetně vyloučení nezbytných k účinnému zmírnění rizik a definování odpovědnosti, pokud jde o klíčová aktiva definovaná v rámci koordinovaného posouzení rizik na úrovni EU jako kritická a citlivá.

1.7 EHSV se domnívá, že je nezbytné, aby se Evropa ve střednědobém horizontu zaměřila na samostatnost a soběstačnost v této oblasti, a to výraznou podporou výzkumu a plurality evropských společností. EHSV považuje za důležité navýšit zdroje Unie v oblasti digitálního výzkumu a digitálních inovací a podpořit investice provozovatelů a dodavatelů do nových technických bezpečnostních prvků – investice, které musí jít ruku v ruce se schopností trhu uznávat a odměňovat všechny iniciativy zaměřené na zvýšení bezpečnosti a odolnosti systémů.

1.8 Je důležité zaručit bezpečnost všem členským státům také prostřednictvím udržení výzkumných středisek ve více územních celcích EU. EHSV rovněž trvá na návrhu mít pro každou zemi alespoň dva dodavatele, z nichž nejméně jeden bude evropský, což může zaručit politickou bezpečnost údajů a dodržování zdravotních požadavků.

1.9 Podle EHSV je třeba klást větší důraz na nástroje pro uživatele, občany a příslušné organizace občanské společnosti, které jsou omezené a nedostatečně účinné, a to nad rámec správného důrazu na správná opatření týkající se pravomoci vnitrostátních regulačních orgánů a úlohy telekomunikačních operátorů s cílem posílit postavení spotřebitelů posílením jejich schopnosti stát se aktivními subjekty na trhu.

1.10 Evropská komise, Evropský parlament, Rada a vlády a parlamenty členských států musí poskytnout demokratický rámec pro konzultace, v němž budou moci být veřejnosti předkládána vědecká nebo technologická témata, právní záruky a odpovědi příslušných institucí na otázky občanské společnosti.

1.11 EHSV doporučuje posílit evropskou technologickou diplomacii, aby EU zajistila vyváženější a reciproční podmínky pro obchod a investice, zejména pokud jde o přístup podniků na trh, dotace, veřejné zakázky, transfer technologií, průmyslové vlastnictví a sociální a environmentální normy.

2. **Úvod**

2.1 Bezpečnost sítí 5G má strategický význam pro občany, podniky, celý jednotný trh a technologickou suverenitu EU. Již v roce 2013 zahájila Komise stěžejní iniciativu EU vytvořením partnerství veřejného a soukromého sektoru v oblasti sítí 5G s cílem urychlit výzkum a inovace v oblasti technologií 5G.

2.2 Se ziskem odhadovaným na celosvětové úrovni na více než 100 miliard EUR v roce 2025 je technologie 5G pro Evropu klíčovým zdrojem konkurenceschopnosti na světovém trhu a její kybernetická bezpečnost je proto nepostradatelná pro zajištění strategické autonomie Unie.

2.3 Sítě 5G jsou založeny na současné 4. generaci (4G) síťových technologií a na infrastruktuře optických vláken, poskytují nové kapacity služeb a stávají se ústřední infrastrukturou a faktorem, který umožňuje pro velkou část hospodářství Unie vytvořit nosnou strukturu pro širokou škálu základních služeb zajišťujících fungování vnitřního trhu a udržování a řízení životně důležitých hospodářských a sociálních funkcí, jako je energetika, doprava, bankovní a zdravotnické služby a zemědělské a průmyslové systémy výroby, distribuce a spotřeby.

2.4 Vzhledem k ústřední úloze sítí 5G při provádění digitální transformace hospodářství a společnosti EU a vzhledem k vzájemné propojenosti a mezinárodní povaze infrastruktury, z níž digitální systém vychází, a k přeshraniční povaze příslušných hrozeb by jakákoli významná zranitelná místa a/nebo významné incidenty v oblasti kybernetické bezpečnosti týkající se sítí 5G, které se vyskytnou v jednom členském státě, měly dopad na Unii jako celek. Proto by měla být přijata opatření na podporu vysoké společné úrovně kybernetické bezpečnosti sítí 5G.

2.5 V roce 2016 Evropská komise – v rámci souboru iniciativ zahájeného sdělením o gigabytovém připojení pro konkurenceschopný jednotný digitální trh ([1]) ([2]) a zahrnujícího reformu regulačního rámce pro elektronické komunikace ([3]) a funkcí Sdružení evropských regulačních orgánů v oblasti elektronických komunikací (BEREC) ([4]), priority v oblasti normalizace IKT pro jednotný digitální trh ([5]) a opatření na podporu internetového připojení v místních komunitách ([6]) – přijala akční plán EU pro sítě 5G ([7]), k němuž se EHSV pozitivně vyjádřil ([8]), s cílem posílit úsilí EU o zavedení infrastruktury a služeb pro sítě 5G na jednotném digitálním trhu pomocí plánu pro veřejné a soukromé investice do infrastruktury 5G v EU a cílem zavést do roku 2020 komerční sítě 5G.

2.6 Podle definice uvedené v doporučení Komise ([9]) se „sítěmi 5G" rozumí „soubor všech relevantních prvků síťových infrastruktur pro mobilní a bezdrátovou komunikační technologii používanou pro připojení a služby s přidanou hodnotou s vyspělými výkonnostními charakteristikami, jako jsou velmi vysoká rychlost přenosu dat a kapacita, komunikace s nízkou latencí, mimořádně vysoká spolehlivost nebo podpora vysokého počtu připojených zařízení".

2.7 V doporučení se uvádí, že Komise bude podporovat provádění přístupu EU ke kybernetické bezpečnosti sítí 5G a bude na žádost členských států pracovat na zajištění bezpečnosti infrastruktury 5G a dodavatelského řetězce, případně s využitím všech dostupných nástrojů, kterými jsou:

— pravidla týkající se telekomunikací, multimédií a kybernetické bezpečnosti,

— koordinace v oblasti standardizace a certifikace na úrovni EU,

— rámec pro kontrolu přímých zahraničních investic na ochranu evropského dodavatelského řetězce sítí 5G,

— nástroje na ochranu obchodu,

— pravidla hospodářské soutěže,

— veřejné zakázky, které zajistí, aby byly řádně zohledněny bezpečnostní aspekty,

— programy financování EU zajišťující, aby příjemci dodržovali příslušné bezpečnostní požadavky.

2.8 V červenci 2019 předložily členské státy skupině pro spolupráci zřízené na základě směrnice o bezpečnosti sítí a informací ([10]) (složené ze zástupců každého členského státu), Komisi a Agentuře Evropské unie pro kybernetickou bezpečnost (ENISA) výsledky svých vnitrostátních posouzení rizik spolu s informacemi o hlavních činnostech, hrozbách a zranitelných místech podle normy ISO/IEC 27005 ohledně infrastruktury 5G a hlavních scénářů rizik, kde popsaly možné způsoby, jimiž by subjekty představující hrozbu mohly využívat určitých zranitelných míst v rámci určité činnosti. Tato vnitrostátní posouzení byla základem následného koordinovaného posouzení a společného „souboru nástrojů" možných opatření ke zmírnění rizik.

2.9 V říjnu 2019 předložila skupina pro spolupráci v oblasti bezpečnosti sítí a informací s podporou Komise a agentury ENISA zprávu o koordinovaném posuzování rizik pro kybernetickou bezpečnost sítí páté generace (5G) v rámci celé EU, která popsala několik důležitých výzev pro bezpečnost souvisejících s klíčovými technologickými inovacemi softwaru, aplikací a služeb, s úlohou dodavatelů při vytváření a používání sítí 5G a se stupněm závislosti na jednotlivých dodavatelích. Patří mezi ně:

— zvýšená míra vystavení útokům a růst počtu potenciálních přístupových bodů pro pachatele takových útoků,

— zvýšená citlivost v důsledku nových charakteristik architektury a funkčních vlastností sítí 5G,

— rizika spojená se závislostí provozovatelů mobilních sítí na dodavatelích, kdy se zvyšují možnosti útoků využitelné původci ohrožení,

---

([1]) Čl. 168 odst. 1 SFEU „Činnost Unie doplňuje politiku členských států…"
([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]) Úř. věst. C 125, 21.4.2017, s. 74.
([9]) Doporučení Komise (EU) 2019/534 ze dne 26. března 2019 Kybernetická bezpečnost sítí 5G Úř. věst. L 88, 29.3.2019, s. 42.
([10]) Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016, s. 1).

— význam rizikového profilu jednotlivých dodavatelů pro možné mimounijní zásahy,

— zvýšená rizika plynoucí ze silné závislosti na dodavatelích v souvislosti s možným přerušením dodávek způsobeným obchodním nebo jiným napětím,

— ohrožení dostupnosti a integrity sítí z hlediska bezpečnosti, důvěrnosti a ochrany soukromí.

2.10 Všechny tyto výzvy vytvářejí nové bezpečnostní paradigma, které si žádá přezkum současného politického a bezpečnostního rámce vztahujícího se na toto odvětví a jeho ekosystém a vyžaduje, aby členské státy přijaly nezbytná zmírňující opatření.

2.11 Dne 21. listopadu 2019 zveřejnila agentura ENISA zprávu nazvanou Přehled hrozeb pro sítě 5G, v níž zhodnotila hrozby související s pátou generací mobilních telekomunikačních sítí a do níž zahrnula zprávu členských států EU.

2.12 Dne 29. ledna 2020 zveřejnila skupina pro spolupráci v oblasti bezpečnosti sítí a informací dokument *Cybersecurity of 5G networks – EU toolbox of risk mitigating measures* ([11]) (Kybernetická bezpečnost sítí 5G – soubor nástrojů EU pro zmírnění rizik) s možným společným souborem opatření schopných zmírnit hlavní rizika v oblasti kybernetické bezpečnosti sítí 5G a poskytnout pokyny pro výběr opatření, která by měla být prioritou v plánech zmírňování na vnitrostátní a unijní úrovni. Ve stejný den přijala Komise sdělení podporující soubor opatření ([12]), které je předmětem tohoto stanoviska.

2.13 Hlavními zúčastněnými stranami síťové infrastruktury 5G jsou:

— občané, spotřebitelé a koneční uživatelé sítí 5G;

— provozovatelé mobilních sítí: subjekty, které poskytují uživatelům služby mobilních sítí a spravují vlastní síť s pomocí třetích stran;

— dodavatelé provozovatelů mobilních sítí: subjekty, které poskytují služby nebo infrastrukturu provozovatelům mobilních sítí za účelem vybudování a/nebo správy jejich vlastních sítí. Tato kategorie zahrnuje: výrobce telekomunikačních zařízení, další dodavatele třetích stran, jako jsou dodavatelé cloudové infrastruktury, systémoví integrátoři, poskytovatelé zabezpečení a údržby nebo výrobci přenosových zařízení;

— výrobci připojených zařízení a poskytovatelé souvisejících služeb: subjekty poskytující objekty nebo služby, které se budou připojovat k sítím 5G (např. chytré telefony, propojená vozidla, elektronické zdravotnictví), a související součásti služeb obsažené v plánu kontroly sítí 5G, který je definován v architektuře založené na službách nebo na Mobile Edge Computing;

— další zúčastněné strany včetně poskytovatelů služeb a obsahu.

Všechny tyto zúčastněné strany jsou důležitými zúčastněnými stranami v oblasti bezpečnosti, a to jak z hlediska přispívání ke kybernetické bezpečnosti sítí 5G, tak jako potenciální vstupní body nebo přenašeče vhodné pro útoky. Proto je důležité posoudit rizika spojená s jejich postavením v ekosystému 5G.

2.14 Hlavní tradiční kategorie hrozeb jsou spojeny s narušením důvěrnosti, integrity a dostupnosti. Konkrétněji bylo zjištěno, že řada scénářů ohrožení zaměřených na sítě 5G se týká zejména:

— přerušení místní nebo globální sítě 5G (dostupnost),

— špionáže datového provozu v infrastruktuře sítí 5G (důvěrnost),

— úpravy nebo přesměrování datového provozu v infrastruktuře sítí 5G (integrita a/nebo důvěrnost),

— zničení nebo změny jiných digitálních infrastruktur nebo informačních systémů prostřednictvím sítí 5G (integrita a/nebo dostupnost).

2.15 Hrozby, které představují státy nebo subjekty podporované státem, jsou považovány za nanejvýš významné, neboť zde jde skutečně o nejzávažnější a nejpravděpodobnější autory hrozeb, protože mohou mít motivaci, úmysly a především schopnost provádět trvalé a sofistikované útoky na bezpečnost sítí 5G.

([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.

Ačkoli řada těchto zranitelných míst není specifická pro sítě 5G, je pravděpodobné, že se jejich počet a význam se sítěmi 5G zvýší v důsledku větší složitosti technologie a budoucí větší závislosti ekonomik a společnosti na této infrastruktuře.

2.16 Zejména proto, že sítě 5G budou z velké části založeny na softwaru, by hlavní bezpečnostní nedostatky (například ty, které jsou důsledkem nedostatečných procesů vývoje softwaru u dodavatelů zařízení) mohly útočníkům usnadnit záměrné vkládání zadních vrátek do výrobků a ztěžovat jejich odhalení. To může zvýšit možnost, že jejich využívání bude mít zvlášť závažný a rozšířený negativní dopad. Problémy s kybernetickou bezpečností sítí 4G ještě nebyly plně vyřešeny a problémy s 5G by mohly exponenciálně růst.

2.17 Je třeba zvážit také zranitelná místa spojená s procesem nebo konfigurací, kterými jsou:

— nedostatek specializovaného a školeného personálu na ochranu, monitorování a údržbu sítí 5G,

— nedostatky týkající se přiměřených vnitřních kontrol bezpečnosti, postupů sledování a systémů řízení bezpečnosti a nedostatky v postupech řízení rizik,

— nepřiměřenost postupů týkajících se zabezpečení nebo provozní údržby, jako je aktualizace softwaru či správa opravných programů (patch) v sítích 5G,

— nedodržování norem 3GPP nebo nesprávné provádění standardů,

— nedostatky v návrhu nebo architektuře sítě včetně chybějících účinných nouzových mechanismů a mechanismů pro zajištění kontinuity a nepřiměřené nebo nesprávné konfigurace, například při virtualizaci nebo v souvislosti s právy v oblasti správy nebo přístupu,

— neodpovídající kritéria pro místní a vzdálený přístup k síťovým komponentům,

— nedostatečné požadavky na bezpečnost v procesu dodávek: toto zranitelné místo může mít podobu nevhodných strategií pro výběr dodavatelů nebo nedostatečného upřednostnění bezpečnosti před jinými aspekty.

2.18 Rizikové profily jednotlivých dodavatelů musí být posouzeny na základě různých faktorů, kterými jsou zejména: možnosti, že dodavatel bude subjektem zásahů ze zemí mimo EU, umožněných silnými vazbami mezi dodavatelem a vládou některé třetí země; právní předpisy třetích zemí, zejména pokud neexistují legislativní nebo demokratické kontroly a rovnováhy a dceřiné společnosti provozující činnost v EU by následně mohly být odrazovány od dodržování právních předpisů EU nebo chybí dohody o bezpečnosti nebo ochraně údajů mezi EU a dotyčnou třetí zemí; charakteristiky podnikového vlastnictví dodavatele; schopnost třetí země vyvinout jakoukoli formu tlaku, a to i ve vztahu k místu výroby zařízení; obecná kvalita produktů a postupů kybernetické bezpečnosti dodavatele, včetně stupně kontroly vlastního dodavatelského řetězce a přiměřených priorit pro bezpečnostní postupy.

2.19 Členské státy se dohodly, že zajistí, aby byla zavedena opatření k odpovídající a přiměřené reakci na již zjištěná rizika a možná budoucí rizika. Zejména odsouhlasily, že zajistí, že budou schopny omezit, zakázat a/nebo uložit v souladu s přístupem založeným na riziku zvláštní požadavky a podmínky pro dodávky, distribuci a provoz zařízení sítě 5G.

2.20 S ohledem na tuto skutečnost by členské státy měly zajistit:

— zpřísnění bezpečnostních požadavků na provozovatele mobilních sítí, jako jsou přísné kontroly přístupu, pravidla bezpečného provozu a sledování a omezení externího zajišťování specifických funkcí;

— posouzení rizikového profilu dodavatele na základě objektivních a jasných kritérií a v souvislosti s tím by měly na základě zásad proporcionality a právní jistoty uplatnit příslušná omezení vůči dodavatelům považovaným za vysoce rizikové, včetně vyloučení nezbytných k účinnému zmírnění rizik, pokud jde o klíčová aktiva, definovaná v rámci koordinovaného posouzení rizik na úrovni EU jako kritická a citlivá;

— přijetí světově uznávaných a zavedených bezpečnostních norem a osvědčených postupů založených na konsensu;

— dostupnost vhodné strategie využívání více prodejců pro každého provozovatele, aby bylo možné zabránit jakékoli velké závislosti na jediném dodavateli nebo dodavatelích s podobným rizikovým profilem, případně takovou závislost omezit;

— důslednou kontrolu přístupu a bezpečné správy, provozu a sledování sítě při používání certifikace pro komponenty a/nebo procesy sítě 5G. Tato strategie musí být založena na analýze rizik provedené členskými státy a provozovateli, aby volba strategie využívání více prodejců nezvyšovala míru rizika pro síť provozovatele;

— přiměřenou rovnováhu dodavatelů na vnitrostátní úrovni a zamezení závislosti na dodavatelích považovaných za vysoce rizikové, a to i formou podpory větší interoperability zařízení;

— udržování diverzifikovaného a udržitelného dodavatelského řetězce technologií 5G, aby se zabránilo dlouhodobé závislosti, a plné využití nástrojů EU pro kontrolu přímých zahraničních investic, nástrojů na ochranu obchodu, pravidel hospodářské soutěže a pravidel EU pro zadávání veřejných zakázek;

— posílení vnitřních kapacit EU v oblasti technologií 5G a technologií dalších generací využitím příslušných programů a finančních prostředků EU, koordinaci mezi členskými státy v oblasti normalizace posílením kapacit „testování" a „auditu" s cílem dosáhnout konkrétních bezpečnostních cílů a vyvíjet příslušné systémy certifikace EU ve smyslu zákona o kybernetické bezpečnosti a podporu interoperability.

2.21 Jak již několikrát zdůraznila Evropské komise, evropský vnitřní trh je a zůstává otevřený těm, kteří chtějí přijít do Evropy, pokud budou všichni dodržovat jasná a přísná pravidla, založená na objektivních kritériích.

2.22 Rada dne 6. června 2020 zdůraznila význam posílení digitální suverenity a digitální spolupráce v EU a vytvoření synergií v programech EU, jako je Nástroj pro propojení Evropy a program Digitální Evropa s rozvojem digitálních dovedností, význam rozvoje datové ekonomiky, umělé inteligence, kybernetické bezpečnosti a aktivní úlohy digitálních technologií při dosahování cílů Zelené dohody.

3. **Sdělení Komise**

3.1 Evropská komise v reakci na soubor bezpečnostních opatření pro sítě 5G vytvořený komunikační skupinou v oblasti bezpečnosti sítí a informací:

— bude na žádost členských států pracovat na zajištění bezpečnosti infrastruktury 5G a dodavatelského řetězce, případně s využitím všech dostupných nástrojů;

— vyzývá členské státy a orgány, aby zajistily provádění účinných strategií ke zmírnění rizik a přijaly další koordinační opatření na úrovni EU pro jednotný přístup ke kybernetické bezpečnosti sítí 5G;

— vyzývá členské státy, aby pokračovaly v provádění opatření doporučených v závěrech souboru opatření a aby připravily společnou zprávu o jejich provádění, zatímco skupina pro spolupráci v oblasti bezpečnosti sítí a informací bude i nadále pracovat na podpoře provádění souboru opatření;

— v oblastech své působnosti definuje kroky k zajištění kybernetické bezpečnosti sítí 5G a diverzifikovaného hodnotového řetězce technologií 5G, technické normalizace a certifikace, přímých zahraničních investic a ochrany obchodu a hospodářské soutěže, zadávání veřejných zakázek a kybernetické diplomacie, jakož i vlastní programy a fondy, zejména na výzkum, vývoj a inovace, soudržnost a rozvoj.

4. **Obecné připomínky**

4.1 EHSV je přesvědčen, že nové technologie 5G jsou schopny změnit způsob naší interakce se světem. Nabízejí příležitosti pro nové aplikace, obchodní modely, nový životní styl, inteligentní továrny, zvýšenou produktivitu a nové kvalitní služby pro občany, potenciálně otevírají dveře revolučním technologiím, jako jsou automatizovaná vozidla a vyspělé výrobní a distribuční systémy, a umožňují vzájemné propojené tisíců zařízení, která by měla vstoupit do našeho každodenního světa jako součást internetu věcí (IoT). EHSV by však očekával, že Komise posílí posouzení dopadu, studii proveditelnosti a analýzu nákladů a přínosů sítí 5G ve srovnání s použitím technologie 4G nebo telekomunikací založených na optických vláknech. EHSV se domnívá, že technologie 5G musí být zaměřena na dosažení lepšího oběhového využívání zdrojů a omezení velké uhlíkové stopy spojené s energetikou. EHSV zdůrazňuje, že je důležité vyrovnat se prostřednictvím podpory spravedlivé a hladké transformace a řešení nedostatku dovedností se sociálními strukturálními změnami a dosáhnout lépe placených, flexibilních a vysoce kvalifikovaných pracovních míst.

4.2 Trojí riziko – nekontrolované pandemie, nedostatečné nástroje hospodářské politiky a nepředvídatelné geopolitické události (tzv. fenomén „černé labutě") – by mohlo způsobit dlouhodobou recesi světové ekonomiky a zhroucení finančních trhů a jejich opouštění, a to právě v okamžiku, kdy si všechny složky evropské společnosti stále více uvědomují, že udržitelný hospodářský rozvoj a **probíhající digitální revoluce – v rámci níž představují technologie 5G jeden z hlavních nástrojů** – vyžadují přístup, který souběžně zohledňuje technologickou suverenitu, zvýšení produktivity a účinnější využívání zdrojů dostupných s podporou přiměřeného právně-regulačního a hospodářsko-finančního rámce.

4.3 EHSV naléhavě žádá orgány EU a členské státy, aby dokončily jednotný digitální trh, včetně budování kapacit pro integraci a využívání služeb sítí 5G k ochraně a zlepšení konkurenceschopnosti evropských průmyslových odvětví. Vyzývá Evropskou komisi, aby důsledně sledovala pokrok při zavádění a skutečném využívání sítí 5G, a vyzývá členské státy, aby tento proces dále urychlily, a to při zohlednění všech aspektů bezpečnosti a ochrany, včetně aspektů týkajících se dopadu technologií 5G na zdraví obyvatel a na živé ekosystémy, socioekonomického dopadu a dopadu na hospodářskou soutěž, dopadu na vzdělávání a odbornou přípravu, a dále také při zohlednění záruk ohledně dodržování základních práv, například práva na vlastnictví nebo práva na soukromí a bezpečnost osobních údajů.

4.4 EHSV žádá, aby byla EU byla světovým lídrem příští generace mobilních technologií 5G s bezpečnou digitální infrastrukturou jako pevným základním prvkem nové moderní průmyslové strategie Evropy prostřednictvím radikální změny mobilního připojení a s obrovským dynamickým potenciálem pro zvýšení produktivity a pro růst ekonomiky a objemu služeb pro občany, jejich blahobyt a ochranu klimatu a životního prostředí tím, že se EU dostane do čela revoluce spojené s technologiemi 5G.

4.5 Vzhledem k tomu, že kybernetická bezpečnost a národní bezpečnost jsou dva neoddělitelně spojené aspekty, se EHSV domnívá, že každé rozhodnutí o národní bezpečnosti některého členského státu EU musí být přijato v kontextu EU, a že netechnická hodnocení musí být uplatňována objektivně na základě kritérií pro posuzování rizik definovaných na evropské úrovni, aby se zajistilo předvídatelné a harmonizované regulační prostředí v celé Evropě, které zaručí plnou interoperabilitu.

4.6 EHSV se domnívá, že možnosti chování příjemců významně ovlivňuje kvalita informací a způsoby komunikace – tzv. rámcový efekt, tj. kontextový efekt, nebo významná pozice (význačný rys). Cíl v podobě posílení postavení spotřebitele se proto promítá do identifikace nástrojů zaměřených na vzdělávání spotřebitelů a posílení jejich schopností, aby se z nich stali aktivní hráči na digitálním trhu. EHSV uznává potřebu poskytovat občanům aktuální a správné informace o přínosech a rizicích technologií 5G na základě konsensu drtivé většiny vědecké obce a poukázat na aspekty, v nichž je tento konsensus nejistý.

4.7 EHSV je přesvědčen, že přístup na evropský digitální trh musí být i nadále volný pro jakýkoliv podnik bez diskriminace, ale jen v rámci dodržování evropského rámce pevných a jasných pravidel, norem a hodnotících a bezpečnostních kritérií, která do středu evropské strategie staví oživení a obnovu technologické suverenity, která je Evropě vlastní.

4.8 Přestože mezi pět největších poskytovatelů infrastruktury patří dva evropští, dva čínští a jeden korejský ([13]), žádná významná evropská společnost nepatří mezi přední výrobce zařízení a čipových sad využívajících technologii 5G. EHSV je přesvědčen, že musí být zaručena pluralita dodavatelů, z nichž alespoň jeden musí mít evropskou mateřskou společnost, a že je třeba zajistit rámec interoperability a plné zastupitelnosti hardwarových a softwarových součástí, aby byla zajištěna mimo jiné plná evropská technologická suverenita v rámci silné mezinárodní spolupráce a úplné reciprocity otevřenosti, přístupu a působení na trzích. Této diverzifikace by bylo možné využít, pokud bude možná interoperabilita služeb a vlivem rozmanitosti se nezvýší kybernetická bezpečnostní rizika.

4.9 EHSV se domnívá, že je nezbytné, aby se Evropa ve střednědobém horizontu zaměřila na samostatnost a soběstačnost v této oblasti, a to výraznou podporou výzkumu a plurality evropských společností. EHSV vítá soubor opatření dohodnutý členskými státy k řešení bezpečnostních rizik (ochrana a bezpečnost) spojených se zavedením technologie 5G, která byla již identifikována v rámci evropského posouzení. Domnívá se však, že přísné a bezpečné limity expozice elektromagnetickým polím doporučené na úrovni EU a založené na aktualizovaných pokynech Mezinárodní komise pro ochranu před neionizujícím zářením (ICNIRP), která byla uznána Světovou zdravotnickou organizací (WHO), by se měly uplatňovat pro všechna frekvenční pásma stanovená pro sítě 5G ([14]). Limity ICNIRP jsou založeny na zásadě předběžné opatrnosti, protože jsou 50krát nižší než hladiny účinku na veřejné zdraví stanovené na základě dostupných vědeckých důkazů.

([13]) Mezi tuto pětici světových dodavatelů v současnosti patří: Ericcson, Nokia, Huawei, ZTE a Samsung.
([14]) EP – E-003040/2019 odpověď paní Kyriakides jménem Evropské komise (17. 1. 2020).

4.10 EHSV však poukazuje na to, že ICNIRP neuznává celá vědecká obec a někteří vědci prosazují mnohem přísnější limity pro expozici obyvatelstva podle zásady ALARA („na co nejnižší rozumně dosažitelné úrovni"). Mezi řešení, která by mohla být navržena k doplnění komunikační infrastruktury 5G, patří využití stálého datového připojení prostřednictvím existujících nerádiových technologií (kabel ethernet, optická vlákna atd.) tam, kde je použití stálé (např. bankomaty, bankovní POS terminály, průmysloví roboti, lékařští roboti na dálkové ovládání atd.), a tam, kde vyvíjejí činnost uživatelé přenosu velkého objemu dat (poskytovatelé digitálních služeb, společnosti/podniky atd.); internet věcí přítomný ve stálých, nemobilních lokalitách (inteligentní domácnosti, inteligentní města, senzory v zařízení technické infrastruktury atd.).

4.11 Evropská komise, Evropský parlament, Rada a vlády a parlamenty členských států musí poskytnout demokratický rámec pro konzultace, v němž budou moci být veřejnosti předkládána vědecká nebo technologická témata, právní záruky a odpovědi příslušných institucí na otázky občanské společnosti.

4.12 Podle EHSV je třeba klást větší důraz na nástroje pro uživatele, občany a příslušné organizace občanské společnosti, které jsou omezené a nedostatečně účinné, a to nad rámec správného důrazu na správná opatření týkající se pravomoci vnitrostátních regulačních orgánů a úlohy telekomunikačních operátorů.

4.13 EHSV uznal ([15]) existenci problému s elektromagnetickou přecitlivělostí (EHS) a vyjádřil své obavy, přičemž považuje za povzbudivé konstatování, že probíhají další hloubkové výzkumy za účelem pochopení problému a jeho příčin, a naléhá na EK, aby pokračovala ve své práci v této oblasti a aktualizovala ji.

4.14 Podle názoru EHSV je nezbytná důvěryhodnost poskytovatelů telekomunikačních a aplikačních služeb v sítích 5G, protože správa informací na internetu je základem služeb v oblasti agregovaných údajů, které uživatelé shromažďují a zpracovávají prostřednictvím technologických, právních a daňových mechanismů, a vytváří tak přímé vzájemné vztahy mezi objekty, stroji a algoritmy.

4.15 EHSV navrhl ([16]) přejít od koncepce vlastnictví údajů k definici práv fyzických i právnických osob v oblasti údajů. Spotřebitelé by měli mít kontrolu nad údaji vytvářenými připojenými zařízeními, aby bylo zaručeno soukromí spotřebitele společně s dostupností, interoperabilitou a přenosem údajů, přičemž by měla být zajištěna odpovídající ochrana a důvěrnost údajů, spravedlivá hospodářská soutěž a širší výběr pro spotřebitele.

4.16 Obecné nařízení o ochraně údajů (GDPR) by mělo být obohaceno o jasné prováděcí pokyny, aby bylo dosaženo jednotného uplatňování a vysoké úrovně ochrany údajů a spotřebitelů s ohledem na vzájemnou propojitelnost strojů a předmětů, a měla by být revidována pravidla občanskoprávní odpovědnosti a pojištění produktů za účelem jejich přizpůsobení situaci, ve které bude rozhodnutí stále více přijímat software, a to při zaručení plné bezpečnosti.

4.17 EHSV se domnívá, že je nezbytné, aby se členské státy řídily strategickými a technickými doporučeními obsaženými v souboru nástrojů EU a vyhýbaly se vývoji konkrétních vnitrostátních přístupů, jako jsou například další testy a certifikace, které by způsobily roztříštěnost trhu, zpoždění při zavádění technologií a nesrovnalosti mezi trhy, což by s sebou neslo riziko oslabení důvěry v systémy testování a certifikace.

4.18 EHSV se domnívá, že je nezbytné využívat globální normy se zvýšenou podporou ze strany Evropy a společné a uznávané osvědčené postupy, aby bylo možné účinně řídit hrozby, vytvářet úspory z rozsahu, zabránit roztříštěnosti a zaručit interoperabilitu evropských systémů. Rozhovory o technických normách jsou nezbytným vyjasněním, které podnikům umožní znovu soutěžit a získat vedoucí pozici v těchto základních činnostech, které umožňují zavádění pokročilých technologií, jako je technologie 5G a umělá inteligence (AI), na všech trzích.

4.19 EHSV se zejména domnívá, že je nezbytné zaručit posouzení rizikového profilu dodavatelů a uplatnit příslušná omezení vůči dodavatelům považovaným za vysoce rizikové, včetně vyloučení nezbytných k účinnému zmírnění rizik, pokud jde o klíčová aktiva definovaná v rámci koordinovaného posouzení rizik na úrovni EU jako kritická a citlivá.

4.20 EHSV považuje za důležité navýšit investice provozovatelů a dodavatelů do nových technických bezpečnostních prvků – investice, které musí jít ruku v ruce se schopností trhu uznávat a odměňovat všechny iniciativy zaměřené na zvýšení bezpečnosti a odolnosti systémů. Větší viditelnost investic do bezpečnosti by mohla přinést nové prvky tržní odměny.

([15]) Úř. věst. C 242, 2.7.2015, s. 31.
([16]) Úř. věst. C 353, 18.10.2019, s. 79.

4.21 EHSV důrazně podporuje společné intervence na podporu průmyslového využití a vývoje technologií 5G: vyhodnocení potenciálních mezer na trhu či jeho selhání v hodnotovém řetězci 5G, jež by byly důvodem k cíleným intervencím v rámci příštího dlouhodobého rozpočtu, případně projektu společného evropského zájmu v oblasti kybernetické bezpečnosti technologií 5G (ochrana a bezpečnost).

4.22 EHSV zdůrazňuje, že ačkoli se digitální infrastruktura ukázala v době krize spojené s COVID-19 jako odolná a spolehlivá, je zapotřebí dalších investic do infrastruktury 5G, aby bylo možné překonat ještě stále existující digitální propast, která může omezit přístup občanů k elektronickému zdravotnictví, elektronickému vzdělávání a práci na dálku.

4.23 Pokud jde o technologickou diplomacii, považuje EHSV za nezbytné, aby EU zajistila vyrovnanější a reciproční podmínky pro obchod a investice, zejména pokud jde o přístup podniků na trh, dotace, zadávání veřejných zakázek, transfer technologií, průmyslové vlastnictví a sociální a environmentální normy, zejména za přítomnosti „systémových soupeřů podporujících alternativní modely řízení“. Současně musí podporovat volnou hospodářskou soutěž a technické inovace na trhu.

4.24 EHSV důrazně podporuje potřebu zachovat diverzifikovaný a udržitelný dodavatelský řetězec technologií 5G, aby se předešlo dlouhodobé závislosti tím, že bude zajištěna přítomnost více dodavatelů v rámci zastupitelnosti a interoperability, a aby se ve finančním rámci na období 2021–2027 dále posilovaly programy a iniciativy zaměřené na budování kapacit a evropskou suverenitu v oblasti technologií 5G a technologií dalších generací.

4.25 V kontextu evropského plánu na podporu oživení, přijatého dne 27. května 2020, se index digitální ekonomiky a společnosti (DESI) roku 2020 použije jako podklad pro analýzu jednotlivých zemí na podporu digitálních doporučení evropského semestru. To pomůže členským státům zaměřit své priority na reformní a investiční potřeby, což usnadní přístup k nástroji na obnovu a odolnost v hodnotě 560 miliard EUR. Tento nástroj poskytne členským státům finanční prostředky na zvýšení odolnosti jejich ekonomik a zajistí, aby investice a reformy podporovaly ekologickou a digitální transformaci. Vzhledem k tomu, že pandemie měla významný dopad na každou z pěti dimenzí indexu DESI, je třeba závěry z roku 2020 týkající se sítí 5G chápat ve spojení s četnými opatřeními přijatými Komisí a členskými státy k řízení krize a podpoře obnovy.

V Bruselu dne 16. září 2020.

předseda
Evropského hospodářského a sociálního výboru
Luca JAHIER