PREBIEHAJÚCE ZMENY V PRÁVNEJ ÚPRAVE KYBERNETICKEJ BEZPEČNOSTI

prof. JUDr. PhDr. Tomáš Gábriš, PhD., LLM, MA*

Abstrakt: Príspevok poukazuje na nedokonalú implementáciu EÚ Toolboxu ku kybernetickej bezpečnosti 5G sietí v podmienkach Slovenskej republiky. Autor približuje a kriticky hodnotí prebiehajúcu (a meškajúcu) novelizáciu príslušnej právnej úpravy. Za hlavné nedostatky predloženého návrhu novely zákona o kybernetickej bezpečnosti považuje nedostatočné vymedzenie politického rizika dodávateľov a absentujúcu reguláciu diverzifikácie dodávateľov produktov a služieb a skríningu priamych zahraničných investícií. Návrh tak na jednej strane ide nad rámec EÚ Toolboxu v rozsahu subjektov a služieb, ktorých sa má novela dotknúť, ale na druhej strane opomína viaceré základné odporúčania Toolboxu.
Kľúčové slová: kybernetická bezpečnosť, 5G siete, EÚ Toolbox

Vývoj právnej úpravy kybernetickej bezpečnosti musí nevyhnutne reagovať na pribúdajúce a meniace sa bezpečnostné riziká a hrozby, vyplývajúce z prebiehajúcich spoločenských a technologických zmien. Spoločenské zmeny súvisia najmä s presunom každodenného života a aktivít všetkých fyzických a právnických osôb, ale i štátov a ich orgánov, do digitálneho priestoru.[1] Uvedený spoločenský vývoj sa stáva obzvlášť očividným práve v súčasných podmienkach pandémie ochorenia COVID-19 a s tým spojenej digitalizácie všetkých druhov sociálnych kontaktov. Technologickým faktorom, na ktorého nástup musí právna úprava kybernetickej bezpečnosti reagovať, je aktuálne najmä

* Autor pôsobí ako profesor teórie a dejín štátu a práva na Právnickej fakulte Trnavskej univerzity v Trnave. Je členom riešiteľského kolektívu projektu Právnickej fakulty Univerzity Palackého v Olomouci k problematike digitálnej suverenity EÚ, podporeného Grantovou agentúrou Českej republiky. Príspevok je výstupom uvedeného projektu GAČR 20-27227S "*The Advent, Pitfalls and Limits of Digital Sovereignty of the European Union*".

1 Porovnaj ŠULC, V. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018.

nástup piatej generácie sietí – „5G sietí" – ktorých využívanie má podľa predpokladov zasiahnuť takmer všetky sféry života, a má mať i významný ekonomický rozmer.[2] V príspevku poukážeme na nový druh politických (hybridných) rizík a hrozieb, ktorým v tejto súvislosti čelí kybernetická bezpečnosť 5G sietí, priblížime reakciu na tieto skutočnosti na úrovni Európskej únie, a predstavíme aktuálny pokus o implementáciu príslušných opatrení na našej vnútroštátnej úrovni.

1. 5G siete ako výzva pre kybernetickú bezpečnosť

Definícia 5G sietí vychádza z Odporúčania Komisie z 26. marca 2019 o kybernetickej bezpečnosti 5G sietí, kde je uvedená v bode II. (2) (a) nasledujúco: „„*siete 5G" sú 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. Môžu zahŕňať tradičné sieťové prvky založené na predchádzajúcich generáciách mobilných a bezdrôtových komunikačných technológií ako 4G alebo 3G. Sieťami 5G by sa mali rozumieť všetky príslušné časti siete*."[3]

Správa „Koordinované zhodnotenie rizika kybernetickej bezpečnosti 5G sietí" („*EU coordinated risk assessment of the cybersecurity of 5G networks*")[4] identifikovala nasledujúce rozdiely medzi 5G sieťami a doteraz používanými generáciami sietí:

---

[2] BARTOCK, M., CICHONSKI, J., SOUPPAYA, M. *5G Cybersecurity : Preparing a Secure Evolution to 5G*. [online] https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32019H0534&from=EN [31.12.2020].

[3] *Odporúčania Komisie z 26. marca 2019 o kybernetickej bezpečnosti 5G sietí*. [online] https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32019H0534&from=EN [31.12.2020].

[4] *EU coordinated risk assessment of the cybersecurity of 5G networks : Report*. [online] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132 [31.12.2020].

– presun k softvéru a virtualizácii prostredníctvom technológií „*Software Defined Networks (SDN)*“ a „*Network Functions Virtualisation (NFV)*“, čo bude predstavovať zásadný posun od tradičnej sieťovej architektúry, pretože funkcie už nebudú založené na špecializovanom hardvéri a softvéri; namiesto toho bude funkčnosť a diferenciácia prebiehať v softvéri;
– „rozkúskovanie siete“, ktoré umožní do veľkej miery podporiť oddelenie rôznych vrstiev služieb v tej istej fyzickej sieti, čím sa zvýšia možnosti ponuky diferencovaných služieb v celej sieti;
– menej centralizovaná architektúra ako v predchádzajúcich generáciách mobilnej siete, čo umožní sieti riadiť prenos k výpočtovým zdrojom a službám tretích strán v blízkosti koncového používateľa, čím sa zaisťujú kratšie doby odozvy, než to bolo doteraz.

Pokiaľ ide o ekonomický význam technológie 5G, podľa oznámenia Komisie s názvom „5G pre Európu: Akčný plán“ by „*Celosvetové príjmy z 5G mali v roku 2025 dosiahnuť ekvivalent 225 miliárd eur*.“[5] Komisia preto už v roku 2013 zahájila partnerstvo medzi verejným a súkromným sektorom 5G (5G-PPP) podporené z verejných zdrojov vo výške 700 miliónov eur, s cieľom zabezpečiť, aby bola technológia 5G v Európe dostupná do roku 2020.

Aj v záujme zaistenia bezpečnosti tejto novej technológie podniká Európska únia (ďalej len „EÚ“) razantné kroky. Je zrejmé, že to znamená nutnosť zaujať ochranný a preventívny postoj, pokiaľ ide o výrobky a služby používané v EÚ, závislé od 5G technológie, s ohľadom na ich predpokladaný široký rozsah využitia a ekonomický aj spoločenský prínos. V prvom rade EÚ v tejto súvislosti vypracovala tzv. EÚ Toolbox (súbor nástrojov), ktorý okrem základných bezpečnostných štandardov navyše vyžaduje, aby technológia 5G nebola závislá od mo-

[5] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (Brussels, 14.9.2016, COM(2016) 588 final): 5G for Europe: An Action Plan*. [online] https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-588-EN-F1-1.PDF [31.12.2020]. Pozri tiež *Commission Staff Working Document: 5G Global Developments (Brussels, 14.9.2016 SWD(2016) 306 final)*. [online] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2016:0306:FIN:EN:PDF [31.12.2020].

nopolných účastníkov trhu ani od zahraničných poskytovateľov, ktorí by mohli podliehať zahraničnému vplyvu, narúšajúcemu čo i len potenciálne suverenitu EÚ a jej členských štátov. EÚ tu teda volí prístup, ktorý je širším než doteraz využívaný prístup technologickej ochrany vo sfére kybernetickej bezpečnosti. Namiesto ochrany pred neželanými zásahmi na technologickej úrovni sa táto nová úprava zameriava aj na možnosť hybridných hrozieb, resp. takého politického zneužívania technológií 5G sietí, ktoré by zasahovalo do digitálnej suverenity EÚ a jej členských štátov. Podobne ako v prípade všeobecných pravidiel kybernetickej bezpečnosti, ktoré sa uplatňujú aj mimo odvetvia elektronických komunikácií [na základe tzv. smernice NIS – Smernice 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], sa však zatiaľ majú povinnosti na zabezpečenie uvedeného cieľa bezpečnosti 5G technológií, a v širšom zmysle aj digitálnej suverenity EÚ, ukladať iba obmedzenému počtu subjektov, konkrétne nateraz iba poskytovateľom služieb elektronických komunikácií v EÚ. Ide tu o realizáciu právnej politiky prenosu povinností na vybrané dominantné subjekty, ktoré musia zaviesť a dodržiavať požadované pravidlá, aby sa zaistila bezpečnosť využívaných technológií, ktorú by inak nemohli zaistiť samotné štáty a EÚ bez priameho riadenia a priamej kontroly každodenného fungovania sektora elektronických komunikácií.

Tento prístup sumarizuje už spomínané odporúčanie Komisie z 26. marca 2019 o kybernetickej bezpečnosti sietí 5G (ďalej len „Odporúčanie"), ktoré v odôvodnení recitálu 19 rozlišuje medzi technickými (technologickými) a inými faktormi kybernetickej bezpečnosti sietí 5G: „*Riešenie rizík v oblasti kybernetickej bezpečnosti sietí 5G by malo zohľadňovať technické aj iné faktory. Medzi technické faktory môžu patriť aj zraniteľné miesta z hľadiska kybernetickej bezpečnosti, ktoré možno využiť na získanie neoprávneného prístupu k informáciám (kybernetická špionáž, či už z ekonomických alebo politických dôvodov) alebo na iné škodlivé účely (kybernetické útoky zamerané na narušenie alebo zničenie systémov a údajov). Medzi dôležité aspekty, ktoré treba zvážiť, by mala patriť potreba chrániť siete počas ich celé-*

ho životného cyklu a potreba zahrnúť všetky príslušné zariadenia, a to aj vo fáze navrhovania, vývoja, obstarávania, zavedenia, prevádzky a údržby sietí 5G."

Recitál (20) objasňuje „iné" faktory kybernetickej bezpečnosti: „*Iné faktory môžu zahŕňať regulačné alebo iné požiadavky, ktoré boli uložené dodávateľom zariadení informačných a komunikačných technológií. Pri posúdení významu týchto faktorov by sa malo okrem iného zohľadniť celkové riziko vplyvu tretej krajiny, najmä v súvislosti s jej modelom riadenia, absenciou dohôd o spolupráci v oblasti bezpečnosti alebo podobných opatrení, ako napr. rozhodnutí o primeranosti, súvisiacich s ochranou údajov medzi Úniou a dotknutou treťou krajinou, alebo či je táto krajina zmluvnou stranou viacstranných, medzinárodných alebo dvojstranných dohôd v oblasti kybernetickej bezpečnosti, boja proti počítačovej kriminalite alebo ochrany údajov.*."

V tomto zmysle sa v Odporúčaní tiež nariadilo, aby Európska agentúra pre kybernetickú bezpečnosť (ENISA) uskutočnila vlastné mapovanie hrozieb v sieťach 5G, a aby do 1. októbra 2019 členské štáty s podporou Komisie spolu s agentúrou ENISA dokončili spoločné preskúmanie vystavenia celej EÚ rizikám súvisiacim so sieťami 5G. Členské štáty predložili výsledky svojich vnútroštátnych hodnotení rizík Komisii a agentúre ENISA v termíne do júla 2019. Príslušná správa bola zverejnená 9. októbra 2019 ako „Koordinované hodnotenie rizika kybernetickej bezpečnosti sietí 5G zo strany EÚ" („*EU coordinated risk assessment of the cybersecurity of 5G networks*") (ďalej len „Správa").[6] V Správe sa skonštatovalo, že pre kybernetickú bezpečnosť sietí 5G majú osobitný význam dve zainteresované strany: operátori mobilných sietí a výrobcovia telekomunikačných zariadení. To sú teda primárne tie subjekty, na ktoré by sa mala regulácia kybernetickej bezpečnosti 5G sietí zameriavať, či už z hľadiska technologických alebo iných faktorov bezpečnosti.

Operátori mobilných sietí (prvá skupina zainteresovaných strán), poskytujúci služby v EÚ, pritom už v súčasnosti podliehajú právu EÚ

[6] *EU coordinated risk assessment of the cybersecurity of 5G networks : Report*. [online] https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049 [31.12.2020].

a detailným vnútroštátnym právnym predpisom členských štátov EÚ, avšak sami zároveň využívajú celý rad subdodávateľov, ktorí im poskytujú rôzne produkty a služby (napr. správu a údržbu siete, dátové centrá atď.), pričom títo subdodávatelia môžu mať sídlo a vykonávať činnosť v inom členskom štáte než sám operátor mobilnej siete, alebo dokonca môžu sídliť aj v tretej krajine mimo EÚ.

Pre trh telekomunikačných zariadení (ktorých výrobcovia predstavujú druhú dôležitú skupinu zainteresovaných strán) je zasa charakteristická predovšetkým obmedzená množina svetových spoločností schopných dodávať požadované technológie veľkým telekomunikačným operátorom. Z hľadiska podielu na trhu sú hlavnými dodávateľmi spoločnosti Huawei, Ericsson a Nokia. Medzi ďalších dodávateľov patria ZTE, Samsung a Cisco10. Niektorí z týchto dodávateľov pritom majú svoje sídlo a hlavné miesto riadenia v EÚ (Ericsson a Nokia), zatiaľ čo ostatní majú ústredie mimo EÚ. Ich správa a riadenie tiež vykazuje značné rozdiely, napríklad pokiaľ ide o úroveň transparentnosti a typ vlastníckej štruktúry spoločnosti.

Tieto skutočnosti samozrejme prinášajú množstvo nových bezpečnostných výziev spojených s oboma skupinami zainteresovaných strán – či už ide o operátorov mobilných sietí s ich dodávateľmi alebo o výrobcov telekomunikačných zariadení. V tejto súvislosti sa v Správe stanovili kritériá, na základe ktorých by malo byť možné hodnotiť rizikové profily jednotlivých dodávateľov, či výrobcov telekomunikačných zariadení, a to z hľadiska iných než technologických faktorov bezpečnosti. Ide najmä o nasledujúce kritériá:

a) pravdepodobnosť, že dodávateľ bude podliehať neželanému vplyvu tretieho štátu mimo EÚ, z dôvodu:
   - silného prepojenia medzi dodávateľom a vládou tretieho štátu;
   - právnej úpravy tretieho štátu, najmä ak neexistujú legislatívne alebo demokratické brzdy a rovnováhy alebo ak neexistujú dohody o bezpečnosti alebo ochrane údajov medzi EÚ a daným tretím štátom;
   - špecifík korporátnej štruktúry dodávateľa;
   - schopností tretieho štátu vyvíjať akúkoľvek formu nátlaku vo vzťahu k miestu výroby zariadenia.

b) schopnosť dodávateľa reálne zabezpečiť dodávku produktov a služieb.[7]

S cieľom zmierniť identifikované riziká a hrozby kybernetickej bezpečnosti sa mal začiatkom roku 2020 na základe najlepších vnútroštátnych postupov pripraviť súbor vhodných, účinných a primeraných možných opatrení na riadenie rizík na vnútroštátnej úrovni aj na úrovni EÚ. Tento súbor nástrojov („*Toolbox*“) mal obsahovať:

a) zoznam druhov bezpečnostných rizík, ktoré môžu ovplyvniť kybernetickú bezpečnosť sietí 5G (napr. riziko dodávateľského reťazca, riziko zraniteľnosti softvéru, riziko kontroly prístupu, riziká vyplývajúce z právneho a politického rámca, do ktorého dodávatelia zariadení informačných a komunikačných technológií patria) a
b) súbor možných zmierňujúcich opatrení (napr. certifikácia pre hardvér, softvér alebo služby, formálne testy hardvéru a softvéru alebo kontroly zhody, procesy zabezpečujúce, aby existovali a boli vymáhané kontroly prístupu, identifikácia výrobkov, služieb alebo dodávateľov, ktorí sa považujú za potenciálne nebezpečných, atď.).

Dňa 29. januára 2020 bol skutočne zverejnený „Súbor nástrojov EÚ na opatrenia na zníženie rizika: Kybernetická bezpečnosť sietí 5G“ („*EU toolbox of risk mitigating measures : Cybersecurity of 5G networks*“) (ďalej len „EÚ Toolbox“), na ktorý sa tu zameriame primárne s ohľadom na jeho doterajšiu (ne)implementáciu v podmienkach Slovenskej republiky. V ten istý deň sprevádzalo EÚ Toolbox aj oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov „Bezpečné zavedenie 5G v EÚ - implementácia súboru nástrojov EÚ“ („*Secure 5G deployment in the EU - Implementing the EU toolbox*“).[8]

---

[7] Tamže, s. 22.

[8] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Secure 5G deployment in the EU - Implementing the EU toolbox" (Brussels, 29.1.2020, COM(2020) 50 final)*. [online] https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-50-F1-EN-MAIN-PART-1.PDF [31.12.2020].

V EÚ Toolboxe boli členské štáty EÚ vyzvané:

- posilniť bezpečnostné požiadavky na operátorov mobilných sietí (napr. zaviesť kontroly prístupu, pravidlá bezpečnej prevádzky, monitorovanie, obmedzenia outsourcingu konkrétnych úloh a funkcií atď.);
- posúdiť rizikový profil dodávateľov a následne uplatniť príslušné obmedzenia pre dodávateľov považovaných za vysoko rizikových;
- zaistiť, aby mal každý operátor vhodnú stratégiu viacerých dodávateľov, aby sa obmedzila akákoľvek závislosť od jedného dodávateľa (alebo dodávateľov s podobným rizikovým profilom), zabezpečiť primeranú rovnováhu dodávateľov na vnútroštátnej úrovni a vyhnúť sa závislosti od dodávateľov považovaných za vysoko rizikových.

EÚ Toolbox pritom konkrétne špecifikoval 1./ strategické opatrenia, 2./ technické opatrenia a 3./ podporné akcie, ktoré majú členské štáty uplatňovať. Z nich sú to predovšetkým strategické opatrenia, ktoré súvisia s „inými" než technologickými faktormi bezpečnosti, a ktoré si v členských štátoch EÚ môžu vyžadovať nové osobitné právne úpravy na vnútroštátnej úrovni, resp. zmeny doterajších právnych úprav.

Celkovo bolo identifikovaných osem strategických opatrení:

- SM01 Posilnenie kompetencií vnútroštátnych orgánov;
- SM02 Vykonávanie auditov operátorov a vyžadovanie informácií;
- SM03 Posudzovanie rizikového profilu dodávateľov a uplatňovanie obmedzení pre dodávateľov považovaných za vysoko rizikových;
- SM04 Kontrola využívania dodávateľov služieb a zariadení;
- SM05 Zabezpečenie rozmanitosti dodávateľov pre jednotlivých operátorov mobilných sietí prostredníctvom vhodných stratégií viacerých dodávateľov;
- SM06 Posilnenie odolnosti na národnej úrovni;
- SM07 Identifikácia kľúčových aktív a podpora rozmanitého a udržateľného 5G ekosystému v EÚ;
- SM08 Udržiavanie a budovanie rozmanitosti a kapacít EÚ v budúcich sieťových technológiách.

Je pritom zrejmé, že potenciálnym zasahovaním zahraničných záujmov do suverenity EÚ a jej členských štátov sa zaoberajú najmä strategické opatrenia pod číslami SM03, SM04 a SM05.

EÚ Toolbox v tejto súvislosti odporúča:

- vytvoriť rámec s jasnými kritériami s prihliadnutím na rizikové faktory;
- vykonávať dôkladné hodnotenia rizikového profilu všetkých relevantných dodávateľov na vnútroštátnej úrovni a/alebo na úrovni EÚ;
- na základe posúdenia rizikového profilu uplatniť vhodné obmedzenia;
- podniknúť kroky na zabezpečenie toho, aby operátori mali zavedené primerané kontroly a procesy na riadenie potenciálnych zvyškových rizík;
- vytvoriť právny regulačný rámec, ktorý určuje podmienky, za ktorých splnenia môžu operátori zveriť určité úlohy a funkcie tretím stranám;
- v prípade externe zabezpečovaných funkcií zaviesť zvýšené bezpečnostné opatrenia.

Stručne povedané, cieľom EÚ Toolboxu je posilniť bezpečnostné požiadavky na operátorov mobilných sietí a ich dodávateľov. Operátori by hlavne mali sami posúdiť rizikový profil svojich dodávateľov a uplatniť príslušné obmedzenia pre dodávateľov považovaných za vysoko rizikových. EÚ Toolbox zároveň vyžaduje, aby mal každý operátor stratégiu viacerých dodávateľov, aby sa zabránilo alebo zamedzilo závislosti od jediného dodávateľa (alebo od dodávateľov s podobným rizikovým profilom).[9]

Komisia vyzvala členské štáty a príslušné inštitúcie, agentúry a ďalšie orgány Únie, aby urýchlene vykonali tieto úkony a dosiahli tak súlad s EÚ Toolboxom. Konkrétne mali členské štáty EÚ do 30. apríla 2020 prijať konkrétne a merateľné kroky na vykonávanie súboru kľúčových opatrení odporúčaných v záveroch EÚ Toolboxu a do 30. júna 2020 pripraviť správu o stave realizácie kľúčových opatrení v jednotlivých členských štátoch.[10]

---

[9] *Secure 5G networks: Questions and Answers on the EU toolbox*. [online] https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127 [31.12.2020].

[10] *Communication from the Commission to the European Parliament, the Coun-*

Dňa 24. júla 2020 členské štáty EÚ s podporou Komisie a agentúry ENISA zverejnili správu o pokroku členských štátov pri implementácii EÚ Toolboxu kybernetickej bezpečnosti 5G sietí, a to na základe vnútroštátnych správ z jednotlivých členských štátov.[11] Podľa tohto vyhodnotenia sa už dosiahol pokrok v prípade niektorých opatrení z Toolboxu, a to najmä v nasledujúcich oblastiach:

– kompetencie národných regulačných orgánov kontrolovať bezpečnosť 5G sietí;
– opatrenia zamerané na obmedzenie zapojenia dodávateľov na základe ich rizikového profilu;
– revízia požiadaviek na bezpečnosť a odolnosť sietí u mobilných operátorov.

Na druhej strane, niektoré opatrenia boli v menej pokročilom štádiu implementácie. Podľa tejto správy išlo najmä o potrebu pokroku pri znižovaní rizika závislosti od vysoko rizikových dodávateľov, zavádzanie vhodných stratégií diverzifikácie dodávateľov, pretože na vnútroštátnej úrovni boli identifikované problémy z dôvodu technických alebo prevádzkových ťažkostí (napr. nedostatočná interoperabilita, veľkosť krajiny atď.) a skríning priamych zahraničných investícií.[12]

Na príkladoch niektorých členských štátov boli pritom identifikované tri základné modelové prístupy implementácie EÚ Toolboxu na vnútroštátnej úrovni:

– prístupy využívajúce „veto": pri nich sa vyžaduje predbežná autorizácia (schválenie) v prípade využívania rizikových dodávateľov,

---

cil, the European Economic and Social Committee and the Committee of the Regions "Secure 5G deployment in the EU - Implementing the EU toolbox" (Brussels, 29.1.2020, COM(2020) 50 final). [online] https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-50-F1-EN-MAIN-PART-1.PDF [31.12.2020].

[11] *Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity*. [online] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68510 [31.12.2020].

[12] Tamže. Pozri tiež *Communication from the Commission : Guidance to the Member States concerning foreign direct investment and free movement of capital from third countries, and the protection of Europe's strategic assets, ahead of the application of Regulation (EU) 2019/452 (FDI Screening Regulation)*. [online] https://trade.ec.europa.eu/doclib/docs/2020/march/tradoc_158676.pdf [31.12.2020].

– prístupy využívajúce „Zoznam neakceptovaných“: pri nich sa vytvára zoznam určitých dodávateľov ako vysoko rizikových alebo nedôveryhodných a
– prístupy využívajúce „Zoznam akceptovaných“: pri nich sa vytvorí zoznam konkrétnych dodávateľov, ktorým je povolené dodávať sieťové zariadenie alebo služby 5G.

Pokiaľ ide o metodiku a faktory na hodnotenie rizikového profilu dodávateľov, podľa správy medzi konkrétne faktory uplatňované jednotlivými členskými štátmi EÚ patria objektívne faktory, ako napríklad pôvod dodávateľov, riziko ovplyvňovania zo strany tretích štátov (napr. pri zohľadnení právneho a politického systému tretieho štátu), informácie špecifické pre konkrétny tretí štát, či spravodajské informácie o možných rizikách a hrozbách.[13]

Napríklad v Taliansku, ktoré využíva prístup „veta“, podľa príslušného zákona dostáva vláda oznámenia týkajúce sa použitia zariadenia alebo služieb súvisiacich so sieťami 5G, ak toto zariadenie alebo služba pochádzajú od dodávateľov zo štátov mimo EÚ.[14] Medzirezortná koordinačná skupina radí vláde o možnom vetovaní takejto zmluvy alebo o ukladaní primeraných bezpečnostných opatrení pri využívaní takéhoto dodávateľa.

V Holandsku zasa vyhláška o bezpečnosti a integrite telekomunikácií z 28. novembra 2019 ustanovuje, že nedôveryhodní dodávatelia budú zaradení na osobitný zoznam neakceptovaných dodávateľov, na základe rôznych kritérií, medzi ktoré patria nasledujúce:
– služba alebo výrobok pochádza zo štátu, ktorého právne predpisy ukladajú neštátnym subjektom povinnosť spolupracovať s vládou tohto štátu, alebo ak je poskytovateľom (dodávateľom) služby alebo produktu priamo štátna (štátom vlastnená) spoločnosť,

[13] *Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity*. [online] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68510 [31.12.2020]. Táto správa ponúka aj porovnanie prístupov jednotlivých členských štátov, ktoré uvádzame nižšie.

[14] Dekrét č. 21 z 15.3.2012 v znení neskorších predpisov.

– služba alebo produkt pochádza zo štátu s aktívnym útočným spravodajským programom zameraným na Holandsko a holandské záujmy, alebo dodávateľ pochádza zo štátu, s ktorým môžu byť vzťahy napäté do takej miery, že sú mysliteľné také vonkajšie aktivity, ktoré môžu mať vplyv na holandské záujmy.[15]

Napokon, Fínsko zaviedlo pravidlo, podľa ktorého sa od prevádzkovateľov vyžaduje, aby zabezpečili, že v prípade potreby môžu byť kritické systémy a ich riadenie, údržba a kontrola bezodkladne presunuté do Fínska.[16]

V mnohých členských štátoch však správa skonštatovala nedostatočný pokrok vo vzťahu k tomu, ako členské štáty EÚ určujú vhodný právny základ na ukladanie povinností z hľadiska diverzifikácie dodávateľov. Doposiaľ sa tak napríklad v Taliansku vyžadovalo od operátorov vypracovanie projektu diverzifikácie, ktorý zahŕňa „vertikálnu" diverzifikáciu (použitie systémov od rôznych dodávateľov v oblasti hardvéru a softvéru) a „horizontálnu" diverzifikáciu (použitie rôznych softvérových riešení).

Slovenská republika pritom patrí do množiny tých štátov, ktoré nielenže nezaviedli pravidlá diverzifikácie dodávateľov, ale zatiaľ ešte ani len reguláciu identifikácie vysoko rizikových dodávateľov, na ktorej sa aktuálne pracuje v podobe novely zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti.

2. Nedostatočná implementácia EÚ Toolboxu v Slovenskej republike

V lete 2020 Národný bezpečnostný úrad Slovenskej republiky (ďalej len „NBÚ") pripravil návrh novely zákona o kybernetickej bezpeč-

[15] *Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity*. [online] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68510 [31.12.2020].

[16] Tamže.

nosti č. 69/2018 Z. z.,[17] s deklarovaným cieľom posilniť právne predpisy v oblasti kybernetickej bezpečnosti so zameraním na posilnenie právomocí príslušných vnútroštátnych orgánov. Predmetom návrhu zákona má byť aj objasnenie niektorých definícií a úprava postupu certifikácie kybernetickej bezpečnosti vyplývajúca z tzv. aktu EÚ o kybernetickej bezpečnosti [*EU Cybersecurity Act* – Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013]. Navyše sa však zavádza i nový inštitút blokovania škodlivého obsahu a má sa tiež podrobnejšie upraviť pozícia audítora kybernetickej bezpečnosti. Verejnosť a orgány verejnej moci mohli predložiť pripomienky k predbežnej informácii o tomto legislatívnom procese v období od 10. júla 2020 do 23. augusta 2020. Už v rámci predbežnej informácie boli pritom k predbežnému návrhu materiálu doručené dve vyjadrenia, ktoré navrhli zohľadniť v návrhu zákona odporúčanie Komisie (EÚ) 2019/534 z 26. marca 2019 o kybernetickej bezpečnosti sietí 5G, ako aj konkrétne opatrenia vyplývajúce z balíka nástrojov EÚ Toolbox.

Napriek tomu navrhovaný text po jeho zverejnení nezohľadňoval EU Toolbox v dostatočnej miere, a naopak sústredil sa práve na tie otázky, ktoré i verejnosť považovala za sporné – najmä blokovanie škodlivého obsahu a prístup NBÚ do všetkých informačných systémov prevádzkovateľov základných služieb. V súvislosti s možnosťou zákazu využívania produktov a služieb niektorých dodávateľov návrh neobsahoval žiadne konkrétne kritériá pre vyhodnotenie rizikovosti týchto dodávateľov a ich produktov a služieb. Napokon, o diverzifikácii dodávateľov návrh úplne mlčal. Pôvodný návrh teda dával NBÚ do rúk príliš široké oprávnenia bez akýchkoľvek bŕzd a protiváh, ale pritom nenapĺňal požiadavky EÚ Toolboxu.

[17] *LP/2020/400 Zákon, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a ktorým sa menia a dopĺňajú niektoré zákony*. [online] https://www.slov-lex.sk/legislativne-procesy/SK/LP/2020/400 [31.12.2020].

Na nasledujúcich riadkoch sa zameriame najmä na dva sporné okruhy problémov v predloženom návrhu novely, ktoré súvisia so zákazom využívania niektorých produktov a služieb a s možnosťou blokovania škodlivého obsahu.

Pokiaľ ide o prvý okruh problémov, novonavrhovaný § 27a zavádzal oprávnenie NBÚ zakázať alebo obmedziť prevádzkovateľovi základnej služby (nielen v odvetví elektronických komunikácií) využívať konkrétny produkt, proces alebo službu z dôvodu bezpečnostných záujmov štátu a z dôvodu závažných okolností predpokladaných zákonom. Podľa dôvodovej správy je táto úprava „*pokračovaním implementácie EÚ Toolbox*". Má pritom platiť, že obmedzenie alebo zákaz možno realizovať len na základe podrobnej analýzy rizík a len na základe vyjadrenia Bezpečnostnej rady Slovenskej republiky. Konkrétne rozhodnutie sa má zverejniť v Zbierke zákonov Slovenskej republiky, pričom sa musí určiť aj primeraná doba na odstránenie nežiaduceho produktu a jeho nahradenie novým.

Vo vzťahu k druhému okruhu problémov má nové ustanovenie § 27b a § 27c umožňovať „*blokovanie infikovaných domén a IP adries, ako reaktívne opatrenie vedúce k zamedzeniu prístupu k škodlivému obsahu*". Navrhované ustanovenie upravilo, že NBÚ vykonáva blokovanie v rámci riešenia kybernetického bezpečnostného incidentu. Konkrétne má o ňom vydať rozhodnutie, v ktorom určí metódu (spôsob) blokovania a sám blokovanie vykoná. Spôsob blokovania má vychádzať z metód uvedených vo všeobecne záväznom právnom predpise, ktorý vydá úrad. Ustanovenie § 27c má v nadväznosti na predchádzajúci paragraf ustanoviť možnosť vykonať blokovanie aj na základe žiadosti iného subjektu.

Najmä proti možnosti blokovania škodlivého obsahu sa pritom v rámci medzirezortného pripomienkového konania vyslovilo množstvo pripomienkujúcich subjektov. Celkovo bolo vznesených až 381 pripomienok, z toho 219 zásadných. Okrem toho sa však namietali aj ďalšie naznačené nedostatky návrhu novely – možnosť prístupu NBÚ do všetkých informačných systémov prevádzkovateľov základných služieb a nedostatočná implementácia EÚ Toolboxu.

Asociácia kybernetickej bezpečnosti (ďalej len „AKB") tak naprí-

klad navrhla vypustiť navrhované znenie § 24 ods. 7 o prístupe do informačných systémov (pripomienku v obdobnom zmysle predložila aj Generálna prokuratúra Slovenskej republiky a Ministerstvo vnútra Slovenskej republiky). Mala totiž za to, že v ňom ide o veľmi široké oprávnenie NBÚ požadovať po ktoromkoľvek prevádzkovateľovi základnej služby zasielať mu ním určené systémové informácie zo sietí a informačných systémov. Podľa AKB, „*úrad sa môže doslova kedykoľvek a vo vzťahu ku ktorémukoľvek prevádzkovateľovi základnej služby rozhodnúť, aby mu ním určeným spôsobom zasielal systémové informácie (logy), čo je neprijateľné a zároveň vysoko rizikové, koncentrovať takto citlivé záznamy, nevynímajúc informácie podliehajúce osobitnému režimu ochrany (napr. bankové tajomstvo, daňové tajomstvo a pod.) na jedinom štátnom orgáne podľa jeho ľubovôle, v nim určenom obsahu, rozsahu a forme*.“ Terčom kritiky pritom bolo i to, že súčasne „*úrad navrhuje pri tomto novom inštitúte vyňať pôsobnosť správneho poriadku, čo ešte viac oslabuje účinnú ochranu jednotlivcov pred takýmto výrazným zásahom a zásadne a neprimerane posilňuje kompetenciu úradu, ktorého konanie by mohol posudzovať až súd, a to dávno po tom, čo by jeho rozhodnutie o presmerovaní systémových informácií bolo vykonané. Prípadný výrok súdu o protiprávnosti alebo nezákonnosti rozhodnutia úradu by tak strácal akýkoľvek význam*.“[18]

AKB však primárne navrhovala vypustiť navrhované znenie § 27a až 27c (pripomienku v obdobnom zmysle predložila aj Generálna prokuratúra Slovenskej republiky, Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky, Ministerstvo vnútra Slovenskej republiky a Ministerstvo hospodárstva Slovenskej republiky), v ktorom si NBÚ navrhuje novú kompetenciu, a to rozhodovať o blokovaní škodlivého obsahu pri riešení kybernetického bezpečnostného incidentu a o zákaze niektorých produktov a služieb. Podľa pripomienky ide vo vzťahu k blokovaniu o veľmi široko a neurčito koncipované oprávnenie NBÚ blokovať škodlivý obsah pri riešení kybernetického bezpečnostného incidentu. Išlo by teda „*o ďalšie oprávnenie úradu, pri ktorom absentujú konkrétne pravidlá zamedzujúce zneužitiu, ktoré je*

[18] Tamže.

nepredvídateľné a nie je možné sa voči nemu účinne (právne) brániť, nakoľko konanie úradu v rozsahu tejto kompetencie je vyňaté z pôsobnosti správneho poriadku, v dôsledku čoho sú dotknuté osoby nútené domáhať sa ochrany svojich práv a nárokov výlučne súdnou cestou." „*Súčasne nie je na základe týchto ustanovení zrejmé, ako bude úrad rozhodovať o blokovaní, hlavne o tom, na ktorej infraštruktúre je potrebné blokovanie vykonať ..., čo sa vlastne blokovať bude, napr. iba IP adresa alebo doména, webové sídlo, DNS dotazy, spam? Alebo čokoľvek podľa vlastného uváženia?*" Pripomienkujúce subjekty kladú aj ďalšie otázky: „*Čo, ak takéto zablokovanie znemožní poskytovanie základnej služby? Čo znášanie nákladov, ktoré prevádzkovateľovi vzniknú? Čo časové ohraničenie rozhodnutia? (z návrhu by malo byť zrejmé, že nebude trvať aj po odstránení škodlivého obsahu. Ako sa bude rozhodovať o odblokovaní? V akej lehote? Aj takéto rozhodnutie úradu bude konečné?*"[19]

AKB aj Americká obchodná komora tiež v rámci svojich pripomienok navrhli viac zohľadniť EÚ Toolbox. Pripomienku v obdobnom zmysle predložilo aj Ministerstvo financií Slovenskej republiky. Argumentovali pritom tým, že „*Potreba a nevyhnutnosť implementácie EU Toolboxu do právneho poriadku Slovenskej republiky je podčiarknutá aj závermi, ktoré prijala Európska rada na svojom mimoriadnom zasadnutí 1. a 2. októbra 2020: „11. Európska rada schvaľuje závery Rady z 9. júna 2020 o formovaní digitálnej budúcnosti Európy. Vyzýva EÚ a členské štáty, aby v plnej miere využívali súbor nástrojov EÚ pre kybernetickú bezpečnosť 5G prijatý 29. januára 2020, a najmä aby uplatňovali príslušné obmedzenia týkajúce sa vysokorizikových dodávateľov v prípade kľúčových aktív, ktoré sú v koordinovaných posúdeniach rizík EÚ vymedzené ako kritické a citlivé. Európska rada zdôrazňuje, že potenciálni dodávatelia technológií 5G sa musia posudzovať na základe spoločných objektívnych kritérií.*""

Návrhu novely pritom vytýkali, že práve tzv. strategické opatrenia „*sú oblasťou, na ktorú zákon žiadnym spôsobom nereflektuje (príp. len veľmi okrajovo a účelovo, vyťahujúc si z nich oprávnenia bez akejkoľvek kontroly), nakoľko mu nie sú známe pojmy ako politické riziká, riziká*

[19] Tamže.

spojené s vplyvmi tretích štátov na dodávateľov, hybridné hrozby a pod." a obmedzuje sa na hrozby, zraniteľnosti a riziká technického či technologického charakteru. Dodajme, že tiež nezohľadňuje potrebu diverzifikácie dodávateľov.

Navrhovaná novela tiež podľa pripomienkujúcich subjektov zavádza veľmi široké oprávnenie NBÚ zakázať alebo obmedziť ktorémukoľvek prevádzkovateľovi základnej služby používať konkrétny produkt, proces alebo službu pod vágne koncipovanou podmienkou „*ak je to potrebné na zaistenie kybernetickej bezpečnosti, alebo z dôvodov bezpečnostného záujmu Slovenskej republiky*", pod čo je možné subsumovať v zásade čokoľvek. Poukázali pritom tiež na skutočnosť, že cestou využitou v iných štátoch je vytvorenie zoznamu „rizikových dodávateľov" podľa „*vopred zadefinovaných parametrov, ktoré sú transparentné a objektívne a ktorý (zoznam) následne poskytuje rámec pre prevádzkovateľov základných služieb, akých dodávateľov nemôžu do budúcna využívať. Zoznam je priebežne aktualizovaný, je vytvorený priestor na „obranu" zo strany dodávateľov na tomto zozname vyviniť sa a preukázať, že dané hybridné hrozby a politické riziká na ich strane nie sú alebo už nie sú*." Obe pripomienkujúce inštitúcie (AKB aj Americká obchodná komora) preto navrhli nové paragrafové znenie príslušných ustanovení.

Tieto zásadné pripomienky skutočne NBÚ sčasti zohľadnil a zapracoval. Do ďalšieho legislatívneho procesu tak predložil už mierne pozmenený text návrhu novely. Do právomocí NBÚ však má i podľa tohto upraveného znenia naďalej patriť možnosť blokovania škodlivého obsahu a škodlivej aktivity, ako aj posudzovanie bezpečnostných rizík tretej strany (ale stále sa nezohľadňuje nutnosť diverzifikácie dodávateľov ani skríning priamych zahraničných investícií) – v ustanovení § 5 sa totiž odsek 1 dopĺňa písmenami, ktoré dopĺňajú výpočet kompetencií NBÚ v oblasti kybernetickej bezpečnosti a znejú:

„*y) vydáva rozhodnutie o blokovaní škodlivého obsahu alebo škodlivej aktivity, ktorá smeruje do alebo z kybernetického priestoru Slovenskej republiky (ďalej len „blokovanie") a zabezpečuje vykonanie tohto rozhodnutia; blokovanie vykonáva aj na základe žiadosti,*

af) posudzuje bezpečnostné riziká tretej strany pre kybernetickú bez-

pečnosť Slovenskej republiky a správu o posúdení predkladá Bezpečnostnej rade Slovenskej republiky." .

Na kritiku vyslovenú v medzirezortnom pripomienkovom konaní sa reaguje podrobnejšou úpravou blokovania, s prepojením na predpokladanú vyhlášku o blokovaní. Rozhodnutie NBÚ o blokovaní tak musí spĺňať presne vymedzené náležitosti, keď musí obsahovať najmä:

a) identifikáciu úradu,
b) identifikáciu osoby, ktorá prevádzkuje infraštruktúru, na ktorej je blokovanie potrebné vykonať,
c) identifikáciu škodlivého obsahu alebo škodlivej aktivity,
d) dôvod blokovania,
e) spôsob blokovania,
f) lehotu na vykonanie blokovania, trvanie blokovania a možnosti jeho odblokovania,
g) poučenie.

Na účely blokovania sa pritom škodlivým obsahom rozumie programový prostriedok alebo údaj, ktorý zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident. Škodlivou aktivitou sa rozumie akákoľvek činnosť, ktorá zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident, ako napr. podvodná činnosť, odcudzenie osobných údajov alebo citlivých údajov.

Podľa navrhovaného ustanovenia § 27c, môže NBÚ vykonať blokovanie aj na základe žiadosti iného subjektu podľa osobitného predpisu. Pritom zodpovednosť za škodu spôsobenú blokovaním v takom prípade znáša žiadateľ.

Podrobnosti blokovania má upravovať osobitná vyhláška NBÚ, podľa ktorej návrhu blokovať možno:

1. IP adresu, doménu alebo URL, na ktorých sa nachádza:
   – phishingová stránka alebo server riadiaci phishingové aktivity,
   – škodlivý kód,
   – riadiaci server pre riadenie botnetovej siete.
2. IP adresu alebo doménu, prostredníctvom ktorej sa vykonáva:
   – DDoS útok,
   – skenovanie,
   – bruteforce útoky alebo pokusy,
   – pokusy o prienik.

Správne právne nadefinovanie týchto pojmov a podradenie škodlivých aktivít pod tieto pojmy je nepochybne náročnou legislatívnou úlohou.

V súvislosti s hodnotením rizika, ktoré predstavujú dodávatelia produktov a služieb, resp. všeobecne tretie strany, sa v ustanovení § 20 návrhu novely má za odsek 4 vložiť nový odsek 5, ktorý znie: „*Bezpečnostné opatrenia sa prijímajú a realizujú na základe analýzy rizík kybernetickej bezpečnosti, ktorá určuje pravdepodobnosť vzniku škodlivej udalosti. Súčasťou analýzy rizík je aj analýza politického rizika tretej strany, pričom politické riziko predstavuje také riziko, ktoré je spôsobené geopolitickou lokalizáciou tretej strany a zahŕňa analýzu právnych predpisov v oblasti ochrany základných ľudských práv a slobôd, ochrany osobných údajov a ochrany informácií. Politické riziká úrad zverejňuje v jednotnom informačnom systéme kybernetickej bezpečnosti.*“ V porovnaní s prvotnou textáciou návrhu novely tu teda vidno určitý posun – zaviedol sa pojem politického rizika, pričom je však toto riziko definované iba príkladmi, ako je „geopolitická lokalizácia tretej strany“, čo je samo osebe dosť neurčité vymedzenie rizika. V porovnaní s inými štátmi EÚ možno tiež poukázať na to, že medzi zdrojmi rizika nie je uvedená napríklad štátna kontrola/štátne vlastníctvo dodávateľa tovarov a služieb, čo možno iba veľmi voľne podradiť pod pojem „geopolitická lokalizácia tretej strany“.

Celý proces má pritom podľa návrhu novely vyzerať tak, že pred zákazom používania niektorých produktov či služieb z dôvodov politického rizika požiada NBÚ o vyjadrenie Bezpečnostnú radu, pričom oznámenie o začatí konania sa zverejní na stránke NBÚ (v jednotnom informačnom systéme kybernetickej bezpečnosti) a konečné rozhodnutie o zákaze sa odpublikuje v Zbierke zákonov, ktorá tým sama začne nadobúdať mierne inú povahu než na akú sme dnes zvyknutí. Rozhodnutie pritom bude súdne preskúmateľné, čo tiež v prípade zvrátenia pôvodného rozhodnutia bude vyžadovať ďalšie publikácie v Zbierke zákonov.

Podľa navrhovanej textácie má mať NBÚ právo rozhodnutím zakázať alebo obmedziť používanie konkrétneho produktu, procesu alebo služby využívaných na poskytovanie základnej služby, ak zistí,

že takéto používanie neumožňuje alebo zásadným spôsobom sťažuje udržanie kybernetickej bezpečnosti, a tým ohrozuje život alebo zdravie osôb, hospodárske fungovanie štátu, verejný poriadok, bezpečnosť alebo majetok osôb, alebo ohrozuje bezpečnostné záujmy Slovenskej republiky.

Aj táto textácia je pritom zjavne veľmi široko koncipovaná, pričom v legislatívnom procese sa predkladateľ vyjadril, že podrobnosti by mali byť upravené v doteraz nezverejnenej vyhláške. Otázne pritom zostáva, či takáto vyhláška nepôjde svojimi podrobnejšími ustanoveniami nad rámec zákona samotného.

Napokon, novela zákona navyše stále ani v tomto upravenom znení neupravuje diverzifikáciu dodávateľov tovarov a služieb, čo je jedna z kľúčových požiadaviek EU Toolboxu.

Pre úplnosť, po zohľadnení pripomienok sa len čiastočne zmiernila povinnosť poskytovať NBÚ súčinnosť – vyňali sa z nej v porovnaní s prvotným návrhom spravodajské služby. Podľa novej právnej úpravy (§ 10a) tak „*orgán verejnej moci, prevádzkovateľ základnej služby, právnická osoba a fyzická osoba sú povinní poskytnúť úradu na plnenie jeho úloh podľa tohto zákona požadovanú súčinnosť a informácie získané z vlastnej činnosti dôležité na zabezpečenie kybernetickej bezpečnosti; informácie sa poskytujú len za podmienky, že ich poskytnutím nedôjde k ohrozeniu plnenia konkrétnej úlohy podľa osobitného predpisu alebo spravodajskej služby podľa osobitného predpisu alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb, ktoré konajú v jej prospech, alebo k ohrozeniu medzinárodnej spravodajskej spolupráce*.“ V nadväznosti na to sa tiež obmedzila pôvodne neobmedzená možnosť NBÚ získavať všetky systémové informácie (logy) – vylúčila sa konkrétne oblasť obrany a bezpečnosti a zaviedli sa dva stupne požadovania takýchto informácií – buď ich poskytne sám prevádzkovateľ podľa požiadaviek určených NBÚ, alebo ak ich neposkytne, až potom môže žiadať NBÚ priamy prístup do sietí prevádzkovateľa (§ 24a).

3. Ďalší vývoj na úrovni EÚ

Kým Slovenská republika stále ešte len pracovala na legislatívnom procese novelizácie zákona o kybernetickej bezpečnosti, v decembri 2020 Komisia zverejnila ďalšiu správu o dopadoch na kybernetickú bezpečnosť sietí 5G.[20] Ukázalo sa, že od schválenia EÚ Toolboxu sa dosiahol značný pokrok, a že väčšina členských štátov je na dobrej ceste dokončiť významnú časť implementácie EÚ Toolboxu už v blízkej budúcnosti, aj keď s určitými národnými rozdielmi a s niektorými pretrvávajúcimi nedostatkami, ktoré boli uvedené už v správe o pokroku zverejnenej v júli 2020.[21]

Konkrétne, podľa správy z decembra 2020,[22] pokiaľ ide o diverzifikáciu a spoľahlivosť dodávateľov (SM05 a SM06), niekoľko členských štátov medzičasom zaviedlo opatrenia, ktoré napríklad požadujú, aby operátori predložili svoje vlastné stratégie diverzifikácie vnútroštátnym orgánom a zabezpečili prijatie opatrení na zvýšenie ich odolnosti a bezpečnostnej spoľahlivosti. Komisia tiež udáva, že tie členské štáty, ktoré zatiaľ neprijali konkrétne opatrenia, argumentujú napríklad svojou geografickou rozlohou a tomu zodpovedajúcemu nízkemu počtu možných dodávateľov, ťažkosťami s definovaním vhodných stratégií, problémami s interoperabilitou a i. Sem zrejme patrí aj Slovenská republika.

Mnoho členských štátov tiež vraj požaduje ďalšie konzultácie na úrovni EÚ za účelom prediskutovania možných praktických postupov na národnej úrovni. Na túto tému uskutočnil aj BEREC (Orgán európ-

---

[20] *Commission Staff Working Document : Report on the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks. SWD(2020) 357 final*. [online] https://data.consilium.europa.eu/doc/document/ST-14354-2020-INIT/en/pdf [31.12.2020].

[21] *Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity*. [online] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68510 [31.12.2020].

[22] *Commission Staff Working Document : Report on the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks. SWD(2020) 357 final*. [online] https://data.consilium.europa.eu/doc/document/ST-14354-2020-INIT/en/pdf [31.12.2020].

skych regulátorov pre elektronické komunikácie) prieskum, ktorý sa podrobnejšie zaoberá stavom implementácie SM05 a SM06 a poskytuje prehľad súčasnej dodávateľskej základne operátorov v EÚ.[23]

Osobitný problém pritom vraj podľa tejto ostatnej správy z decembra 2020[24] predstavuje skríning priamych zahraničných investícií. V súčasnosti existuje 15 členských štátov, ktoré majú zavedené národné mechanizmy skríningu. Niekoľko ďalších členských štátov uviedlo, že u nich prebieha proces vývoja systému skríningu priamych zahraničných investícií.[25] Slovenská republika takýto skríning vo svojej novele zákona o kybernetickej bezpečnosti nezohľadňuje, patrí teda medzi tie členské štáty EÚ, ktoré aj v tejto oblasti možno zaradiť do skupiny štátov nedostatočne implementujúcich EÚ Toolbox. V reakcii na nariadenie EÚ 2019/452 z 19. marca 2019, ktorým sa ustanovuje rámec na preverovanie priamych zahraničných investícií do Únie, však aspoň Ministerstvo hospodárstva Slovenskej republiky pripravilo zodpovedajúcu vnútroštátnu právnu úpravu, umožňujúcu realizáciu tohto nariadenia v podmienkach Slovenskej republiky, ktorá by sa mala primerane vzťahovať aj na investície do elektronických komunikácií. Tento aspekt však novela zákona o kybernetickej bezpečnosti výslovne nereflektuje, čo v spojení s inými vyššie uvedenými nedostatkami naznačuje, že ani aktuálne znenie návrhu novely zákona nemusí byť tým konečným.

Záver

Slovenská republika v prebiehajúcom procese novelizácie zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti nateraz nezohľadnila v plnej miere EÚ Toolbox a neimplementovala jeho požiadavky tak, aby zabezpečila cieľ digitálnej suverenity EÚ, ani digitálnej suverenity Slovenskej republiky. V príspevku sme pritom poskytli prehľad rôznych

[23] Tamže.
[24] Tamže.
[25] Tamže.

regulačných modelov používaných v iných členských štátoch EÚ, ktorými sa môže Slovenská republika a ďalšie členské štáty EÚ inšpirovať pri implementácii EÚ Toolboxu – a to najmä z hľadiska zaistenia bezpečnostnej spoľahlivosti dodávateľov, ako aj z hľadiska ich diverzifikácie. Pokiaľ ide o prvé uvedené, dávame pritom na zváženie či namiesto zoznamu neakceptovaných dodávateľov a s tým spojených komplikácií spojených s vylúčením a následným preskúmavaním takýchto rozhodnutí nezvoliť radšej cestu pozitívneho zoznamu „povolených" dodávateľov, zostaveného na základe žiadostí jednotlivých poskytovateľov o zaradenie do takéhoto zoznamu, vyhodnotených na základe objektívnych kritérií, ktoré môžu byť vytvorené napríklad podľa holandského prikladu. Pokiaľ ide o diverzifikáciu, naznačili sme cestu povinnosti predloženia stratégií diverzifikácií samotnými operátormi, a to ako na úrovni vertikálnej, tak i horizontálnej – napríklad podľa vzoru talianskej úpravy. Právna úprava diverzifikácie dodávateľov by však pritom určite mala brať do úvahy aj prechodné, „intertemporálne" aspekty – rešpektovanie existujúcich zmlúv a ich postupné obmedzovanie čo do rozsahu a trvania, s cieľom dosiahnuť cieľ diverzifikácie v určenom časovom horizonte. Napokon, je nevyhnutné zaistiť tiež súlad zákona o kybernetickej bezpečnosti so všeobecnými požiadavkami skríningu priamych zahraničných investícií. V oboch týchto procesoch má hrať významnú rolu Bezpečnostná rada Slovenskej republiky, bolo by však vhodné, aby tieto procesy aj inak boli zladené a vykazovali obdobné prvky. Napokon, nad rámec EÚ Toolboxu už idú kompetencie NBÚ v oblasti prístupu k systémovým informáciám a v oblasti blokovania škodlivého obsahu, pri ktorých je potrebné dbať na to, aby princípy tejto úpravy boli vyjadrené v samotnom zákone, a nie iba vo vykonávacích predpisoch, ktoré by mohli ísť nad rámec zákonného splnomocnenia, v rozpore s princípmi právneho štátu a princípmi výstavby právneho poriadku Slovenskej republiky.

Zároveň však platí, že vývoj právnej úpravy kybernetickej bezpečnosti sa ani doterajšími aktivitami EÚ v oblasti bezpečnosti 5G sietí zďaleka nekončí. Okrem správy o implementácii EÚ Toolboxu boli totiž v decembri 2020 zverejnené aj návrhy ďalších dôležitých dokumentov pre oblasť kybernetickej bezpečnosti – najmä návrh novej

smernice o odolnosti kritickej infraštruktúry[26], či návrh novej smernice o kybernetickej bezpečnosti (tzv. NIS 2),[27] ktorá má za cieľ odstrániť niektoré nedostatky identifikované v rámci aplikácie pôvodnej smernice NIS. Navrhuje sa najmä prestať rozlišovať medzi prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb, ale i zaviesť jasné kritériá veľkosti subjektov, ktoré budú podliehať povinnostiam zo smernice, pričom sa však má zároveň i rozšíriť okruh oblastí, ktoré majú predstavovať predmet ochrany z hľadiska kybernetickej bezpečnosti.[28] Majú sa tiež zaviesť konkrétne minimálne požiadavky na zaistenie kybernetickej bezpečnosti. Predpokladá sa tiež väčší dôraz na preverovanie dodávateľov služieb a väčšia harmonizácia sankcií naprieč členskými štátmi EÚ.[29] V dohľadnej dobe tak zrejme slovenský zákon o kybernetickej bezpečnosti bude čeliť ďalšej podstatnej novelizácii, alebo priamo nahradeniu novým zákonom.

---

26 *Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities*. [online] https://ec.europa.eu/home-affairs/sites/home-affairs/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf [31.12.2020].

27 *Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148*. [online] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823 [31.12.2020].

28 Na viaceré nedostatky právnej úpravy v tejto súvislosti upozorňujú autori komentára ANDRAŠKO, J., GÁBRIŠ, T., HOCHMANN, J., OLEJÁR, D. *Zákon o kybernetickej bezpečnosti. Komentár*. Bratislava: Wolters Kluwer, 2018.

29 Bližšie pozri *Proposal for directive on measures for high common level of cybersecurity across the Union*. [online] https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union [31.12.2020].