Právní analýza:

Kybernetická bezpečnost obnovitelných zdrojů energie

frank bold

frank bold

Obsah

Tato publikace vznikla jako příspěvek expertní skupiny Frank Bold do důležité debaty o zajištění kybernetické bezpečnosti obnovitelných zdrojů energie. Analýza obsahuje robustní know-how, které experti Frank Bold poskytují ve veřejném zájmu bez nároku na honorář – věříme, že poznatky poslouží všem zúčastněným stranám jako hodnotný základ pro diskuzi a identifikaci řešení.

1. Manažerské shrnutí

Tato analýza se zabývá otázkami zajištění kybernetické bezpečnosti obnovitelných zdrojů energie (OZE), a to z právního pohledu. Analýza zkoumá předpisy, které stanoví povinnosti nebo motivují provozovatele OZE k zajištění kybernetické bezpečnosti, či ke zvýšení jejích standardů.

Proč je třeba zabývat se tímto problémem?

Kybernetická bezpečnost OZE je klíčovou otázkou pro zajištění stability a bezpečnosti energetické infrastruktury. Technologie OZE (zejména solární panely a střídače) jsou dodávány včetně softwaru, který není dostatečně chráněný. Hackerské útoky na OZE proto mohou způsobit výpadky dodávek elektřiny s vážnými důsledky pro ekonomiku a společnost. Současná právní úprava však dostatečně neřeší specifika kybernetické bezpečnosti OZE u jejich drtivé většiny (do 100 MW).

Pomůže nový zákon o kybernetické bezpečnosti?

Nový zákon o kybernetické bezpečnosti (Novela) výrazně rozšiřuje okruh regulovaných subjektů. Povinnosti zajišťovat kybernetickou bezpečnost se budou nově vztahovat i na některé provozovatele OZE jako "poskytovatele regulované služby". Týká se však pouze větších výrobců elektřiny z OZE (licencovaných výrobců, kteří jsou středním či velkým podnikem, příp. disponují výrobnou o výkonu 50, resp. 100 MW a více). Drtivá většina provozovatelů OZE však stále nebude přímo regulována.

Jak lze právně řešit kybernetické útoky na OZE?

Právní úprava mimořádných stavů (nouzový stav, stav kybernetického nebezpečí) umožňuje dočasné zásahy do provozu OZE v krizových situacích. Neřeší však dlouhodobé nastavení podmínek pro kybernetickou bezpečnost OZE.

Je možné klást nároky na kybernetickou bezpečnost u veřejných zakázek?

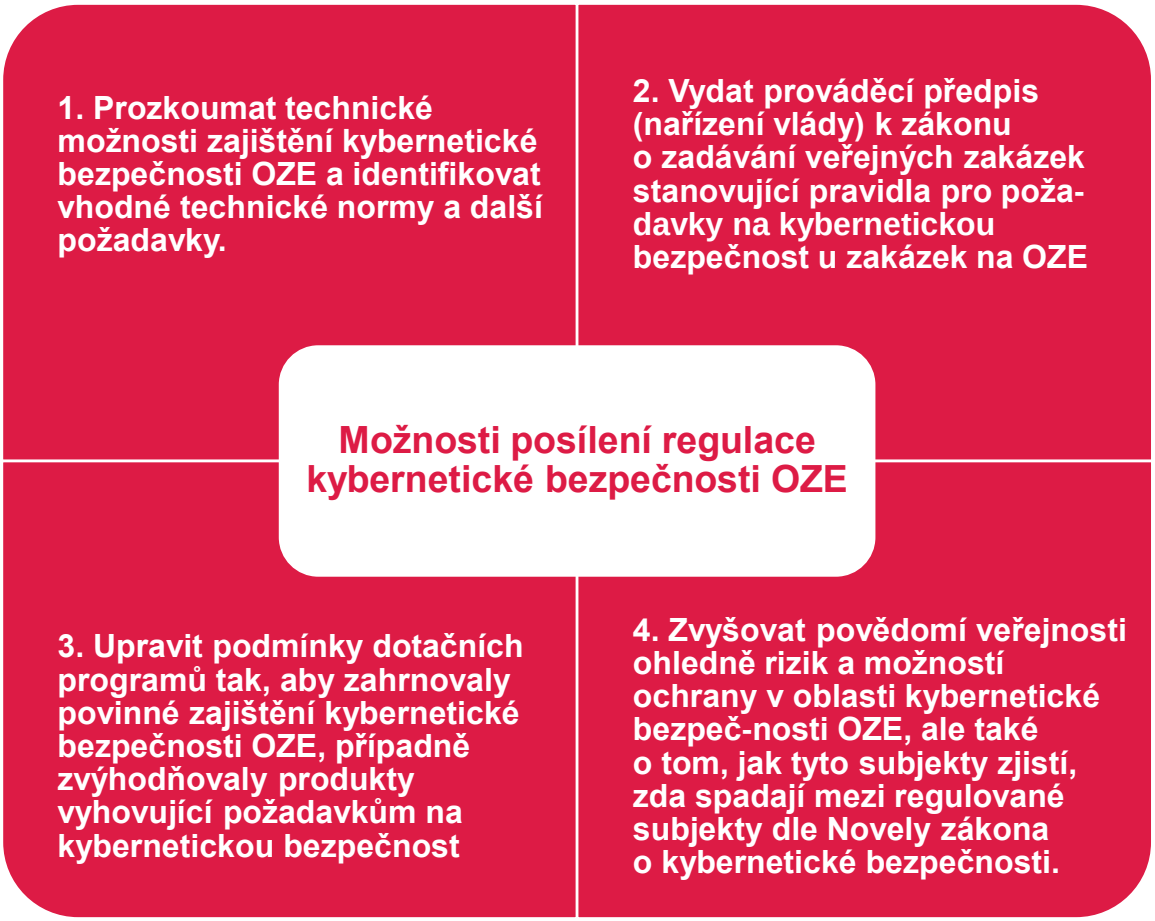
Zákon o zadávání veřejných zakázek umožňuje zadavatelům požadovat zajištění kybernetické bezpečnosti OZE v rámci zadávacích podmínek. Nové nařízení EU o technologiích s nulovými emisemi bude od zadavatelů přímo vyžadovat zohlednění kybernetické bezpečnosti u zakázek na OZE (pokud nezohlední např. sociální nebo zaměstnanecké aspekty, tj. i požadavku v nařízení se lze vyhnout).

Jakou roli hraje v kybernetické bezpečnosti právo EU?

Klíčová je směrnice NIS2, kterou implementuje Novela a dává NÚKIB nové pravomoci a zmocnění k vydání prováděcích právních předpisů. Další relevantní předpisy zahrnují směrnici o odolnosti kritických subjektů a nařízení o technologiích s nulovými emisemi.

Hlavní závěry analýzy:

- Současná právní úprava přímo nepokrývá kybernetickou bezpečnost menších OZE.
- Novela zákon a o kybernetické bezpečnosti zavádí povinnosti pro větší provozovatele OZE, ale většina zůstává neregulována.
- Zadávání veřejných zakázek a poskytování dotací představují nástroje pro nepřímou regulaci kybernetické bezpečnosti OZE.



Závěrem lze konstatovat, že současný právní rámec poskytuje určité nástroje pro regulaci kybernetické bezpečnosti OZE, ale existuje prostor pro jeho zdokonalení. Klíčové je najít rovnováhu mezi potřebou zajistit bezpečnost a nezatěžovat nadměrně menší provozovatele OZE. Využití nepřímých nástrojů regulace přes veřejné zakázky a dotace se jeví jako vhodný doplněk k přímé regulaci větších subjektů.

1. Vymezení problému – rizika v oblasti kybernetické bezpečnosti obnovitelných zdrojů

Provozování výroben elektřiny z obnovitelných zdrojů energie (dále jen **„OZE**"), ať už v podobě rozsáhlých fotovoltaických elektráren[1], nebo malých, „domácích" výroben elektřiny z obnovitelných zdrojů, a s tím související decentralizace a potřeba řízení přenosové a distribuční soustavy na dálku, s sebou nese zvýšené riziko z hlediska kybernetické bezpečnosti.

Například nizozemští hackeři ve svých testech prokázali, že jsou schopní naráz deaktivovat miliony fotovoltaických elektráren. Důsledkem takové deaktivace je výrazná nerovnováha v elektrizační soustavě, která může vést primárně k výpadkům dodávek elektrické energie a k poškození prvků elektrizační soustavy a sekundárně k řadě dalších závažných důsledků z hlediska bezpečnosti, života a zdraví obyvatel, a životního prostředí. Za bezpečnostní riziko jsou často považované také větrné elektrárny[2].

Lze konstatovat, že výrobny elektřiny z obnovitelných zdrojů jsou často jen slabě nebo vůbec softwarově zabezpečené před podobnými hackerskými útoky (zastaralý software bez instalace aktualizací reagujících na zjištěné bezpečnostní nedostatky, ponechávání defaultních hesel), případně je problém již v jednotlivých komponentech, v jejich hardware (který může být vyráběn tak, aby jej nebylo možné zcela zabezpečit), tedy o stejný problém, jaký vedl v minulosti k vyloučení čínské společnosti Huawei z budování 5G sítí v řadě evropských států.

Typickým příkladem jsou např. střídače, tedy zařízení, které převádí stejnosměrný proud (DC) z fotovoltaických elektráren na střídavý proud (AC), který je kompatibilní s elektrizační soustavou. Individuální střídač nemá šanci ovlivnit přenosovou či distribuční soustavu, avšak jejich velké množství již tuto schopnost má – proto se na střídače uplatní pravidla stanovující parametry, podmínky připojení a pravidla provozu (tzv. grid kódy, pravidla provozování přenosové soustavy a pravidla provozování distribuční soustavy).

Střídače jsou součástí v zásadě každé výrobny OZE, problémem je, že téměř všechny druhy v ČR masivně využívaných střídačů obsahují jen minimální či žádné zabezpečení z hlediska kybernetické bezpečnosti – což je problém, který lze snadno zneužít např. hackerským útokem na konkrétní střídač.

[1] https://www.euractiv.com/section/politics/news/dutch-solar-panels-vulnerable-for-hacking-study-finds/, https://www.rdi.nl/actueel/nieuws/2023/05/30/omvormers-kunnen-storing-veroorzaken-en-zijn-vaak-makkelijk-te-hacken

[2] https://www.euractiv.com/section/energy-environment/news/europe-quietly-works-on-huawei-treatment-for-chinese-wind-turbines/

Tato analýza se zabývá otázkami zajištění kybernetické bezpečnosti OZE, resp. výroben OZE a jejich komponent, a to právními předpisy předepisující nebo motivující provozovatele OZE k zajištění kybernetické bezpečnosti, či ke zvýšení jejích standardů.

2. Český právní rámec

Tato část analýzy je zaměřena čistě na vnitrostátní právní úpravu, tedy na české právní předpisy. Ačkoliv součástí českého právního řádu je též primární a sekundární komunitární právo (právo Evropské unie) a mezinárodní smlouvy (viz čl. 10a Ústavy), ty jsou popsány v samostatné části analýzy.

2.1 Vymezení základních pojmů – OZE a kybernetická bezpečnost

Obnovitelné zdroje energie

Obnovitelné zdroje energie jsou definovány v § 2 odst. 1 písm. a) zákona č. 165/2012 Sb., o podporovaných zdrojích energie a o změně některých zákonů, ve znění pozdějších předpisů, jako *„obnovitelné nefosilní zdroje energie, jimiž jsou energie větru, energie slunečního záření (termální a fotovoltaická), geotermální energie, energie okolního prostředí, energie z přílivu nebo vln a jiná energie z oceánů, energie vody, energie biomasy a paliv z ní vyráběných, energie skládkového plynu, energie kalového plynu z čistíren odpadních vod a energie bioplynu.“*

Výrobnou elektřiny se pak podle § 2 odst. 2 písm. a) bodu č. 18 zákona č. 458/2000 Sb., energetického zákona, ve znění pozdějších předpisů (dále jen „**EnerZ**“) rozumí energetické zařízení pro přeměnu různých forem energie na elektřinu, zahrnující všechna nezbytná zařízení; výrobna elektřiny o celkovém instalovaném elektrickém výkonu 100 MW a více, s možností poskytovat podpůrné služby k zajištění provozu elektrizační soustavy, výrobna elektřiny z obnovitelných zdrojů energie o celkovém instalovaném elektrickém výkonu 1 MW a více a nízkouhlíková výrobna elektřiny o celkovém instalovaném elektrickém výkonu 1 MW a více je zřizována a provozována ve veřejném zájmu.

Ačkoliv se nejedná o obecné definice (neboť oba citované předpisy je definují „pro účely tohoto zákona“), **lze s nimi jako s obecnými definicemi pracovat**, a to na základě obecných zásad normotvorby (zásada souladnosti a bezrozpornosti právního

řádu), podle kterých by jeden a ten samý pojem neměl být obsahově odlišný. **Pro účely této analýzy zkratka „OZE“ označuje „výrobny elektřiny z obnovitelných zdrojů“.**

Provozovatel OZE

V návaznosti na definici OZE chápeme v této analýze za „provozovatele OZE“ nejen každou fyzickou či právnickou osobu, která je výrobcem elektřiny tak, jak jej chápe EnerZ, tedy osoba provozující výrobnu elektřiny s instalovaným výkonem nad 50 kW a **disponující licencí** vydanou Energetickým regulačním úřadem (srov. § 3 odst. 3 EnerZ), ale i další osoby, které vlastní či provozují **výrobny OZE s nižším instalovaným výkonem** - typicky se může jednat o vlastníky malých fotovoltaických systémů v rodinných domech (ty se pohybují obvykle kolem 10 kW) nebo instalace na střechách bytových domů a obecních budov (opět v řádu nižších desítek kW). Takto široké pojetí provozovatele OZE přijímáme proto, že z hlediska kybernetické bezpečnosti jsou podstatné obnovitelné zdroje všech velikostí.

Kybernetická bezpečnost

Kybernetická bezpečnost nemá vlastní právní definici, a to ani v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „**ZKB**“), který sice v § 2 písm. a) až c) definuje dílčí pojmy, jako je „kybernetický prostor“, „kritická informační infrastruktura“ nebo „bezpečnost informací“[3], ale sousloví „kybernetická bezpečnost“ nedefinuje. Lze však vyjít z § 4 odst. 1 ZKB, který definuje „bezpečnostní opatření“, a z § 21 odst. 1 ZKB, který definuje „stav kybernetického nebezpečí“ a definovat kybernetickou bezpečnost (dále též „**kyberbezpečnost**“) jako „**zajištění bezpečnosti a integrity sítí elektronických komunikací a zajištění bezpečnosti informací a informačních systémů v kybernetickém prostoru**“.

Kybernetickou bezpečností se nerozumí ochrana samotného kybernetického prostoru, protože ten ze své definice (digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací) přesahuje hranice států.

Při definici kyberbezpečnosti lze odkázat na zvláštní část důvodové zprávy vládního návrh nového zákona o kybernetické bezpečnosti, ve znění sněmovního tisku č. 759/0, která k § 1 uvádí: *„**Pojmu kybernetické bezpečnosti je v souladu s dosavadní právní úpravou kontinuálně užito k odlišení od pojmu informační bezpečnosti, resp. počítačové bezpečnosti** a ke zdůraznění specifického zaměření zákona na ochranu*

[3] Bezpečností informací se rozumí zajištění důvěrnosti, integrity a dostupnosti informací a dat (§ 2 písm. c) ZKB).

regulovaných služeb z pohledu zajištění všech relevantních aktiv sloužících ve svém důsledku pro shromáždění, zpracování, uchování, užití, sdílení, rozšiřování nebo jiné nakládání s informacemi a daty v elektronické podobě.

*Tento postup je zvolen s ohledem na skutečnost, že **zajišťování kybernetické bezpečnosti výrazně přesahuje technologickou rovinu a vyžaduje ucelený přístup**, jak uvádí také Národní strategie kybernetické bezpečnosti České republiky.“*[4]

2.2 Relevantní právní předpisy

2.2.1 Ústavní zákon o bezpečnosti ČR

Základním právním předpisem upravujícím bezpečnost – a tedy nutně zahrnujícím také kybernetickou bezpečnost – je ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů (dále jen „**ZBezp**“). Tento zákon ukládá v čl. 1 státu – tedy České republice – několik základních povinností, mezi které patří ochrana životů, zdraví a majetkových hodnot, tedy toho, co může být ohroženo také nezajištěním kyberbezpečnosti OZE (např. přepětí v přenosové či distribuční soustavě vedoucí až k lokálnímu blackoutu, požáry elektrického vedení či bateriového úložiště), přestože ZBezp výslovně o kybernetické bezpečnosti nehovoří v žádném svém článku.

Čl. 2 ZBezp pak definuje mimořádné stavy, které se vyhlašují v případě, že je bezprostředně ohrožena ve značném rozsahu vnitřní pořádek a bezpečnost, životy a zdraví, majetkové hodnoty nebo životní prostředí, a to v závislosti na intenzitě, charakteru a územním rozsahu, a které zahrnují nouzový stav, stav ohrožení státu nebo válečný stav. Z hlediska předmětu této analýzy je relevantní jen nouzový stav, který může být vyhlášen podle čl. 5 odst. 1 ZBezp v případě *„živelních pohrom, ekologických nebo průmyslových havárií, nehod nebo jiného nebezpečí, které ve značném rozsahu ohrožují životy, zdraví nebo majetkové hodnoty anebo vnitřní pořádek a bezpečnost.“* Podle čl. 3 odst. 2 ZBezp jsou pak Státní orgány, orgány územních samosprávných celků a právnické a fyzické osoby povinny podílet se na zajišťování bezpečnosti České republiky. Rozsah povinností a další podrobnosti stanoví zákon – Zbezp žádný konkrétní zákon neuvádí, patrně se však bude jednat zejména o zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (dále jen „**KriZ**“), zmíněný níže, vyloučeny však nejsou ani jiné zákony.

---

[4] Srov. https://nukib.gov.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf, str. 5: *„Zajišťování kybernetické bezpečnosti dnes výrazně přesahuje technologickou rovinu a vyžaduje ucelený přístup.“*

V této souvislosti je třeba uvést. že **ZBezp nevymezuje stav kybernetického nebezpečí** ve smyslu § 21 ZKB, kterým se rozumí *„**stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech** nebo bezpečnost služeb elektronických komunikací **anebo bezpečnost a integrita sítí elektronických komunikací**, a tím by mohlo dojít k **porušení nebo došlo k ohrožení zájmu České republiky** ve smyslu zákona upravujícího ochranu utajovaných informací.“* Na rozdíl od mimořádných stavů upravených ZBezp vyhlašuje stav kybernetického nebezpečí ředitel Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „**NÚKIB**“).

Pro pochopení „stavu kybernetického nebezpečí“ a jeho souvislosti s OZE je třeba vymezit pojmy „sítě elektronických komunikací“ a „zájmy České republiky“, definované ve zvláštních zákonech:

- **Sítě elektronických komunikací** jsou vymezeny v § 2 odst. 2 písm. b) zákona č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů (dále jen „**ZEK**“), jako: *„**přenosové systémy, bez ohledu na to, zda jsou založeny na trvalé infrastruktuře nebo jsou centralizovaně kapacitně řízené, nebo nikoli, a popřípadě i spojovací nebo směrovací zařízení a jiné prostředky, včetně neaktivních síťových prvků, které umožňují přenos signálů po vedení**, rádiovými, optickými nebo jinými elektromagnetickými prostředky, **včetně** družicových sítí, pevných sítí okruhově nebo paketově komutovaných včetně internetu, mobilních sítí, **sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů**, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na typ přenášené informace“*, lze tedy konstatovat, že **sítí elektronických komunikací je též přenosová nebo distribuční soustava, resp. elektrizační soustava. Tento závěr ostatně potvrzují definice:**

    - **distribuční soustavy** ve smyslu § 2 odst. 2 písm. a) bod č. 1 EnerZ, kterou je **vzájemně propojený soubor vedení a zařízení** o napětí 110 kV, s výjimkou vybraných vedení a zařízení o napětí 110 kV, která jsou součástí přenosové soustavy, a vedení a zařízení o napětí 0,4/0,23 kV, 1,5 kV, 3 kV, 6 kV, 10 kV, 22 kV, 25 kV nebo 35 kV provozovaný držitelem licence na distribuci elektřiny a **sloužící k zajištění distribuce elektřiny** na vymezeném území České republiky, **včetně systémů měřicí, ochranné, řídicí, zabezpečovací, informační a telekomunikační techniky** včetně elektrických přípojek ve vlastnictví provozovatele distribuční soustavy;

    - **přenosové soustavy** ve smyslu § 2 odst. 2 písm. a) bod č. 10 EnerZ, kterou se rozumí **vzájemně propojený soubor vedení a zařízení** 400 kV, 220 kV a vybraných vedení a zařízení 110 kV, uvedených v příloze

Pravidel provozování přenosové soustavy, **sloužící pro zajištění přenosu elektřiny pro celé území České republiky a propojení s elektrizačními soustavami sousedních států, včetně systémů** měřicí, ochranné, **řídicí, zabezpečovací, informační a telekomunikační techniky**; a

- **elektrizační soustavy** ve smyslu § 2 odst. 2 písm. a) bod č. 4 EnerZ coby **vzájemně propojeným souborem zařízení pro výrobu, přenos, transformaci a distribuci elektřiny, včetně** elektrických přípojek, přímých vedení, a systémy měřicí, ochranné, **řídicí, zabezpečovací, informační a telekomunikační techniky,** a to na území České republiky. Z této definice rovněž vyplývá, že OZE jsou součástí elektrizační soustavy.

- **zájmy České republiky** definuje § 2 písm. b) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „**ZOUI**“) jako *„zachování její ústavnosti, svrchovanosti a územní celistvosti, **zajištění vnitřního pořádku a bezpečnosti**, mezinárodních závazků a obrany, **ochrana ekonomiky a ochrana života nebo zdraví** fyzických osob.“*

Z dosud uvedeného plyne, že **stav kybernetického nebezpečí je z hlediska ohrožení bezpečnosti, životů, zdraví a ekonomiky méně intenzivní, než mimořádné stavy dle ZBezp**, na druhou stranu to neznamená, že by porušení kyberbezpečnosti nemohlo vést svými důsledky, resp. hrozícími důsledky, k vyhlášení např. nouzového stavu – ustanovení § 21 odst. 6 ZKB uvádí, že pokud nelze odvrátit ohrožení bezpečnosti informací v informačních systémech nebo bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v rámci stavu kybernetického nebezpečí, ředitel NÚKIB neprodleně požádá vládu o vyhlášení nouzového stavu, ředitel NÚKIB je oprávněn vydávat opatření obecné povahy jak za stavu kybernetického nebezpečí, tak za nouzového stavu (§ 21 odst. 4 ZKB) a stav kybernetického nebezpečí končí buď uplynutím doby, na kterou byl vyhlášen, nebo vyhlášením nouzového stavu (§ 21 odst. 7 ZKB).

Z hlediska předmětu této analýzy lze konstatovat, že jak **mimořádné stavy dle ZBezp, tak stav kybernetického nebezpečí, slouží toliko k dočasným a mimořádným zásahům do provozování OZE**. Jako takové se proto nehodí k dlouhodobému nastavení podmínek výstavby a provozování OZE, zahrnujících zvýšení kyberbezpečnosti OZE.

2.2.2 Krizový zákon a prováděcí předpisy

V souvislosti s výše uvedenými mimořádnými stavy a stavem kybernetického nebezpečí je třeba zmínit rovněž krizový stav. Tím se podle § 2 písm. b) KriZ rozumí *„mimořádná událost podle zákona o integrovaném záchranném systému, narušení kritické infrastruktury nebo jiné nebezpečí, při nichž je vyhlášen stav nebezpečí, nouzový stav nebo stav ohrožení státu“*.

Výčet nezahrnuje shora uvedený stav kybernetického nebezpečí, ale až nouzový stav, tedy jeho vyšší formu. Pro úplnost uvádíme, že **stav nebezpečí**, definovaný v § 3 KriZ, je nižší formou „mimořádných stavů“, vyhlašuje se na území kraje nebo jeho části, a to v případě, kdy jsou ohroženy životy, zdraví, majetek, životní prostředí, pokud nedosahuje intenzita ohrožení značného rozsahu (tj. kdy se nejedná o mimořádné stavy) a není možné odvrátit ohrožení běžnou činností správních úřadů, orgánů krajů a obcí, složek integrovaného záchranného systému nebo subjektů kritické infrastruktury. **Stav nebezpečí v KriZ tak představuje obecnou právní úpravu** umožňující řešit méně závažné problémy, zatímco **stav kybernetického nebezpečí dle ZKB představuje zvláštní právní úpravu, která se použije namísto obecné** právní úpravy v KriZ. **Z tohoto důvodu se krizovým stavem** v této analýze **dále nezabýváme**.

Kromě krizového stavu a možností jeho řešení však § 2 písm. g) KriZ upravuje také tzv. kritickou infrastrukturu, pod kterou chápe *„prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.“*

Prvkem kritické infrastruktury je podle § 2 písm. i) KriZ **zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií** (obecně vymezených v § 2 písm. l) a m) KriZ); je-li prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury (která je definována v § 2 písm. h) KriZ jako kritická infrastruktura na území České republiky, jejíž narušení by mělo závažný dopad i na další členský stát Evropské unie). **S vymezením kritické infrastruktury pak souvisí její ochrana** (§ 2 písm. j) KriZ) **a úprava povinností subjektu** (evropské) **kritické infrastruktury**, tedy každého, kdo provozuje prvek (evropské) kritické infrastruktury (§ 2 písm. k) KriZ), neboť „subjekt kritické infrastruktury“ odpovídá podle § 29a KriZ za ochranu prvku kritické infrastruktury. **Je tedy třeba odpovědět na otázku, zda lze OZE pokládat za prvek kritické infrastruktury nebo ne**, neboť výše uvedené definice tuto možnost nevylučují.

Kromě shora uvedených definic KriZ prvek (evropské) kritické infrastruktury dále podrobněji nedefinuje a zmocňuje vládu k vydání nařízení, které bude obsahovat průřezová a odvětvová kritéria pro určení prvku kritické infrastruktury (§ 4 odst. 1 písm. d) KriZ

v kombinaci s § 40 odst. 1 KriZ). Jedná se o nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů (dále jen „**nařízení vlády č. 432/2010 Sb.**“). Podotýkáme, že prvek kritické infrastruktury musí splňovat alespoň jedno průřezové a jedno odvětvové kritérium současně, konkrétně:

- **vliv narušení funkce prvku kritické infrastruktury je určen mezními hodnotami**:
    - **obětí s mezní hodnotou více než 250 mrtvých** nebo více než 2 500 osob s následnou hospitalizací po dobu delší než 24 hodin;
    - **ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu** (HDP) – nařízení neurčuje, zda se jedná o nominální nebo reálný hrubý domácí produkt, pokud však vyjdeme z nominálního HDP, ten v roce 2023 činil 7344 miliard Kč. Nařízením stanovená mez by tak byla dosažena, pokud by narušení prvku kritické infrastruktury vedlo ke ztrátě ve výši 36,72 miliard Kč[5]. Je zřejmé, že této hodnoty by bylo dosaženo patrně v případě rozsáhlého výpadku výroby elektřiny z OZE;
    - dopadu na veřejnost s mezní hodnotou **rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob**. Toto průřezové kritérium by v případě vystavení OZE hackerskému útoku a následnému výpadku výroby elektřiny bylo nejsnáze splnitelné;
- **technické nebo provozní hodnoty prvku kritické infrastruktury, které se týkají elektřiny**:
    - **výrobna elektřiny s celkovým instalovaným elektrickým výkonem nejméně 500 MW** – toto by splňovaly jen rozsáhlé instalace OZE, typicky velké FVE nebo „větrné parky“ VTE;
    - **výrobna poskytující podpůrné služby s celkovým instalovaným elektrickým výkonem nejméně 100 MW** – podpůrnými službami se podle § 2 odst. 2 písm. a) bodu č. 8 EnerZ rozumí činnosti fyzických či právnických osob, jejichž zařízení jsou připojena k elektrizační soustavě, které jsou určeny k zajištění systémových služeb, a po jejichž aktivaci zpravidla dochází k dodávce regulační energie – **OZE nicméně obvykle budou výrobnami elektřiny umožňujícími dodávku regulační energie**

[5] https://www.mfcr.cz/cs/rozpoctova-politika/makroekonomika/makroekonomicka-predikce/2024/makroekonomicka-predikce-duben-2024-55475

jištěny. Ačkoliv podle § 23 odst. 3 písm. d) EnerZ je výrobce elektřiny povinen instalovat u nově budovaných výroben o celkovém instalovaném elektrickém výkonu 30 MW a více a provozovat zařízení pro poskytování podpůrných služeb, nepůjde o výrobnu poskytující podpůrné služby, ale o zařízení pro poskytování podpůrných služeb;

- **vedení pro vyvedení výkonu a zabezpečení vlastní spotřeby výrobny elektřiny**;
- **dispečink výrobce elektřiny** – podotýkáme, že OZE nemusí mít nutně vlastní dispečink, avšak povinností výrobce elektřiny je podle § 23 odst. 3 písm. h) EnerZ předávat provozovateli soustavy, ke které je výrobna elektřiny připojena, informace nezbytné pro dispečerské řízení, a kromě toho předávat další informace (§ 23 odst. 3 písm. g) EnerZ) a řídit se pokyny technického dispečinku provozovatele přenosové soustavy nebo provozovatele distribuční soustavy, ke které je výrobna elektřiny připojena (§ 23 odst. 3 písm. e) EnerZ).

Z dosud uvedeného vyplývá, že pouze malou část z veškerých OZE provozovaných na území ČR bude možné označit za prvek kritické infrastruktury.

Pro úplnost dodáváme, že odvětvová kritéria jsou v nařízení vlády č. 432/2010 Sb. stanovena též pro přenosovou a distribuční soustavu.

2.2.3 Zákon o kybernetické bezpečnosti a nový zákon o kybernetické bezpečnosti

Stávající právní úprava v ZKB relevantní pro OZE

Předmětem právní úpravy ZKB jsou dle jeho § 1 odst. 1 práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Podle § 1 odst. 2 ZKB tento zákon implementuje jednak směrnici Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. 7. 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů (dále jen „**směrnice NIS**“) a navazuje na nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. 4. 2019 o agentuře ENISA („**Agentuře Evropské unie pro kybernetickou bezpečnost**“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („**akt o kybernetické bezpečnosti**“).

Relevantní jsou z hlediska předmětu této analýzy především ustanovení § 4 až 20 ZKB, upravující systém zajištění kybernetické bezpečnosti, spočívající v ukládání povinností orgánům a osobám vymezeným v § 3 ZKB.

ZKB má být jako celek nahrazen dále uvedenou Novelou, a to **již k datu 18. 10. 2024**, přičemž platí, že **jádro právní úpravy kyberbezpečnosti zůstává v zásadě shodné**, Novela však stanovuje celou řadu změn, zejména výrazně rozšiřuje okruh subjektů, na které dopadá (a to až patnáctinásobně), zahrnuje také části prováděcích právních předpisů vydaných k provedení ZKB a mění některé definice, např. vymezení kritické informační soustavy. **Proto se ZKB v této analýze podrobněji nezabýváme** a namísto toho podrobně analyzujeme nově navrženou právní úpravu.

Vládní návrh zákona o kybernetické bezpečnosti

Vládní návrh nového zákona o kybernetické bezpečnosti, ve znění sněmovního tisku č. 759/0 (dále jen „**Novela**“)[6] obsahuje výrazně podrobnější právní úpravu kyberbezpečnosti už s ohledem na téměř dvojnásobný počet ustanovení ve srovnání se ZKB. Z § 1 odst. 3 Novely vyplývá, že Novela implementuje do českého právního řádu směrnici Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. 12. 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (dále též „**směrnice NIS 2**“), a navazuje na řadu nařízení Evropského parlamentu a Rady (EU), včetně již zmíněného nařízení 2019/881 ze dne 17. 4. 2019 o agentuře ENISA, o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013. S ohledem na transpoziční lhůtu směrnice NIS 2

[6] https://psp.cz/sqw/text/tiskt.sqw?O=9&CT=759&CT1=0

se **očekává nabytí účinnosti Novely 18. 10. 2024** – tedy v den, kdy má uplynout transpoziční lhůta směrnice NIS 2. Nelze proto očekávat, že by v průběhu zákonodárného procesu mohlo dojít k podstatným změnám Novely, naopak lze očekávat její urychlené přijetí.

Pro úplnost dodáváme, že **spolu s Novelou byl předložen návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti,** ve znění sněmovního tisku č. 760/0[7], a **dále byly předloženy teze prováděcích právních předpisů** – vyhlášek NÚKIB – bohužel zdaleka ne všechny, s jejichž vydáním Novela počítá.

Obecné povinnosti subjektů z hlediska zajištění kybernetické bezpečnosti

Novela je stejně jako ZKB založena na rozlišování jednotlivých subjektů z hlediska rozsahu jim ukládaných povinností z hlediska zajištění kyberbezpečnosti, kdy jsou rozlišováni poskytovatelé regulované služby v režimu vyšších a nižších povinností, kterým jsou stanovena odlišná organizační a technická opatření, která musí splnit. Ustanovení § 3 až 19 Novely představují jádro analyzované právní úpravy z hlediska zajištění kyberbezpečnosti, přičemž je třeba – stejně jako v případě ZKB – **odpovědět na otázku, zda a za jakých podmínek jsou provozovatelé OZE povinni či oprávněni postupovat podle právní úpravy kyberbezpečnosti?**

Pro odpověď na položenou otázku je třeba vyjít z **definice poskytovatele regulované služby**. Ta není obsažena v úvodních definicích § 2 Novely[8], ale je třeba ji dovodit z ustanovení § 6 Novely (a souvisejících ustanovení) **jako poskytovatel služby, se kterou je spojena povinnost jejího ohlášení NÚKIB pro následnou registraci regulované služby dle § 4 odst. 1 Novely**. Z Novely je tak patrná flexibilita při vymezení, co je a co není „regulovanou službou“, což bylo jedním z cílů předkladatelů návrhu zákona[9].

Ačkoliv § 3 Novely definuje jako regulovanou službu, o které tak rozhodl NÚKIB[10], **lze při jejím určení vyjít z § 4 odst. 1 Novely, podle něhož jsou podmínky pro registraci regulované služby splněny, pokud** jsou splněny dvě kumulativní podmínky:

---

[7] https://psp.cz/sqw/text/tiskt.sqw?O=9&CT=760&CT1=0

[8] Pro úplnost lze citovat ze zvláštní části důvodové zprávy k § 2 Novely: *„Návrh zákona ve svém znění před Legislativní radou vlády měl ambici definovat v rámci odstavce 1 také pojmy regulovaná služba a poskytovatel regulované služby. Tyto pojmy však byly z legislativně technických důvodů následně převedeny do příslušných ustanovení, kde se používají nejvíce.“*

[9] Podle zvláštní části důvodové zprávy k § 3 Novely: *„Potřebu určité flexibility lze dokumentovat na procesu vyjednávání samotného textu směrnice NIS 2, při němž docházelo k živým diskusím nad okruhem odvětví, která by do její působnosti měla spadat…Okruh odvětví, která mají být tímto zákonem regulována, je tak potřeba i do budoucna přizpůsobovat aktuálním společenským potřebám a rovněž potřebám České republiky. Ke zvýšení flexibility však přispívají další podmínky pro registraci regulované služby, uvedené v § 5 návrhu zákona.“*

[10] Podle zvláštní části důvodové zprávy k § 3 Novely je regulovaná služba *„stěžejním institutem návrhu zákona, od kterého se odvíjí podstatná část činností regulovaných subjektů. Vlastností regulované služby je skutečnost, že její narušení by mohlo mít určitý dopad na zabezpečení důležitých společenských nebo ekonomických činností nebo bezpečnost v České*

a) se **jedná o službu významnou pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v ČR v odvětví energetiky** nebo digitální infrastruktury a služeb (jiná odvětví nejsou z hlediska předmětu této analýzy relevantní); a

b) **poskytovatel služby je středním nebo velkým podnikem, nebo je významný pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v ČR.** Naposled uvedené kritérium (významnost poskytovatele z hlediska uvedených činností) není dále definováno. Malé a střední podniky naproti tomu definuje sdělení Ministerstva průmyslu a obchodu č. 7/2023 Sb., o vyhlášení českého znění doporučení Komise 2003/261/ES ze dne 6. 5. 2003 o definici mikropodniků a malých a středních podniků, a toto sdělení je dále modifikováno § 7 Novely, přičemž platí, že:

- **podnikem se rozumí každý subjekt vykonávající hospodářskou činnost, bez ohledu na jeho právní formu**. K těmto subjektům patří zejména osoby samostatně výdělečně činné a rodinné podniky vykonávající řemeslné či jiné činnosti a obchodní společnosti nebo sdružení, která běžně vykonávají hospodářskou činnost;

- **malým podnikem** je podnik, který zaměstnává méně než 50 osob a jehož roční obrat a/nebo bilanční suma roční rozvahy nepřesahuje 10 milionů Euro, a který není mikropodnikem;

- **středním podnikem** se rozumí podnik, který zaměstnává méně než 250 osob a jehož roční obrat nepřesahuje 50 milionů eur, a/nebo jehož bilanční suma roční rozvahy nepřesahuje 43 milionů Euro, a který není malým podnikem;

- **mikropodnik** je vymezen jako podnik, který zaměstnává méně než 10 osob a jehož roční obrat a/nebo bilanční suma roční rozvahy nepřesahuje 2 miliony Euro;

- **malým ani středním podnikem není takový podnik, jestliže je 25 % nebo více procent základního kapitálu nebo hlasovacích práv přímo nebo nepřímo ovládáno, společně či jednotlivě, jedním či více veřejnými subjekty[11]. Podle § 7 písm. a) Novely se tato výjimka** při určování, zda

republice; v opačném případě by do regulace nebyla zařazena (účelem návrhu zákona není regulovat všechny služby nezávisle na jejich důležitosti).“

[11] Výjimku z tohoto pravidla obsahuje čl. 3 odst. 2 sdělení Komise, když uvádí, že: *„Podnik však může být zařazen mezi nezávislé podniky a nemá tedy žádný partnerský podnik, přestože je následujícími investory tento práh 25 % dosažen nebo je překročen, za předpokladu, že tito investoři nejsou jednotlivě ani společně propojeni ve smyslu odstavce 3*

poskytovatel služby je středním nebo velkým podnikem, **neuplatní**[12]. Podle zvláštní části důvodové zprávy k § 7 Novely má výjimka zamezit tomu, aby osoby majetkově spřízněné s veřejnými subjekty (zejm. s obcemi a organizačními složkami státu) byly automaticky považovány za velké podniky;

- **za podnik se nepovažují organizační složky státu, územní samosprávné celky a Česká národní banka** (§ 7 písm. b) Novely);
- za partnerský nebo propojený podnik se nepovažují osoby, jejichž technická aktiva jsou zcela oddělena od technických aktiv, která používá posuzovaná osoba při poskytování regulované služby (§ 7 písm. c) Novely);
- pravidla pro určování velikosti se použijí i na poskytovatele regulované služby v odvětví věda, výzkum a vzdělávání, který není podnikem (§ 7 písm. d) Novely).

Uvedené sdělení dále obsahuje podrobnější pravidla ohledně počítání zaměstnanců a stanovování finančních hodnot a sledovaného období, avšak výše uvedené vymezení je pro tuto analýzu dostačující.

Pro úplnost je třeba dodat, že obě podmínky dále upřesní vyhláška NÚKIB (§ 4 odst. 2 Novely). Podle zvláštní části důvodové zprávy § 4 Novely probíhá určení, zda konkrétní provozovatel OZE poskytuje regulovanou službu podle Novely (a měl by se tedy registrovat u NÚKIB) na základě *„relativně jednoduchých a v zásadě jednoznačných kritérií, neměla by tedy pro povinné subjekty představovat významnější komplikace.“* **Ve srovnání se stávající právní úpravou** základních služeb ve **vyhlášce NÚKIB č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby**, ve znění vyhlášky č. 573/2020 Sb., **která vymezuje „odvětvová a dopadová kritéria“** (nyní seznam služeb) **provozovatele základní služby** a speciální kritéria zohledňující významnost provozovatele základní služby v daném odvětví (nyní podmínky významnosti poskytovatele základních služeb) **přehledně v příloze, ze které je na první pohled patrné, jací provozovatelé OZE mohou být v současnosti provozovateli základních služeb**, **je Novela méně přehledná, byť v zásadě replikuje stávající**

*s dotyčným podnikem: **a)** veřejné investiční společnosti, společnosti rizikového kapitálu, jednotlivci či skupiny jednotlivců provozující běžnou činnost spojenou s investováním rizikového kapitálu (business angels), které investují vlastní kapitál do nekotovaných podniků, za předpokladu, že celkové investice těchto business angels do stejného podniku činí méně než 1.250.000 eur; **b)** univerzity nebo nezisková výzkumná střediska, **c)** institucionální investoři včetně fondů pro regionální rozvoj, **d)** samostatné místní orgány s ročním rozpočtem nižším než 10 milionů eur a s méně než 5.000 obyvatel.“*

[12] Pokud by se výjimka ve sdělení Ministra průmyslu a obchodu uplatnila, pak by do okruhu velkých a středních podniků dle § 5 Novely nebyly zahrnuty právnické osoby, jejichž alespoň 25% podílníkem (vlastníkem) bude malá obec s ročním rozpočtem nižším než 10 milionů Euro a s méně jak 5000 obyvateli. Takových obcí je přitom v ČR několik tisíc, viz např. https://denik.obce.cz/clanek.asp?id=6911400

právní úpravu. Je tomu tak patrně proto, že Novela používá tyto podmínky odlišně při určení, zda je konkrétní osoba poskytovatelem regulované služby[13].

Podmínky pro registraci jsou dále splněny v případech uvedených v § 5 Novely, konkrétně:

a) pokud jde o **službu významnou pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v ČR v odvětví energetiky** nebo digitální infrastruktury a služeb (tedy o službu uvedenou v § 4 odst. 1 písm. a) Novely)[14] **a současně platí některá z níže uvedených podmínek:**

- **její poskytovatel je jediným poskytovatelem této služby v ČR** a tato služba je zásadní pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v ČR – takovým případem může být např. společnost ČEPS, a.s., která jako jediná provozuje přenosovou soustavu, ale **nebudou jím jednotliví provozovatelé OZE**;

- **narušení takové služby by mohlo mít významný dopad na bezpečnost ČR, vnitřní pořádek nebo život a zdraví;**

- **narušení této služby by mohlo vyvolat významná systémová rizika**, zejména v odvětvích, kde by takové narušení mohlo mít přeshraniční dopad. Podle zvláštní části důvodové zprávy k § 5 Novely: *„Systémovými riziky, o nichž hovoří bod 3. písmena a), lze obecně chápat taková rizika, která mohou ohrozit fungování dotčeného odvětví nebo celých složek společnosti či státu, nikoli pouze jednoho poskytovatele. Tato podmínka tedy bude relevantní zejména u takových subjektů, u nichž by narušení poskytování jejich služeb mohlo ohrozit celé odvětví.“*; Interpretace tohoto kritéria bude záviset na výkladu příslušných orgánů, zejména NÚKIB, přičemž ale máme za to, že tuto podmínku pravděpodobně splní provozovatelé distribučních soustav, provozovatel přenosové soustavy, obchodníci s energiemi (přinejmenším dle velikosti portfolia).

---

[13] Zvláštní část důvodové zprávy k § 4 Novely k tomu uvádí, že: *„Oproti předchozí úpravě je však stanoven odlišný způsob použití těchto podmínek při zařazování subjektů pod regulaci. **Cílem nového pojetí identifikace povinných subjektů vycházejícího ze směrnice NIS 2 je odstranit značné rozdíly mezi členskými státy v určování povinných subjektů** a zajistit právní jistotu pro všechny regulované subjekty, pokud jde o opatření k řízení kybernetických bezpečnostních rizik a oznamovací povinnosti. **Za tím účelem stanoví směrnice NIS 2 základní jednotné kritérium (velikost podniku), které určí subjekty, jež spadají do oblasti působnosti této směrnice**. Tento požadavek je promítnut do jedné z podmínek pro registraci regulované služby (se specifiky upravenými v § 7 návrhu zákona).“*

[14] Podle zvláštní části důvodové zprávy k § 5 Novely: *„Úřad v tomto případě, na rozdíl od případů upravených v ustanovení § 5 písm. b) až d) návrhu zákona, rozhoduje o splnění podmínek vůči již regulované službě, a může tak dojít k povýšení režimu poskytovatele regulované služby na režim vyšších povinností.“*

- její **poskytovatel je kvůli svému specifickému významu na regionální nebo celostátní úrovni zásadní pro konkrétní odvětví**, ve kterém působí, nebo typ služby, kterou poskytuje anebo pro jiná vzájemně propojená odvětví v České republice – toto kritérium patrně provozovatelé OZE splňovat nebudou, tedy alespoň ne na celostátní úrovni, mohou jej však naplnit na regionální úrovni, např. ČEZ, a.s. coby provozovatel přečerpávací elektrárny Dlouhé stráně, kterou lze pokládat za OZE[15];

b) jde o **službu, jejíž narušení může způsobit závažný zásah do života více než 125 000 osob**, a to prostřednictvím ohrožení bezpečnosti České republiky, vnitřního pořádku, života a zdraví, majetkové hodnoty nebo životního prostředí – v tomto ohledu se nabízí srovnání s výše vymezenými prvky kritické infrastruktury, u kterých je toto narušení jedním z průřezových kritérií[16], nicméně v § 5 písm. b) Novely obstojí toto kritérium samo o sobě, tj. poskytovatel takové služby nemusí být současně subjektem kritické infrastruktury (v takovém případě se totiž uplatní § 5 písm. d) Novely níže)[17];

c) jde o **službu, jejíž narušení může způsobit závažný zásah do schopnosti poskytovat jinou regulovanou službu poskytovatele v režimu vyšších povinností** – toto určit může být poměrně komplikované, neboť provozovatel OZE si tohoto nemusí být sám vědom; nebo

d) jde o **službu, jejíž poskytovatel je subjektem kritické infrastruktury podle** KriZ; v takovém případě je regulovanou službou služba odpovídající prvku kritické infrastruktury určenému u tohoto subjektu – jak již bylo uvedeno výše, **někteří provozovatelé OZE mohou splňovat toto kritérium** coby subjekty kritické infrastruktury ve smyslu § 2 písm. k) KriZ. To potvrzuje zvláštní část důvodové zprávy k § 5 písm. d) Novely: *„Obsah tohoto písmene je přímým odrazem obsahu čl. 2 odst. 3 směrnice NIS 2. Do doby přijetí změn obsažených ve směrnici CER, resp. její transpozice do národního práva, odkazuje prováděcí právní předpis na obsah dosavadní právní úpravy kritické infrastruktury, a to na prvky kritické infrastruktury podle zákona č. 240/2000 Sb., o krizovém řízení…“*[18]. Termín pro určení kritických subjektů podle čl. 6 směrnice CER je 17. 6. 2026.

---

[15] Pro úplnost, obsah § 5 odst. 1 písm. a) Novely odpovídá čl. 2 odst. 2 písm. b) až e) směrnice NIS 2.

[16] To potvrzuje zvláštní část důvodové zprávy k § 5 písm. b) Novely: *„Podmínka uvedená v písmenu b) vychází z průřezového kritéria nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů.“*

[17] Ve srovnání se stávající úpravou provozovatele základní služby dle vyhlášky NÚKIB č. 437/2017 Sb. došlo k navýšení tohoto kritéria, neboť za „závažné omezení, narušení či nedostupnost druhu služby“ je pokládáno takové narušení coby dopad kybernetického bezpečnostního incidentů, které postihuje více než 50 000 osob.

[18] Směrnicí CER se rozumí směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. 12. 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES.

Zvláštní část důvodové zprávy k tomuto ustanovení uvádí, že **podmínky v § 5 Novely jsou *„záměrně formulovány tak, aby k nim Úřad mohl přihlédnout v souvislosti s konkrétním zjištěným skutkovým stavem*. *Stanovení bližší* *univerzální definice některých obecných pojmů se nejeví jako vhodné*, *neboť tyto definice by byly poměrně obecné a nepřinášely by adresátům normy žádnou přidanou hodnotu. Bližší výklad těchto pojmů bude prováděn v závislosti na konkrétních skutkových okolnostech posuzovaného případu a co nejvíce v souladu s výkladem aplikovaným vůči těmto pojmům v rámci jiných právních předpisů, ve kterých jsou taktéž používány. Obecně však tyto pojmy slouží k vydefinování situací, které dosahují natolik nadstandardně vysoké intenzity, že stát považuje za nezbytné je podřadit pod zákonnou regulaci.“*** Pro úplnost dodáváme, že na rozdíl od § 4 Novely řada provozovatelů OZE nebude mít jak vyhodnotit, zda splňuje podmínky v § 5 Novely nebo ne[19].

Z dosud uvedeného vyplývá, že **alespoň někteří provozovatelé OZE mohou být poskytovateli regulované služby**, pokud:

- **budou buď splněny obě podmínky v § 4 Novely**, tedy budou poskytovateli **služby významné pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v ČR v odvětví energetiky** v odvětví energetiky, a současně budou splňovat definici velkého nebo středního podniku; nebo

- bude splněna některá z podmínek v § 5 Novely.

V této souvislosti lze odkázat na zvláštní část důvodové zprávy k § 4 Novely, podle kterého bude naprostá většina poskytovatelů regulované služby (a tedy i provozovatelů OZE) podléhat regulaci kyberbezpečnosti v Novele na základě splnění podmínek v § 4 odst. 1 Novely, a jen malá část na základě podmínek v § 5 Novely.

Poskytovatele regulované služby je dále nutné zařadit do odpovídajícího režimu poskytovatele regulované služby ve smyslu § 8 odst. 1 Novely, přičemž je rozlišován:

- **režim vyšších povinností** – do něj by měli spadat poskytovatelé regulované služby, kteří z důvodů své velikosti, počtu uživatelů, geografického rozšíření služby, dopadu na fungování odvětví nebo jiného poskytovatele regulované služby nebo rizikovosti provozu, jsou značně ekonomicky, společensky nebo bezpečnostně významní pro Českou republiku;

[19] Zvláštní část důvodové zprávy k § 5 Novely tento závěr potvrzuje: *„…není možné ani praktické uvažovat v těchto případech o samoidentifikaci, a to zvláště z toho důvodu, že subjekty často nemusí disponovat informacemi nezbytnými pro vyhodnocení splnění některých podmínek. Z toho důvodu je konstatování splnění těchto podmínek spojeno s rozhodnutím Úřadu…“.*

- **režim nižších povinností** – do něj by měli spadat všichni ostatní poskytovatelé regulované služby.

Toto rozlišení odpovídá Směrnici NIS 2, která rozlišuje „esenciální“, resp. základní subjekty (*„essential“*) a důležité subjekty (*„important“*). **Podrobnější rozdělení poskytovatelů regulovaných služeb** podle odvětví a jimi poskytovaných služeb Novela neobsahuje, namísto toho § 8 odst. 2 Novely zmocňuje NÚKIB k vydání vyhlášky, kterou budou poskytovatelé regulovaných služeb rozděleni do režimů dle § 8 odst. 1 Novely. Poskytovatel regulované služby je navíc podle § 9 odst. 1 Novely povinen hlásit NÚKIB změny regulované služby, pokud mohou vést k jeho zařazení do odlišného režimu.

Důležité z hlediska poskytovatelů služeb rovněž je, že **pokud poskytovatelé poskytují regulované služby, z nichž některé splňují podmínky zařazení do vyššího režimu a jiné ne, musí poskytovat všechny regulované služby ve vyšším režimu** – alespoň podle důvodové zprávy k § 8 Novely, která vychází z čl. 3 odst. 2 Směrnice NIS 2.

Obecné povinnosti poskytovatelů regulované služby pak upravuje § 11 an. Novely a zahrnují ohlašování kontaktních a doplňujících údajů o poskytovateli regulované služby (§ 11 Novely)[20], stanovení rozsahu řízení kybernetické bezpečnosti, totiž vymezení primárních a podpůrných „aktiv“ (§ 12 Novely)[21], a provádění bezpečnostních opatření (§ 23 Novely), jejichž účelem je zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv, mezi které spadá jak technické a programové vybavení, tak dodavatelé poskytovatelů regulovaných služeb (jak plyne z § 2 odst. 1 písm. c) až f) Novely)[22]. **Každý poskytovatel regulované služby tak bude muset zavádět bezpečnostní opatření uvedená v § 14 Novely** (v závislosti na režimu, do něhož bude poskytovatel regulované služby spadat), a **pokud bude provádění bezpečnostních opatření přenášet na své dodavatele, pak má poskytovatel** regulované služby **povinnost**

---

[20] V zásadě administrativní údaje zahrnující identifikační údaje fyzických osob, které jsou oprávněny jednat za poskytovatele regulované služby ve věcech upravených Novelou a dále informace o vlastnické struktuře poskytovatele regulované služby, technické údaje týkající se regulované služby a informace o jejím geografickém rozšíření a přeshraničním poskytování.

[21] Aktivem se rozumí *„fyzický nebo digitální prostředek, osoba nebo činnost související se zpracováváním informací a dat v elektronické podobě“*, primárním aktivem pak *„aktivum v podobě zpracovávané informace nebo poskytované služby,“* a **podpůrným aktivem** *„aktivum zajišťující fungování primárních aktiv, zejména zaměstnanec, **dodavatel**, **technické aktivum**, budova a jiný ohraničený prostor, ve kterém se nachází aktivum regulované služby*,“ přičemž „technickým aktivem“ se rozumí *„**technický nebo programový prostředek anebo vybavení**.“* Viz § 2 odst. 1 písm. c) až f) Novely. Zvláštní část důvodové zprávy k § 2 Novely k tomu uvádí, že: *„Aktiva je pojem používaný při výkladu dosavadní právní úpravy obsažené ve vyhlášce o kybernetické bezpečnosti, přičemž došlo kromě jeho rozpracování i k jeho přesunutí z úrovně vyhlášky do úrovně zákona. **Aktiva tvoří naprostý základ úvah o kybernetické bezpečnosti**, resp. jejím řízení, v rámci jakékoliv subjektu, tento pojem tak slouží jako základní stavební kámen pro správný výklad obsahu návrhu zákona. **Aktivem může být prakticky cokoli relevantního, s čím je potřeba v rámci řízení kybernetické bezpečnosti počítat,** resp. to zohledňovat a vést o tom úvahu**. Definice aktiva již ve svém obsahu tuto relevanci stanovuje,** a to **vázaností na zpracování informací a dat v elektronické podobě**.“*

[22] Zvláštní část důvodové zprávy uvádí, že: *„Právě u podpůrných aktiv je nejlépe vidět, že v **případě řešení kybernetické bezpečnosti není možné na tento problém pohlížet jen technickým pohledem** – **neopominutelnou roli mají** zaměstnanci a **dodavatelé, se kterými je potřeba v rámci řízení bezpečnosti informací také počítat** (dokonce se jedná o jeden z nejčastějších problémů v řešení kybernetické bezpečnosti), a proto mají své zvláštní místo a návrh zákona na ně pohlíží jako na druh podpůrného aktiva.“*

vybírat svého dodavatele v souladu s požadavky vyplývajícími z bezpečnostního opatření a zahrnovat požadavky vyplývající z bezpečnostního opatření do smluv s dodavatelem (§ 13 odst. 5 Novely). **Toto bude mít zásadní vliv na zadávání veřejných zakázek**.

Seznam bezpečnostních opatření v § 14 Novely zahrnuje jednak bezpečnostní opatření pro poskytovatele regulované služby v režimu vyšších povinností (§ 14 odst. 1 Novely), jednak bezpečnostní opatření pro poskytovatele regulované služby v režimu nižších povinností (§ 14 odst. 2 Novely), která jsou vždy kombinací organizačních a technických opatření a která (mimo jiné) zahrnují také „řízení aktiv", detekci a zaznamenávání kybernetických bezpečnostních událostí, bezpečnost komunikačních sítí, aplikační bezpečnost, kryptografické algoritmy.

Z toho vyplývá, že provozovatelé OZE, kteří budou poskytovateli regulované služby, budou muset řešit kyberbezpečnost OZE, mimo jiné zajištěním bezpečnosti střídačů a výběrem „bezpečných" dodavatelů dodávek a služeb souvisejících s regulovanou službou (poskytovatel regulované služby nebude muset bezpečnostní opatření zavádět a dodržovat „plošně" na veškeré své služby a činnosti, jak plyne z definice bezpečnostního opatření v § 13 odst. 1 Novely)[23]. **Tyto povinnosti provozovatelů OZE navíc Novelou nejsou omezeny pouze na dodavatele ve smyslu § 5** zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále též „**ZZVZ**")[24], provozovatelé OZE, kteří budou poskytovateli regulované služby, je tak budou muset zohlednit i v případě, že nebudou uzavírat smlouvy na veřejné zakázky.

Ustanovení § 15 až 17 Novely se týká hlášení kybernetických bezpečnostních incidentů a jejich zvládání se zapojením NÚKIB a CERT a z hlediska předmětu této analýzy se jimi dále nezabýváme.

Specifické povinnosti subjektů z hlediska zajištění kybernetické bezpečnosti se vztahem k veřejným zakázkám

Kromě obecných povinností subjektů z hlediska zajištění kyberbezpečnosti ustanovení § 18 Novely ukládá zvláštní povinnosti poskytovatelům regulovaných služeb v odvětví digitální infrastruktury a služeb, v § 25 odst. 1 **Novela vymezuje „strategicky významné služby"** coby regulované služby, **jejichž narušení by mohlo mít závažný dopad na bezpečnost České republiky nebo vnitřní pořádek** – konkrétní strategicky

[23] Bezpečnostními opatřeními jsou organizační a technická opatření, jejichž účelem je zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv.

[24] Podle § 5 ZZVZ se „pro účely tohoto zákona" dodavatelem rozumí osoba, která nabízí poskytnutí dodávek, služeb nebo stavebních prací, nebo více těchto osob společně. Za dodavatele se považuje i pobočka závodu; v takovém případě se za sídlo dodavatele považuje sídlo pobočky závodu. ZZVZ tedy neobsahuje obecnou definici pojmu „dodavatel", ale vztahuje ji k veřejným zakázkám, které se v § 14 ZZVZ dělí na veřejné zakázky na dodávky, služby a stavební práce.

významné služby v odvětví energetiky stanoví NÚKIB vyhláškou, a poskytovatel regulované služby se o tom, že se jedná o „strategicky významnou službu“, dozví z odůvodnění rozhodnutí o registraci regulované služby (§ 25 odst. 2 Novely), a **stanoví další povinnosti a postupy** související se „strategicky významnými službami“, např. **prověřování bezpečnosti dodavatelského řetězce poskytovatele strategicky významné služby** (§ 27 Novely), nebo **omezení rizik spojených s dodavatelem poskytovateli strategicky významné služby** (§ 29 Novely)[25], pokud z nich NÚKIB nepovolí výjimku (§ 30 Novely), dále **povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce** (§ 31 Novely).

Z dosud uvedeného vyplývá, že ti provozovatelé OZE, kteří budou poskytovateli strategicky významné služby, budou muset povinnosti plynoucí z § 27, 29 a 31 Novely zohlednit při uzavírání smluv na veřejné zakázky i mimo ně (platí, co bylo uvedeno výše, Novela pojem „dodavatel“ neomezuje na osoby podřaditelné pod § 5 ZZVZ).

Problémem Novely je, že řadu aspektů uvedených povinností ponechává na podzákonné právní úpravě, totiž na vyhláškách či opatřeních obecné povahy, vydávaných NÚKIB. Například § 27 odst. 2 Novely upravuje podrobnosti **prověřování bezpečnosti dodavatelského řetězce ze strany NÚKIB,** přičemž k tomuto prověřování **nemá docházet plošně, ale pouze** v souvislosti s *„kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu strategicky významné služby, u kterých poskytovatel strategicky významné služby* ***postupem podle vyhlášky Úřadu ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby*** *úrovní vysoká nebo kritická“.* Jinými slovy, **prověřování se má týkat pouze kritických částí „aktiv“** (např. technického vybavení nebo dodavatele) strategicky významné služby, kterými jsou vždy alespoň části zajišťující „nepominutelné funkce strategicky významné služby“ ve smyslu § 27 odst. 3 Novely[26], přičemž ovšem **seznam těchto nepominutelných funkcí strategicky významných služeb stanoví NÚKIB vyhláškou** (§ 27 odst. 4 Novely)[27].

Spolu s Novelou jsou navrženy rovněž teze prováděcích právních předpisů, ve kterých lze nalézt bližší podrobnosti k obsahu celkem 5 vyhlášek, nicméně návrh vyhlášky o nepominutelných funkcích stanoveného rozsahu je v současnosti omezen pouze na nepominutelné funkce stanoveného rozsahu pro regulovanou službu zajišťování veřejné

---

[25] Na omezení rizik spojených s dodavatelem ve smyslu § 29 Novely je navázána možnost poskytovatele strategicky významné služby podle § 32 Novely vypovědět závazek ze smlouvy, pokud v jeho plnění nelze pokračovat, pokud by plnění vedlo k porušení opatření obecné povahy vydané podle § 29 Novely.

[26] Nepominutelnou funkcí je činnost nebo vlastnost aktiva zajišťující provoz strategicky významné služby, jejichž narušení by mohlo mít závažný dopad na poskytování strategicky významné služby.

[27] Podle zvláštní části důvodové zprávy k § 27 odst. 4 Novely: *„Stanovení seznamu nepominutelných funkcí v prováděcím právním předpise představuje proporcionální řešení konfliktu mezi neomezeným správním uvážením Úřadu… na straně jedné a vymezením nepominutelných funkcí na úrovni návrhu zákona na straně druhé.“* Problém je v tom, že samotný seznam stanovuje a prováděcí předpis vydává NÚKIB.

komunikační sítě a regulovanou službu poskytování veřejně dostupné služby elektronických komunikací. Strategicky významné služby však zahrnují služby z celé řady odvětví, včetně energetiky (viz § 25 odst. 1 Novely), a návrhy odpovídajících vyhlášek dosud nebyly předloženy veřejnosti.

Právní úprava omezení rizik spojených s dodavatelem předpokládá v § 29 odst. 1 Novely **vydání opatření obecné povahy ze strany NÚKIB, kterým stanoví poskytovatelům strategicky významných služeb podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu**, zjistí-li na základě vyhodnocení rizikovosti dodavatele významné ohrožení bezpečnosti České republiky nebo vnitřního pořádku. **Provozovatelé OZE, kteří budou poskytovateli takových strategicky významných služeb, tak budou povinni např. vyřadit konkrétního dodavatele z možnosti ucházet se o veřejnou zakázku, případně poskytovat plnění z již uzavřené smlouvy na veřejnou zakázku** (typickým příkladem by mohlo být vyřazení čínských společností Huawei a ZTE z možnosti budovat v České republice 5G sítě)[28]. **Z tohoto zákazu** pak podle § 30 Novely **může NÚKIB udělit výjimku**, pokud:

- to povaha daného ohrožení bezpečnosti České republiky nebo vnitřního pořádku připouští, a
- by dodržování zákazu vyplývajícího z plnění opatření obecné povahy poskytovatelem strategicky významné služby mohlo podstatným způsobem ohrozit poskytování strategicky významné služby.

O tuto výjimku je však třeba žádat a **NÚKIB její udělení posoudí v řízení o povolení výjimky** (§ 30 odst. 2 a 3 Novely).

Prověřování bezpečnosti dodavatelského řetězce ve smyslu § 31 Novely pak v odstavci 1 písm. a) požaduje po poskytovateli strategicky významné služby, aby „s vynaložením přiměřeného úsilí“ zjišťoval informace o „dodavatelích bezpečnostně významných dodávek“, kterými jsou podle § 27 odst. 2 písm. c) Novely ti, kteří poskytovateli strategicky významné služby poskytnou přímo nebo jako poddodavatelé „bezpečnostně významnou dodávku“ ve smyslu § 27 odst. 2 písm. b) Novely, tedy plnění směřující do kritické části stanoveného rozsahu ve smyslu § 27 odst. 2 písm. a) Novely, spočívající v poskytnutí, vývoji, výrobě, sestavení, správě, provozu nebo servisu aktiv. **Zjednodušeně řečeno, poskytovatel strategicky významné služby bude muset sám aktivně zjišťovat jemu dostupné informace o svých dodavatelích či poddodavatelích plnění v podobě např. technického vybavení, které slouží k zajištění „nepominutelné**

[28] https://www.novinky.cz/clanek/internet-a-pc-mobil-nemecko-zakrocilo-proti-cinskym-firmam-komponenty-huawei-a-zte-zmizi-z-5g-siti-40480232, v této souvislosti se zvažuje také plošný zákaz na úrovni EU: https://www.novinky.cz/clanek/internet-a-pc-mobil-eu-zvazuje-plosny-zakaz-pro-cinsky-huawei-kvuli-bezpecnosti-5g-siti-40433919

funkce strategicky významné služby“. Tyto informace pak bude muset poskytovatel strategicky významné služby **evidovat v rozsahu stanoveném v § 31 odst. 1 písm. b) Novely**, tedy bude muset alespoň identifikovat všechny bezpečnostně významné dodávky a jejich dodavatele, **a případné změny hlásit do 10 dní od jejich zjištění NÚKIB** (§ 31 odst. 1 písm. c) Novely).

NÚKIB pak s těmito informacemi (jakož i s informacemi zjištěnými podle § 27 a 28 Novely) dále pracuje v rámci evidence dodavatelů bezpečnostně významných dodávek (§ 31 odst. 3 Novely).

Další povinnosti, např. povinnost poskytovatele strategicky významné služby zajišťovat její dostupnost (§ 33 Novely), **už nemají přímý dopad na zadávání veřejných zakázek souvisejících s OZE**. Z hlediska předmětu této analýzy nejsou relevantní ani povinnosti osob poskytujících služby registrace doménových jmen a osoba spravující a provozující registr domény nejvyšší úrovně (§ 34 a 35 Novely).

Povinnosti plynoucí z protiopatření vydávaných NÚKIB

Dále **je třeba zmínit úpravu protiopatření ve smyslu § 20 odst. 1 Novely**, která vydává (nebo o kterých rozhoduje) NÚKIB, a **která nahrazuje dosavadní úpravu „opatření“ v § 11 ZKB.**

Protiopatření kromě výstrahy a varování – spočívajících v informování veřejnosti nebo dotčených provozovatelů regulované služby o kybernetických bezpečnostních incidentech, porušováních povinností stanovených Novelou nebo o závažné hrozbě nebo zranitelnosti v oblasti kybernetické bezpečnosti, jak plyne z § 21 a 22 Novely, přičemž je na adresátech, zda a jakým způsobem na takové výstrahy a varování zareagují – **zahrnují také „reaktivní protiopatření“ ve smyslu § 23 odst. 1 Novely,** kdy NÚKIB buď rozhodnutím uloží konkrétnímu poskytovateli regulované služby, nebo opatřením obecné povahy blíže neurčenému okruhu poskytovatelů regulovaných služeb (§ 23 odst. 4 Novely), povinnost provést konkrétní „reaktivní protiopatření“ ať už k řešení hrozícího nebo probíhajícího kybernetického bezpečnostního incidentu ve smyslu § 2 odst. 2 písm. f) Novely[29], k zabezpečení aktiv (zejména technických prostředků nebo vybavení, ale i zpracovávaných informací)[30] před kybernetickým bezpečnostním incidentem, nebo za účelem zvýšení ochrany aktiv na základě analýzy již vyřešeného kybernetického bezpečnostního incidentu. **Tato „reaktivní protiopatření“ musí provozovatel regulované služby provést v rámci NÚKIB stanoveného rozsahu,** ledaže je stanoveno jinak (§ 23 odst. 2 Novely). Ze souvisejících ustanovení § 23 odst. 3 a 5 Novely lze dovodit, že

[29] Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informace (tedy narušení důvěrnosti, integrity a dostupnosti informací a dat) v kybernetickém prostoru, tedy v souboru sítí elektronických komunikací a dalších technologií, ve kterém dochází ke zpracování informací a dat v elektronické podobě.

[30] Viz § 2 odst. 1 písm. c) až f) Novely.

„reaktivní protiopatření“ mohou být ze strany NÚKIB vydávány velmi rychle, aby bylo možno reagovat na hrozící či probíhající kybernetické bezpečnostní incidenty (takže rozhodnutí o uložení reaktivního protiopatření může být prvním úkonem ve správním řízení, opatření obecné povahy ukládající reaktivní protiopatření nabývají účinnosti okamžikem vydání), přičemž poskytovatel regulované služby musí provedení reaktivního protiopatření a jeho výsledek bez zbytečného odkladu hlásit NÚKIB (§ 23 odst. 6 Novely).

Změny v právní úpravě stavu kybernetického nebezpečí

Ustanovení § 37 Novely upravuje stav kybernetického nebezpečí, který lze vyhlásit v případě, že je *„značně ohrožena nebo narušena bezpečnost informací v kybernetickém prostoru, což může mít za následek negativní dopady na poskytování regulovaných služeb nebo může dojít k ohrožení bezpečnosti České republiky, vnitřního pořádku, života a zdraví, majetkových hodnot nebo životního prostředí.“*

Jednou ze změn oproti stávající právní úpravě stavu kybernetického nebezpečí v § 21 ZKB je jednak délka, kdy lze nově stav kybernetického nebezpečí vyhlásit na dobu „nezbytně nutnou“, nejdéle však na 30 dní (namísto původních 7 dní), a navíc lze dobu jeho trvání prodloužit až na 60 dní (namísto původních 30 dní), přičemž pokud by důvody pro vyhlášení stavu kybernetického nebezpečí trvaly i po této době, požádal by NÚKIB vládu o vyhlášení nouzového stavu k řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru (viz § 38 odst. 1 a 2 Novely). Další změnou oproti původní právní úpravě je možnost souběhu nouzového stavu, stavu ohrožení státu nebo válečného stavu k řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru, kdy stav kybernetického nebezpečí zůstává v platnosti po celou dobu těchto mimořádných stavů, stejně jako opatření vyhlášená NÚKIB, ledaže vláda rozhodne jinak (§ 38 odst. 3 Novely).

Další změnou je konkretizace opatření za stavu kybernetického nebezpečí, obsažená v § 39 Novely, která nahrazují stávající „reaktivní opatření“ upravená v § 11 odst. 3 ZKB a § 13 ZKB, která byla určena právě k řešení stavu kybernetického nebezpečí. Samotnou konkretizaci lze vnímat pozitivně, kromě toho však došlo k podstatnému rozšíření těchto opatření, kdy je lze ukládat komukoliv, bez ohledu na to, zda je provozovatelem regulované služby, provozovatelem informačního systému kritické informační infrastruktury apod (srov. § 3 a 11 ZKB s nově navrženou úpravou v § 39 Novely). **Lze tedy konstatovat, že opatření za stavu kybernetického nebezpečí budou moci být ze strany NÚKIB ukládána též provozovatelům OZE**. V této souvislosti je třeba zmínit § 40 Novely, který umožňuje nahrazovat škody v příčinné souvislosti s opatřeními za stavu kybernetického nebezpečí obdobnou aplikací § 36 KriZ, zatímco stávající ZKB náhradu škod v příčinné souvislosti s reaktivními opatřeními neupravoval. Ustanovení § 41 Novely pak upravuje náhradu za omezení vlastnického práva nebo uložení povinnosti, a to opět obdobnou aplikací KriZ.

Zcela nově je v § 68 Novely upraveno finanční zabezpečení stavu kybernetického nebezpečí. Podotýkáme, že v zásadě totožná právní úprava je již nyní obsažena v § 25 KriZ a týká se finančního zabezpečení krizových opatření.

Další ustanovení Novely

Právní úprava NÚKIB a CERT a jejich kompetencí, obsažená v § 42 až 58 Novely, **není předmětem této analýzy**.

Ustanovení § 59 Novely pak **upravují přestupky poskytovatele regulované služby, § 60 Novely** upravuje **přestupky dalších osob v oblasti kybernetické bezpečnosti**, **§ 61 Novely** upravuje **přestupky v oblasti certifikace kybernetické bezpečnosti** a **§ 63 Novely upravuje ukládání pořádkových pokut**. Nelze přehlédnout, že **Novela zásadním způsobem zvyšuje limity pro ukládání pokut za přestupky** ve srovnání s § 25 odst. 14 ZKB a § 26 ZKB. Za nejzávažnější přestupky upravené v ZKB šlo uložit pokutu do výše 5 milionů Kč, za nejzávažnější přestupky upravené v Novele lze uložit pokutu do výše 250 milionů Kč č nebo až do výše 2 % čistého celosvětového ročního obratu dosaženého podnikem podle čl. 101 a 102 Smlouvy o fungování Evropské unie. Takové sankce lze bez nadsázky označit jako drakonické, případně likvidační, **problematika přestupků však přesahuje rámec této analýzy, proto jsou zmíněny pouze stručně**. Související změnou v právní úpravě přestupků je rovněž vyloučení některých ustanovení zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, ve znění pozdějších předpisů (viz § 62 odst. 2 Novely), jejichž aplikaci ZKB nevylučoval.

Další ustanovení Novely se netýkají předmětu této analýzy.

2.2.4 Zákon o zadávání veřejných zakázek

Zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“) **přímo s kyberbezpečností nepracuje, obsahuje však některá ustanovení, která mohou být využitelná k dosažení vyšší kyberbezpečnosti OZE**, **pokud ovšem bude podle ZZVZ při realizaci OZE či úpravách OZE postupováno**. Následující text proto odpovídá:

1. na otázku, kdo je povinen podle ZZVZ postupovat (přičemž odpověď na tuto otázku implikuje, jak jej lze ovlivnit, tedy jak takového zadavatele přimět k tomu, aby ve svých veřejných zakázkách zohledňoval kyberbezpečnost OZE);

2. na otázku, zda takový zadavatel vůbec může ve veřejných zakázkách uplatňovat požadavky na kyberbezpečnost OZE, a to z hlediska možné diskriminace dodavatelů;

3. a na otázku, jaké jsou mezery, resp. možnosti právní úpravy zadávání veřejných zakázek v souvislosti se zajištěním kyberbezpečnosti OZE?

Novela ani s ní související zákon (sněmovní tisk č. 760/0) nemění ZZVZ ani jeho prováděcí předpisy. Do pravidel ZZVZ se naopak promítnou nové požadavky evropského nařízení č. 2024/1735 ze dne 13. června 2024, kterým se zřizuje rámec opatření pro posílení evropského ekosystému výroby technologií pro nulové čisté emise a mění nařízení (EU) 2018/1724 (tzv. **Net Zero Industry Act**, podrobněji v části analýzy týkající se evropského práva).

Kdo je povinen zadat veřejnou zakázku

Z definice zadavatelů veřejných zakázek, obsažených v § 4 ZZVZ, vyplývá, že lze rozlišit:

- **veřejné zadavatele**, kterými je Česká republika a jeho organizační složky, státní příspěvkové organizace, územní samosprávné celky a jejich příspěvkové organizace, Česká národní banka a dále „jiné právnické osoby“ splňující kumulativní podmínky v § 4 odst. 1 písm. e) ZZVZ (založení či zřízení za účelem uspokojování potřeb veřejného zájmu, které nemají průmyslovou nebo obchodní povahu, a financování této jiné právnické osoby jiným veřejným zadavatelem, případně uplatňování rozhodujícího vlivu jiného veřejného zadavatele nebo jmenování či volení více než poloviny členů statutárního nebo kontrolního orgánu této jiné právnické osoby jiným veřejným zadavatelem).

  S ohledem na předmět této analýzy bude veřejným zadavatelem obvykle osoba, která bude poptávat např. vybudování fotovoltaické elektrárny (tedy vybudování OZE) **na své nemovitosti;**

- **„dotované zadavatele“**, kterými je každá osoba, která splňuje kritéria v § 4 odst. 2 ZZVZ (k úhradě nadlimitní nebo podlimitní veřejné zakázky použije více než 200 000 000 Kč, nebo více než 50 % peněžních prostředků, poskytnutých z rozpočtu veřejného zadavatele nebo Evropské unie).

  S ohledem na předmět této analýzy bude veřejným zadavatelem obvykle osoba, která bude poptávat např. vybudování fotovoltaické elektrárny (tedy vybudování OZE) **na své nemovitosti, a která bude současně příjemcem dotace nebo návratné finanční výpomoci či jiné srovnatelné podpory z veřejného rozpočtu;**

- **zadavatele „sektorových zakázek“** ve smyslu § 4 odst. 3 ZZVZ v kombinaci s § 151 odst. 2 ZZVZ, kterými je:

  - **každá osoba při výkonu relevantní činnosti, buď vykonávané na základě zvláštního nebo výhradního práva podle § 152 ZZVZ**. Těmi se rozumí: *„práva udělená příslušným orgánem veřejné moci na základě právního předpisu, jejichž obsahem je vyhrazení výkonu relevantních činností vymezených v § 153 ZZVZ jedné nebo více osobám a která podstatně ovlivňují možnost jiných osob vykonávat tuto činnost.“* **Relevantní činnosti** pak **zahrnují** (mimo jiné) následující činnosti, uvedené v § 153 odst. 1 písm. c) ZZVZ:

    - **poskytování nebo provozování přenosové nebo distribuční soustavy** podle EnerZ **v souvislosti s výrobou, přenosem nebo distribucí elektřiny**,

    - **dodávka elektřiny do přenosové nebo distribuční soustavy**.

    - Za relevantní činnosti se navíc podle § 153 odst. 3 písm. b) ZZVZ nepovažuje činnost uvedená v § § 153 odst. 1 písm. c) ZZVZ, pokud takový zadavatel vyrábí elektřinu pro účely jiné než relevantní činnosti a současně jeho vlastní spotřeba činí alespoň 70% průměrné celkové výroby elektřiny za předcházející 3 roky včetně aktuálního roku; Kromě toho § 154 ZZVZ dále omezuje okruh relevantních činností např. vyloučením činnosti, která je přímo vystavena hospodářské soutěži na trhu, na který není přístup omezen. pokud tak rozhodla Evropská unie;

  - **nebo každá osoba při výkonu relevantní činnosti, pokud nad takovouto osobou může veřejný zadavatel přímo či nepřímo uplatňovat dominantní vliv ve smyslu § 151 odst. 3 ZZVZ**.

Limit pro sektorové zakázky stanovené v nařízení vlády č. 172/2016 Sb., je ve výši **11 247 000 Kč** (shodně pro dodávky i služby).

S ohledem na předmět této analýzy bude sektorovým zadavatelem například osoba, která bude buď poskytovat nebo provozovat přenosovou nebo distribuční soustavu a **bude poptávat vybudování např. vybudování prvku této soustavy**.

- **„dobrovolné zadavatele“** ve smyslu § 4 odst. 5 ZZVZ, kterými je každá osoba, která zahájila zadávací řízení, ačkoliv k tomu nebyla povinna.

Všichni tito zadavatelé pak mají povinnost postupovat v souladu se ZZVZ, tedy zadávat veřejné zakázky v zadávacím řízení, ledaže zákon stanoví jinak (viz níže).

Výjimky ze zadávacího řízení

Co se týká výjimek z postupu pro zadávání veřejných zakázek, ty jsou obsaženy v § 29 až 31 a 158 ZZVZ, a umožňují zadavateli nezadávat veřejnou zakázku v zadávacím řízení (nejde tedy o úplné vynětí postupu zadavatele z působnosti ZZVZ), zadavatel se však může rozhodnout i přesto takovou zakázku zadat v zadávacím řízení jako „dobrovolný“ zadavatel. Platí přitom, že všechny výjimky ze ZZVZ je třeba vykládat restriktivně.

Z hlediska předmětu této analýzy mohou být relevantní následující obecné výjimky (a to bez ohledu na předpokládanou hodnotu veřejné zakázky a bez ohledu na druh veřejné zakázky):

- § 29 odst. 1 písm. a) ZZVZ – **pokud by provedení zadávacího řízení ohrozilo ochranu základních bezpečnostních zájmů České republiky ve smyslu čl. 1 ZBezp a současně nelze učinit takové opatření, které by provedení zadávacího řízení umožňovalo**. Výjimku budou moci využít zejména subjekty zajišťující bezpečnost České republiky podle čl. 3 odst. 1 ZBezp, tedy ozbrojené síly, ozbrojené bezpečnostní sbory, záchranné sbory a havarijní služby, není ale vyloučeno, aby se jednalo i o další subjekty, tedy také provozovatelé OZE. Podle komentáře: *„Možnost aplikace komentované výjimky se nevztahuje jen na období vyhlášeného nouzového stavu, stavu ohrožení státu nebo válečného stavu; rozhodné bude vždy to, zda existuje (byť potencionální) hrozba pro základní fungování státu (např. ohrožení pořádku, bezpečnosti, životů, zdraví či majetkových hodnot). Dalším omezujícím předpokladem aplikace dané výjimky je skutečnost, že hrozba je takové intenzity, že objektivně znemožňuje realizaci standardního zadávacího řízení k zadání příslušné veřejné zakázky. O takové znemožnění se jednat nebude, pokud v rámci zadávacího řízení lze přijmout opatření v rozsahu,*

který umožní výběr dodavatele v zadávacím řízení."[31] Z toho plyne, že využití této výjimky provozovateli OZE bude spíše teoretická, neboť tito nespadají do okruhu subjektů uvedených v čl. 3 odst. 1 ZBezp, pro které je výjimka primárně určena, a ačkoliv její uplatnění není vázáno na mimořádné stavy, které zahrnují též stav kybernetického nebezpečí, pokud bude možné využít např. opatření v rámci podmínek stanovených NÚKIB podle § 29 Novely, resp. pokud bude možné využít výjimky ze „standardních" zadávacích řízení, pak patrně nebude možné výjimku v § 29 odst. 1 písm. a) ZZVZ aplikovat;

- § 29 odst. 1 písm. c) ZZVZ – **jde-li o zadávání nebo plnění veřejné zakázky v rámci zvláštních bezpečnostních opatření stanovených jinými právními předpisy a současně nelze učinit takové opatření, které by provedení zadávacího řízení umožňovalo**. Tímto „jiným právním předpisem" je jak KriZ, tak ZKB, resp. Novela, případně EnerZ. Zadání a plnění veřejné zakázky musí být realizováno v rámci bezpečnostního opatření, např. v rámci „reaktivního protiopatření" ve smyslu § 23 odst. 1 Novely, kdy NÚKIB přímo nařídí provozovateli OZE, který je poskytovatelem regulované služby provést takové opatření, které může spočívat např. v uzavření smlouvy. Vyloučeny nejsou ani jiné mimořádné stavy a jiná bezpečnostní opatření.

  Podle komentáře: *„**Výjimku nebude možné využít, pokud krizová situace ještě nenastala nebo již pominula**, anebo neexistuje-li okolnost časové tísně vyvolávající potřebou zásahu. **Konstrukce výjimky neumožňuje, aby veřejné zakázky byly plněny po ukončení vyhlášeného stavu**. Jedná se o případy, v nichž je potřeba pořídit plnění, která jsou nezbytná k bezprostřednímu řešení situace spojené s vyhlášeným stavem či situací popsanou ve výše uvedených právních předpisech.*

  *Obdobně jako v případech uvedených pod písmeny a) a b) **musí být i u této komentované výjimky současně naplněna podmínka, podle které je zadavateli znemožněno učinit taková opatření, která by provedení zadávacího řízení umožňovala**. Jelikož se často bude jednat o záležitost časové tísně, bude pro aplikaci výjimky nutné vyloučit, že cíle (např. zajištění bezpečnosti osob či majetku) nelze dosáhnout minimalizací (zkrácením) zákonných lhůt v zadávacím řízení podle § 57 odst. 2 písm. b), § 59 odst. 5 a § 62 odst. 3, popř. zadáním veřejné zakázky v JŘBU podle § 63 odst. 5ZZVZ."* Podle metodického doporučení MMR může tuto výjimku využít osoba, která je dotčena konkrétním právním předpisem (např. je definovaným subjektem krizového řízení) a dostala takovým předpisem oprávnění vykonávat opatření podle zvláštního právního předpisu.

[31] *Šebesta, M., Novotný, P., Machurek, T., Dvořák, D. a kol.* Zákon o zadávání veřejných zakázek. Komentář. 2. vydání. Praha: C. H. Beck, 2022, s. 193.

> K aplikaci ustanovení § 29 písm. c) ZZVZ tedy postačí, pokud je zadavatel osobou povinnou ze zvláštních právních předpisů nebo dotčenou zvláštním bezpečnostním opatřením, v důsledku čehož má zadat veřejnou zakázku, přičemž nelze použít takové opatření, které by realizaci zadávacího řízení umožňovalo.

Podotýkáme, že § **29 ZZVZ se použije i pro sektorové veřejné zakázky**, a to v souladu s § 158 odst. 2 ZZVZ. Pro úplnost lze odkázat na § 174 odst. 1 ZZVZ s tím, že ustanovení § 29 ZZVZ je uplatnitelné i na koncese.

Z výjimek pro podlimitní veřejné zakázky v § 30 ZZVZ není pro provozovatele OZE relevantní žádná.

Výjimka v § 31 ZZVZ se týká zakázek malého rozsahu, které zadavatel není povinen zadávat v zadávacím řízení a je povinen dodržet (zejména) zásady v § 6 odst. 1 až 3 ZZVZ. Finanční limit pro tyto veřejné zakázky činí v případě dodávek či služeb částku 2.000.000, - Kč bez DPH (§ 27 ZZVZ).

Další okruh výjimek se týká sektorových veřejných zakázek, relevantní je pouze výjimka upravená v **§ 158 odst. 1 ZZVZ, podle něhož není sektorový zadavatel povinen zadávacím řízení zadat sektorovou veřejnou zakázku, jejíž předpokládaná hodnota nedosahuje finanční limit stanovený podle § 25 ZZVZ** pro nadlimitní veřejnou zakázku. Finanční limit není určen přímo zákonem, ale až nařízením vlády č. 172/2016 Sb., o stanovení finančních limitů a částek pro účely zákona o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**LimNař**“), přičemž pro sektorové zakázky jsou stanoveny podstatně vyšší finanční limity, než pro nesektorové – např. v případě veřejné zakázky na dodávky činí finanční limit pro většinu zadavatelů (vyjma České republiky, ČNB a státních příspěvkových organizací) 5.401.000,- Kč bez DPH, v případě sektorových zadavatelů tento limit činí 10.826.000,- Kč bez DPH (srov. § 2 LimNař). Jinými slovy, pokud bude provozovatel OZE sektorovým zadavatelem, nebude muset do tohoto limitu vůbec zadávat sektorové veřejné zakázky v zadávacím řízení (tj. bude moci postupovat stejně, jako by se jednalo o veřejnou zakázku malého rozsahu.

Pro úplnost je třeba zmínit rovněž § 32 odst. 4 ZZVZ, který řeší tzv. smíšenou veřejnou zakázku, která je z části veřejnou zakázkou, kterou je zadavatel povinen zadat v zadávacím řízení, a z části zakázkou, na niž se tato povinnost nevztahuje. Obecně platí, že smíšenou zakázku je zadavatel povinen zadat v odpovídajícím zadávacím řízení, vyjma případu, kdy jsou části smíšené zakázky objektivně neoddělitelné a na jednu z částí se vztahuje výjimka podle § 29 odst. 1 písm. a), b), c) nebo s) ZZVZ (viz výše).

Podmínky účasti dodavatelů v zadávacím řízení

Pojem „dodavatel“ v této části analýzy používáme promiscue nejen jako dodavatele ve smyslu ZZVZ (tedy vybraného dodavatele, se kterým je ze strany provozovatele OZE coby zadavatele uzavírána smlouva na veřejnou zakázku dle § 39 odst. 4 ZZVZ), **ale též jako účastníka zadávacího řízení**[32], tedy jako synonymum pro uchazeče o veřejnou zakázku. Současně zdůrazňujeme, že **pojem „dodavatel“ v Novele je ještě širší**, neboť není omezen pouze na dodavatele veřejných zakázek, ale **zahrnuje smluvní partnery obecně**.

Požadavky na kyberbezpečnost OZE může zadavatel veřejné zakázky zohlednit v rámci podmínek účasti dodavatelů v zadávacím řízení ve smyslu § 37 odst. 1 písm. a) až d) ZZVZ, konkrétně jako:

a) **kvalifikační podmínky** – tedy způsobilost a schopnost dodavatele plnit veřejnou zakázku, upravená v § 73 až 88 ZZVZ. Relevantní z hlediska kyberbezpečnosti OZE mohou být následující kvalifikační podmínky:

- **profesní způsobilost** ve smyslu § 77 odst. 2 písm. c) ZZVZ, podle něhož může provozovatel OZE po dodavateli požadovat předložení dokladu, že je odborně způsobilý nebo disponuje osobou, jejímž prostřednictvím odbornou způsobilost zabezpečuje, je-li pro plnění veřejné zakázky odborná způsobilost jinými právními předpisy vyžadována (včetně způsobilosti v oblasti kybernetické bezpečnosti);

- **technická kvalifikace** ve smyslu § 79 odst. 2 ZZVZ, kterou dodavatel prokazuje lidské a technické zdroje anebo odborné schopnosti a zkušenosti nezbytné pro plnění veřejné zakázky v odpovídající kvalitě, která může zahrnovat též zajištění kyberbezpečnosti. **Zadavatel může po dodavateli požadovat v rámci prokázání technické kvalifikace** např. **seznam významných dodávek** nebo významných služeb poskytnutých za poslední 3 roky před zahájením zadávacího řízení (§ 79 odst. 2 písm. b) ZZVZ), **seznam techniků, kteří se budou na plnění veřejné zakázky podílet** (§ 79 odst. 2 písm. c) ZZVZ), **přehled o řízení dodavatelského řetězce** a systémy sledování dodavatelského řetězce, které dodavatel bude moci uplatnit při plnění veřejné zakázky (§ 79 odst. 2 písm. f) ZZVZ)[33], **anebo doklad prokazující shodu požadovaného výrobku s požadovanou technickou normou** nebo technickým dokumentem (§ 79 odst. 2 písm. l) ZZVZ),

[32] Podle § 47 odst. 1 se dodavatel stává účastníkem zadávacího řízení ve chvíli, kdy projeví zájem účastnit se zadávacího řízení jedním ze způsobů, uvedených v písm. a) až c) ustanovení § 47 odst. 1 ZZVZ.
[33] Tímto způsobem může zadavatel, který je současně poskytovatelem regulované služby, splnit povinnost plynoucí z § 31 Novely.

přičemž **technickou normou nebo jiným technickým dokumentem mohou být stanoveny požadavky na kybernetickou bezpečnost komponentů OZE**[34]. V případě uplatnění naposled uvedeného požadavku si ovšem zadavatel musí ověřit, zda konkrétní výrobky (komponenty OZE), pro které požaduje doložení shody, vůbec podléhá posuzování shody podle zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů, či nikoliv. V případě, že se jedná o výrobky ve smyslu § 12 tohoto zákona[35], musí být před jejich uvedením na trh posouzena shoda s technickými normami. V těchto případech je zadavatel rovněž v rámci zadávací dokumentace oprávněn tento doklad požadovat. Je však pouze na uvážení zadavatele, zda tento dokument do svých požadavků na prokázání splnění technické kvalifikace zahrne či nikoliv.[36]

b) **technické podmínky** – tedy podmínky vztahující se k samotnému technickému řešení, upravené v § 89 až 95 ZZVZ. Podle § 89 odst. 1 ZZVZ může zadavatel stanovit technické podmínky jako požadavky na vlastnosti předmětu veřejné zakázky (výrobny OZE) prostřednictvím parametrů vyjadřujících požadavky na výkon nebo funkci, popisu účelu nebo potřeb, které mají být naplněny, odkazu na normy nebo technické dokumenty (viz § 90 ZZVZ, pokud ovšem tyto technické normy upravují kyberbezpečnost – odkázat lze např. na sadu ČSN EN ISO/IEC 27000, upravující různé aspekty kyberbezpečnosti), nebo odkazu na štítky (§ 94 ZZVZ, za předpokladu, že by existovaly štítky osvědčující kyberbezpečnost komponent OZE). **Technické požadavky lze vymezit jak pozitivně** (tedy požadovat při plnění veřejné zakázky, např. realizaci výrobny OZE, použití určitých technologií), **tak negativně** (tedy zákazem použití určitých komponent, např. takových, u kterých nelze zajistit kyberbezpečnost).

   Zadavatel dále musí dodržet § 89 odst. 5 ZZVZ, tedy pokud to není odůvodněno předmětem veřejné zakázky, nesmí zvýhodnit nebo znevýhodnit určité dodavatele nebo výrobky tím, že technické podmínky stanoví prostřednictvím přímého nebo nepřímého odkazu na určité dodavatele nebo výrobky, patenty na vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu.

---

[34] Příkladem certifikace může být Sunspec Alliance: https://sunspec.org/certification/.

[35] Podle § 12 odst. 1 písm. a) zákona č. 22/1997 Sb. stanoví vláda nařízením výrobky (tedy jakoukoliv věc, která byla vyrobena nebo jinak získána a je určena k uvedení na trh jako nová nebo použitá), které představují zvýšenou míru ohrožení oprávněného zájmu (kterým se rozumí ohrožení zdraví nebo bezpečnost osob, majetek nebo životní prostředí, popřípadě jiný veřejný zájem) a u kterých proto musí být posouzena shoda.

[36] *Šebesta, M., Novotný, P., Machurek, T., Dvořák, D. a kol.* Zákon o zadávání veřejných zakázek. Komentář. 2. vydání. Praha: C. H. Beck, 2022, s. 626.

c) **obchodní nebo jiné smluvní podmínky** vztahující se k předmětu veřejné zakázky – vzhledem k tomu, že ZZVZ umožňuje zadavateli zahrnout do zadávacích podmínek návrh smlouvy na veřejnou zakázku (obvykle smlouvy o dílo), lze v rámci smluvních podmínek podrobně řešit i otázky týkající se kyberbezpečnosti OZE, resp. jednotlivých komponentů OZE;

d) **zvláštní podmínky plnění veřejné zakázky**, a to zejména v oblasti vlivu předmětu veřejné zakázky na životní prostředí, sociálních důsledků vyplývajících z předmětu veřejné zakázky, hospodářské oblasti nebo inovací (srov. § 6 odst. 4 ZZVZ). Podle komentáře: *„Tyto zvláštní požadavky se tedy mohou vztahovat jak k samotnému průběhu či okolnostem plnění veřejné zakázky, tak k vlastnostem poptávaného plnění, nelze však stanovit takové požadavky, které jsou zcela mimo rámec poptávaného plnění.“*[37] Není vyloučeno, aby tyto zvláštní podmínky plnění veřejní zakázky zohledňovaly kyberbezpečnost OZE.

Jiné podmínky účasti v zadávacím řízení nesmí zadavatel stanovit.

V souvislosti s dosud uvedeným upozorňujeme na specifickou úpravu sektorových veřejných zakázek, u kterých je třeba rozlišit, zda je provozovatel OZE veřejným zadavatelem nebo ne (§ 151 odst. 1 a 2 ZZVZ) – toto rozlišení má vliv na aplikaci **§ 167 ZZVZ**, obsahující **zvláštní úpravu zadávacích podmínek sektorových veřejných zakázek**.

Podle komentáře: *„Veřejný zadavatel je při zadávání sektorových veřejných zakázek povinen vymezit v zadávacích podmínkách požadavky na prokázání základní způsobilosti dle § 74 včetně způsobů prokázání dle § 75. Dále je veřejný zadavatel povinen požadovat prokázání profesní způsobilosti dle § 77 odst. 1 s výjimkou zadávání sektorových veřejných zakázek v JŘBU. Využití dalších kritérií profesní způsobilosti stanovených v § 77, kritérií ekonomické kvalifikace dle § 78 a kritérií technické kvalifikace dle § 79 je pouze na uvážení veřejného zadavatele.*

Pro potřeby sektorové veřejné zakázky může veřejný zadavatel také stanovit jiná kritéria kvalifikace, než která jsou vymezena v části čtvrté zákona, přičemž ustanovení o obnovení způsobilosti účastníka zadávacího řízení a společná ustanovení o kvalifikaci by měla být použita shodně.

Jiná osoba ve smyslu § 151 odst. 2 není při zadávání sektorových veřejných zakázek vázána povinností vymezit v zadávacích podmínkách požadavky na prokázání základní způsobilosti dle § 74 a profesní způsobilosti dle § 77 odst. 1. Stanovení kritérií kvalifikace je tak bez dalšího na uvážení jiné osoby ve smyslu § 151 odst. 2 a tato může stanovit i jiná kritéria kvalifikace než ta, která jsou vymezena v části čtvrté zákona. Pravidla

[37] *Šebesta, M., Novotný, P., Machurek, T., Dvořák, D. a kol.* Zákon o zadávání veřejných zakázek. Komentář. 2. vydání. Praha: C. H. Beck, 2022, s. 272.

o obnovení způsobilosti účastníka zadávacího řízení a společná ustanovení o kvalifikaci by měla být také jinou osobou ve smyslu § 151 odst. 2 vyžita shodně."[38]

Podmínky pro účast dodavatele ve smyslu § 37 ZZVZ **musí souviset s předmětem veřejné zakázky** – nelze tedy požadovat kvalifikaci dodavatele, která je z hlediska plnění veřejné zakázky – např. výstavby OZE – nepoužitelná. Současně platí, že zadavatel musí při jejich stanovení dodržet základní zásady v § 6 ZZVZ, zahrnující:

a) **zásadu přiměřenosti dle § 6 odst. 1 ZZVZ** – zadávací podmínky veřejné zakázky musí být stanoveny tak, aby nebyly nepřiměřené z hlediska předmětu veřejné zakázky, tj. zadávací podmínky nesmí vytvářet překážky hospodářské soutěže, které jsou bezdůvodné. **Pokud tedy zadavatel veřejné zakázky bude např. stanovovat určité technické požadavky** (viz výše), **musí být schopen odůvodnit, proč a na základě čeho je stanovil.** Takovým důvodem může být též zajištění kyberbezpečnosti, kdy například zadavatel vyloučí použití určitých technologií nebo komponentů, které jsou z hlediska kyberbezpečnosti podstatně rizikovější, než jiné. Tuto „rizikovost" však zadavatel neurčuje arbitrárně, ale opírá se zejména o výsledky odborných testů, výzkumu, varování NÚKIB apod.

b) **zásadu rovného zacházení a nediskriminace** dle § 6 odst. 2 ZZVZ – zadávací podmínky veřejné zakázky nesmí bez dalšího vylučovat určitý okruh dodavatelů, nebo je vymezit tak, že je může splnit jen jeden dodavatel. S tím souvisí i výše zmíněné stanovení technických požadavků z hlediska kyberbezpečnosti – ty by měly vždy směřovat ke konkrétním technologiím, komponentům apod., nikoliv ke konkrétním výrobcům těchto komponentů;

c) **zákaz omezování účasti dodavatelů podle sídla** – § 6 odst. 3 ZZVZ obsahuje výjimku z obecného zákazu diskriminace dodavatele podle sídla, tedy podle země původu, kdy stanoví, jaké dodavatele nelze omezit v účasti v zadávacích řízeních: jsou to dodavatelé se sídlem v některém z členských států EU nebo se sídlem v členském státu Evropského hospodářského prostoru nebo se sídlem ve Švýcarsku, a dále jsou to dodavatelé z jiných států, kteří mají buď s ČR nebo s EU uzavřenou mezinárodní smlouvu zaručující přístup dodavatelům z těchto států k zadávané veřejné zakázce.

   Dodavatelům se sídlem v jiných než dosud uvedených státech tedy zadavatel veřejné zakázky může omezit účast v zadávacím řízení. V této souvislosti upozorňujeme např. na sdělení Komise s názvem Pokyny k účasti uchazečů a zboží

[38] *Šebesta, M., Novotný, P., Machurek, T., Dvořák, D. a kol.* Zákon o zadávání veřejných zakázek. Komentář. 2. vydání. Praha: C. H. Beck, 2022, s. 1126.

ze třetích zemí na trhu EU s veřejnými zakázkami 2019/C 271/02, které řeší (mimo jiné) účast čínských dodavatelů.[39]

Kromě toho lze omezit účast dodavatele u sektorové veřejné zakázky podle § 168 odst. 1 ZZVZ, tedy podle původu převážné části dodávek (nikoliv podle sídla dodavatele): možnost vyloučení účastníka zadávacího řízení (tj. dodavatele) nabízejícího pro plnění veřejné zakázky převážně zboží ze třetích zemí (např. Čína) se uplatní výhradně ve vztahu k sektorovým veřejným zakázkám a zároveň se musí jednat o veřejnou zakázku na dodávky, přičemž podíl hodnoty dodávek zahrnuje též „programového vybavení používaného v zařízeních telekomunikačních sítí, původem ze států, s nimiž Evropská unie neuzavřela dohodu zajišťující srovnatelný a účinný přístup pro dodavatele z Evropské unie na trhy těchto zemí, určený přímo použitelným předpisem Evropské unie“.[40]

Toto programové vybavení souvisí s budováním 5G sítí, nesouvisí však přímo s OZE. Současně je třeba mít při aplikaci této výjimky na paměti, že ji nelze použít v případě, že vyhlášená mezinárodní smlouva uzavřená ČR nestanoví něco jiného.

Kromě dosud uvedeného lze omezit účast dodavatelů ze třetích zemí také § 105 odst. 2 ZZVZ, tedy vymezením „významných činností“, jejichž plnění bude muset zajistit přímo vybraný dodavatel a nikoliv jeho subdodavatelé. Toto opatření vychází z širšího oprávnění zadavatele veřejné zakázky požadovat v souladu s § 105 odst. 1 ZZVZ, aby dodavatel již ve své nabídce určil části veřejné zakázky, které hodlá plnit prostřednictvím poddodavatelů, nebo aby předložil seznam poddodavatelů, pokud jsou účastníkovi zadávacího řízení známi a uvedl, kterou část veřejné zakázky bude každý z poddodavatelů plnit. Tím zadavatel (mimo jiné) zajistí kontrolu dodavatelského řetězce dle § 31 Novely (viz výše).

Kromě výše uvedeného může vláda podle § 37 odst. 7 ZZVZ stanovit svým nařízením některé závazné podmínky účasti v zadávacím řízení v určitých kategoriích veřejných zakázek a rozsah jejich používání, nebo bližší podmínky pro posuzování přiměřenosti některých podmínek účasti v zadávacím řízení a rozsah jejich používání.

Toto ustanovení nepochybně dává široký prostor pro podrobnější úpravu podmínek účasti dodavatelů v zadávacím řízení i z hlediska kyberbezpečnosti OZE, podotýkáme však, že v současnosti není tato možnost ze strany vlády využívána,

[39] https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52019XC0813(01)&qid=1724667311443
[40] Např. Dohoda o veřejných zakázkách (Government Procurement Agreement – GPA), dostupná zde: https://www.wto.org/english/trato-p_e/gproc_e/memobs_e.htm.

s výjimkou nařízení vlády č. 173/2016 Sb., o stanovení závazných zadávacích podmínkách pro veřejné zakázky na pořízení silničních vozidel, kterým byly stanoveny např. emisní limity, jaké musela vozidla splňovat (toto nařízení vlády však bylo nařízením vlády č. 361/2022 Sb. bez náhrady zrušeno).

V souvislosti s možností NÚKIB vydávat „reaktivní protiopatření“ podle § 23 Novely je třeba zmínit § 99 ZZVZ, který umožňuje zadavateli veřejné zakázky i v průběhu zadávacího řízení – pokud ovšem neuplynula lhůta pro podání nabídek, předběžných nabídek nebo žádosti o účast – **změnit zadávací podmínky**, např. doplněním požadavků na kyberbezpečnost OZE, resp. jejích komponentů.

V souladu s § 99 odst. 2 ZZVZ si však taková změna zadávacích podmínek vyžádá prodloužení lhůty pro podání nabídek (přestože se obvykle bude jednat o změnu která bude zužovat okruh možných dodavatelů), přičemž lze jen doporučit, aby došlo k prodloužení o celou původní délku.

V případě, že již uplynula lhůta pro podání nabídek, a NÚKIB přesto vydá „reaktivní protiopatření“, **nezbude zadavateli veřejné zakázky, než** postupovat podle § 127 odst. 2 písm. d) ZZVZ a **zadávací řízení zrušit**, a to z důvodů hodných zvláštního zřetele, pro které nelze po zadavateli požadovat, aby v zadávacím řízení pokračoval, bez ohledu na to, zda tyto důvody zadavatel způsobil či nikoliv.

2.2.5 Právní úprava poskytování dotací

Úvodem této části analýzy odkazujeme na **návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti,** ve znění sněmovního tisku č. 760/0, a konstatujeme, že tento zákon nemění žádný z dále uvedených zákonů upravujících podmínky podpory výroby elektřiny z OZE. S ohledem na předmět této analýzy budou **níže uvedené předpisy zkoumány z hlediska toho, zda umožňují poskytování dotací provozovatelům OZE** (ať už půjde o dotace na vybudování OZE, o dotace na jejich provoz), **zda lze poskytovat dotace na zlepšení kyberbezpečnosti OZE**, **a zda podmínky poskytování dotací provozovatelům OZE zohledňují**, resp. mohou zohledňovat, **kyberbezpečnost OZE**. Předmětem této analýzy nebude zkoumání konkrétních dotačních programů použitelných pro provozovatele OZE.

Podle důvodové zprávy Novely (str. 79), která se týká předpokládaných hospodářských a finančních dopadů Novely na veřejné rozpočty a podnikatelské prostředí a která uvádí, že: *„Podstatná část subjektů veřejné správy je již nyní povinným subjektem podle zákona o kybernetické bezpečnosti a jsou jim uloženy téměř totožné povinnosti jaké vyplývají z tohoto návrhu zákona.* ***Podstatným rozdílem je šíře navrhované regulace, která v souladu s přístupem zvoleným směrnicí NIS 2 rozšiřuje rozsah zajišťovaných systémů z jednotlivých ohraničených informačních systémů na služby v rozsahu výkonu činnosti daného subjektu veřejné správy, což náklady navyšuje****. Přestože tedy subjekty veřejné správy budou moci v části nákladů na zajištění kybernetické bezpečnosti pokračovat podle dosavadního rozpočtování, bude stejně tak potřeba promítnout ostatní nově navýšené náklady do budoucích rozpočtů těchto subjektů… Nad rámec výše uvedeného je* ***pro financování nákladů také možné využívat k tomu vzniklé nebo do budoucna vznikající dotační programy na úrovni Evropské unie, případně dotační programy původně na financování kybernetické bezpečnosti nezaměřené, ale dílčím způsobem k tomu využitelné*** *(např. the Digital Europe Programme apod.).“*

Na str. 87 obecná část důvodové zprávy Novely uvádí, že: *„****S ohledem na směrnicí NIS 2 požadované podstatné rozšíření počtu povinných osob (nejméně 15násobné navýšení oproti současnému stavu)*** *– a to jednak stávajících regulovaných odvětví o nové regulované služby, ale také především rozšířením regulovaných odvětví – jsou předpokládány zvýšené dopady na podnikatelské prostředí České republiky a na soukromý sektor celkově. Z odhadovaných nejméně šesti tisíc regulovaných subjektů tvoří veřejný sektor přibližně jen tisíc organizací, zbývající počet pak spadá do soukromého sektoru (mezi nimi především dva tisíce podnikatelů poskytujících veřejně dostupné služby elektronických komunikací), a z toho důvodu také přináší významný dopad na podnikatelské prostředí v České republice.“* Na str. 90 pak obecná část důvodové zprávy Novely uvádí, že: *„Shrnutím všech výše uvedených výpočtů a metodik je možné konstatovat,* ***že v případě výpočtu nákladů na zavedení a následné provádění především***

bezpečnostních opatření se jedná o velmi hrubé odhady, pohybující se přibližně mezi 800 000 Kč a 1 500 000 Kč vůči jednomu zabezpečovanému systému (nikoli společnosti jako celku). *Změny v přístupu k regulaci zavedené návrhem zákona, výše uvedené proměnné (především různý stav již současného zabezpečení u jednotlivých společností), rozdělení povinností uložených těmto společnostem, stejně tak jako agregace řady bezpečnostních opatření u více systémů v rámci společnosti pak mohou tyto hodnoty ovlivnit, nicméně s ohledem na výše uvedené* ***je možné očekávat dopady na podnikatelské prostředí ve zvýšené míře****. Podstatnou proměnnou tak bude především to, jaký je stav kybernetické bezpečnosti ve společnosti a jaký je daný počet jednotlivých systémů u každé konkrétní společnosti, neboť takový násobek výše uvedené částky bude potřeba vedením společnosti alokovat na zavedení či zvýšení kybernetické bezpečnosti v souladu s návrhem zákona. Stejně jako v případě zákona o kybernetické bezpečnosti je možné zdůraznit, že s jednotlivými oblastmi jsou spojena specifika, která mohou značně ovlivňovat dopady navrhované regulace.* ***Např. v odvětví energetiky budou muset regulované subjekty projednávat náklady a investice vyplývající z návrhu zákona s Energetickým regulačním úřadem, jakožto správním orgánem pro výkon cenové regulace v energetice. Lze předpokládat, že náklady vyvolané návrhem zákona by mohly být pro účely regulace cen považovány za ekonomicky oprávněné náklady*** *(uznatelné náklady na implementaci právních předpisů) a že by tak mohlo dojít k tomu, že investice realizované za účelem splnění povinností stanovených návrhem zákona budou uznatelnou součástí regulační báze aktiv regulované společnosti.“*

Zákon č. 165/2012 Sb.

Z hlediska předmětu této analýzy je relevantní zejména zákon č. 165/2012 Sb., o podporovaných zdrojích energie a o změně některých zákonů (dále jen „**ZPZE**“). Jeho předmětem je podle § 1 odst. 1 písm. a) ZPZE (mimo jiné) podpora elektřiny, tepla a biometanu z obnovitelných zdrojů energie ve smyslu § 2 odst. 1 písm. a) ZPZE. Dále je předmětem právní úpravy financování podpory elektřiny z podporovaných zdrojů, tepla a biometanu z obnovitelných zdrojů a poskytnutí dotace operátorovi trhu na úhradu těchto nákladů (§ 1 odst. 1 písm. e) ZPZE. Podpora podle ZPZE se však použije pouze, pokud je v souladu s právem EU nebo rozhodnutími Komise (§ 1 odst. 3 ZPZE).[41]

Předmětem podpory elektřiny z OZE je podle § 4 odst. 2 ZPZE: *„Podpora elektřiny z obnovitelných zdrojů se vztahuje na výrobu elektřiny z obnovitelných zdrojů ve výrobnách elektřiny na území České republiky připojených k elektrizační soustavě České republiky přímo nebo prostřednictvím odběrného místa nebo prostřednictvím jiné výrobny elektřiny*

[41] Ustanovení tohoto zákona upravující poskytování podpory a postup pro stanovení výše a rozsahu podpory se nepoužijí, pokud by podpora stanovená na jejich základě byla v rozporu s podmínkami pro poskytování veřejné podpory stanovenými právem Evropské unie nebo rozhodnutími Komise vydanými na jeho základě.

připojené k elektrizační soustavě České republiky. ***U výroben elektřiny uvedených do provozu od 1. ledna 2022 se podpora elektřiny z obnovitelných zdrojů může vztahovat pouze na výrobny elektřiny využívající energii vody ve výrobnách elektřiny do instalovaného výkonu 10 MW, větru, slunečního záření****, skládkového a kalového plynu. U výroben elektřiny uvedených do provozu od 1. ledna 2024 se podpora elektřiny z obnovitelných zdrojů může vztahovat také na výrobny elektřiny do 500 kW instalovaného výkonu využívající energii bioplynu.“*

Teoreticky se tak může podpora výroby elektřiny z OZE týkat i provozovatelů OZE, kteří jsou současně poskytovateli regulované služby ve smyslu Novely, byť omezení podpory výroby elektřiny ve vodních elektrárnách do výkonu 10 MW takovéto OZE z podpory v zásadě vylučuje (srov. parametry prvku kritické infrastruktury, kdy výrobna elektřiny musí mít instalovaný výkon alespoň 500 MW, resp. 100 MW v případě výrobny poskytující podpůrné služby). Jiné druhy OZE než vodní elektrárny nejsou co do instalovaného výkonu omezeny.

Z právní úpravy obsažené v ZPZE však plyne, že tato se podrobně zabývá způsoby podpory výroby elektřiny z OZE a požadavky, jaké tyto OZE musí splňovat, neřeší však jejich kyberbezpečnost, ani **neumožňuje podmínit poskytnutí podpory podle ZPZE provedením opatření ke zvýšení kyberbezpečnosti**, nebo prokázáním toho, že provozovatel OZE podporované dle ZPZE zajišťuje kyberbezpečnost OZE. Viz například ustanovení:

d) § 4 ZPZE, které podrobně vymezuje, co se rozumí podporou elektřiny z OZE, a stanoví řadu podmínek, které musí být splněny (kromě již uvedeného § 4 odst. 2 ZPZE) také minimální účinnost užití energie stanovenou prováděcím právním předpisem, která se však na většinu OZE nevztahuje[42], podmínky uvedené v § 4 odst. 4 ZPZE, které např. z podpory vylučují FVE umístěné na zemědělské půdě I. nebo II. třídy ochrany, nebo podmínky v § 4 odst. 5 ZPZE, které např. vylučují z podpory elektřinu z OZE vyrobenou výrobcem, který nesplňuje povinnosti stanovené v § 11a ZPZE (tedy povinnosti týkající se měření a evidence elektřiny z OZE).

e) § 11 ZPZE, v němž jsou vymezeny podmínky podpory elektřiny a výkupu elektřiny z obnovitelných zdrojů, druhotných zdrojů a vysokoúčinné kombinované výroby elektřiny a tepla, přičemž žádná z nich se netýká zajištění kyberbezpečnosti OZE, nebo

[42] Podle § 4 odst. 3 ZPZE: *„Požadavky na minimální účinnost užití energie se nestanoví pro výrobny elektřiny využívající geotermální energii, energii slunečního záření, energii větru a vody.“*

f) § 28 odst. 3 ZPZE, v němž je podrobně popsán způsob, jakým vláda stanoví prostředky státního rozpočtu pro poskytnutí dotace na úhradu složky ceny služby distribuční soustavy a složky ceny služby přenosové soustavy na podporu elektřiny, na úhradu provozní podpory tepla, přechodné transformační podpory tepla a podpory biometanu, a to do 30. září kalendářního roku, který předchází kalendářnímu roku, pro který Energetický regulační úřad (§ 2 odst. 1 písm. u) ZPZE) stanoví složku ceny služby distribuční soustavy a složku ceny služby přenosové soustavy na podporu elektřiny.

Na druhou stranu, ustanovení § 53 odst. 1 písm. a) ZPZE zmocňuje Ministerstvo průmyslu a obchodu k vydání vyhlášky, která stanoví (mimo jiné) druhy **a parametry podporovaných obnovitelných zdrojů** a způsoby jejich využití pro výrobu elektřiny z obnovitelných zdrojů, přičemž při vymezení parametrů OZE by bylo možné stanovit též parametry na kyberbezpečnost OZE. Další zmocnění v § 53 odst. 1 ZPZE se pak podrobně věnují řadě konkrétních požadavků, které musí podporované OZE splňovat, např. podmínky a požadavky na modernizaci výrobny elektřiny u jednotlivých druhů podporovaných zdrojů energie a rozsah uchovávaných dokladů prokazujících provedení modernizace výrobny elektřiny, žádný z nich se však netýká kyberbezpečnosti.

Pokud by měla být kyberbezpečnost OZE zohledněna v rámci podpory výroby elektřiny z OZE dle ZPZE, bylo by nutné změnit samotný zákon, resp. rozsah jeho zmocnění ministerstva průmyslu a obchodu k vydání prováděcích předpisů tak, aby výslovně zmiňovaly kyberbezpečnost a aby proto prováděcí právní předpisy musely požadavek kyberbezpečnost OZE obsahovat a vymezit jeho podrobnosti.

Zákon č. 218/2000 Sb., o rozpočtových pravidlech

Zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla), ve znění pozdějších předpisů (dále jen „**ZRP**“), obsahuje obecnou právní úpravu poskytování dotací a návratných finančních výpomocí v § 12 až 18. Podotýkáme, že ačkoliv ZRP rozlišuje v § 3 písm. a) a b) dotace a návratnou finanční výpomoc, právní úprava jejich poskytování je až na výjimky shodná[43], proto co bude dále uvedeno o „dotaci“, platí též o „návratné finanční výpomoci“.

Dotace mohou poskytovat tzv. poskytovatelé, kterými jsou subjekty uvedené v § 14 odst. 2 ZRP: ústřední orgán státní správy ve smyslu § 1 a 2 zákona č. 2/1969 Sb., kompetenčního zákona, ve znění pozdějších předpisů, Akademie věd České republiky, Grantová agentura České republiky, Technologická agentura České republiky nebo organizační složka státu, kterou určí zvláštní zákon. Poskytovatelem dotace tak může být také NÚKIB, který je jedním z ústředních orgánů státní správy.

[43] Např. § 13 odst. 3 písm. c), d) a e) ZRP rozlišuje individuální dotace, systémové dotace a návratné finanční výpomoci.

Aby bylo možné dotaci poskytnout, je třeba vypsat program a vyhlásit výzvu k podávání žádostí o dotaci z daného dotačního programu. Obecná úprava dotačních programů (dále jen „programů“), kterým je soubor věcných, časových a finančních podmínek pro konkrétní činnosti směřující k dosažení stanoveného cíle, obsažena v § 12 ZRP. Z ní vyplývá, že každý program, pokud obsahuje dotační investiční či dotační neinvestiční akce[44], musí mít dokumentaci obsahující (mimo jiné) specifikaci cílů programu a podprogramu spolu s jejich technickoekonomickým zdůvodněním a kritéria vyhodnocení efektivnosti vynaložených peněžních prostředků (§ 12 odst. 3 písm. c) ZRP. Účast státního rozpočtu na financování programu je podrobně upravena v § 13 ZRP a souvisejícím nařízení vlády, z hlediska předmětu této analýzy však není relevantní, postačí konstatování, že právní úprava poskytování dotací v ZRP zahrnuje dotace nejen ze státního rozpočtu, ale i z rozpočtu Evropské unie.

Výzva k podání žádosti o dotaci je upravená v § 14j ZRP, musí být zveřejněna a jejím **obsahem je věcné zaměření, okruh oprávněných žadatelů o dotaci,** lhůta pro podání žádosti, popřípadě další požadavky, které žadatel o dotaci musí naplnit, a informace o podkladech pro rozhodnutí poskytovatele dotace podle § 14 odst. 3 písm. f) ZRP. **Žádost o dotaci lze podávat pouze v návaznosti na konkrétní výzvu** (jak plyne z náležitostí žádosti o dotaci, která musí podle § 14 odst. 3 písm. g) ZRP obsahovat identifikaci výzvy, na jejímž základě je podána), **nelze tedy žádat o dotaci mimo zveřejněné výzvy konkrétního dotačního programu**, což se projevuje i v § 14j odst. 3 ZRP, podle něhož se k žádosti o dotaci před zveřejněním výzvy nepřihlíží.

Okruh oprávněných žadatelů je stanoven v konkrétní výzvě, z § 14 odst. 3 písm. e) ZRP plyne, že žadatelem o dotací může být fyzická i právnická osoba (v případě právnické osoby musí být v žádosti uvedeny údaje o jejím skutečném majiteli).

V případě, že je žádosti o dotaci vyhověno, vydá poskytovatel rozhodnutí o dotaci podle § 14m odst. 1 písm. a) ZRP, jehož obsahem je podle § 14 odst. 4 ZRP (mimo jiné) účel, na který je poskytovaná částka určena, lhůtu, v níž má být stanoveného účelu dosaženo, případné další podmínky, které musí příjemce v souvislosti s použitím dotace nebo návratné finanční výpomoci splnit. Nadto může být podle § 14 odst. 5 ZRP v rozhodnutí o poskytnutí dotace stanoveno, že nesplnění některých podmínek uvedených v § 14 odst. 4 ZRP bude postiženo odvodem za porušení rozpočtové kázně (viz § 44 a 44a ZRP).

---

[44] Toto členění programu obsahuje § 12 odst. 2 písm. a) a b) ZRP, samotné pojmy jsou definovány v § 3 písm. p) a q) ZRP, přičemž dotační investiční akcí se rozumí soubor věcných, časových a finančních podmínek pro činnosti k dosažení stanoveného cíle realizovaný prostřednictvím výdajů na pořízení nebo technické zhodnocení dlouhodobého hmotného nebo nehmotného majetku podle právních předpisů upravujících účetnictví, případně souvisejících výdajů poskytovaných jako dotace nebo návratné finanční výpomoci, dotační neinvestiční akcí se rozumí soubor věcných, časových a finančních podmínek pro činnosti k dosažení stanoveného cíle realizovaný výhradně prostřednictvím dotací nebo návratných finančních výpomocí jiných než podle § 3 písmene p) ZRP.

Z tohoto obecného vymezení vyplývá, že shora uvedeným **poskytovatelům ZRP nebrání ve vyhlášení dotačního programu na podporu zajištění kyberbezpečnosti OZE**. ZRP **rovněž nebrání tomu, aby byli do okruhu způsobilých žadatelů zahrnuti také provozovatelé OZE**. Stejně tak ZRP **nebrání podmínit poskytování dotací provozovatelům OZE zajištěním kyberbezpečnosti OZE**, přičemž nedodržení těchto podmínky může být sankcionováno jako porušení rozpočtové kázně**. Vše záleží na jednotlivých poskytovatelích dotací,** jaké podmínky pro jejich poskytnutí stanoví ve svých programech a na ně navazujících výzvách. Na samotné poskytnutí dotace není právní nárok.

Pro úplnost uvádíme, že **podmínky jednotlivých dotačních programů i jednotlivých výzev obvykle ukládají žadatelům, resp. příjemcům dotace** (tedy žadatelům, kterým byla dotace poskytnuta) **postupovat při realizaci účelu podpořeného dotací v souladu se ZZVZ**, přičemž programy mohou obsahovat i zvláštní pravidla pro zadávání veřejných zakázek malého rozsahu, resp. jiných veřejných zakázek zadávaných mimo zadávací řízení (obdobně, jako si mohou jednotlivé obce stanovit vlastní podmínky zadávání veřejných zakázek malého rozsahu).

Zákon č. 250/2000 Sb.

Zákon č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů, ve znění pozdějších předpisů (dále jen „**ZPÚR**“) obsahuje vlastní právní úpravu poskytování dotací a návratných finančních výpomocí z rozpočtů územních samosprávných celků v § 10a až 10d, přičemž tato úprava je jednodušší než v případě ZRP. Stejně jako v případě poskytování dotací či návratné finanční výpomoci (dále jen „**dotace**“)[45] ze státního rozpočtu dle ZRP jsou i dotace z rozpočtů územních samosprávných celků poskytovány na základě předchozí žádosti, podané způsobilým žadatelem, a to buď na účel určený poskytovatelem dotace v předem zveřejněném programu ve smyslu § 10a odst. 1 písm. f) ZPÚR[46] obsahujících podmínky poskytování dotací, jak plyne z § 10c odst. 1 ZPÚR, nebo na jiný, v žádosti uvedený účel (již nyní lze žádat o dotaci na zajištění kyberbezpečnosti OZE), nebo na účel stanovený zvláštním právním předpisem – Novela ani doprovodný zákon však takovými zvláštními předpisy nejsou.[47]

---

[45] ZPÚR sice v § 10a odst. 1 písm. b) a c) rozlišuje dotace a návratné finanční výpomoci (rozdíl je v tom, že dotace spočívá v nevratném poskytnutí peněžních prostředků), avšak dále je právní úprava jejich poskytování shodná. Proto co platí pro „dotace“, platí též pro „návratnou finanční výpomoc“.

[46] Programem se rozumí souhrn věcných, časových a finančních podmínek podpory účelu určeného poskytovatelem v programu.

[47] Ustanovení § 68 Novely upravuje finanční zabezpečení stavu kybernetického nebezpečí a ukládá NÚKIB vyčlenění prostředků v rozpočtu své kapitoly na daný rok k zajištění přípravy na stav kybernetického nebezpečí. Netýká se však poskytování dotací ze státního rozpočtu, ani financování kyberbezpečnosti OZE.

Poskytovatelem dotací mohou být kromě územních samosprávných celků též městské části hl. m. Prahy, svazek obcí nebo Regionální rada regionů soudržnosti (§ 10a odst. 1 písm. a) ZPÚR).

Samotný program musí podle § 10c odst. 2 ZPÚR obsahovat (kromě jiného) účel, na který mohou být peněžní prostředky poskytnuty, důvody podpory stanoveného účelu, okruh způsobilých žadatelů, kritéria pro hodnocení žádosti a podmínky pro poskytnutí dotace. Obsahu programu pak odpovídá žádost o poskytnutí dotace v § 10a odst. 3 ZPÚR a rovněž obsah veřejnoprávní smlouvy o poskytnutí dotace dle § 10a odst. 5 ZPÚR.

Z tohoto obecného vymezení vyplývá, že shora uvedeným **poskytovatelům ZPÚR nebrání ve vyhlášení dotačního programu na podporu zajištění kyberbezpečnosti OZE**. ZPÚR **rovněž nebrání tomu, aby byli do okruhu způsobilých žadatelů zahrnuti také provozovatelé OZE**, neboť podle § 10a odst. 3 písm. a) ZPÚR může být žadatelem fyzická či právnická osoba, přičemž právnická osoba musí doložit údaje o svém skutečném majiteli. Stejně tak ZPÚR **nebrání podmínit poskytování dotací provozovatelům OZE zajištěním kyberbezpečnosti OZE. Vše záleží na jednotlivých poskytovatelích dotací,** jaké podmínky pro jejich poskytnutí stanoví.

Kromě toho může každý provozovatel OZE požádat o dotaci mimo dotační program a poskytovatel mu ji může poskytnout, přičemž i v takovém případě může poskytovatel stanovit podmínky, které je příjemce dotace povinen splnit, tyto podmínky mohou zahrnovat i prokázání zajištění kyberbezpečnosti OZE (pokud právě to není účelem žádosti o dotaci). **Obdobnou možnost žadatel o dotaci podle ZRP** (ani její poskytovatel) **nemá**.

Nad rámec této právní analýzy podotýkáme, že proti sdělení, resp. rozhodnutí o neposkytnutí dotace se lze odvolat, nicméně na dotaci nebo návratnou finanční výpomoc není právní nárok, ledaže zvláštní zákon stanoví jinak (§ 10a odst. 2 ZPÚR).

3. Přehled práva EU

Tato část analýzy je uvedena spíše pro úplnost, neboť právo Evropské unie je součástí českého právního řádu a jak ZKB, tak Novela a další výše citované právní předpisy obvykle právo EU – zejména směrnice – v určité míře implementují. Z toho pak plyne (mimo jiné) povinnost jejich eurokonformního výkladu, tedy řešit případné pochybnosti či nejasnosti tak, aby bylo dosaženo výkladu souladného s výkladem příslušných právních norem EU zejména Komisí či Soudním dvorem EU.

3.1 Směrnice NIS

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. 7. 2016, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, implementovaná do českého právního řádu mimo jiné ZKB, pozbude platnosti ke dni 18. 10. 2024, a to díky čl. 44 Směrnice NIS 2, která ji nahrazuje. Z tohoto důvodu se touto směrnicí dále nezabýváme.

3.2 Směrnice NIS 2

Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. 12. 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (tedy „**směrnice NIS 2**“) je hlavním důvodem předložení Novely, jak ostatně uvádí zvláštní část důvodové zprávy k § 1 Novely: *„**Návrh zákona je téměř zcela transpozičním předpisem směrnice NIS 2.** Je-li právním předpisem prováděno přizpůsobení právního řádu přímo použitelnému předpisu EU a je-li jím souběžně promítána do právního předpisu celá směrnice EU nebo její podstatná část, je nezbytné, aby tyto předpisy EU byly uvedeny v referenčním ustanovení, jak stanoví Legislativní pravidla vlády. Spolu se směrnicí NIS 2 je tento zákon také adaptačním zákonem pro akt o kybernetické bezpečnosti, nařízení (EU) 2021/887, nařízení Evropského parlamentu a Rady (EU) 2021/696 ze dne 28. dubna 2021, kterým se zavádí Kosmický program Unie a zřizuje Agentura Evropské unie pro Kosmický program a zrušují nařízení (EU) č. 912/2010, (EU) č. 1285/2013 a (EU) č. 377/2014 a rozhodnutí č. 541/2014/EU, a dále rozhodnutí Evropského parlamentu a Rady č. 1104/2011/EU ze dne 25. října 2011 o podmínkách přístupu k veřejné regulované službě nabízené globálním družicovým navigačním systémem vytvořeným na základě programu Galileo.“* **Z dosud uvedeného vyplývá, že nemá smysl analyzovat samotnou směrnici NIS 2, neboť takovou analýzou je výše uvedený**

popis Novely a jeho dopadu na kyberbezpečnost OZE. Současně z uvedeného vztahu Novely a NIS 2 plyne, že by Novela měla být vykládána eurokonformním způsobem. Konečně, pokud nedojde k transpozici směrnice NIS 2 do 18. 10. 2024, tedy nedojde k nabytí účinnosti Novely, bude obsah směrnice NIS 2 přímo vykonatelný. V podrobnostech odkazujeme na rozdílovou tabulku Novely s předpisy EU, ze které je patrné, že Novela je do značné části doslovným přepisem směrnice NIS 2 do českého právního řádu.[48]

3.3 Směrnice 2022/2557 o odolnosti kritických subjektů

Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES, má být podle svého čl. 26 provedena do 17. 10. 2024 (přesněji řečeno, ČR musí do 17. 10. 2024 přijmout a zveřejnit opatření nezbytná pro dosažení souladu s touto směrnicí, oznámit je Komisi a tato opatření používat od 18. 10. 2024). Zvláštní část důvodové zprávy k § 1 Novely k tomu uvádí, že: *„V době vytváření návrhu zákona se na úrovni Evropské unie připravuje celá řada dalších právních předpisů dotýkajících se obsahu směrnice NIS 2, resp. tohoto návrhu zákona, případně byly tyto právní předpisy již přijaty a je očekávána jejich transpozice nebo adaptace do národních právních řádů.* ***V prvé řadě se jedná o transpozici směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES, kterou připravuje Ministerstvo vnitra, resp. Generální ředitelství Hasičského záchranného sboru*** *(transpoziční lhůta je obdobná jako v případě směrnice NIS 2), která ovlivňuje vztah návrhu zákona ke kritické infrastruktuře.* ***Přímá transpozice do návrhu zákona se neočekává, nicméně do návrhu zákona je transponována povinnost ze směrnice NIS 2*** *(zejm. čl. 1 odst. 2 písm. b) nebo čl. 2 odst. 3 atd.) týkající se vazby na obsah směrnice Evropského parlamentu a Rady (EU) 2022/2557.“*

3.4 Nařízení pro nulové čisté emise (Net Zero Industry Act)

Nařízení Evropského parlamentu a Rady (EU) 2024/1735 ze dne 13. 6. 2024, kterým se zřizuje rámec opatření pro posílení evropského ekosystému výroby technologií pro

[48] Rozdílová tabulka dostupná zde: https://psp.cz/sqw/text/orig2.sqw?idd=244068

nulové čisté emise a mění nařízení (EU) 2018/1724 (dále jen „**Nařízení**“)[49], jehož účelem je podpora OZE, v odst. 2 své preambule uvádí, že:

„Vzhledem ke složitosti a nadnárodní povaze technologií pro nulové čisté emise by nekoordinovaná vnitrostátní opatření za účelem zajištění přístupu k těmto technologiím představovala riziko narušení hospodářské soutěže a tříštění vnitřního trhu. Taková opatření členských států mohou vést k tomu, že se pro hospodářské subjekty na trhu zavede rozdílná regulace, která by poskytovala různé úrovně přístupu k dodávkám technologií pro nulové čisté emise v jednotlivých členských státech, a to i poskytováním různých úrovní podpory projektům výroby uvedených technologií, zaváděním odlišných pravidel a nekoordinovaných forem zadávání zakázek, rozdílných procesů a dob trvání v souvislosti s povolovacími postupy, což by vytvořilo překážky přeshraničnímu obchodu mezi členskými státy, a tudíž bránilo řádnému fungování vnitřního trhu. Pro zajištění fungování vnitřního trhu je proto nezbytné vytvořit společný právní rámec Unie, který by ***společně řešil tento hlavní problém tím, že dojde ke zvýšení odolnosti a bezpečnosti dodávek v Unii v oblasti technologií pro nulové čisté emise****.“*

Relevantní je z hlediska této analýzy čl. 25 an. Nařízení, který se týká zadávacích řízení spadajících do oblasti působnosti směrnic č. 2014/23/EU o udělování koncesí, č. 2014/24/EU, o zadávání veřejných zakázek a o zrušení směrnice 2004/18/ES, nebo č. 2014/25/EU, o zadávání zakázek subjekty působícími v odvětví vodního hospodářství, energetiky, dopravy a poštovních služeb a o zrušení směrnice 2004/17/ES[50], pokud mají zakázky jako součást svého předmětu technologie pro nulové čisté emise uvedené v čl. 4 odst. 1 písm. a) až k) Nařízení, tedy zjednodušeně technologie OZE[51], nebo v případě zakázek na stavební práce a koncesí na stavební práce zahrnujících uvedenou technologii OZE. Čl. 25 odst. 1 Nařízení ukládá veřejným zadavatelům a sektorovým zadavatelům uplatňovat *„minimální povinné požadavky týkající se environmentální udržitelnosti stanovené v prováděcím aktu uvedeném v odstavci 5 tohoto článku.“* Čl. 25 odst. 5 Nařízení odkazuje na budoucí prováděcí akt Komise, jímž stanoví pokyny pro minimální požadavky na environmentální udržitelnost pro zadávací řízení podle odstavce 1. Tyto minimální požadavky budou muset být součástí zadávacích podmínek.

Kromě toho však čl. 25 odst. 1 Nařízení nebrání výše uvedeným veřejným zadavatelům a sektorovým zadavatelům v tom, aby v souvislosti s environmentální udržitelností

---

[49] https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=OJ:L_202401735&qid=1722545521703

[50] Jde o směrnice upravující zadávání veřejných zakázek, které jsou do českého právního řádu implementovány ZZVZ.

[51] Jde o technologie zahrnující solární technologie, včetně fotovoltaických, solárních termoelektrických a solárních termálních technologií, technologie pro výrobu větrné energie, bateriové technologie a technologie ukládání energie, tepelná čerpadla a technologie pro využití geotermální energie, vodíkové technologie, technologie CCS, technologie v oblasti elektrizačních soustav, včetně technologií elektrického dobíjení pro dopravu a technologií pro digitalizaci soustavy; technologie v oblasti hydroelektrické energie. Výčet zahrnuje též technologie v oblasti udržitelné výroby bioplynu a biometanu, technologie v oblasti energie z jaderného štěpení a technologie v oblasti udržitelných alternativních paliv.

používali další minimální požadavky nebo kritéria pro udělení zakázky (čl. 25 odst. 2 Nařízení).

Konečně, **ustanovení čl. 25 odst. 3 Nařízení ukládá veřejným zadavatelům a sektorovým zadavatelům bez ohledu na čl. 25 odst. 1 Nařízení uplatnit alespoň jednu z následujících podmínek**, požadavků nebo smluvních závazků:

a) zvláštní podmínku vztahující se na sociální nebo zaměstnanecké aspekty;

b) **požadavek na prokázání souladu s platnými požadavky na kybernetickou bezpečnost stanovenými v nařízení o kybernetické odolnosti**, a to i prostřednictvím příslušného evropského systému certifikace kybernetické bezpečnosti, je-li to vhodné a je-li k dispozici; Nařízení o kybernetické odolnosti, na které odkazuje písm. b), **bude přijato pravděpodobně na podzim 2024**[52], v platnost by mělo vstoupit po třech letech, tedy na podzim 2027.

c) konkrétní smluvní závazek dodat včas součást smlouvy týkající se technologií pro nulové čisté emise uvedených v čl. 4 odst. 1 písm. a) až k) Nařízení (tedy technologie OZE), z něhož může vyplynout povinnost zaplatit přiměřený poplatek, pokud tento závazek není splněn, a který jde nad rámec požadavků stanovených v platných vnitrostátních právních předpisech, pokud takové právní předpisy existují.

Navazující čl. 25 odst. 4 Nařízení k tomu dodává, že minimální povinné požadavky podle čl. 25 odst. 1 Nařízení mají podobu buď technických specifikací nebo technických a funkčních požadavků (srov. § 89 an. ZZVZ), nebo zvláštních podmínek plnění veřejné zakázky.

Z dosud uvedeného vyplývá, že pokud bude provozovatel OZE současně veřejným či sektorovým zadavatelem veřejných zakázek, bude muset do podmínek zadávání veřejných zakázek zapracovat také požadavek na zajištění kyberbezpečnosti, pokud nezvolí zapracování podmínek podle písm. a) nebo c) výše citovaného ustanovení. Stanovení požadavků na kybernetickou bezpečnost lze provést způsoby podrobně popsanými v části analýzy týkající se ZZVZ.

Pro úplnost je třeba dodat, že zohlednění požadavků na kyberbezpečnost se netýká jen čl. 25 Nařízení, ale pracuje s ním i čl. 26 Nařízení upravující dražby za účelem využívání obnovitelných zdrojů energie, podle kterého členské státy při navrhování dražeb pro zavádění energie z obnovitelných zdrojů zahrnou u technologií uvedených v čl. 4 odst. 1 písm. a) až j) Nařízení, které jsou technologiemi v oblasti energie z obnovitelných zdrojů,

[52] Viz NÚKIB: https://nukib.gov.cz/cs/infoservis/aktuality/2130-proces-prijeti-aktu-o-kyberneticke-odolnosti-je-o-krok-blize/

předvýběrová kritéria, která se budou týkat (kromě jiného) kybernetické bezpečnosti a bezpečnosti údajů. Relevantní je také čl. 28 Nařízení, který upravuje možnost členských států přijmout další nástroje podpory čistých technologií na základě necenových kritérií, kterým může být i cíl zajištění kybernetické bezpečnosti.

3.5 Další směrnice a nařízení

Pro úplnost podotýkáme, že z hlediska aplikace Novely bude v brzké době relevantní také Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011, které vstoupilo v platnost 16. 1. 2023 a je vymahatelné 24 měsíců po vstupu v platnost, tedy od 17. 1. 2025.

Podle zvláštní části důvodové zprávy k § 1 Novely: *„Toto nařízení a očekávání dalších jemu podobných předpisů (k tomu srov. rec. 28 směrnice NIS 2) vedlo k vytvoření speciálního ustanovení v návrhu zákona řešícího vztah mezi přímo použitelnými právními předpisy na úrovni Evropské unie, které zasahují do obecné působnosti směrnice NIS 2, resp. jejího transpozičního předpisu.* ***Toto ustanovení je odrazem čl. 4 směrnice NIS 2 a zakotvuje aplikační přednost přímo použitelných právních předpisů Evropské unie, které upravují vybrané otázky zajišťování kybernetické bezpečnosti ve srovnatelných nebo větších podrobnostech než tento návrh zákona.“*** Jedním z takových právních předpisů je výše uvedené „Nařízení“.

Důvodová zpráva Novely zmiňuje také připravované nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020 s tím, že: *„(datum přijetí je zatím neznámé, nicméně po vstupu v platnost budou mít regulované subjekty 24 měsíců na to, aby se přizpůsobily novým požadavkům, s výjimkou omezenějšího 12měsíčního období odkladu ve vztahu k ohlašovací povinnosti výrobců), nebo také návrh nařízení Evropského parlamentu a Rady, kterým se stanoví opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických bezpečnostních hrozeb a incidentů a pro připravenost a reakci na ně.“*

V evropském legislativním procesu jsou navíc již navrženy další právní předpisy, např. EU Cyber Resilience Act (Nařízení o kybernetické odolnosti), které se zaměřuje na ochranu spotřebitelů při nákupu zboží s prvkem digitalizace, ať už hardware či software.[53]

[53] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

4. Příklady ze zahraničí

Nad rámec právní analýzy uvádíme pro inspiraci odkazy na další zdroje ze zahraničí. České orgány se mohou inspirovat, pokud jde o dostupné technické certifikace, zjišťování tržně dostupných technologických řešení a návrhy regulace.

USA

Problematice kybernetické bezpečnosti OZE se věnuje Department of Energy, konkrétně specializovaná část Office for Cybersecurity. Již v roce 2022 tento orgán vydal zprávu[54], kde na rizika plynoucí z rozvoje decentralizovaných zdrojů energie upozorňuje. Ze zprávy vyplývá, že stávající standardy kybernetické bezpečnosti bude nutné přizpůsobit pro konkrétní případy decentralizovaných zdrojů energie.

V roce 2024 vydala kancelář prezidenta USA (Office of the National Cyber Director Executive Office of the President) Zprávu o kybernetické bezpečnosti v USA[55], kde je zajištění bezpečnosti v oblasti energetiky jednou z priorit. Mezi zvolená opatření patří vzdělávání pracovníků v sektoru, alokace finančních prostředků pro zřízení kyberbezpečnostních center na půdě amerických univerzit, přijetí technických norem a certifikací a také využití principu “secure-by-design” při rozvoji energetických projektů na federální úrovni.

Národní institut pro standardy a technologie (National Institute of Standards and Technology, NIST) v červnu 2024 zveřejnil návrh doporučení pro zajištění kybernetické bezpečnosti střídačů[56]. V současnosti probíhá finalizace tohoto doporučení.

Německo

Německá energetická agentura (DENA) založila platformu “Future Energy Lab” sdružující experty z řad průmyslu, policy-makerů, vědy a výzkumu. Součástí této platformy je také pracovní skupina pro kybernetickou bezpečnost v elektrotechnickém průmyslu[57]. Jejím cílem je podpořit firmy v celém řetězci elektroenergetického průmyslu, podpořit inovace, zvýšit povědomí o otázkách kybernetické bezpečnosti a publikovat relevantní doporučení. Německá energetická agentura vydala také studii o kybernetické

[54] Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid October 2022, dostupné online: https://www.energy.gov/sites/default/files/2022-10/Cybersecurity%20Considerations%20for%20Distributed%20Energy%20Resources%20on%20the%20U.S.%20Electric%20Grid.pdf
[55] Dostupné online: https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf.
56 Doporučení je dostupné zde: https://csrc.nist.gov/pubs/ir/8498/ipd.
[57] https://future-energy-lab.de/projects/branchenplattform-cybersicherheit/.

bezpečnosti[58], která doporučuje zaměřit se na regulaci, certifikaci, integrace IT-OT (propojení informační technologie s provozní technologií) a reakci na kybernetické útoky.

Austrálie

Ministerstvo klimatu, energetiky a životního prostředí (DCCEEW) vydalo spolu s Centrem pro kybernetickou bezpečnost (Cyber Security Cooperative Research Centre, CRC) zprávu[59], která poukazuje na rizika v oblasti kybernetické bezpečnosti v souvislosti s rozšířením střídačů. Doporučení plynoucí ze zprávy jsou:

- Pro všechny prodávané solární střídače je třeba provést hodnocení dopadu na kybernetickou bezpečnosti Austrálie. Identifikované zranitelnosti budou oznámeny výrobcům za účelem nápravy.
- Pro střídače a další zařízení internetu věcí (IoT), která jsou zásadní pro provoz kritické infrastruktury, bude zavedeno povinné hodnocení kybernetické bezpečnosti.
- Střídače, u kterých byla zjištěná závažná rizika v oblasti kybernetické bezpečnosti, by měly být staženy z prodeje a staženy z provozu nebo by měly být použity vhodné opravy zabezpečení, jsou-li k dispozici.

[58] https://future-energy-lab.de/app/uploads/2024/05/STUDIE_Themenroadmap_Branchenplattform_Cybersicherheit.pdf
[59] https://cybersecuritycrc.org.au/power-out-solar-inverters-and-silent-cyber-threat

5. Závěry právní analýzy

Z výše uvedené české právní úpravy a souvisejícího práva EU lze dovodit následující:

1. Z právní úpravy bezpečnosti ČR v širokém slova smyslu, zahrnující nejrůznější „mimořádné stavy“ vyplývá, že **stav kybernetického nebezpečí** je z hlediska ohrožení bezpečnosti, životů, zdraví a ekonomiky **méně intenzivní, než mimořádné stavy dle ZBezp**. Na druhou stranu to neznamená, že by porušení kyberbezpečnosti nemohlo vést svými důsledky, resp. hrozícími důsledky, k vyhlášení např. nouzového stavu. Dále platí, že stav kybernetického nebezpečí ve smyslu ZKB představuje zvláštní právní úpravu stavu, který je jinak řešen jako stav nebezpečí v KriZ.

2. Jak **mimořádné stavy** dle ZBezp, tak stav kybernetického nebezpečí dle ZKB, **slouží toliko k dočasným a mimořádným zásahům do provozování OZE**. Jako takové se proto nehodí k dlouhodobému nastavení podmínek výstavby a provozování OZE, zahrnujících zvýšení kyberbezpečnosti OZE.

3. **Malá část výroben OZE naplní znaky prvku kritické infrastruktury** dle KriZ, totiž průřezová a odvětvová kritéria (aby se jednalo o prvek kritické infrastruktury, musí být splněno aspoň jedno průřezové a jedno odvětvové kritérium současně).

   a) Jedním z průřezových kritérií je dopad na veřejnost s mezní hodnotou **rozsáhlého omezení** poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života **postihujícího více než 125 000 osob**. Toto průřezové kritérium by v případě vystavení OZE hackerskému útoku a následnému výpadku výroby elektřiny bylo nejsnáze splnitelné.

   b) Co se týká odvětvových kritérií, ta zahrnují jednak **výrobny** elektřiny s celkovým instalovaným elektrickým výkonem **nejméně 500 MW**, jednak **výrobny poskytující podpůrné služby** s celkovým instalovaným elektrickým výkonem **nejméně 100 MW**, vedení pro vyvedení výkonu a zabezpečení vlastní spotřeby výrobny elektřiny anebo dispečink výrobce elektřiny.

4. To, zda je výrobna OZE prvkem kritické infrastruktury nebo ne, je pak relevantní i z hlediska právní úpravy zajištění kyberbezpečnosti OZE, a to ve smyslu nově navržené právní úpravy v Novele, která má nahradit dosavadní právní úpravu kybernetické bezpečnosti, obsažené v ZKB.

5. **Jádrem právní úpravy kyberbezpečnosti OZE je Novela, implementující do českého právního řádu směrnici NIS 2.** Povinnosti týkající se kyberbezpečnosti OZE, které jsou buď přímo upravené v Novele, nebo lze tyto povinnosti

ukládat na základě Novely (např. zmocněním NÚKIB), dopadají v zásadě pouze na ty provozovatele OZE, kteří naplní definici „poskytovatele regulované služby“.

Poskytovatelem regulované služby bude každý provozovatel OZE, který splní buď podmínky v § 4 Novely, nebo alespoň jednu z podmínek v § 5 Novely.

Lze konstatovat, že provozovatel OZE bude poskytovatelem regulované služby podle § 4 Novely, pokud bude poskytovat službu **významnou pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v ČR v odvětví energetiky, současně se bude jednat o velký nebo střední podnik, nebo bude provozovatel OZE významný pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v ČR. Středním podnikem** se rozumí podnik, který zaměstnává méně než 250 osob a jehož roční obrat nepřesahuje 50 milionů eur, a/nebo jehož bilanční suma roční rozvahy nepřesahuje 43 milionů Euro, a který není malým podnikem, **velkým podnikem** se pak rozumí podnik, který tato kritéria překonává, tj. zaměstnává alespoň 250 osob a jeho roční obrat přesahuje 50 milionů EUR. Z toho je zřejmé, jen malá část provozovatelů OZE bude současně poskytovatelem regulované služby dle § 4 Novely. Navíc vymezení v § 4 Novely bude ještě upřesněno vyhláškou vydanou NÚKIB, její znění však není v současnosti k dispozici.

Co se týká kritérií obsažených v § 5 Novely, jejich vyhodnocení je z hlediska určení, zda je provozovatel OZE současně poskytovatelem regulované služby nebo ne, složitější. Poskytovatelem regulované služby je podle tohoto ustanovení Novely (vyjma subjektů podřaditelných pod § 4 Novely, které splňují některou z dodatečných podmínek) buď

- subjekt kritické infrastruktury (tedy provozovatel prvku kritické infrastruktury podle KriZ), nebo
- ten, kdo poskytuje službu, jejíž narušení může způsobit závažný zásah do života více než 125 000 osob (aniž by se nutně muselo jednat o subjekt kritické infrastruktury dle KriZ), nebo
- ten, kdo poskytuje službu, jejíž narušení může způsobit závažný zásah do schopnosti poskytovat jinou regulovanou službu poskytovatele v režimu vyšších povinností.

Výklad § 5 Novely bude opět záviset na NÚKIB.

Lze uzavřít, že minimálně část provozovatelů OZE bude, resp. může být, poskytovatelem regulovaných služeb. Na rozdíl od stávající právní úpravy

v ZKB došlo k podstatnému – až patnáctinásobnému – rozšíření okruhu těchto poskytovatelů regulovaných služeb, a to změnami jejich definicí.

6. **Každý poskytovatel regulované služby tak bude muset zavádět bezpečnostní opatření uvedená v § 14 Novely** (v závislosti na režimu, do něhož bude poskytovatel regulované služby spadat), a **pokud bude provádění bezpečnostních opatření přenášet na své dodavatele, pak má poskytovatel** regulované služby **povinnost vybírat svého dodavatele v souladu s požadavky vyplývajícími z bezpečnostního opatření** a zahrnovat požadavky vyplývající z bezpečnostního opatření do smluv s dodavatelem (§ 13 odst. 5 Novely). **Toto bude mít zásadní vliv na zadávání veřejných zakázek.**

7. Kromě toho všichni poskytovatelé regulované služby budou moci být adresáty protiopatření, vydávaných NÚKIB, zahrnujících kromě výstrahy a varování před kybernetickým nebezpečím také „reaktivní opatření“ ve smyslu § 23 Novely, která se opět mohou týkat i zadávaných veřejných zakázek či jejich plnění. Tato „reaktivní protiopatření“ jsou **dočasnými a mimořádnými zásahy do provozování OZE**. Jako takové **se proto nehodí k dlouhodobému nastavení podmínek výstavby a provozování OZE z hlediska kyberbezpečnosti OZE.**

8. **Lze shrnout, že provozovatelé OZE, kteří budou poskytovateli regulované služby, budou muset řešit kyberbezpečnost OZE, mimo jiné zajištěním bezpečnosti střídačů a výběrem „bezpečných“ dodavatelů dodávek a služeb souvisejících s regulovanou službou. Pojem „dodavatel“, používaný v této souvislosti Novelou, je přitom podstatně širší, než jak je chápán „dodavatel“ ve smyslu právní úpravy zadávání veřejných zakázek v ZZVZ. To platí i pro níže uvedené prověřování bezpečnosti dodavatelského řetězce.**

9. **Na některé poskytovatele regulovaných služeb –** totiž na ty, kteří budou současně poskytovateli strategicky významné služby, přičemž nelze vyloučit, že někteří provozovatelé OZE budou poskytovateli strategicky významné služby – **budou dopadat další povinnosti plynoucí z § 27, 29 a 31 Novely**, a takoví poskytovatelé strategicky významných služeb je budou muset zohlednit při uzavírání smluv na veřejné zakázky i mimo ně. **Tyto povinnost zahrnují prověřování bezpečnosti dodavatelského řetězce**, a to

   - jak ze strany NÚKIB, který pak na základě výsledků tohoto prověření může poskytovateli strategické služby uložit buď dodatečné podmínky (které bude muset poskytovatel strategicky významné služby zohlednit v rámci zadávání veřejné zakázky i mimo něj), nebo mu zakáže plnit z již uzavřené smlouvy;

   - tak ze strany samotného poskytovatele strategicky významné služby, který bude muset s vynaložením přiměřeného úsilí zjišťovat informace o svých

dodavatelích bezpečnostně významných dodávek. **Tyto informace pak bude muset poskytovatel** strategicky významné služby **evidovat v rozsahu stanoveném v § 31 odst. 1 písm. b) Novely**, tedy bude muset alespoň identifikovat všechny bezpečnostně významné dodávky a jejich dodavatele, **a případné změny hlásit do 10 dní od jejich zjištění NÚKIB.**

Předpokládáme však, že okruh provozovatelů OZE, kteří budou poskytovateli strategicky významné služby, bude velmi malý ve srovnání s počtem provozovatelů OZE, kteří splní obecnou definici poskytovatele regulované služby.

10. Z dosud uvedeného vyplývá, že **většina provozovatelů OZE nebude ani subjektem kritické infrastruktury** (neboť jimi provozovaná OZE nenaplní definici prvku kritické infrastruktury), **ani poskytovatelem regulovaných služeb nebo poskytovatelem strategicky významných služeb**. Nebudou se na ně tudíž vztahovat povinnosti týkající se kyberbezpečnosti OZE, plynoucí z výše uvedených právních předpisů. **Nabízí se proto otázka, zda lze takové provozovatele OZE motivovat k zajištění kyberbezpečnosti jimi vlastněných, resp. provozovaných, OZE? Odpověď dává právní úprava zadávání veřejných zakázek a právní úprava poskytování dotací z veřejných rozpočtů.**

11. **Provozovatelé OZE, kteří naplní některou z definic zadavatele veřejné zakázky, budou muset jak výstavbu OZE, tak její úpravy, rozšiřování či provoz řešit zadáním veřejné zakázky, obvykle v zadávacím řízení**. Ačkoliv samotný ZZVZ výslovně o kyberbezpečnosti OZE nehovoří, umožňuje zadavatelům veřejných zakázek v rámci zadávacích podmínek zajištění kyberbezpečnosti OZE požadovat, a to na různých úrovních a v různém rozsahu.

12. Ustanovení **§ 37 odst. 7 ZZVZ umožňuje vládě stanovit svým nařízením některé závazné podmínky účasti v zadávacím řízení** v určitých kategoriích veřejných zakázek a rozsah jejich používání, nebo bližší podmínky pro posuzování přiměřenosti některých podmínek účasti v zadávacím řízení a rozsah jejich používání. **Toto ustanovení nepochybně dává široký prostor pro podrobnější úpravu podmínek účasti dodavatelů v zadávacím řízení i z hlediska kyberbezpečnosti OZE**, podotýkáme však, že v současnosti není tato možnost ze strany vlády využívána.

13. **Provozovatelé OZE, kteří budou současně buď veřejným nebo sektorovým zadavatelem, pak budou muset splnit požadavky čl. 25 Nařízení Evropského parlamentu a Rady (EU) 2024/1735** ze dne 13. 6. 2024, kterým se zřizuje rámec opatření pro posílení evropského ekosystému výroby technologií pro nulové čisté emise a mění nařízení (EU) 2018/1724, a tedy **zahrnout do zadávacích podmínek veřejné zakázky požadavek na prokázání souladu s platnými**

požadavky na kybernetickou bezpečnost stanovenými v nařízení o kybernetické odolnosti. Tyto požadavky specifikuje nařízení o kybernetické odolnosti, které bude pravděpodobně přijato na podzim 2024 a vstoupí v platnost v roce 2027.

14. **Ze související právní úpravy poskytování dotací z veřejných rozpočtů pak vyplývá, že poskytovatelé dotací mohou například podmínit poskytnutí dotace související s realizací OZE zajištěním kyberbezpečnosti OZE**, případně mohou příjemci dotace uložit povinnost při plnění účelu dotace (např. výstavbě výrobny OZE na střeše nemovitosti vlastněné příjemcem dotace) zadávat veřejné zakázky v zadávacím řízení, ve kterém lze dodavatelům klást podmínky týkající se kyberbezpečnosti OZE. Jak ZPÚR, tak ZRP umožňují poskytovatelům dotací stanovit podmínky poskytnutí dotace v zásadě libovolně.

Září 2024

Hlavní autor: Mgr. Petr Bouda
Frank Bold Advokáti, s.r.o
Další autorky: Mgr. Laura Otýpková, Ph.D., Mgr. Kristína Šabová
Frank Bold Society, z.s.

frank bold