Analýzy a trendy výzkumu,
technologií a inovací

TECHNOLOGICKÉ CENTRUM PRAHA

ergo

ročník 18 / číslo 01 / červenec 2023

Editorial

Vážené čtenářky, vážení čtenáři,

v jednom ze svých předchozích editorialů jsem psal o rostoucím významu výzkumné a inovační politiky orientované na mise. S ohledem na aktuálnost se k tomuto tématu opět vracím.

Je zřejmé, že v dnešním dynamicky se měnícím světě čelí naše společnost různým výzvám, které jsou svojí povahou velmi komplexní. Změna klimatu narušuje ekosystémy a vyžaduje inovativní řešení v oblasti energetiky, dopravy a využívání zdrojů a surovin. Stárnutí populace představuje významnou výzvu pro systém zdravotní péče a sociální systémy. Rychlý technologický vývoj vyvolává obavy o soukromí, kybernetickou bezpečnost a zachování integrity společnosti. Agrese Ruska vůči Ukrajině a předtím pandemie covidu-19 ukázaly, jak jsme zranitelní a nepřipravení.

Pro účinné řešení současných společenských výzev je nezbytné zaměřit úsilí na hledání nových řešení, která pomohou transformovat existující systémy (produkční, bezpečnostní, energetické, dopravní, sociální, zdravotní, vzdělávací a další) a účinně koordinovat různé zdroje a nástroje na podporu výzkumu, vývoje a zavádění inovací. Tento přístup výzkumné a inovační politiky zaměřený na mise je nyní akcentován jak v evropské politice, tak i v národních politikách (např. Německa, Rakouska, Velké Británie či Nizozemska).

Česko má nyní unikátní příležitost připojit se k těmto progresivním zemím a stanovit si mise ve formě konkrétních měřitelných cílů a strategicky orientovat své investiční priority na řešení naléhavých společenských výzev. Prostor je k tomu při přípravě nových Národních priorit orientovaného výzkumu, které by se nově měly soustředit na řešení výzev v oblastech dopadů změny klimatu, demografických změn, energetické transformace, technologických změn a jejich dopadů na společnost a v neposlední řadě v oblasti obrany, bezpečnosti a ochrany demokracie.

Vedle strategického zaměření však bude důležitým krokem nastavení mechanismů pro koordinaci různých zdrojů (veřejných i soukromých) a nástrojů podpory výzkumu, vývoje a inovací a zajištění jejich konzistentní implementace tak, aby jako doposud nedocházelo pouze k deklaratornímu vykazování příspěvku podpory k naplňování Národních priorit orientovaného výzkumu. K tomu bude zapotřebí věnovat náležitou pozornost (a personální kapacity) strategickému řízení procesu implementace nových národních priorit – misí a užšímu provázání výzkumných a inovačních aktivit s dalšími opatřeními realizovanými na úrovni sektorových politik. Inspirativní pro nás v tomto může být Rakousko, které zavedlo propracovaný systém řízení misí pro výzkum a inovace, nebo zkušenosti z experimentálního zavedení misí v Národní výzkumné a inovační strategii inteligentní specializace ČR.

Bez efektivního řízení misí a koordinace podpory z úrovně Rady pro výzkum, vývoj a inovace budou nové priority jen aktualizovaným seznamem pro vykazování souladu v programech a projektech výzkumu, vývoje a inovací, nikoliv však užitečným nástrojem pro orientaci výzkumných a inovačních aktivit na řešení velkých výzev naší společnosti.

Přeji vám zajímavé a inspirativní čtení.

Michal Pazour
vedoucí oddělení strategických studií
Technologického centra Praha

Analýzy a trendy výzkumu, technologií a inovací

Recenzovaný časopis
ISSN 1802-2006 – tištěná verze
ISSN 1802-2170 – elektronická verze
www.tc.cz/ergo
Evidenční číslo MK ČR E 16622

Vydavatel:
Technologické centrum Praha
(IČ: 60456540)
Ve Struhách 1076/27, 160 00 Praha 6
tel.: +420 234 006 100
www.tc.cz, *www.strast.cz*

Uzávěrka tohoto čísla: 26. 6. 2023
Články uvedené v přehledu na titulní straně prošly recenzním řízením.

Redakce:
Mgr. Martin Faťun (odpovědný redaktor),
fatun@tc.cz
Ing. Iva Vančurová (copy editor, distribuce),
vancurova@tc.cz

Grafická úprava:
MgA. Martin Procházka

Elektronická verze časopisu je volně dostupná na adrese *www.tc.cz/publikace*, kde si lze rovněž objednat bezplatné zaslání tištěné verze (do vyčerpání zásob). Pravidla pro přijímání příspěvků a pokyny pro autory jsou k dispozici na *www.tc.cz/publikace*.

Ergo 2023, 18, 1, 1–8
10.5281/zenodo.8111035

Mezinárodní porovnání publikační a patentové aktivity v oblasti kybernetické bezpečnosti

Technologie zajišťující kybernetickou bezpečnost na všech úrovních infrastruktury veřejné a soukromé sféry se staly jednou z klíčových strategických komodit, bez nichž nelze zajistit funkčnost a přežití všech systémových, ekonomických a společenských struktur. Cílem příspěvku je posoudit výzkum a vývoj v této oblasti na základě analýzy světové publikační a patentové aktivity. Celková světová publikační aktivita v oblasti kybernetické bezpečnosti od počátku milénia vzrostla přibližně 17krát a podíl na celkovém světovém publikačním výstupu téměř šestkrát. Nejvíce publikací v oboru pochází z Čínské lidové republiky, USA, Indie a Spojeného království, které v letech 2019–2020 vytvořily přibližně polovinu světového výstupu. V ČR je podíl publikací z oboru na celkovém počtu publikací zhruba na úrovni evropských zemí a dynamika růstu sleduje světový trend. Světový počet prioritních patentových přihlášek týkajících se kybernetické bezpečnosti od počátku milénia vzrostl více než třikrát, daleko nejvíce v Čínské lidové republice. V časovém okně 2016–2020 bylo v oblasti kybernetické bezpečnosti u čínského patentového úřadu (CNIPA) podáno více než 60 % a u amerického patentového úřadu (USPTO) přibližně 14 % světového počtu prioritních přihlášek. Patentové přihlášky v kybernetické bezpečnosti jsou v celkovém počtu patentových přihlášek zastoupeny téměř 2 %. V evropských zemích je nejvyšší zastoupení patentových přihlášek v kybernetické bezpečnosti ve Finsku, Estonsku, Švédsku, Irsku, Spojeném království a Francii. V ČR je zastoupení kybernetické bezpečnosti v patentových přihláškách v evropském měřítku mírně nadprůměrné. Počet patentových přihlášek v kybernetické bezpečnosti však v ČR narůstá daleko rychleji než v jiných zemích EU, což svědčí o výrazném rozvoji VaV v této technologické oblasti.

Klíčová slova: kybernetické bezpečnost; patentová aktivita; publikační aktivita

Martin Faťun
Zdeněk Kučera
Tomáš Vondrák
Technologické centrum Praha, CZ

Recenzovaná vědecká stať
Obdrženo redakcí: 19. 1. 2022
Přijato k publikování: 4. 5. 2022

International comparison of publication and patent activity in the field of cybersecurity

Technologies providing for cybersecurity at all levels of both public and private sphere infrastructure became one of the key strategic commodities which are essential for maintaining the functionality, survivability, and resilience of all systemic, economic, and societal structures. The aim of this contribution is to evaluate research and development (R&D) in this field based on the analysis of the world publication and patent activities. The whole world's publication activity in the field of cybersecurity increased almost 17 times since the turn of the millennium and their share in the world output grew almost sixfold. The largest number of publications comes from China, the USA, India, and the United Kingdom, which produced in years 2016 - 2020 approximately half of the world output. In the Czech Republic, the share of the cybersecurity publications in the country's output is approximately on par with the European countries and its dynamics follows the world trend. The world's number of priority patent applications grew since the turn of the millennium more than threefold. The largest increase occurred in China: In years 2016–2020, the Chinese Patent Office (CNIPA) registered more than 60 % and the American patent office (USPTO) registered approximately 14 % of the world's number of priority patent applications. Cybersecurity covers almost 2 % of the world's patent applications. In Europe, Finland, Estonia, Sweden, Ireland, the United Kingdom, and France have the highest share of patent applications in cybernetic security. In the Czech

Martin Faťun
Zdeněk Kučera
Tomáš Vondrák
Technology Centre Prague, CZ

Peer–reviewed scientific paper
Received: 19. 1. 2022
Accepted for publication: 4. 5. 2022

Republic, the share of these patent applications is, on the European scale, slightly above average. However, the number of patent applications grows faster than in the other EU countries. This indicates a significant growth of cybernetic security R&D in the Czech Republic.

Keywords: cybersecurity; patent activity; publication activity

Úvod

Zajištění kybernetické bezpečnosti na úrovni digitální infrastruktury státu, firem a institucí i jednotlivých fyzických osob se v dnešním světě stalo jedním z klíčových předpokladů pro přežití a nezávislý rozvoj všech systémových, ekonomických a společenských struktur. Technologie zajišťující kybernetickou bezpečnost tak představují pro každý stát specifickou strategickou komoditu, která je zárukou vlastní bezpečnosti a která zároveň může být i cenným exportním artiklem, zdrojem mezinárodního vlivu i nezanedbatelných ekonomických příjmů. V našem geopolitickém prostoru si strategický význam výzkumu a vývoje v oblasti kybernetické bezpečnosti uvědomují nejen jednotlivé státy, ale i Evropská unie, která si klade za cíl podpořit společný postup a koordinaci členských států v této oblasti [1]. Mimo jiné na základě nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021 [2] dochází ke vzniku Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost (ECCC) a sítě národních koordinačních center.

Cílem tohoto příspěvku je posoudit výsledky VaV zaměřeného na otázky kybernetické bezpečnosti a zjistit, jak VaV reaguje na rozvíjející se hrozby v oblasti kybernetické bezpečnosti. Cílem je také porovnat výsledky takto zaměřeného VaV v jednotlivých zemích a identifikovat země, které představují lídry ve VaV v oblasti kybernetické bezpečnosti.

Česká republika má na základě svých strategických rozvojových dokumentů, zejména Národní strategie kybernetické bezpečnosti ČR na období let 2021–2025 [3] a Akčního plánu k této strategii [4], s ohledem na existující výzkumné a vývojové kapacity ambice stát se aktivním hráčem na poli výzkumu a inovací v nových technologiích v oblasti kybernetické bezpečnosti. V návaznosti na tento příspěvek je proto záměrem autorů v dalším připravovaném článku detailněji vyhodnotit reálnou pozici ČR ve VaV v oblasti kybernetické bezpečnosti v porovnání se světem a dalšími evropskými státy a analyzovat její předpoklady pro naplnění deklarovaných ambicí.

Metodický přístup

Pro vyhodnocení publikační aktivity byla využita databáze publikací Clarivate Web of Science (WoS) [5]. Do analýzy byly zahrnuty publikace typu Article, Review, Letter a Proceedings paper publikované v časovém intervalu od roku 2000 do roku 2020. Počty publikací byly stanoveny jednotkovou metodou, která nezohledňuje ve společných publikacích počet zemí původu autorů (tj. každé zemi je započtena celá publikace).

Pro vyhodnocení patentové aktivity byla využita světová databáze patentových přihlášek, která byla Evropským patentovým úřadem zveřejněna na podzim roku 2021 (EPO Worldwide Patent Statistical Database – PATSTAT 2021b) [6]. Patentové přihlášky byly sledovány podle roku podání bez ohledu na to, zda byl, či nebyl získán patent. Pro stanovení nejvýznamnějších přihlašovatelů byly využity tzv. harmonizované názvy přihlašovatelů, které jsou pro databázi PATSTAT zpracovávány v rámci projektu OECD (OECD HAN database[1]). Pro stanovení počtu patentových přihlášek byla využita frakční metoda, která zohledňuje počet přihlašovatelů v patentové přihlášce.

Vzhledem k tomu, že u patentových přihlášek podaných u patentových úřadů v Čínské lidové republice (ČLR), Japonsku, Korejské republice a u řady dalších méně významných patentových úřadů nejsou v databázi PATSTAT často uvedeny údaje o zemích a názvech přihlašovatelů, byly pro mezinárodní porovnání využity údaje o patentových přihláškách podaných podle Smlouvy o patentové spolupráci (Patent Cooperation Treaty[2], PCT), u kterých jsou tyto informace většinou uvedeny. Přihlášky podané podle PCT zároveň do značné míry „potlačují“ rozdíly mezi zeměmi, neboť podáním jedné mezinárodní patentové přihlášky mohou jejich přihlašovatelé žádat o ochranu ve více než 150 signatářských zemích této smlouvy. Pro mezinárodní porovnání patentové aktivity členských států EU byly kromě PCT přihlášek využity patentové přihlášky podané u Evropského patentového úřadu (EPO[3]), u nichž jsou též v databázi PASTSTAT dostupné údaje o jejich přihlašovatelích.

Publikace a patentové přihlášky zaměřené na VaV v oblasti kybernetické bezpečnosti byly identifikovány s využitím souboru více než 150 klíčových slov v anglickém jazyce a jejich logických kombinací, které byly vyhledávány v názvech a abstraktech publikací, resp. patentových přihlášek. Klíčová slova vycházela z informací o problematice kybernetické bezpečnosti v odborných časopisech a dalších dokumentech, které charakterizují tuto technologickou oblast. Klíčová slova pokryla významné oblasti kybernetické bezpečnosti, mezi něž patří zejména bezpečnost sítí a síťových komunikací, přenos a ukládání dat a jejich bezpečnost, kryptografie, přístup k sítím a autentizace, kybernetické útoky a ochranu proti těmto útokům, ochrana před škodlivým softwarem a další. Klíčová slova pokryla také problematiku bezpečnosti digitálních nástrojů, produktů a systémů, mezi něž patří například umělá inteligence, internet věcí (IoT), cloudová infrastruktura, blockchain, autonomní dopravní prostředky, chytrá města apod.

Snahou bylo, aby nalezený soubor publikací a patentových přihlášek obsahoval minimální počet „falešných“ záznamů, které nesouvisí s problematikou kybernetické bezpečnosti. Z tohoto důvodu do výběru nebyla zařazena klíčová slova, která v některých případech identifikují záznamy z jiných oblastí (typickým příkladem jsou počítačové viry a viry biologické povahy). Pokud to bylo možné, byla tato problematická klíčová slova kombinována s jinými slovy tak, aby byly z výběru vyloučeny záznamy, které do problematiky kybernetické bezpečnosti nespadají.

Výběr patentových přihlášek nalezených podle klíčových slov byl následně rozšířen o patentové přihlášky nalezené podle jejich oborového zařazení v Mezinárodním patentovém třídění (International Patent Classification[4], IPC). Přehled oborů v IPC třídění, které byly využity pro výběr patentových přihlášek v kybernetické bezpečnosti, je uveden v tabulce 1.

Tabulka 1: Přehled oborů v Mezinárodním patentovém třídění (IPC), které byly využity pro výběr patentových přihlášek v kybernetické bezpečnosti

IPC obor	Popis
G06F 21	Security arrangements for protecting computers, components thereof, programs or data against unauthorised activity
H04L 9	Arrangements for secret or secure communication
H04W 12	Security arrangements, e.g. access security or fraud detection; Authentication, e.g. verifying user identity or authorisation; Protecting privacy or anonymity

Zdroj: TC Praha

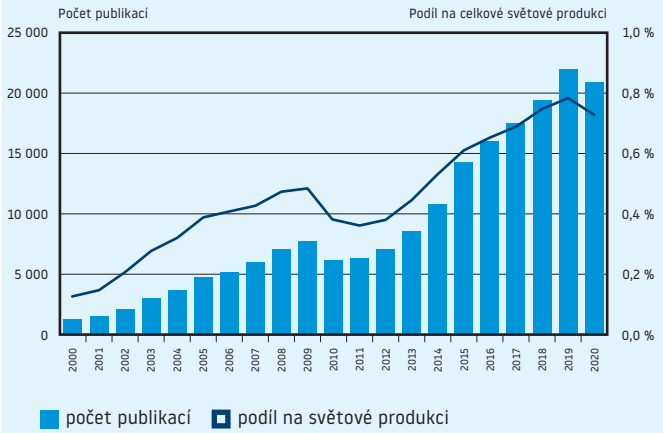
Pro ověření kvality výběru byl vybrán náhodný vzorek sta publikací / patentových přihlášek, u něhož bylo s využitím informací v abstraktech a názvech publikací individuálně posouzeno, zda daná publikace / patentová přihláška skutečně spadá do kybernetické bezpečnosti. Na základě tohoto posouzení lze odhadnout, že výběr publikací / patentových přihlášek obsahuje méně než 10 % „falešných“ záznamů.

Výsledky analýzy

Publikační aktivita

Počet publikací zaměřených na problematiku kybernetické bezpečnosti výrazně roste již od počátku tohoto milénia (viz graf 1). Na vývoji publikační aktivity je patrný pokles počtu publikací po roce 2009, což může být důsledkem hospodářské krize. Po roce 2010 se publikační aktivita opět zvyšuje a od roku 2010 do roku 2020 se počet publikací zaměřených na problematiku kybernetické bezpečnosti více než ztrojnásobil.

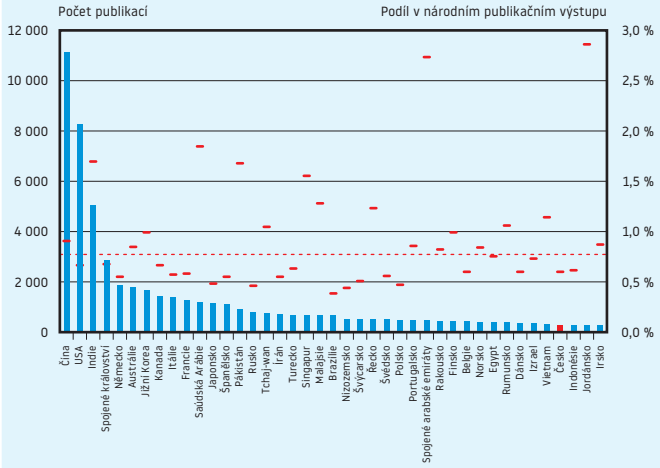
Graf 1: Světový počet publikací v oblasti kybernetické bezpečnosti v letech 2000 až 2020 a jejich podíl v celkovém světovém počtu publikací



Zdroje: WoS, záznamy typu Article, Review, Letter a Proceeedings paper

Výrazně roste také zastoupení tematiky kybernetické bezpečnosti v celkovém počtu publikací (viz graf 1), což ukazuje, že oblast kybernetické bezpečnosti nabývá na významu a výzkumné aktivity se postupně rozšiřují. V grafu je také patrný pokles zastoupení publikací v kybernetické bezpečnosti v celkovém počtu publikací po roce 2009, což potvrzuje, že výzkumné aktivity v oblasti kybernetické bezpečnosti byly v souvislosti s ekonomickou krizí výrazně utlumeny. Od roku 2012 se zastoupení publikací v kybernetické bezpečnosti ve světovém počtu publikací začalo zvyšovat a do roku 2020 se jejich podíl zhruba zdvojnásobil (viz graf 1).

Graf 2: Publikační výstup zemí v letech 2019–2020 v oblasti kybernetické bezpečnosti a jejich podíly na celkových národních publikačních výstupech



Poznámka: Vodorovná linie znázorňuje celosvětový průměr.

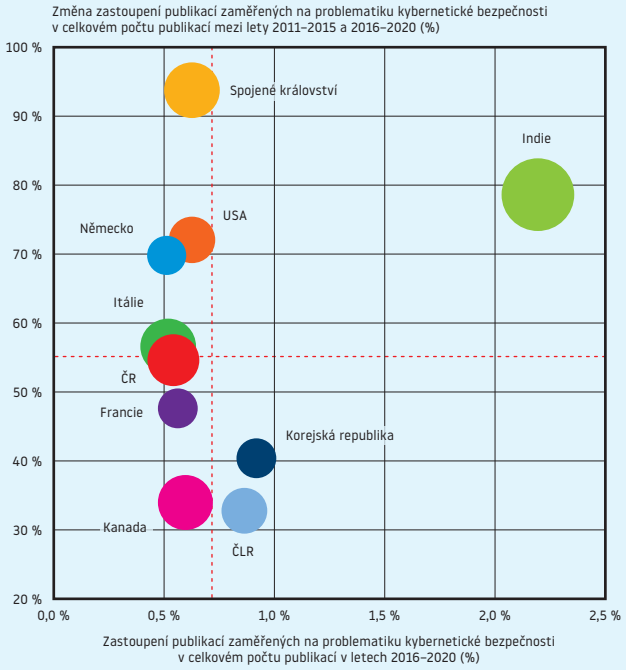
Zdroje: WoS, záznamy typu Article, Review, Letter a Proceedings paper. Uvedené země představují 92 % světového výstupu v oblasti v uvedeném časovém okně.

Jak je patrné z grafu 2, kde je znázorněn počet publikací zaměřených na kybernetickou bezpečnost vytvořených v jednotlivých zemích a jejich zastoupení v národním publikačním výstupu, nejvyšší počet publikací zaměřených na kybernetickou bezpečnost vzniká v Čínské lidové republice (ČLR). Také další velké a výzkumně významné země, jako jsou USA, Indie a Spojené království, se značnou měrou podílejí na celkovém počtu publikací v kybernetické bezpečnosti.

Průměrné zastoupení kybernetické bezpečnosti v celkovém počtu publikací se pohybuje okolo 0,8 %. Nejvyšší podíl takto zaměřených publikací v celkovém publikačním výstupu země je v Jordánsku, Spojených arabských emirátech a Saudské Arábii. Příčinou může být celkový nízký publikační výstup těchto zemí v tradičních VaV oblastech a případně rozvojová pomoc ve formě účasti na výzkumných projektech v rozvinutých zemí. Z výzkumně významných zemí je vysoké zastoupení publikací v kybernetické bezpečnosti v celkovém počtu publikací v Indii (viz graf 2). Celkově mají nadprůměrné zastoupení publikačních výstupů v tomto oboru spíše výzkumně méně intenzivní země. Z evropských zemí je podíl publikačního výstupu výrazněji

nad světovým průměrem v Řecku, Finsku a Rumunsku. Z asijských výzkumně intenzivních zemí je výzkum kybernetické bezpečnosti silně zastoupen na Tchaj-wanu a v Singapuru.

Graf 3: Mezinárodní porovnání publikační aktivity v kybernetické bezpečnosti



Poznámka: Na vodorovné ose je zastoupení publikací zaměřených na problematiku kybernetické bezpečnosti v celkovém počtu publikací v letech 2016–2020, na svislé ose změna zastoupení publikací zaměřených na problematiku kybernetické bezpečnosti v celkovém počtu publikací mezi lety 2011–2015 a 2016–2020. Plocha kruhů odpovídá počtu publikací v oblasti kybernetické bezpečnosti vztažené na počet výzkumných pracovníků země v přepočtu na plný pracovní úvazek (FTE)[5]. Červené přerušované linie představují hodnoty pro světový průměr.

Zdroje: WoS, záznamy typu Article, Review, Letter a Proceedings paper

Porovnání zastoupení publikací zaměřených na kybernetickou bezpečnost v celkovém počtu publikací v pětiletém období 2016–2019 v ČR a ve vybraných zemích s vysokou publikační aktivitou je uvedeno v grafu 3 (vodorovná osa). V grafu je dále porovnána změna zastoupení těchto publikací mezi dvěma pětiletými obdobími 2011–2015 a 2016–2020 (svislá osa) a počet publikací v kybernetické bezpečnosti vztažený na počet výzkumných pracovníků (průměr kruhů). Z grafu je patrné, že nejvyšší podíl publikací zaměřených na problematiku kybernetické bezpečnosti je v Indii. Nadprůměrné zastoupení publikací v kybernetické bezpečnosti v celkovém počtu publikací je také v Korejské republice a ČLR. Nejvyšší nárůst zastoupení publikací v kybernetické bezpečnosti v národním publikačním výstupu je ve Spojeném království, a dále v USA a Německu. Nejvyšší počet publikací se zohledněním velikosti výzkumného systému (počtu výzkumných pracovníků) je v Indii, Itálii, Spojeném království a Kanadě (viz graf 3).

V ČR je zastoupení publikací v kybernetické bezpečnosti v celkovém počtu publikací sice mírně pod světovým průměrem, ale zhruba na úrovni evropských zemí, jako jsou Itálie, Německo či Francie (viz graf 3). Nárůst publikační aktivity v oblasti kybernetické aktivity v ČR odpovídá zhruba světovému průměru. Počet publikací vztažený na počet výzkumníků je v ČR sice nižší než ve Spojeném království či v Itálii, ale vyšší než například v Německu (viz graf 3).

Patentová aktivita

Také počet patentových přihlášek chránících nová řešení v oblasti kybernetické bezpečnosti má od roku 2000 do současnosti vzestupný trend (viz graf 4). Dlouhodobě roste i podíl těchto přihlášek v celkovém počtu patentových přihlášek, což svědčí o tom, že problematika kybernetické bezpečnosti nabývá na významu i z hlediska patentové aktivity. Podobně jako ve vývoji publikační aktivity je i ve vývoji patentové aktivity patrný pokles počtu patentových přihlášek v oblasti kybernetické bezpečnosti i jejich zastoupení v celkovém počtu patentových přihlášek po roce 2008. Po roce 2010 však začíná patentová aktivita v této technologické oblasti opět strmě stoupat (viz graf 4).

Kolem roku 2000 bylo nejvíce prioritních patentových přihlášek podáváno u Japonského patentového úřadu (JPO). Po roce 2006 se však začal počet patentových přihlášek podávaných u JPO snižovat. Počet prioritních patentových přihlášek podávaných u Národního úřadu duševního vlastnictví v ČLR (CNIPA) se naopak zvyšoval, a i přes nárůst počtu patentových přihlášek podaných u USPTO je již od roku 2009 nejvíce prioritních patentových přihlášek v kybernetické bezpečnosti podáváno v ČLR (viz graf 4).

Z grafu 4 je také patrné, že se v průběhu let 2000 až 2020 postupně zvyšoval i počet patentových přihlášek podaných u Korejského úřadu duševního vlastnictví (KIPO), Evropského patentového úřadu a patentových přihlášek podaných podle Smlouvy o patentové spolupráci (PCT). V porovnání s USPTO a zejména CNIPA je podíl těchto patentových úřadů na celkovém počtu prioritních patentových přihlášek v kybernetické bezpečnosti nízký. Podíl ostatních patentových úřadů na celkové patentové aktivitě v kybernetické bezpečnosti je velmi nízký.

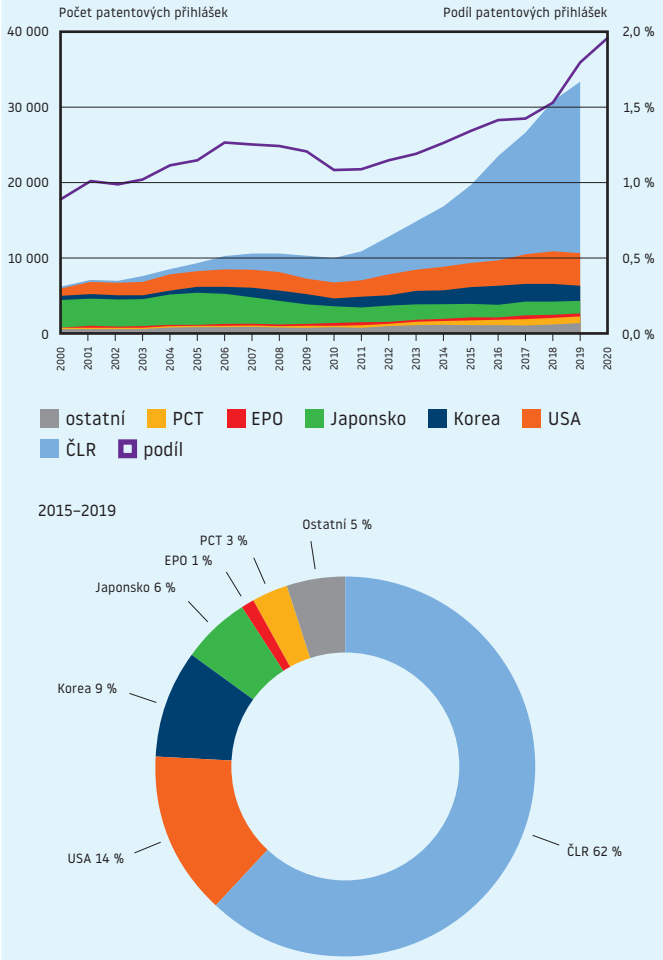
V letech 2015 až 2019 bylo v ČLR podáno více než 60 % z celkového počtu patentových přihlášek chránících nová řešení v oblasti kybernetické bezpečnosti (viz pravá část grafu 4). U patentového úřadu v USA bylo v tomto období podáno přibližně 14 % z celkového počtu prioritních patentových přihlášek. U patentových úřadů v Korejské republice a v Japonsku bylo v tomto období podáno 9 %, resp. 6 % z celkového počtu prioritních patentových přihlášek v kybernetické bezpečnosti, u Evropského patentového úřadu pouze 1 %. V pěti nejvýznamnějších patentových úřadech na světě, které jsou označovány jako IP5 Offices[6], bylo v tomto období podáno více než 90 % z celkového počtu prioritních patentových přihlášek chránících nová řešení v oblasti kybernetické bezpečnosti (viz graf 4).

Pro porovnání počtu patentových přihlášek v oblasti kybernetické bezpečnosti podaných subjekty z různých zemí jsou v další části příspěvku využity patentové přihlášky podané podle Smlouvy o patentové spolupráci (bližší vysvětlení je v metodické části příspěvku). Přibližně třetina z celkového počtu 26 tisíc patentových přihlášek chránících nová řešení v oblasti kybernetické bezpečnosti podaných v letech 2015 až 2019 podle Smlouvy o patentové spolupráci (PCT) byla podána subjekty z USA (viz tabulka 2).

Nejvyšší zastoupení patentových přihlášek zaměřených na kybernetickou bezpečnost v jejich celkovém počtu je v ostrovním státě Antigua a Barbados, který patří mezi daňové ráje. V patento-

vých přihláškách v oblasti kybernetické bezpečnosti však dominuje pouze jedna společnosti – nChain, která poskytuje řešení v oblasti blockchainu.

Graf 4: Vývoj počtu prioritních patentových přihlášek chránících nová řešení v oblasti kybernetické bezpečnosti mezi lety 2000 a 2020 (nahoře) a podíly patentových úřadů na celkovém počtu prioritních patentových přihlášek v oblasti kybernetické bezpečnosti podaných v pětiletém období 2016–2019 (dole)



Poznámka: Patentové přihlášky jsou barevně rozlišeny podle toho, u jakého patentového úřadu byly podány: Patentový a známkový úřad USA (USPTO) – oranžová, Japonský patentový úřad (JPO) – zelená, Korejský úřad duševního vlastnictví (KIPO) – tmavě modrá, Evropský patentový úřad (EPO) – červená, Národní úřad duševního vlastnictví Čínské lidové republiky (CNIPA) – světle modrá, ostatní patentové úřady ve světě – šedá. Žlutou barvou jsou v grafu vyznačeny patentové přihlášky podané podle Smlouvy o patentové spolupráci (PCT). Fialovou čarou je znázorněn podíl patentových přihlášek chránících nová řešení v oblasti kybernetické bezpečnosti v celkovém počtu patentových přihlášek. Údaje z roku 2020 ještě nejsou v databázi PATSTAT úplné.

Zdroje: EPO Worldwide Patent Statistical Database – podzim 2020 (PATSTAT 2021b)

Přehled nejvýznamnějších přihlašovatelů patentových přihlášek podle PCT v letech 2016 až 2020 chránících nová řešení v oblasti kybernetické bezpečnosti je uveden v tabulce 3. Nejvíce takto zaměřených patentových přihlášek podaly společnosti, které jsou výrobci mobilních zařízení, počítačů a elektronických zařízení nebo jejich součástí (resp. součástek) a výrobci softwaru. Nejvýznamnějším přihlašovatelem je korejská společnost Samsung Electronics, která v uvedeném období podala více než 1,6 tis. patentových přihlášek podle PCT (stanoveno frakčně). Dalšími významnými přihlašovateli jsou společnosti Huawei Technologies a Microsoft. Mezi významnými přihlašovateli patentových přihlášek v oblasti kybernetické bezpečnosti jsou i společnosti působící v oblasti elektronického obchodování (Alibaba) a elektronických plateb (VISA).

Tabulka 2: Počet patentových přihlášek podaných podle Smlouvy o patentové spolupráci (PCT) v letech 2016 až 2020 chránících nová řešení v oblasti kybernetické bezpečnosti

Země	Počet patentových přihlášek v kybernetické bezpečnosti	Podíl na celkovém počtu patentových přihlášek v kybernetické bezpečnosti	Zastoupení přihlášek v kybernetické bezpečnosti celkovém počtu patentových přihlášek země
USA	8 497,7	32,6%	3,1%
Čínská lidová republika	6 076,7	23,3%	2,6%
Korejská republika	2 809,1	10,8%	3,5%
Japonsko	2 238,0	8,6%	1,0%
Německo	1 097,5	4,2%	1,2%
Francie	791,4	3,0%	2,1%
Spojené království	765,6	2,9%	2,7%
Švédsko	635,0	2,4%	3,6%
Izrael	351,6	1,3%	3,8%
Kanada	302,1	1,2%	2,5%
Finsko	293,1	1,1%	3,8%
Švýcarsko	275,5	1,1%	1,3%
Singapur	226,6	0,9%	4,9%
Nizozemsko	200,6	0,8%	1,0%
Antigua a Barbados	183,0	0,7%	73,5%
Indie	162,7	0,6%	1,9%
Austrálie	157,4	0,6%	1,8%
Ostatní	1 011,4	3,9%	1,2%
Celkem	**26 075,0**		**2,2%**

Poznámka: Přihlášky jsou rozděleny podle zemí jejich přihlašovatelů. Údaje jsou stanoveny frakčně. V tabulce jsou uvedeny pouze země, které v uvedeném období podaly sto a více patentových přihlášek v kybernetické bezpečnosti (stanoveno frakčně).

Zdroj: EPO Worldwide Patent Statistical Database – podzim 2020 (PATSTAT 2021b)

Tabulka 3: Patentové přihlášky podle Smlouvy o patentové spolupráci (PCT) v kybernetické bezpečnosti podané v letech 2016 až 2020 – nejvýznamnější přihlašovatelé patentových přihlášek

Společnost	Země	Počet patentových přihlášek
SAMSUNG ELECT CO LTD	Korejská republika	1 610,5
HUAWEI TECH CO LTD	ČLR	1 073,4
MICROSOFT TECH LICENSING LLC	USA	858,7
ALIBABA GROUP HOLDING LTD	USA, ČLR	548,8
TELEFON AB LM ERICSSON PUBL	Švédsko	459,0
ZTE CORP	ČLR	454,0
NEC CORP	Japonsko	446,2
QUALCOMM INC	USA	401,7
HEWLETT PACKARD DEV CO LP	USA	359,0
INTEL CORP	USA	352,7
PING AN TECH SHENZHEN CO LTD	ČLR	341,0
SIEMENS AG	Německo	312,3
VISA INT SERVICE ASSOCIATION	USA	269,1
NOKIA CORP	Finsko	261,9
GOOGLE INC	USA	260,3
SONY CORP	Japonsko	259,3
GUANGDONG OPPO MOBILE TELECOM CORP LTD	ČLR	251,5
NIPPON TELEGRAPH & TELEPHONE CORP	Japonsko	251,0
MITSUBISHI ELECT CORP	Japonsko	211,5

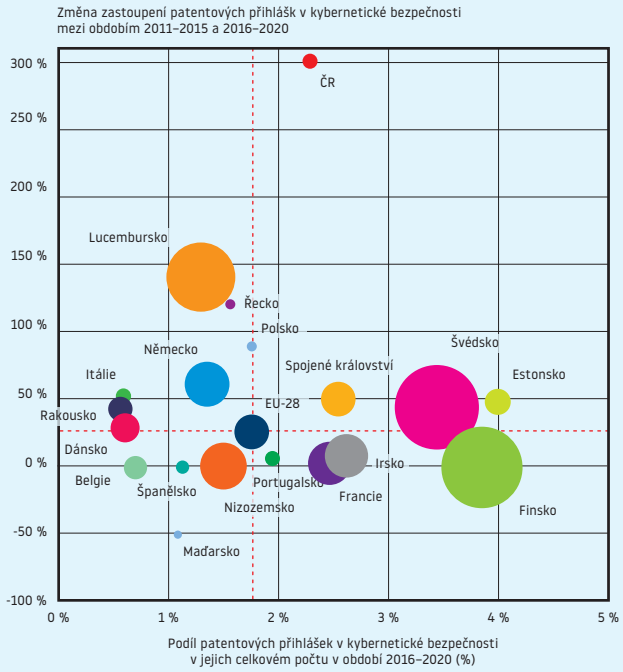
Poznámka: Počty přihlášek jsou stanoveny frakční metodou. V tabulce jsou uvedeny pouze subjekty, které v uvedeném období podaly více než dvě stě patentových přihlášek v kybernetické bezpečnosti podle PCT.
Zdroj: EPO Worldwide Patent Statistical Database – podzim 2020 (PATSTAT 2021b)

Vysoký počet patentových přihlášek podle PCT má také přihlašovatele z dalších technologicky významných asijských zemí – z ČLR (přibližně 23 % z celkového počtu přihlášek v kybernetické bezpečnosti podle PCT) a Korejské republiky (přibližně 11 % patentových přihlášek). Necelých 9 % z celkového počtu patentových přihlášek v oblasti kybernetické bezpečnosti podaných podle PCT v letech 2016–2020 má přihlašovatele z Japonska. Z členských států EU má nejvíce patentových přihlášek podle PCT v kybernetické bezpečnosti přihlašovatele z Německa, Francie a Švédska. Vysoký počet přihlášek v kybernetické bezpečnosti podaly také subjekty ze Spojeného království (viz tabulka 2).

Zastoupení patentových přihlášek v kybernetické bezpečnosti v celkovém počtu patentových přihlášek podle PCT se pohybuje mírně nad dvěma procenty (viz tabulka 2). V zemích s nejvyšším počtem patentových přihlášek v kybernetické bezpečnosti (USA, ČLR a Korejská republika) je zastoupení patentových přihlášek v kybernetické bezpečnosti vyšší a pohybuje se na úrovni cca 3 %. V členských státech EU s nejvyšším počtem přihlášek (Francie a Německo) je zastoupení kybernetické bezpečnosti v celkovém počtu přihlášek ve světovém srovnání podprůměrné. Nadprůměrné je naopak v severských zemích, jako jsou Švédsko a Finsko.

Porovnání počtu patentových přihlášek chránících nová řešení v oblasti kybernetické bezpečnosti podaných členskými státy EU (včetně Spojeného království) podle Smlouvy o patentové spolupráci (PCT) a u Evropského patentového úřadu (EPO) je v grafu 5. V letech 2016 až 2020 bylo přihlašovateli z členských států podáno u EPO a podle PCT více než osm tisíc patentových přihlášek v kybernetické bezpečnosti, což je přibližně 1,7 % z celkového počtu patentových přihlášek v oblasti kybernetické bezpečnosti. Se zohledněním počtu obyvatel země bylo nejvíce těchto přihlášek podáno subjekty ze Švédska a Finska (viz graf 5, kde plocha kruhu znázorňuje počet patentových přihlášek v kybernetické bezpečnosti vztažený na počet obyvatel země).

Graf 5: Porovnání patentové aktivity členských států EU-28 (včetně Spojeného království) v kybernetické bezpečnosti



Poznámka: Zastoupení kybernetické bezpečnosti v celkovém počtu patentových přihlášek podaných přihlašovateli z jednotlivých členských států EU u EPO a podle PCT v letech 2016–2020 (vodorovná osa) a procentuální změna podílu patentových přihlášek v kybernetické bezpečnosti v celkovém počtu patentových přihlášek podaných u EPO a podle PCT mezi dvěma pětiletými obdobími 2011–2015 a 2016–2020 (svislá osa). Plocha kruhu je úměrná počtu patentových přihlášek v kybernetické bezpečnosti s přihlašovatelem z dané země vztažených na 1 mil. obyvatel této země (resp. EU-28). V grafu jsou pouze země, kde bylo v období 2015–2020 podáno přihlašovateli z těchto zemí více než deset patentových přihlášek v kybernetické bezpečnosti. Údaje byly stanoveny frakční metodou.
Zdroje: EPO Worldwide Patent Statistical Database – podzim 2020 (PATSTAT 2020b)

Vysoký počet přihlášek v kybernetické bezpečnosti vztažený na počet obyvatel země byl také podán v Lucembursku, kde má zřejmě sídlo řada přihlašovatelů patentů v této technologické oblasti. Z grafu 5 je také patrné, že ve většině původních členských států EU (EU-15) je počet patentových přihlášek se zohledněním velikosti země výrazně vyšší než nových členských státech EU.

Nejvyšší zastoupení patentových přihlášek v oblasti kybernetické bezpečnosti v celkovém počtu patentových přihlášek je v severských státech – ve Švédsku, Finsku a v Estonsku. V zemích, jako jsou například Německo, Rakousko, Itálie, Belgie a Dánsko, je zastoupení takto zaměřených přihlášek nižší.

V ČR byl v letech 2016–2020 podíl patentových přihlášek v kybernetické bezpečnosti v jejich celkovém počtu přibližně 2,3 %, což je mírně nad průměrem EU-28. Jejich absolutní počet je však velmi nízký – subjekty z ČR v tomto období podaly pouze necelých čtyřicet patentových přihlášek v oblasti kybernetické bezpečnosti (počítáno frakčně). V přepočtu na 1 mil. obyvatel je jejich počet v porovnání s průměrem EU-28 přibližně pětinový (viz graf 5).

Počet patentových přihlášek v kybernetické bezpečnosti se mezi obdobími 2011–2015 a 2016–2020 v průměru EU-28 zvýšil přibližně o čtvrtinu (viz graf 5, svislá osa). Ve většině zemí s vysokým počtem patentových přihlášek v kybernetické bezpečnosti, jako je například Švédsko, Německo, Francie či Spojené království, se podíl patentových přihlášek příliš neměnil, resp. jeho změna odpovídala průměru EU-28. V ČR se však počet patentových přihlášek podle PCT a u EPO v kybernetické bezpečnosti mezi obdobími 2011–2015 a 2016–2020 zhruba ztrojnásobil, což je nejvíce ze všech členských států EU-28 (viz graf 5). To svědčí o rostoucím potenciálu aplikovaného VaV v oblasti kybernetické bezpečnosti a stále intenzivnějším využívání jeho výsledků v aplikacích, které jsou patentově chráněny.

Shrnutí a diskuse

Cílem příspěvku bylo vyhodnotit vývoj publikační a patentové aktivity v oblasti kybernetické bezpečnosti a identifikovat země, které jsou výzkumnými lídry v této technologické oblasti. Zároveň bylo posouzeno, jakou pozici má ČR ve VaV zaměřeném na oblast kybernetické bezpečnosti v porovnání s ostatními členskými státy EU. Pro analýzu byly využity bibliometrické údaje o vědeckých publikacích uvedené v databázi Web of Science a údaje o patentových přihláškách v databázi PATSTAT Evropského patentového úřadu.

Z analýzy publikační a patentové aktivity vyplynulo, že výzkumné aktivity v oblasti kybernetické bezpečnosti se v posledních dvaceti letech postupně zvyšují. Po mírném poklesu po roce 2009, zřejmě v souvislosti s globální ekonomickou krizí, se počet publikací i patentových přihlášek začal opět zvyšovat. Výrazný nárůst počtu publikací i patentových přihlášek svědčí o tom, že VaV se stále více orientuje na řešení otázek kybernetické bezpečnosti. Tento nárůst zřejmě souvisí s dynamickým rozvojem digitálních a komunikačních technologií a jejich využíváním v širokém spektru aplikací, který je zároveň doprovázen negativními jevy, jako jsou nárůst kybernetické kriminality a zvyšující se hrozby v oblasti kybernetické bezpečnosti.

V publikační aktivitě dominují velké země jako Čínská lidová republika (ČLR), USA a Indie. Z evropských zemí se na celkovém počtu publikací s tematikou kybernetické bezpečnosti nejvíce podílí Spojené království. Na problematiku kybernetické bezpečnosti je v průměru zaměřeno necelé jedno procento všech publikací. Ze zemí, které se na počtu takto zaměřených publikací podílejí nejvíce, je nadprůměrné zastoupení publikací v kybernetické bezpečnosti, a tedy i orientace VaV na tuto oblast, v Indii, ČLR a Korejské republice. ČR se jako malá země na celkovém počtu publikací v kybernetické bezpečnosti významně nepodílí. Rovněž zastoupení těchto publikací v národním publikačním výstupu je v ČR ve světovém srovnání podprůměrné. Počet publikací v kybernetické bezpečnosti se však v ČR postupně zvyšuje, přičemž jejich nárůst se od jiných evropských zemí příliš neliší.

Podobná situace je i v patentové aktivitě. Nejvíce patentových přihlášek je podáváno u patentového úřadu v ČLR, kde bylo v letech 2015 až 2019 podáno více než 60 % z celkového počtu prioritních patentových přihlášek v oblasti kybernetické bezpečnosti. Vysoký počet patentových přihlášek chránících nová řešení v oblasti kybernetické bezpečnosti je také podáván v USA, které se podílejí na celkovém počtu prioritních patentových přihlášek v oblasti kybernetické bezpečnosti přibližně ze 14 %. V Korejské republice a Japonsku bylo podáno 9 %, resp. 6 % z celkového počtu prioritních patentových přihlášek v kybernetické bezpečnosti. V asijských zemích a USA mají také sídlo nejvýznamnější přihlašovatelé patentů z podnikového sektoru. Evropské země v patentové aktivitě za USA a asijskými zeměmi poněkud zaostávají. U Evropského patentového úřadu byla v období 2015–2019 podána pouze 3 % z celkového počtu prioritních patentových přihlášek v kybernetické bezpečnosti, což je výrazně méně, než v asijských zemích.

Z mezinárodního porovnání počtu patentových přihlášek podaných v letech 2016–2020 u EPO a podle PCT subjekty z EU vyplývá, že se zohledněním velikosti země je nejvyšší počet patentových přihlášek v kybernetické bezpečnosti podáván ve Švédsku a Finsku. V těchto zemích je také zastoupení patentových přihlášek v kybernetické bezpečnosti v evropském porovnání nadprůměrné. Nadprůměrné zastoupení patentových přihlášek v oblasti kybernetické bezpečnosti v celkovém počtu patentových přihlášek je i v některých dalších zemích, jako jsou Estonsko, Irsko, Spojené království a Francie. Naopak v zemích s vysokým podílem průmyslu na tvorbě HDP, jako jsou například Německo a Itálie, je zastoupení patentových přihlášek v kybernetické bezpečnosti v evropském měřítku podprůměrné. To zřejmě souvisí s tím, že v těchto zemích jsou více chráněna řešení v oblasti průmyslových technologií. Zastoupení kybernetické bezpečnosti v celkovém počtu patentových přihlášek u EPO a podle PCT se v EU mezi obdobími 2011–2015 a 2016–2020 zvýšilo přibližně o čtvrtinu.

V ČR je sice podíl patentových přihlášek v kybernetické bezpečnosti v jejich celkovém počtu mírně nad průměrem EU, ale jejich počet vztažený na velikost země je v evropském srovnání podprůměrný. Počet patentových přihlášek z oblasti kybernetické bezpečnosti však narůstá daleko rychleji než v jiných zemích EU, což společně se zvyšující se publikační aktivitou svědčí o výrazném rozvoji VaV aktivit v oblasti kybernetické bezpečnosti v ČR. V návaznosti na tento příspěvek je proto záměrem autorů v dalším připravovaném článku detailněji analyzovat VaV v ČR v oblasti kybernetické bezpečnosti, kde bude mj. vyhodnocena veřejná podpora VaV zaměřeného na problematiku kybernetické bezpečnosti, výsledky podpořených projektů i zapojení ČR do mezinárodních výzkumných projektů.

Odkazy

[1] European Commission (2020): Joint communication to the European Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade.
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN

[2] The European Parliament and the Council of the European Union (2021): Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. *https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32021R0887*

[3] NÚKIB (2020): Národní strategie kybernetické bezpečnosti České republiky na období let 2021–2025. *https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/strategie-akcni-plan/*

[4] NÚKIB (2021): Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021–2025. *https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/strategie-akcni-plan/*

[5] Web of Science, Clarivate Analytics. *https://clarivate.com/webofsciencegroup/solutions/web-of-science/*

[6] EPO Worldwide Patent Statistical Database (PATSTAT). *https://www.epo.org/searching-for-patents/business/patstat.html*

---

[1] OECD, Intellectual property (IP) statistics and analysis, *https://www.oecd.org/sti/inno/intellectual-property-statistics-and-analysis.htm*

[2] The Patent Cooperation Treaty (PCT), *https://www.wipo.int/pct/en/*

[3] European Patent Office (EPO), *https://www.epo.org/*

[4] International Patent Classification (IPC), *https://www.wipo.int/classifications/ipc/en/*

[5] S výjimkou Indie, kde není z dostupných dat jasné, zda se jedná o FTE nebo počet fyzických osob.

[6] Evropský patentový úřad, Patentový a známkový úřad USA, Japonský patentový úřad, Korejský úřad duševního vlastnictví, Národní úřad duševního vlastnictví Čínské lidové republiky (*https://www.fiveipoffices.org/home*)

Ergo 2023, 18, 1, 9–15
10.5281/zenodo.8111043

COVID-19 pandemic boost to digitisation of the Czech society

The research focused on four digital technology areas (digitisation of common citizens' lives, telemedicine, digitalised education and additive production) for which the pandemic COVID-19 opened a window of opportunity. The objective of the research was to assess if the temporal dominance of the digital technologies changed the attitudes of the citizens and norms and institutions of the society towards their further expansion when the pandemic restrictive measures phase out.

In the analysis, we explored the actors' COVID-19 pandemic experience and investigated the resulting changes in the sociotechnical landscape. The followed foresight assumed that these changes would determine the extent and speed of the diffusion of the selected technologies in the future.

Generally, it is expected that digital technologies will temporarily step down from their sociotechnical dominance as a counter-reaction to their rather involuntary use during the pandemic restrictions. However, gradually they will develop in hybrid systems, keeping some features of the current systems, while a vast majority of operations will be carried out electronically. Digital technologies will save time and costs, and enhance the quality of goods and services tailored to the customer's character. Technological optimism dominated in expert panels and workshops while only a narrow range of risks were emphasized: loss of closer social contacts and loss of necessary habits, discipline and motivation in education, home office or even in telemedicine, physical and mental health risk and digital divide.

We provide two sorts of policy recommendations: the first one follows the instrumental perspective where the policy should (a) concentrate on mitigating digital divide and (b) regulate negative impacts and risks. The second one reflects the common perception of digital technologies as "necessary evil" to survive. It is mainly because users were little involved in their development. To address it, the government should promote transdisciplinary research and co-creation.

Tomáš Ratinger[1]
Iva Vančurová[1]
Ondřej Pecha[1]
Lenka Hebáková[1]
Lukáš Zagata[2]
Jiří Hrabák[2]

[1] Technology Centre Prague, CZ
[2] Czech University of Life Sciences, Prague, CZ

Peer–reviewed scientific paper
Received: 1. 3. 2023
Accepted for publication: 24. 5. 2023

Keywords: digital technologies; telemedicine; education; additive production; sociotechnical regime and landscape; foresight; COVID-19 pandemic
JEL Classification: O31, O32, R00, A13

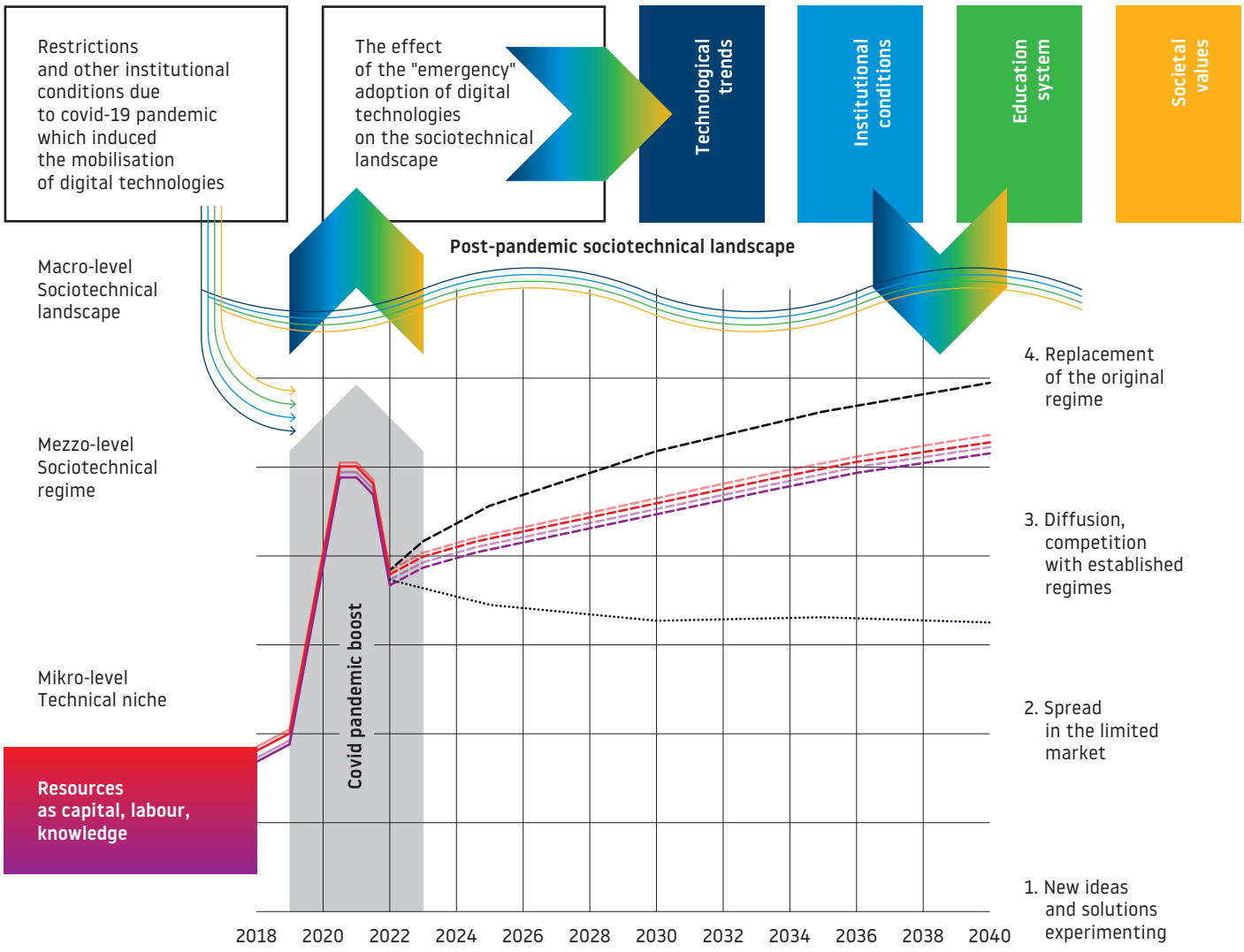
Introduction

In the projects 4TECH of the Programme ETA of the Technology Agency of the Czech Republic (TA CR, 8/2020 – 7/2022) and STRATIN + (MEYS, 2021 – 2024) we focused on four technologies or technological systems (digiti-sation of citizens' lives, telemedicine, digital forms of distant education and additive production) for which the pandemic COVID-19 opened a window of opportunity due to restrictions on personal contacts. The ultimate objective of the research was to assess if the temporal dominance of the digital technologies changed the attitudes of the citizens and norms and institutions of the society towards further expansion of these technologies even when the pandemic restrictive measures would be phased out.

Approach

To capture the complexity and dynamics of the diffusion of digital technologies in business and everyday life of citizens we use the multilevel innovation concept (Geels, 2002 and Geels, 2006) in which the new technology applies first only in limited market/space (micro-level), gradually spreads and competes with other technological regimes at the mezzo-level, and eventually establishes in the sociotechnical landscape (macro-level) see Figure 1. We aim at changes in four areas of the sociotechnical landscape (technological trends, institutional conditions, learning processes / educational system and societal values – see the top part of Figure 1. In the analytical part of the project, we first explored secondary sources referring to the use of selected technol-

Figure 1: Multilevel innovation concept



Source: Own concept based on Geels (2002), Geels (2006)

ogies during the COVID-19 pandemic crisis (Work Package /WP1) and then we collected the experience and opinions of actors providing services with these technologies (WP2). In the third work package, we carried out a survey among the households – the final customers of digital services. The sec-ondary sources included various statistics of the Czech Statistical Office and professional organisations as well as scientific literature. They constituted the knowledge base upon which we identified information gaps and designed the questionnaires for the interviews with stakeholders; the number of interviews and characterisation of experts are presented in Table 1. Both WP1 and WP2 fed the design of the household survey in WP3; semi-random quota sampling with 1518 respondents for more details see Table 2.

These three work packages enabled us to understand the resulting changes in the above mentioned four areas of the sociotechnical landscape, i.e. in norms, institutions and actors' positions in the sociotechnical landscape (showed in the top part of Figure 1). Then we carried out foresight assuming that these changes would determine the extent and speed of the diffusion of the selected technologies in the future (up to 2040). In the foresight, we worked with four technological expert panels (general digitisation, telemedicine, digitalised education and distributed additive production) and we organised three interactive workshops with stakeholders and experts. The workshops were adhered to the two project dissemination conferences and one international scientific conference and thus the participants recruited from the respective conference audience. The panels included 4 to 8 experts; the experts were selected from the list of stakeholders (representatives of these stakeholders) gathered in the first two work packages. The national (online) workshops attracted more than 10 participants thus we split the participants into two groups of up to 6 experts and stakeholders in order to facilitate better discussion on scenarios. We used Miro online white boards to easy communication among experts and stakeholders. It helped to visualise interactions among various factors determining the future diffusion of the selected technologies.

The foresight exercise was organised in three steps (Summary report 4, 2022). First, the experts identified critical conditions and drivers of the diffusion of the digital technologies in question. Second, they depicted the future in two scenarios - a Proscenario (optimistic),

when most of the critical conditions develop in favour of the diffusion), and a Sceptical one (assuming some substantial barriers to the technology adoption). The second step comprised the description of the effects on the life of firms and citizens, and geographical and social differentiations of these effects too. Finally, we conducted workshops with the stakeholders and experts to verify the outlined futures and to identify the need for public policy interventions.

Table 1: Number of interviews and characterisation of experts. In case studies (thematic areas, technologies) in WP2

No.	Case study	Number of interviews	Characteristics of experts / stake-holders
1	Digitisation	6	Representatives of service providers (digital infrastructure, e-commerce, e-government, artists, dramaturgs etc.)
2	Additive production	4	Researchers/academia and entrepreneurs in additive production
3	Telemedicine	6	Doctors, telemedicine promoters
4	Online education	6	Teachers and representatives of their associations

Source: Own description

Table 2: Characteristics of the household (final consumer) survey sample (HWP3)

Age	18–25 (9.7 %) 26–35 (17.5 %) 36–45 (21.3 %) 46–55 (19.2 %) 56–65 (16.3 %) 66–75 (15.8 %)
Gender	Male (50.0 %) Female (50.0 %)
Education	Basic (7.3 %) Secondary without A level (31.7 %) Secondary with A level (38,2 %) Tertiary (22.8 %)
Regional class (Perlín et al, 2019)	Developed (45,7 %) Socially disadvantaged (13.4 %) Socially and geographically disadvantaged (14.4 %) Geographically disadvantaged (13.4 %) Other (13.2 %)

Source: Own description

Research results

Analysis

The results of the analytical part can be summarised in five blocks: 1) Technical capacities of providers and consumers of digitised services; 2) Learning and change of stakeholders' attitudes; 3) Institutions and the respective mechanism governing the adoption of digital technologies; 4) Overcoming the disadvantages of the rural areas and digital divide (see Summary Report 2, 2021). In this part we combine information from secondary and primary (interviews with actors and household survey) sources and draw conclusions on the processes and changes determining diffusion of the selected technologies

Technical capacities

The pandemic showed to the actors that their seemingly good digital capacities and infrastructure might be insufficient to cope with the challenges of the extensive demand for digitised (contactless) services. The most dramatic jump in the digital world happened in the education system neither grammar and secondary schools nor universities were used and equipped for online teaching in sufficient extent. In spite of the rapid expansion of e-commerce already before the pandemic, most of the large retailers like IKEA were not technically prepared for the transition to almost exclusive online shopping. However, the lack of technical equipment limited the use of these services only in the first wave of the COVID-19 pandemic, the actors invested in the technologies and improved their technical capacities very quickly (before the autumn wave in 2020) as it resulted from the interviews with stakeholders.

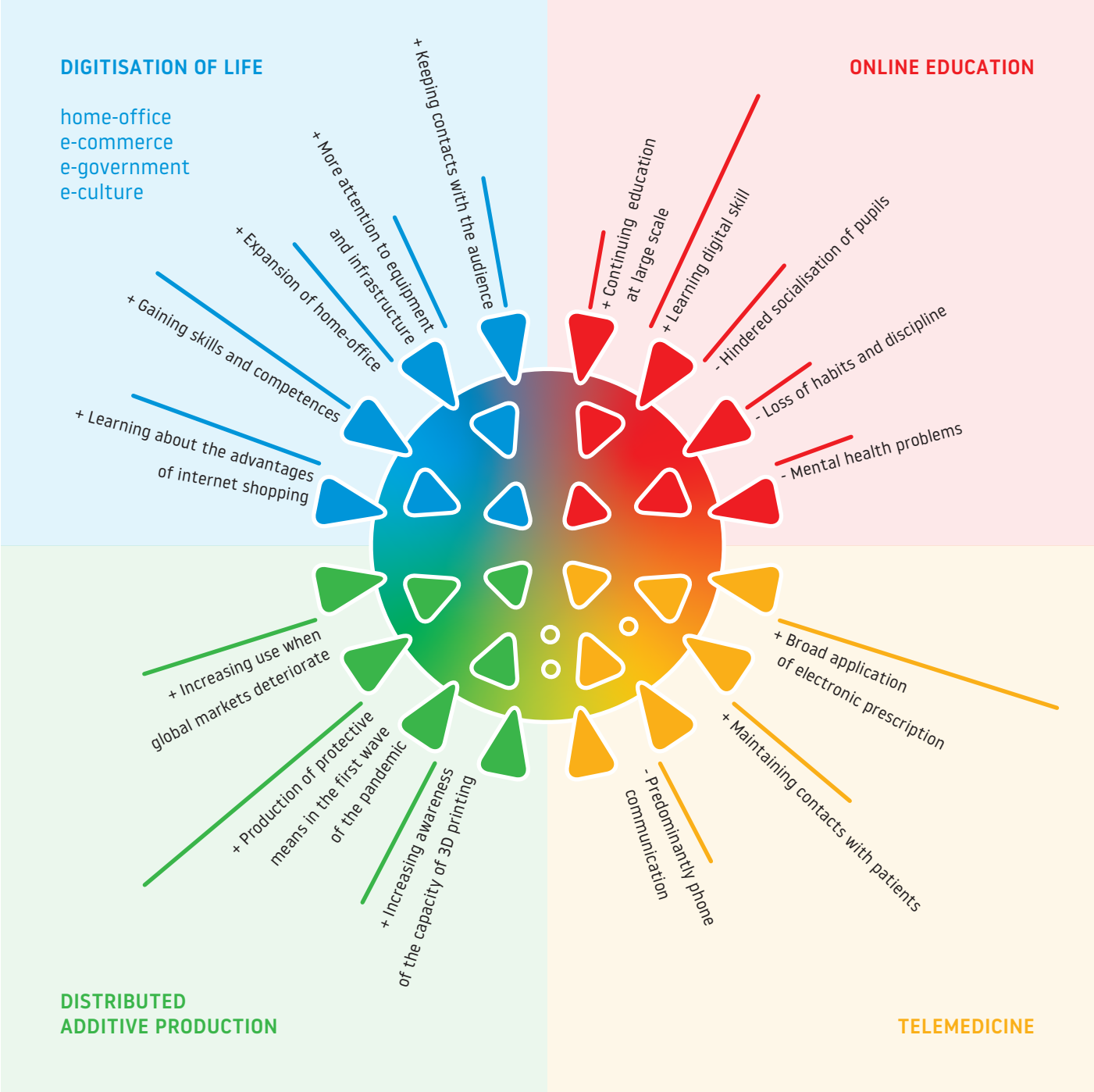
Learning and change of stakeholders' attitudes

The sudden (emergency) transfer into the online space required rapid and intensive learning to acquire the necessary digital skills and to understand functioning of the digitalised society. A great deal of improvisation featured this trans-fer particularly in the first wave of the pandemic. It was learning by doing, resulting eventually in actors' enhancement of knowledge, and shifts in lifestyle and values. According to the experts, these shifts are likely irreversible (WP2 – Summary Report 2, 2021), despite common declarations of the project survey respondents that households would like to limit digitalised services in the future (WP3 - Summary Report 3, 2023). The survey also showed considerable digi-tal competences (at the scale proposed in Van Deursen et al., 2014) of households concerning the use of ICT, social networks and information sources. Undoubtedly, the length of lockdowns contributed to breaking mental blocks and changing actors' attitudes. Two years of tough restrictions on social contacts gave time to all actors to understand new possibilities of digital technologies, test them and verify their benefits. Coping with challenges of the pandemic emer-gency required mobilisation of many skills and resources, and openness to new approaches and solutions. On the other hand, a number of actors feel to be forced to change their attitudes and habits, and thus a counterreaction (a temporary refusal of the digital technology use) can be expected.

Institutions and the respective governance mechanism

The adopted innovation concept (Figure 1) assumes that new technology converts in the sociotechnical regime only under favourable institutional conditions. The interviews with experts and key stakeholders indicated that such a change of institutions had happened since the outbreak of the COVID-19 pandemic or it at least triggered a debate on needed changes of legislation, norms and other rules. The legal right on capacity internet connection can be mentioned as an example. The progress was made by accepting the wellestablished bank identity as suitable identity verification for e-government services. Moving teaching from classrooms to online conferences raised question as if such education is still compulsory. It is important to stress that online education changed the distribution of responsibilities between the school and parents. In spite of the fact that online education was well managed (given the circumstances) and had grad-ually improved, the quality varied among schools, which turned attention to the need for standards and guidelines. The Act on Healthcare Electronisation (2021) provided an important legal framework for the development of telemed-

Figure 2: The adoption of the technologies during the COVID-19 pandemic critical period 2020–2021



Source: Own illustration based on Summary Report 4 (2022)

icine, but most of the institutional challenges including the rights for telemedicine care and its financial coverage will need to be resolved in the future.

One of the most critical institutional challenge is finding the balance between extensive digitisation of the services and prevention of the exclusion of those who have reservation or lack of financial resources, capacities and skills to manage electronic means and digital applications. The technical digital divide occurred mainly in the first wave of the COVID-19 pandemic in spring 2020. The public administration intervention and the assistance provided by civil society organisations reduced it substantially. The most serious problem arose in the area of the application of the technical means. It appeared that some groups of citizens had difficulty to cope with new settings given by extensive use digital technolo-gies in order to bridge pandemic restrictions. In contrast, it created new opportunities for some social groups and indi-viduals. The socially conditioned digital divide is an important phenomenon, which needs to be explored more (see also Beaunoyer et al., 2020).

Overcoming the disadvantages of the rural areas and digital divide

The interviews with stakeholders (Summary Report 2, 2021) showed that the investigated technologies had and would have capacity to moderate disadvantages of some rural regions - particularly significantly rural regions according to the OECD classification (OECD, 2011) and to integrate them more with urban areas. Pandemic of COVID-19 boosted home office, otherwise very limitedly used in the Czech Republic before (Grossmann et al., 2021). The (temporary) migration from metropolitan to rural areas appeared in regions with good internet connection. On the other hand, digitisation might not help (or bring only marginal benefits) in remote regions since low density of customers limits the private sector to provide services (high speed internet connection, delivery of online purchased products, etc.) at acceptable price. The problems might then allocate to otherwise weak social group in the "digitally" disadvantaged regions. We can call it sociogeographically conditioned digital divide. In contrast, geographical differentiation (based on the typology given by Perlín et al, 2019) of opinions and attitudes was not confirmed as statistically significant in the household survey (WP3 -Summary report 3, 2022) It has probably two reasons:

- It was an online survey, thus those completely excluded were missing in the sample.
- In the typology itself which does not reflect important parameters relevant to digitisation.

There are significant differences in the extent and ways of the adoption of the investigated technologies during the most critical period (spring 2020 – spring 2022) of the COVID-19 pandemic in the Czech Republic. These are illustrated in Figure 2. While online education and online shopping (in some segments) completely replaced the conventional technology, digital means in culture, public administration or medicine aimed primarily at keeping contacts and providing information.

Most of the "telemedicine" consultations happened on phone, since there were no specific telemedicine platforms avail-able and the both parties (i.e. doctors and patients) were not used to apply available conference systems efficiently. On the other hand, the electronic prescription, electronic registration and digital vaccination certificates were used extensively.

There is a specific story of additive production. It demonstrated convincingly the advantages of flexible distributive production in the time of the critical shortage of protective means. Although it was later replaced by cheaper mass production (plastic injection), additive production attracted attention of industry. With disruptions in the global market following the COVID-19 pandemic, 3D print has become deployed still more in the production of various spare parts or components, which are used in low numbers.

Foresight (WP4)

The critical conditions on which builds the foresight exercise mirror to large extent the above mentioned analytical findings. They comprise: (i) Technical conditions including the development of digital instruments for the interactions among actors or the control of processes as well as their availability for actors; (ii) Institutional conditions which de-termine anchoring the technical advances in the sociotechnical landscape: in legislation and technical and societal norms. (iii) Financial conditions which determine the use of digital instruments (it might be particularly important for the diffusion / use of telemedicine); (iv) A specific issue is to secure skilled ICT professional in the public sector; (v) Symbolic recognition of the digital technologies (like online education, telemedicine or digital culture) to be equivalent alternatives to the established systems were stressed especially by educational experts. The importance of these critical conditions for the diffusion of the investigated technologies is shown in Table 3.

Generally, it is assumed that digital technologies will step down temporarily from their sociotechnical dominance as a counterreaction to their rather involuntary use during the COVID-19 pandemic restric-

Table 3: Critical conditions

	Digitisation	Telemedicine	Digitalised education	Additive pro-duction
Critical internal factors	**x**	**xx**	**xx**	**x**
Available technical equipment	x	xx	x	xx
Development and availability of hardware	x	xx	xx	x
Training and education of actors	xx	xx	xx	xx
Specific legislation	x	xx	xx	x
Setting up standards and norms	x	xx	xx	xx
Convenient financial conditions	x	xx	x	x
Critical external factors	**x**	**xx**	**xx**	**x**
General progress in hardware and software	x	xx	xx	xx
Digital technology oriented education	x	xx	xx	xx
Suitable general legal framework	xx	x	x	x
Favourable conditions for IT specialists in public administration	xx	x	xx	
Symbolic recognition of the technology		xx	xx	x

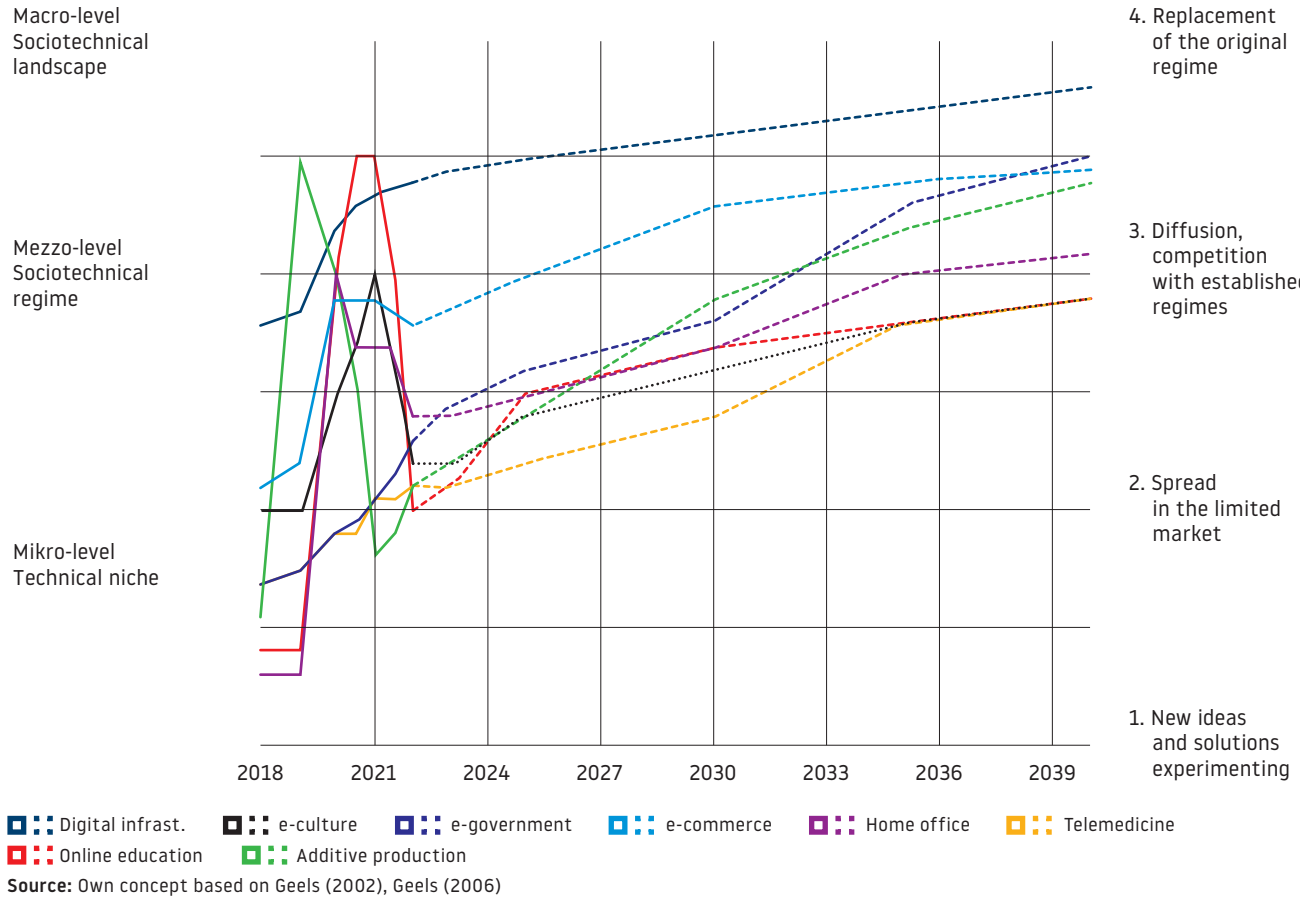
Source: Own illustration based on Summary Report 4 (2022)

tions. However, gradually the studied technologies develop in hybrid systems, which will still keep some features of the current (conventional) systems, while a vast number of operations will be carried out electronically. Experts stressed that digital technologies would save time and costs, and when integrated with Artificial Intelligence (AI) would also enhance the quality of services and goods and would tailor them to the character of customers. Technological optimism of the Proscenario dominated in expert panels and workshops. It would confirm that the society / sociotechnical landscape absorbed a lot from the pandemic digital experience.

issue). Physical and mental health risks were emphasized too, but in smaller extent in contrast to Varanauskas (2022) – who paid strong attention to these issues.

The technological optimism built on the assumption that digitation allows almost unlimited collection and processing of measurable data which will help improve diagnoses, estimate human behaviour and control processes/ treatments better than humans with limited capacities, and thus reduce uncertainty. Only few experts warned that absence of un-measurable information like emotions or trust in digital communication might in contrast increase the uncertainty and

Figure 3: Illustration of experts' projections of the diffusion of the investigated digital technologies



Source: Own concept based on Geels (2002), Geels (2006)

Conclusions and policy implications

Rather a narrow range of risks appeared in expert panels or in foresight workshops. First, it was a loss of closer social contacts due to digital technologies which might eventually lead to the problem of socialisation of certain social groups (e.g. pupils - similarly reported by Varanauskas (2022), or old people). Further, there was mentioned a loss of necessary habits, discipline and motivation in education as stressed by Sotoudeh (2022) for Austria, in home office work (see Grossmann et al. 2022) or even on the side of patients in telemedicine. The entire digitisation of private and public services will threaten disadvantaged social groups which members have no means, capacity or will to acquire necessary skills and knowledge (digital divide this might even amplify with larger adoption of artificial intelligence applications. Teacher or doctor thus might lose some important views on the subject of the treatment and the client the responsibility. In the effect, the education process or treatment might deteriorate. It will be very relevant to follow the experience from psychotherapy and psychological counselling where online sessions are rather common (Weinberg, Rolnick, 2019).

Two sorts of policy recommendations are provided to reflect research results: the first set of recommendations reflects technological optimism, thus determinism in which technologies are perceived as instruments for resolving problems (De Hond, Moser, 2022). That

what actually happened in the period of COVID-19 pandemic. From the instrumental perspective, the policy should (a) concentrate on mitigating digital divide by supporting purchase of the technology, training and advisory for individuals and small firms (in the accord with Beaunoyer et al. (2020); and (b) regulate nega-tive impacts and risks of digitisation, particularly, concerning privacy and security. The second set of recommendations refers to the fact that the technologies in the question attracted a rather limited part of the population while for the rest they were "necessary evil" to survive as it resulted from the household survey that respondents would like to limit use of digital instruments in the future. It is to large extent because users were little involved in the development of these technological systems. Thus, the government might consider addressing this problem by supporting transdisciplinary research and co-creation (Bijker, 1994). Institutionalisation of technology assessment (Hoppe, 2010, Ganzevles and van Est, 2012) in the Czech Republic will help the government to cover the both areas of policy recommendations.

Acknowledgement

The project 4TECH (TL04000390, 8/2020–7/2022) was supported from the Programme ETA of the Technology Agency of the Czech Republic (TA CR).

The project STRATIN+ (MS2104, 2022–2024) has been supported by the Ministry of Education, Youth and Sports (MEYS).

References

[1] The Act on Healthcare Electronisation, Act No. 325/2021 Coll. (Zákon o elektronizaci zdravotnictví, č. 325/2021 Sb.)

[2] Bijker, W.E., Law, J. (eds.) (1994): Shaping Technology / Building Society. Cambridge (Mass.).

[3] Beaunoyer, E., Dupéré, S., & Guitton, M. J. (2020): COVID-19 and digital inequalities: Reciprocal impacts and miti-gation strategies. Computers in Human Behavior, 111, 106424. *https://doi.org/10.1016/j.chb.2020.106424*

[4] De Hond, F., Moser, C. (2022): Useful Servant or Dangerous Master? Technology in Business and Society Debates. Business & Society, 1–30. DOI: 10.1177/00076503211068029.

[5] Ganzevles, J. and van Est, R. (eds.) (2012): TA Practices in Europe, Deliverable 2.2., PACITA. Pp.238.

[6] Geels, F.W. (2002): Technological transitions as evolutionary reconfiguration processes: A multi-level perspective and a case-study, Research Policy, 31 (8/9), 1257–1274.

[7] Geels, F. (2006): Multi-Level Perspective on System Innovation: Relevance for Industrial Transformation. In: Olsthoorn, X., Wieczorek, A. (eds.): Understanding Industrial Transformation. Environment & Policy, vol. 44. Springer, Dordrecht.

[8] Grossmann, J., Korbel, V., Münich, D. (2021): Práce z domova, možnost nebo nutnost (Home office, Opportunity or Necessity). A study of the Think-Tank IDEA. *https://idea.cerge-ei.cz/studies/prace-z-domova-moznost-nebo-nutnost*

[9] Hoppe, R. (2010): The governance of problems: Puzzling, powering and participation. Bristol: The Policy Press.

[10] Perlín, R., Komárek, M., Marada, M., Havlíček, T., Jančák, V., Chromý, P., Bednářová, H. (2019): Typologie mikro-regionů Česka, Urbanismus a územní plánování 4/2019, 8–13.

[11] Sotoudeh, M. (2022): Chances and limits of distance learning from a pedagogical and social perspective. The contribu-tion presented at the session COVID-19 pandemic boosting digital technologies 25. 7. 2022 – ETAC5 session 15:45–17:15 CET.

[12] Scully, D., Lehane, P., & Scully, C. (2021): 'It is no longer scary': digital learning before and during the covid-19 pandemic in Irish secondary schools. Technology, Pedagogy and Education, 00(00), 1–23. *https://doi.org/10.1080/1475939X.2020.1854844*

[13] Van Deursen, A.J.A.M., Helsper, E.J. & Eynon, R. (2014): Measuring Digital Skills. From Digital Skills to Tangible Outcomes project report. *www.oii.ox.ac.uk/research/projects/?id=112*

[14] Varanauskas, A. (2022): The most affected area is "learning", but it's not only negative; the contribution presented at the session COVID-19 pandemic boosting digital technologies 25. 7. 2022 – ETAC5 session 15:45–17:15 CET.

[15] Weinberg, H., Rolnick, A. (eds.) (2019): Theory and Practice of Online Therapy: Internet-delivered Interventions for Individuals, Groups, Families, and Organizations. Routledge, New York, pp. 292.

4Tech Project outputs (see *https://venkov3.cz/4tech/*, page Výstupy, only in Czech):

- Summary Report 1 (2021): Výzkumná zpráva V1: Rozsah a formy využívání vybraných technologií v souvislosti s opatřeními proti pandemii covid-19.
- Summary Report 2 (2021): Výzkumná zpráva V2: Výsledky případových studií o využívání vybraných technologií v souvislosti s opatřeními proti pandemii covid-19.
- Summary Report 3 (2022): Výzkumná zpráva V3: Výsledky kvantitativního šetření o využívání vybraných technologií v souvislosti s opatřeními proti pandemii covid-19.
- Summary Report 4 (2022): Výzkumná zpráva V4: Foresight 4 technologií, které dostaly impuls v době pandemie co-vid-19, a doporučení pro politiku.

Ergo 2023, 18, 1, 16–20
10.5281/zenodo.8111071

Co přináší nová pravidla veřejné podpory v oblasti výzkumu, vývoje a inovací?

Na podzim roku 2022 vydala Evropská komise nové sdělení, Rámec pro státní podporu výzkumu, vývoje a inovací. Zároveň byla schválena významná změna Obecného nařízení o blokových výjimkách, která významně rozšířila možnosti podpory výzkumu a vývoje v podnicích. Hlavním cílem příspěvku je popsat změny obsažené v novém Rámci a novelizovaném nařízení oproti předcházejícím dokumentům a také případné dopady těchto dokumentů na politiky výzkumu, vývoje a inovací v České republice. Nový Rámec ani novelizované nařízení by neměly znamenat pro českou politiku výzkumu, vývoje a inovací zásadní změny na národní ani na institucionální úrovni.

Klíčová slova: hospodářská soutěž; veřejná podpora; výzkum, vývoj a inovace

Aleš Vlk
Univerzita Karlova, Fakulta tělesné výchovy a sportu, CZ

Matej Kliman
Matej Kliman, CZ

Recenzovaná přehledová stať
Obdrženo redakcí: 2. 5. 2023
Přijato k publikování: 22. 6. 2023

What do the new rules on state aid for research, development and innovation bring?

The European Commission published a new Framework for State aid for research and development and innovation at the fall 2022. At the same time, significant changes were made in the General Block Exemption Regulation (GBER) allowing bigger support for research and development in enterprises. The main purpose of our contribution is to describe main differences between the new Framework and amended GBER and their predecessors as well as to discuss their potential impact on the Czech RDI policy. We conclude that the new state aid regulation should mean no major changes with respect to the Czech RDI policy neither on the national nor on the institutional level.

Keywords: competition; state aid; research, development and innovation

Aleš Vlk
Charles University, Faculty of Physical Education and Sport, CZ

Matej Kliman
Matej Kliman, CZ

Peer-reviewed synoptic paper
Received: 2. 5. 2023
Accepted for publication: 22. 6. 2023

Úvod

Vnímání a přístup k veřejné podpoře v oblasti výzkumu, vývoj a inovací prošly v České republice zajímavým vývojem. České republiky se tato problematika týká plně od roku 2004, kdy se stala plnohodnotným členem Evropské unie (EU). Ve výzkumu a vývoji se veřejná podpora začala intenzivně řešit především v souvislosti s přípravou Operačního programu Výzkum a vývoj pro inovace (OP VaVpI) v rámci programovacího období strukturálních fondů EU (SF EU) v období 2007–13.

V atmosféře tlaku vysokých škol a ostatních výzkumných organizací včetně Akademie věd ČR na vyhlášení výzev, které byly zpožděny především kvůli tehdejší turbulentní politické situaci (výměna politické garnitury po volbách v roce 2006, první vláda Mirka Topolánka bez důvěry atd.), bylo nutné se na straně poskytovatele (MŠMT) kromě budování samotné administrativní kapacity a tvorby příslušné programové dokumentace vyrovnat také s problematikou veřejné podpory.

Po spuštění prvních projektů OP VaVpI stála oblast veřejné podpory určitou dobu mimo pozornost světa výzkumu, vývoje a inovací. Začala se opět diskutovat až v souvislosti s přípravou a aplikací tzv. nového Rámce [1] a Nařízení Evropské komise o blokových výjimkách [2], které byly zveřejněny v červnu 2014. Poskytovatel dotace, respektive Řídicí orgán OP VaVpI (MŠMT) zahájil v souvislosti s platností nových evropských předpisů tzv. monitorovací návštěvy podpořených center v oblasti veřejné podpory. V průběhu roku 2015 začal do svých nálezů problematiku veřejné podpory uvádět i Auditní orgán, tj. Odbor 52 Ministerstva financí ČR. Konalo se několik konferencí, specializovaných seminářů a workshopů a představitelé výzkumné sféry začali veřejnou podporu řešit také v souvislosti s úpravou vnitřních předpisů.

Problematika veřejné podpory byla v minulosti nahlížena rozdílně a často nesprávně. A to jak ze strany příjemců finančních prostředků, tak ze strany jednotlivých poskytovatelů a státní správy obecně. Závažná témata se často podceňovala, zatímco podružné a nedůležité záležitosti se zdůrazňovaly a zcela zbytečně a dlouze řešily. Postupně se situace uklidnila a v současné době již veřejná podpora nereprezentuje v politice výzkumu, vývoje a inovací nějaké zásadně kontroverzní či rizikové téma.

V rámci nového programovacího období 2021 až 2027 Evropská komise upravila dva základní dokumenty, které pravidla veřejné podpory v oblasti výzkumu, vývoje a inovací vymezují: aktualizovala Obecné nařízení o blokových výjimkách [2] a vydala Sdělení, tj. Rámec pro státní podpo-

ru výzkumu, vývoje a inovací [3]. Cílem tohoto příspěvku je popsat, jak se nově přijaté a novelizované dokumenty liší od svých předchůdců, a také to, zda nové předpisy mají nějaký zásadní dopad na českou vědní politiku – a to jak na úroveň národní, tak na úroveň jednotlivých institucí. Pro lepší pochopení celé problematiky jsou na začátku příspěvku stručně uvedeny principy hospodářské soutěže, práva veřejné podpory a základy regulace výzkumu, vývoje a inovací na úrovni EU.

Principy hospodářské soutěže

V rámci EU byly základy hospodářské soutěže položeny v roce 1952, kdy byla podepsána Pařížská smlouva o vytvoření Evropského společenství uhlí a oceli. Politika hospodářské soutěže byla v době své konstituce jedním z pilířů společných politik Evropských společenství a představovala významný nástroj Evropské komise ve vztahu k soukromým podnikům a vládám. Specifickým posláním evropské politiky hospodářské soutěže je zajištění fungování soutěže v rámci celé EU.

Pramenem primárního práva EU v oblasti hospodářské soutěže je Smlouva o fungování Evropské unie (SFEU), ve které je politika hospodářské soutěže promítnuta zejména v článcích 2 a 3 a dále pak v článcích 101 až 109 [4]. Pramenem sekundárního práva jsou vedle smluvních aktů (např. mezinárodních smluv, které EU podepsala) zejména jednostranné akty vydané příslušnými orgány EU, které jsou uvedeny v článku 288 SFEU: nařízení, směrnice, rozhodnutí, stanoviska a doporučení. Dále jsou to například sdělení, bílé či zelené knihy apod.

Právo veřejné podpory

Pro samotné právo veřejné podpory EU jsou stěžejní především články 107–109 SFEU. Článek 107 dále stanoví, jaké podpory jsou s vnitřním trhem EU slučitelné. Článek 108 vymezuje pravomoc Evropské komise ve věci zkoumání režimů podpory a jejich zrušení či úpravu. Na základě článku 109 může Evropská rada na návrh Evropské komise a po konzultaci s Evropským parlamentem vydávat veškerá prováděcí nařízení ke článkům 107 a 108, tzn. vymezovat výjimky.

Problematika hospodářské soutěže a potažmo veřejné podpory patří v souladu s článkem 3 SFEU do výlučné kompetence EU, která smí jako jediná vydávat a přijímat závazné akty. Členské státy tyto akty pouze provádějí. Pravidla upravující oblast veřejné podpory jsou tedy přímo závazná pro Českou republiku i jednotlivé subjekty, aniž by musela (respektive mohla) být transponována do českého právního řádu.

Veřejná podpora je v současné době již velmi složitým a specifickým právním oborem, a to především v rámci EU. Kromě vydávání základních aktů se příslušné orgány Evropské unie, a to především Evropská komise a Soudní dvůr EU, snaží v rámci legislativní a rozhodovací praxe tuto oblast systematicky vysvětlovat a zároveň shrnovat dosavadní poznatky – obecně či v rámci jednotlivých odvětví. I zde platí, že pro posouzení otázek v oblasti veřejné podpory mají oprávnění poskytovat závazný výklad pouze orgány EU.

Právní úprava veřejné podpory v oblasti výzkumu, vývoje a inovací

Výzkum, vývoj a inovace jsou jednou z oblastí, pro kterou platí určité výjimky z jinak obecně zakázané veřejné podpory. Zásadním a přímo aplikovatelným předpisem je Nařízení Komise (EU) č. 651/2014 ze dne 17. června, kterým se v souladu s články 107 a 108 Smlouvy prohlašují určité kategorie podpory za slučitelné s vnitřním trhem (Nařízení) [2]. Tento dokument vstoupil v platnost 1. 7. 2014. Dokument je znám především pod zkráceným názvem Obecné nařízení o blokových výjimkách – GBER (General Block Exemption Regulation). Následně v červenci 2015 Evropská komise zveřejnila Průvodce Obecným nařízením o blokových výjimkách [5], který vznikl jako reakce na otázky obdržené od členských států při implementaci Nařízení. Materiál poskytuje interpretační vodítka k článkům 1 až 35, ale není pro Evropskou komisi závazný.

Dalším důležitým dokumentem je Sdělení komise Rámec pro státní podporu výzkumu, vývoje a inovací, který se váže vždy na dané programovací období. Platný dokument, jehož význam a dopady budeme diskutovat ve zbytku našeho příspěvku, má referenční číslo 2022/C 7388[3] a nahradil Rámec (2014/C 198/01) [1]. Rámec sice není přímo aplikovatelným předpisem, ale je velmi důležitý, protože prezentuje pohled Evropské komise na problematiku posuzování slučitelnosti veřejné podpory s vnitřním trhem v oblasti výzkumu, vývoje a inovací a obsahuje některé zásadní definiční vymezení.

Dále existují dokumenty, kterými Evropská komise upřesňuje podmínky aplikace pravidel veřejné podpory. Infrastrukturních projektů se týkají takzvané Analytické přehledy financování infrastruktury (Analytical Grids). První formuláře vydala Evropská komise v roce 2012 a další byly vydány 21. 9. 2015, přičemž tyto analytické přehledy jsou postupně upravovány a aktualizovány [6]. Evropská komise připravila také výkladový dokument zásadní povahy, kterým shrnuje problematiku veřejné podpory jako takové (včetně problematiky financování infrastruktur) s názvem Sdělení Komise o pojmu státní podpora podle článku 107 odst. 1 Smlouvy o fungování Evropské unie [7].

Nový Rámec pro státní podporu výzkumu, vývoje a inovací

V rámci nového programovacího období (tj. pro období 2021 až 2027) Evropská komise aktualizovala Obecné nařízení o blokových výjimkách [2] a vydala dne 19. 10. 2022 nové Sdělení, tj. Rámec pro státní podporu výzkumu, vývoje a inovací C(2022) 7388 [3]. Rámec má obdobnou základní strukturu, tedy rozdělení na části definice, metodický výklad k formám podpory výzkumu a vývoje, které nezakládají veřejnou podporu, a navazující metodický výklad pro případ oznámení (notifikace) podpory v oblasti výzkumu a vývoje. Nový Rámec je dostupný na serveru EURLEX v jazycích států Evropské unie. Formálně se od dosavadního Rámce liší tím, že je rozdělen do dvou souborů. V jednom je text Rámce rozdělený na kapitoly 1 až 6 a v druhém jsou obsaženy přílohy upravující způsobilost nákladů a intenzitu podpory pro notifikované projekty. Aktuálně je nový Rámec podstatně rozsáhlejší než dosavadní, oproti původním 29 stranám má nový Rámec včetně příloh celkem 48 stran. Textové rozšíření úpravy se však týká zejména té části nového Rámce, která se zabývá přístupem Evropské komise k notifikovaným podporám, což je institut, který se v České republice nevyužívá.

Co se týká režimů financování výzkumu a vývoje výzkumných organizací na rozdíl od dvou předchozích rámců nový dokument nepřináší žádné zásadní změny. Jde spíše o lépe (srozumitelněji) formulované potvrzení dosavadního výkladu. Potvrzuje se i to, že Rámec rozlišuje režimy financování směřující výhradně do nehospodářských činností a režimy financování výzkumných organizací a infastruktur „jako cel-

ků“, kde je relevantní podíl výkonu hospodářských aktivit se stejným limitem, tedy 20 %. Potvrzuje se také, že součástí nezávislého výzkumu je výzkum ve spolupráci.

Změny v definicích pojmů a vztah ke Sdělení o pojmu veřejné podpory

Určité formulační změny lze identifikovat jako vždy v části 1.3. označené jako definice. Tyto změny by však neměly mít zásadní dopad na výklad Rámce. Jednou ze změn, které stojí za zmínku, je rozšíření definic pojmů „průmyslového výzkumu“ a „experimentálního vývoje“ o výslovnou zmínku vývoje digitálních produktů, jakými jsou například superpočítače, kvantové technologie, technologie blokových řetězců, umělá inteligence, kybernetická bezpečnost, velká data a cloudové nebo edge technologie. Rámec tím nepochybně reaguje na rozvoj těchto oblastí v Evropské unii [8]. Stěžejní pojmy jako „výzkumná organizace“ nebo „transfer znalostí“ zůstávají bez významnějších změn.

Z hlediska systematizace dokumentů měkkého práva vykládajících pravidla veřejné podpory je zajímavé, že nový Rámec v úvodu kapitoly 2, v odstavci 17 výslovně odkazuje na Sdělení Komise o pojmu státní podpora [7] uvedeném v čl. 107 odst. 1 Smlouvy o fungování Evropské unie (2016/C 262/01) jak na obecný výkladový dokument s tím, že Kapitola 2 Rámce představuje specifický pohled na situace, které vznikají v oblasti výzkumu, vývoje a inovací. Komise ale upozorňuje na to, že nelze předjímat možný vývoj těchto otázek v rozhodovací praxi Evropského soudního dvora.

Financování nehospodářských aktivit a účinnost Rámce

Rámec v novém a jen velmi málo formulačně upraveném znění podkapitoly 2.1.1. potvrzuje dosavadní výklad pravidel veřejné podpory. Za primární činnosti výzkumných organizací lze i nadále považovat za prvé vzdělávání organizované státem a převážně financované z veřejných zdrojů, za druhé nezávislý výzkum a vývoj včetně tzv. účinné spolupráce a za třetí šíření výsledků na neexkluzivním a nediskriminačním základě.

Sekundární aktivitou výzkumných organizací, které Evropská komise v Rámci i nadále přiznává status nehospodářské činnosti, je transfer znalostí, pokud je prováděn přímo výzkumnou organizací, ve spolupráci výzkumných organizací či prostřednictví jejich dceřiných subjektů za podmínky reinvestice zisku do primárních činností výzkumné organizace či výzkumné infrastruktury.

Rámec i nadále zmiňuje dva možné režimy financování výzkumné organizace či výzkumné infrastruktury. Za prvé v odstavci 19 připouští financování výhradně nehospodářských aktivit za podmínky, že výzkumná organizace je schopna efektivně oddělit své hospodářské a nehospodářské činnosti na úrovni každého nákladu, výnosu a zdroje financování, tak aby bylo zabráněno křížovému financování hospodářských aktivit. Jako doklad pro oddělené sledování dle Rámce může posloužit roční finanční výkaz relevantní entity. Toto v české praxi činí a i do budoucnosti může činit jisté obtíže, protože obsah finančních výkazů upravuje v ČR zákon č. 563/1991 Sb., o účetnictví, v platném a účinném znění a jeho prováděcí vyhlášky pro jednotlivé typy účetních jednotek. Účetní legislativa v ČR je převážně kogentního charakteru. To znamená, že od jejich ustanovení se nedá odchýlit. Přitom platí, že daňově účetní legislativa obsahuje vlastní úpravu kategorizace hospodářských činností a účetních jednotek a nákladových středisek, které se liší od kategorií hospodářské a nehospodářské činnosti a relevantní entity, jak jsou popsány v Rámci.

Druhým režimem, odlišným od režimu dle odstavce 19, je režim dle odstavce 21. Dle tohoto ustanovení platí, že pokud je výkon hospodářských činnosti ve výzkumné organizaci nebo při výzkumné infrastruktuře tzv. čistě vedlejšího charakteru, nevztahují se na jejich financování „jako celků“ pravidla veřejné podpory dle čl. 107 Smlouvy o fungování Evropské unie. Za čistě vedlejší výkon hospodářských činností Evropská komise v Rámci považuje situaci, kdy (i) na hospodářské aktivity není alokováno více než 20 % celkových ročních kapacit relevantní entity (myšleno zejména materiál, infrastruktura a práce) a na tyto aktivity jsou spotřebovány tytéž zdroje jako na aktivity nehospodářské.

Volba těchto režimů je dána nepochybně poskytovateli veřejných prostředků na podporu výzkumu, vývoje a inovací. Ten může vyhradit použití prostředků dle odstavce 19 výhradně na nehospodářské aktivity. Pak poskytovatel kontroluje, zda výzkumná organizace odděleně sleduje své hospodářské a nehospodářské aktivity a zda zároveň poskytnuté prostředky použila výhradně na podporu svých nehospodářských aktivit. Druhou variantou pro poskytovatele je poskytnout prostředky dle odstavce 21 Rámce na výzkumnou organizaci nebo infrastrukturu jako „na celek“. V takovém režimu poskytovatel dle tohoto odstavce již nekontroluje použití prostředků na nehospodářské aktivity ani oddělené sledování na úrovni každého nákladu, výnosu a zdroje financování, ale pouze to, zda pro hospodářské činnosti jsou spotřebovány stejné zdroje jako na činnosti hospodářské a zároveň zda celkový objem kapacit alokovaných na hospodářské činnosti v daném roce nepřesáhl 20 %.

Pokud poskytovatel aplikuje obě dvě výše uvedená ustanovení najednou, jedná se dle našeho názoru o závažné neporozumění úpravě pravidel veřejné podpory. Nové znění Rámce princip dvou různých variant uplatnění aplikace pravidel financování potvrzuje.

Úprava pravidel smluvního výzkumu dle podkapitoly 2.2.1., účinné spolupráce dle podkapitoly 2.2.2. a veřejného zadávání zakázek na služby ve výzkumu a vývoji (exkluzivní vývoj a zadávání zakázek v předobchodní fázi) dle podkapitoly 2.3. zůstávají také bez významnějších změn.

Zajímavé je také to, co se do nového Rámce nakonec nedostalo. Jedná se zejména o odpověď na otázku, jak dlouho poté, co výzkumná organizace nebo výzkumná infrastruktura přijme prostředky na své primární nehospodářské činnosti, je výzkumná organizace nebo výzkumná infrastruktura povinna vykazovat čistě doplňkový charakter nehospodářských činností. V květnu roku 2021 byl zveřejněn první pracovní návrh Rámce, který se pokusil v čl. 2.1.1. odst. 22 tuto otázku řešit tím, že stanovil minimální lhůtu deseti let. Tato zajímavá úprava se nakonec do znění tohoto ustanovení v novém Rámci nedostala. A tak tato otázka zůstává i nadále nejasná.

Nový Rámec nabyl účinnosti 19. října 2022. Jde o výkladový dokument, a proto neplatí zákaz retroaktivity. Definice a úprava čl. 2 Rámce se tak aplikují jak na stávající, tak na minulé a všechny budoucí projekty.

Nová ustanovení Obecného nařízení o blokových výjimkách

V době sepsání tohoto článku (květen 2023) je již známé, byť dosud není účinné nové znění výše zmíněného Obecného nařízení o blokových výjimkách. Obecné nařízení o blokových výjimkách upravuje tzv. výjimky ze zá-

kazu veřejné podpory, tedy definuje situace, kdy se má za to, že veřejná podpora je slučitelná s vnitřním trhem, aniž by bylo nutné takovou podporu oznamovat Evropské komisi a čekat na její vyjádření.

V minulých programovacích obdobích byl vždy Rámec vydán v návaznosti na nové nařízení o blokových výjimkách. V tomto případě Evropská komise přikročila zatím pouze k sérii významnějších novelizací nařízení. Poslední z nich zasáhla významně i do oddílu 4 nařízení, který se týká podpory výzkumu a vývoje.

Lze říci, že úprava Rámce funguje jako doplněk úpravy oddílu 4 nařízení v tom smyslu, že Rámec se soustředí na podporu výzkumných organizací v režimu, který vůbec nenaplňuje znaky veřejné podpory (a umožňuje až 100% financování výzkumných organizací a výzkumných infrastruktur), zatímco oddíl 4 Obecného nařízení upravuje financování výzkumu a vývoje v podnicích, kde je tzv. maximální intenzita podpory (podíl úhrady způsobilých výdajů) omezena dle kategorií výzkumu s určitým zvýhodněním pro malé a střední podniky a pro účinnou výzkumnou spolupráci.

V České republice v minulosti docházelo k používání obecného nařízení i na výzkumné organizace. To je sice možné, protože volbu režimu veřejné podpory určuje její poskytovatel. Dle našeho názoru však jde o neefektivní použití pravidel veřejné podpory s ohledem na administrativní zátěž vykazování kategorií výzkumu, a to zejména z důvodu nutnosti tzv. kofinancování s ohledem na maxima intenzity podpory, které obecné nařízení stanovuje pro podniky.

Od nabytí účinnosti nového znění GBER mají poskytovatelé podpory na výzkum a vývoj širší paletu nástrojů podpory podniků. Přibyla nová specifická úprava článků 25a až 25d. Tato nová úprava doplnila již tradiční obecné kategorie podpory projektů výzkumu, vývoje a inovací a studií proveditelnosti v čl. 25 a podpory výzkumných infrastruktur v článku 26, jakož i v roce 2014 zavedené kategorie podpory určené inovačním klastrům (čl. 27), podpory na inovace určené malým a středním podnikům (čl. 28), podpory na inovace postupů a organizační inovace a podpory výzkumu a vývoje v oblasti rybolovu a akvakultury (čl. 30). Všechna čtyři nová ustanovení jsou velmi specifická tím, že se týkají specifických režimů na podporu výzkumu a vývoje v kompetenci DG Research, tedy Horizon 2020 a Horizon Europe.

Prvním nově definovaným nástrojem je podpora na projekty, kterým byla udělena značka kvality – pečeť excelence, dle čl. 25a s maximálním omezením financování 2,5 milionu eur na jeden malý nebo střední podnik a výzkumný a vývojový projekt nebo studii proveditelnosti. Druhým zcela novým ustanovením je čl. 25b, který upravuje podporu na akce „Marie Skłodowska-Curie„ a na podporu v rámci grantů ERC na tzv. ověření koncepce (Proof of Concept).

Třetím novým ustanovením je čl. 25c, který upravuje podporu obsaženou ve spolufinancovaných výzkumných a vývojových projektech. Jedná se o akce zahrnující zejména výzkumné a vývojové projekty prováděné v rámci evropských institucionalizovaných partnerství podle článku 185 nebo článku 187 Smlouvy nebo akce na spolufinancování programů definované v pravidlech programu Horizon Europe, které provádějí nejméně tři členské státy, případně dva členské státy a nejméně jedna přidružená země a které jsou vybrány na základě vyhodnocení a seřazení provedeného nezávislými odborníky na základě nadnárodních výzev v rámci programů Horizon 2020 nebo Horizon Europe. Příspěvek z programu Horizon 2020 nebo Horizon Europe je nejméně 30 % způsobilých výdajů na výzkumnou a inovační akci nebo na inovační akci.

Posledním novým ustanovením je čl. 29d, který upravuje podporu na akce označované jako Teaming. Tedy akce, kterých se účastní nejméně dva členské státy a které byly vybrány na základě vyhodnocení a seřazení provedeného nezávislými odborníky na základě nadnárodních výzev v rámci programů Horizon 2020 nebo Horizon Europe. Článek umožňuje podporu podniků s intenzitou až 70 % a umožňuje i podporu tzv. „tvrdých“ projektů, tedy projektů zahrnujících podporu pořizování dlouhodobého investičního majetku.

Na těchto nových ustanoveních je zajímavé to, že výslovně odkazují na evropské programy podpory výzkumu a vývoje. U těchto programů se dosud mělo za to, že se na ně pravidla veřejné podpory nevztahují vzhledem k tomu, že není naplněn znak přítomnosti prostředků členských států (šlo tradičně o prostředky z rozpočtu EU). Zdá se, že čím více jsou do implementace programů Horizon 2020 a Horizon Europe zapojovány i členské státy, vyvstává potřeba umožnit financování podniků v těchto programech.

Zajímavý a netradiční je také legislativní mechanizmus těchto ustanovení. Více méně u všech tradičně upravovaných parametrů (maximální výše podpory, kategorie způsobilých výdajů, intenzita podpory apod.) vesměs odkazuje na úpravu těchto programů a pouze v několika případech obsahuje specifickou úpravu.

Dopad nového Rámce a novelizace Obecného nařízení o blokových výjimkách na politiku výzkumu, vývoje a inovací v České republice

Poprvé od vstupu České republiky do EU nepřinese vydání Rámce zásadní změny pro politiku výzkumu, vývoje a inovací. Lze očekávat, že bude narůstat podpora výzkumných projektů v oblasti informačních technologií a nový Rámec tento trend zdůrazňuje rozšířením definice „průmyslového výzkumu“ a „experimentálního vývoje“. Z našeho pohledu by tato změna jako jediná měla být promítnuta do úpravy zákona č. 130/2002 Sb., o podpoře výzkumu a vývoje z veřejných prostředků, v platném a účinném znění. Nový Rámec by tím, že nepřináší žádné závažné změny ani nezavádí novou terminologii, mohl spíše přispět ke stabilizaci vědní politiky a prostředí výzkumu, vývoje a inovací v České republice.

Stabilizace úpravy Rámce by měla přispět také ke korekci některých výkladových tendencí, které se občas objevují v praxi českých poskytovatelů dotací a správních orgánů. Jako příklad lze uvést výklad prosazovaný Ministerstvem školství, mládeže a tělovýchovy (MŠMT), a to zejména při posuzování zápisu na seznam výzkumných organizací, dle kterého není výzkum v účinné spolupráci považován, přes výslovné znění odst. 20 Rámce, za součást aktivit nezávislého výzkumu výzkumné organizace. Jako další příklad lze uvést nesprávný postup některých poskytovatelů institucionální podpory, u nichž dochází k nevhodnému směšování dvou režimů upravených Rámcem v odstavcích 19 a 21.

Na úrovni jednotlivých výzkumných organizací lze konstatovat, že vydání nového Rámce nevyžaduje na rozdíl od minulosti žádné změny ve vnitřních přepisech či interních procesech.

Pokud jde o změny v Obecném nařízení o blokových výjimkách, ty podpoří větší participaci České republiky v rámcových programech EU pro výzkum a inovace a umožní také financování podniků v jednotlivých projektech. Lze jen doufat, že tato nová úprava obecného nařízení nebude v ČR poskytovateli dotací využívána na podporu nehospodářských činností výzkumných organizací a výzkumných infrastruktur, kde i nadále plně postačí mnohem efektivnější využití Rámce.

Odkazy

[1] Sdělení Komise – Rámec pro státní podporu výzkumu, vývoje a inovací 2014/C 198/1. *https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=OJ:C:2014:198:TOC*

[2] NAŘÍZENÍ KOMISE (EU) č. 651/2014. *https://eur-lex.europa.eu/eli/reg/2014/651/oj*

[3] Sdělení Komise – Rámec pro státní podporu výzkumu, vývoje a inovací 2022/C 414/01. *https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=OJ:C:2022:414:TOC*

[4] Smlouva o fungování Evropské unie. Konsolidované znění. *https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:12012E/TXT*

[5] Guidance on the notion of State aid. *https://competition-policy.ec.europa.eu/state-aid/legislation/notion-aid_en*

[6] INFRASTRUCTURE ANALYTICAL GRID FOR RESEARCH INFRASTRUCTURE. *https://ec.europa.eu/competition/state_aid/modernisation/grid_research_en.pdf*

[7] Sdělení Komise o pojmu státní podpora uvedeném v čl. 107 odst. 1 Smlouvy o fungování Evropské unie. *https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=OJ:C:2016:262:TOC*

[8] EU Science Hub. ICT industry and ICT R&D in Europe. *https://joint-research-centre.ec.europa.eu/scientific-activities-z/ict-industry-and-ict-rd-europe_en*

Informace pro autory

Ergo je recenzovaný časopis se zaměřením na analýzy a trendy výzkumu, technologií a inovací. Do časopisu mohou být zařazeny jen původní a dosud nepublikované články, které úspěšně projdou recenzním řízením.

Příjem článků a recenzní řízení

- Články jsou od autorů přijímány průběžně v elektronické formě na adrese uvedené v tiráži časopisu. Přijímány jsou pouze články, které dosud nebyly publikovány v jiném periodiku a ani nejsou současně jinému periodiku k publikování nabídnuty.
- Každý došlý článek nejprve posoudí odpovědný redaktor a rozhodne o jeho přijetí do recenzního řízení. O přijetí či nepřijetí článku do recenzního řízení informuje odpovědný redaktor autora článku.
- V recenzním řízení posuzují každý článek nezávisle na sobě minimálně dva recenzenti.
- Recenzní řízení probíhá anonymně. Pokud si recenzent přeje zůstat v anonymitě i po skončení recenzního řízení, nebude jeho totožnost zveřejněna mimo okruh redakční rady.
- Každý z recenzentů se vysloví pro publikování (bez výhrad nebo s drobnými úpravami), přepracování nebo zamítnutí článku a své rozhodnutí zdůvodní v recenzním posudku.
- Redakční rada se seznámí s recenzními posudky a rozhodne o publikování, přepracování nebo zamítnutí článku. Odpovědný redaktor oznámí rozhodnutí redakční rady autorovi článku.
- Pokud dojde k přepracování článku a odpovědný redaktor bude mít pochybnosti o kvalitě tohoto přepracování, bude novou verzi článku konzultovat s recenzentem, který přepracování doporučil.
- Redakce si vyhrazuje právo upravit článek a všechny jeho části podle redakčních zvyklostí; provedené úpravy budou s autorem konzultovány formou autorské korektury článku.

Formální náležitosti rukopisu

- Články jsou přijímány v českém, slovenském nebo anglickém jazyce a v textovém formátu kompatibilním s editorem MS Word.
- Článek musí mít standardní strukturu vědeckého článku, tj. kromě vlastního textu musí navíc obsahovat zejména abstrakt (v rozmezí 500 až 1 000 znaků), klíčová slova a seznam použité literatury. Vhodné je doplnit rovněž stručnou informaci o autorech. Název článku, abstrakt a klíčová slova musí být dodány kromě původního jazyka rovněž v angličtině.
- Doporučený rozsah článku je cca 15 000 znaků, doplněný 3 grafy, obrázky nebo tabulkami standardní velikosti, což odpovídá zhruba třem tiskovým stranám v časopise.
- Rukopisy je nejlépe psát v co nejjednodušší grafické podobě, pokud možno bez různých grafických odrážek a speciálního formátování.
- V jednom článku je vhodné použít nejvýše dvě úrovně mezititulků.
- Všechny grafy a tabulky jsou při sazbě vytvářeny znovu. Kromě náhledu jejich požadované podoby v textu je proto vždy vhodné dodat také zdrojová data v samostatných souborech (grafy nejlépe v MS Excelu, tabulky v MS Wordu).
- Optimální rozlišení fotografií a obrázků pro tisk je 300 dpi, tj. běžná fotografie na šířku jednoho sloupce sazby by měla mít cca 1 200 × 900 bodů (větší rozlišení nevadí, menší ano).
- Odkazy na použitou literaturu v souladu s ČSN ISO 690 (viz konkrétní příklady použití v časopise).
- Poznámky pod čarou (pokud jsou nutné – např. vysvětlení podružných detailů, které by v textu odvádělo od právě probírané problematiky) jsou obvykle z grafických důvodů umisťovány na konec článku a je vhodné uvádět je tam všechny souhrnně už v rukopise; poznámky pod čarou se číslují od začátku dokumentu a v textu jsou vyznačeny horním indexem.

Submission of manuscripts

Ergo is a reviewed journal oriented at analyses and trends in research, technologies, and innovations. The journal only accepts original, unpublished articles that pass the review process.

Article acceptance and the review process

- Articles are accepted from their authors continuously, in electronic form, at the address listed in the imprint. Only articles that have not been published in any other periodical and are not at the same time offered to another periodical are accepted.
- Every received article is first considered by the executive editor who decides whether to accept it for the review process. The executive editor informs the author of the article whether the article was or was not accepted for the review process.
- A minimum of two reviewers assess every article during the review process.
- The review process is anonymous. If a reviewer wishes to remain anonymous even after the end of the review process, their identity will not be disclosed to anyone outside of the editorial board.
- Each reviewer gives their opinion as to whether to publish (without qualifications or with minor modifications), rework, or reject the article and provides reasons for their decision in a review assessment.
- The editorial board reads the review assessments and decides whether to publish, rework, or reject the article. The executive editor informs the author of the article of the board's decision.
- If the article is reworked and the executive editor has doubts about the quality of the reworking, the new version of the article will be discussed with the reviewer who recommended the reworking.
- The editors reserve the right to modify articles and all their parts according to editorial custom; performed modifications will be discussed with the author through an author's editing of the article.

Formal requisites for manuscripts

- Articles are accepted in Czech, Slovak, or English in a text format compatible with the MS Word text processor.
- Articles must have the standard structure of scientific articles, i.e. in addition to the text itself, they must contain an abstract (between 500 and 1000 characters), keywords, and a list of used literature.Brief information about the authors may also be included. The name of the article, abstract, and the keywords must be also supplied in English in addition to the original language.
- The recommended length of articles is 15 000 characters with 3 charts, pictures, or tables of standard size which corresponds to three print pages in the journal.
- Manuscripts should use simple formatting, ideally without graphical bullets and other special formatting.
- A single article should use no more than two levels of subheadings.
- All charts and tables are reset during typesetting. In addition to their requested form within the text, source data should be included in separate files (charts in MS Excel, tables in MS Word).
- The optimum resolution for photos and images for printing is 300 dpi, i.e. a regular photo of the width of one typeset column should have approximately 1 200×900 pixels (higher resolution is fine, lower is not).
- Links to used literature should comply with ČSN ISO 690 (see specific examples in the journal).
- Footnotes (if required – for example, to explain secondary details that would distract from the discussed topic in the text) are usually placed at the end of the text for graphical reasons and should be placed there in the manuscript as well; footnotes are numbered from the beginning of the document and indicated by superscript.