Ministerstvo zahraničních věcí
České republiky

Kybernetická bezpečnost a trh s cloudovými službami Skandinávie

Stav, perspektivy a obchodní příležitosti

Pro
Odbor ekonomické diplomacie, MZV ČR

Od
Šárka Waisová a Ladislav Cabada
Západočeská univerzita v Plzni

Květen 2022

Realizováno v rámci grantu Technologické agentury ČR

Projekt č. TL03000150 „Zvyšování konkurenční výhody vnějších ekonomických vztahů ČR: využití kombinace regionálně-sektorového přístupu“ (KOVYVEV ČR)

Obsah

Obsah

1. Metodologie, zdroje dat a prohlášení o etice vědecké práce a nepodjatosti

Předložená analýza byla zpracována na základě veřejně přístupných dat a informací metodou desk research. Využita byla data statistických úřadů, mezinárodních organizací, vlád analyzovaných zemí a firem pohybujících se na analyzovaných trzích. Pokud to bylo možné, data a informace byly triangulovány. K tomu byly využity zprávy z novin a dalších médií a další zdroje jako databáze příslušných států, OECD či Světové banky. Tam, kde to bylo účelné, byly kontaktovány místní agentury pro podporu obchodu a zahraničních investic. Všechny zdroje využité pro zpracování této analýzy jsou uvedeny pod čarou nebo na konci textu v kapitole „použité zdroje“.

Autoři této zprávy deklarují, že na realizaci jakéhokoliv obchodu či investice zmiňovaných v této analýze nemají žádný osobní, ekonomický nebo politický zájem a nemají žádný vztah k žádné ze zde zmiňovaných firem, úřadů či států.

Autoři také prohlašují, že analýzu zpracovali samostatně na základě uvedených zdrojů a text není plagiátem.

2. Shrnutí a hlavní výsledky analýzy

V této zprávě jsou analyzovány obchodní a investiční příležitosti při zajišťování kybernetické bezpečnosti a v oblasti cloudových služeb na trhu skandinávských zemí. Tyto státy – Dánsko, Finsko, Norsko a Švédsko[1] – patří k pionýrům digitalizace. Vlády uvedených čtyř zemí systematicky podporují digitalizaci veřejných politik i obchodních procesů a všechny čtyři země se chtějí stát světovými technologickými centry. Tomu přizpůsobují politická rozhodnutí, legislativu i obchodní prostředí. Největší obchodní a investiční příležitosti v digitalizačních procesech se ve Skandinávii generují ve třech oblastech: 1) výstavba a provoz datových center, 2) infrastruktura a služby v oblasti cloud computing a 3) infrastruktura a služby v oblasti kybernetické bezpečnosti.

Největšími zákazníky v sektoru ICT jsou ve skandinávských zemích státní správa a velké firmy. Již před pandemií Covid začaly skandinávské státy a firmy s digitalizací, tlak na práci z domova a distanční komunikaci v době pandemie poptávku po digitalizaci zvýšily a uspíšily. Všechny čtyři analyzované země mají ve svých strategických prioritách digitalizaci veřejné správy, veřejných politik a digitální komunikace s občany (např. dánský cíl je digitalizovat až 80 % komunikace s občany a 100 % komunikace s firmami jen digitálně). Skandinávské vlády deklarují investice velkých objemů do digitálních procesů, a kromě programových dokumentů přijímají i příslušnou legislativu. K masivní digitální transformaci dochází ve finančních službách, ve výrobě a distribuci energií a ve zdravotnictví. Již dnes komunikují všechny skandinávské státy s občany a firmami prostřednictvím různých portálů a aplikací a vydávají nejrůznější e-dokumenty (e-ID či e-řidičský průkaz) (tabulka 1). Podle legislativy skandinávských zemí musejí být některé druhy dat (např. ve Finsku se jedná o zdravotní a osobní data občanů) uložena v datových centrech nacházejících se na území příslušného státu. I když s postupující digitalizací roste využívání datových center a cloudových služeb lokalizovaných na serverech v jiných zemích, strmě roste i poptávka po skandinávských datových centrech a jejich službách. S ohledem na politickou, bezpečnostní a energetickou nestabilitu v třetích zemích a nároky na

[1] Do Skandinávie je obvykle řazen i Island, nicméně v této analýze zahrnut není. Tato analýza také nepokrývá obchodní a investiční příležitosti dvou dánských autonomních oblastí – Grónska a Faerských ostrovů.

rychlost při přenosu velkých objemů dat a jejich ochranu, navíc skandinávské firmy i státy preferují využívání datových center na vlastním území, resp. v regionu.[2] Při rozhodování mezinárodních firem o lokalizaci datových center patří skandinávské země k nejatraktivnějším destinacím; důvodem jsou stabilní dodávky elektrické energie a její nízká cena, silná přenosová soustava a fungující podmořské kabely, dostupné možnosti chlazení a minimální politická, ekonomická i environmentální rizika. Velká datová centra ve skandinávských zemích vybudovaly např. Google a Microsoft, další firmy, např. Volkswagen, zde budují centra pro High-Performance Computing.

Tabulka 1: Digitální platformy skandinávských vlád: příklady

Dánsko	Borger.dk: centrální informační a komunikační portál pro občany
	Virk.dk: centrální informační a komunikační portál pro firmy
Finsko	Suomi.fi: národní digitální servis pro občany a firmy
	Demokratia.fi: portál zpřístupňující občanům informace o politických procesech
	Paikkatietoikkuna.fi: národní portál pro katastrální data
Norsko	Ovelse.no: portál informující o kybernetické bezpečnosti s cílem mj. poskytnout návody korporátnímu sektoru i jedincům, jak zvýšit kybernetickou bezpečnost zařízení
	Norge.no: portál pro digitální komunikaci mezi občany a státem, zajišťuje digitální dokumenty jako e-ID
	GeoNorge: portál pro firmy i občany poskytující geografická a katastrální data
Švédsko	Verksamt.se: portál pro digitální komunikaci s domácími a zahraničními firmami
	Lakemedelskollen.se: portál digitální zdravotní péče – e-recept, digitalizace zdravotních záznamů

Zdroj: uvedené internetové stránky

Ve skandinávských zemích roste zájem o cloud computing a jak ukazují mezinárodní srovnání (tabulka 2), patří ke světové špičce jak ve využívání cloud computing, tak v oblasti nezbytné legislativy, nadšení a vůli vlády a společnosti pro použití cloud computing a lidském kapitálu schopném se do sektoru cloud computing zapojit. V oblasti cloud computing a kybernetické bezpečnosti nacházíme obchodní příležitosti (výběr viz tabulka 3) při budování infrastruktury i při poskytování služby a v poradenství; u firem i úřadů roste zájem o využívání multi-cloud (nejčastěji SaaS), to však s ohledem na neznalost procesů či jejich nevhodné nastavení uvnitř firem a úřadů zvyšuje náklady a snižuje profity z přechodu na cloud computing. Firmy i stát vyhledávají poradenství s cílem optimalizovat využití cloud computing

[2] Mapa datových center a bližší informace (místo, provozovatel, energetická spotřeba) ke každému centrum ve skandinávských zemích viz Baxtel (baxtel.com/data-center/nordics). Mapa zahrnuje i datová centra ve výstavbě.

a minimalizovat rizika plynoucí z využívání více cloudů. Ve snaze vybudovat uhlíkově neutrální ekonomiku roste poptávka po optimalizaci energetické spotřeby. Uhlíková neutralita je základní podmínkou pro všechny firmy, produkty a investice vstupující na skandinávské trhy. Např. ve Švédsku uhlíkově neutrální ekonomika již není jen otázkou preference spotřebitelů, ale byla stanovena jako oficiální cíl, který by měl být splněn do roku 2030.

Tabulka 2: Připravenost skandinávských zemí pro cloud computing

	Dánsko	Finsko	Norsko	Švédsko	Česko
Celkové pořadí v Global Cloud Ecosystem Index	4	2	9	3	24
Infrastruktura a přístup ke cloudovým službám	2	9	8	5	21
Přístup k telekomunikačním sítím a jejich kvalita	10	3	14	4	32
Bezpečnost a kvalita regulatorního prostředí umožňující progresivní budování cloud computing a digitální důvěry	3	1	6	4	27
Lidský kapitál pro budování cloud computing	9	5	11	6	16

Zdroj: MIT Technology Review 2022

Pokračující digitalizace s sebou nese růst poptávky po poradenství v oblasti zajištění kybernetické bezpečnosti. Firmy i státní úřady skandinávských zemí se v posledních třech letech opakovaně staly terčem kybernetických útoků. Cílem útoků bylo buď narušit fungování infrastruktury a politických procesů, nebo krádeže dat a následné vydírání.[3] Pro rok 2022 i následující období pěti let vlády všech skandinávských zemí avizovaly navýšení rozpočtů pro zajištění kybernetické bezpečnosti státních úřadů i kritické infrastruktury.

[3] Všechny skandinávské vlády uvádějí, že počet kybernetických útoků na cíle na jejich území narostl v průběhu let 2020 a 2021. Dvakrát byl napaden norský parlament a emailové účty poslanců, byla ukradena data zákazníků firmy Nordic Choice Hotels či data dánské firmy Vestas Wind Systems. Norsko opakovaně zveřejnilo, že za útoky na jeho parlament a další státní úřady stojí ruské skupiny. Poté, co Rusko napadlo Ukrajinu, se skandinávské země spojily s baltskými státy, aby kybernetickým útokům z Ruska čelily společně. Firmy ze skandinávských a pobaltských zemí vytvořily masivní kampaň pomáhající Ukrajině čelit ruským kybernetickým útokům. Příkladem může být postup švédské IT firmy Beetroot (itukraine.org.ua/en/beetroot.html nebo beetroot.co/newsroom/).

Tabulka 3: Obchodní příležitosti v oblasti kybernetické bezpečnosti a cloudových služeb ve skandinávských zemích: výběr

Příležitosti	Globální hráči na skandinávském trhu
Endpoint security	
• Endpoint detection and response • Cloud based a SaaS Endpoint bezpečnostní řešení • Bezpečnost IoT	Broadcom, McAfee, Trend Micro, Microsoft, CrowdStrike, Kaspersky, Sophos, Cisco
Identify and Access Management (IAM)	
• Robotic Process Automation založený na IAM • Kontextualizovaný/adaptovaný IAM • IAM pro IoT • Rozvoj vztahů s hráči v PIM/PAM	IBM, Microsoft, Oracle, Broadcom, SailPoint, Ping Identity, Okta, Cisco, Saviynt
Threat Intelligence	
• Threat Intelligence Platform[4] • Forenzní analýza incidentu • Threat Hunting řešení	Palo Alto Networks, Anomali, IBM, SolarWinds, LogRhythm, FireEye, Looking Glass, AT&T Cyber Security, Kaspersky
Cloud Workload Protection (CWP)	
• Integrace CWP s Threat Intelligence službami • Bezpečnostní služby v oblasti CWP • Cloud Security Training	Palo Alto Networks, Check Point Software Technologies, McAfee, Cisco, Broadcom, VMware, Trend Micro, CrowdStrike
Služby v oblasti kybernetické bezpečnosti	
• Řízená detekce a odpověď • Bezpečnostní poradenství a GRC • Technické služby	Wipro, IBM, Dimension Data, NTT, DXC Technology, Capgemini, Accenture, PwC, KPMG

Zdroj: Internetové stránky konkrétních firem

[4] Zahrnuje mj. forenzní analýzu incidentu či managment bezpečnostních informací a událostí,

Tabulka 4: SWOT analýza obchodního prostředí skandinávských zemí v sektoru cloud computing a kybernetické bezpečnosti

Silné stránky	Slabiny
• rozvinutá infrastruktura datových center a rostoucí zájem je využívat • rozvinutá veřejná digitální infrastruktura včetně pokrytí celého regionu 5G sítí • vysoká konektivita, spojení optickými kabely do západní Evropy, severní Ameriky i Asie • vysoká počítačová gramotnost a pozitivní vztah k ICT • existence jasných vládních strategií digitalizace a systematická podpora rozvoje digitální ekonomiky • vysoký podíl vládních i soukromých investic do digitální infrastruktury • vysoké R&D výdaje do digitalizačních procesů • zájem o zajištění kybernetické bezpečnosti i využívání cloudových služeb ze strany státu i firem • nízké ceny energií, stabilní dodávky elektrické energie • finanční a politická stabilita	• vysoké ceny nemovitostí a vysoké nároky na mzdy • vysoká daň z příjmu • neznalost možností a využití cloud computing • banalizace kybernetických hrozeb, podceňování ztrát způsobených kybernetickými útoky, zejména mezi SME • u řady firem chybějící vize v oblasti digitalizace operací • nedostatek financí pro výdaje v oblasti zajištění kybernetické bezpečnosti či cloud computing, zejména mezi SME
Příležitosti	**Hrozby**
• jasné plány digitalizace veřejného sektoru a politik s jasně alokovanými zdroji • telemedicína a zajištění bezpečnosti dat pacientů • chytrá města a chytrá doprava • bezpečnost IoT • obavy z kybernetických útoků ze zahraničí v důsledku vstupu Švédska a Finska do NATO zvýšily poptávku po kybernetické odolnosti • nové obchodní modely využívající digitální komunikaci a služby formující se pod vlivem pandemie COVID a inovací v oblasti vnitrofiremní i vně-firemní komunikace • důsledné naplňování GDPR • poptávka po IT službách převyšuje počet IT expertů	• odlišná kultura řízení firmy • přísná legislativa, zejména v oblasti využívání ICT • vysoký počet inovativních start-upů, vysoce kompetitivní prostředí • vysoké nároky na služby, plnění podmínky uhlíkové neutrality

3. Úvod

Tato analýza se zabývá obchodními a investičními příležitostmi, které vznikají v souvislosti s rozvojem digitalizace ve Finsku, Dánsku, Norsku a Švédsku.[5] Zaměřuje se na sektor kybernetické bezpečnosti a cloud computing. Trh s IT službami se ve skandinávských zemích rozvíjí mimořádně rychle. Hlavními důvody jsou:

- dlouhodobá systematická vládní podpora digitalizace,
- příznivé legislativní prostředí a existence systému podpory výzkumu, vývoje a inovací v oblasti digitálních technologií,
- spolehlivost dodávek elektrické energie a její nízké ceny,[6]
- inovativní energetická řešení,
- rozvinutá infrastruktura a existující podmořské optické kabely spojující skandinávské státy se západní Evropou, severní Amerikou i Asií,
- kompetentní pracovní síla s vysokou digitální gramotností,
- dostatek prostoru pro budování nových zařízení, např. datových center,
- snadná dosažitelnost zákazníků,
- chladné klima i přístup k vodním zdrojům snižující náklady na chlazení IT zařízení,
- minimální rizika přírodních katastrof,
- politická stabilita a liberální transparentní ekonomické prostředí,
- výrobní kapacity i přenosová soustava počítající s nárůstem výroby a spotřeby elektrické energie, a
- regionální spolupráce a harmonizace norem a pravidel pro rozvoj digitálních procesů.

Severské trhy jsou důvěryhodné a poptávka po IT službách setrvale roste. Pro období 2021 až 2027 je růst odhadován na 4 % ročně. U některých segmentů IT služeb, např. datová centra, zajištění kybernetické bezpečnosti či cloud computing, je očekáván růst rychlejší, cca 7 až 12 %. Zákazníci ve skandinávských zemích poptávají analýzu velký dat, IoT a zjištění bezpečnosti a správy zařízení napojených na internet, umělou inteligenci, robotiku a cloud computing (SaaS, IaaS a optimalizaci multi-cloud). Skandinávští zákazníci chtějí rychleji a účinněji komunikovat s trhem

[5] Z pohledu cloud computing a zajištění kybernetické bezpečnosti je zajímavým trhem i Estonsko, to však není zahrnuto v této analýze.

[6] Nejnižší ceny elektrické energie jsou ve Švédsku, dále pak následuje Norsko a Finsko. V Dánsku je cena 10 MW dvakrát vyšší, než ve Švédsku.

a zákazníky (státní úřady s občany), optimalizovat náklady, redukovat počet pracovních sil a snížit uhlíkovou stopu. Střední a menší firmy však pro IT často nemají vlastní odborníky a poptávají tyto služby na trhu. Průzkum z roku 2022 (PA Consulting[7]) mezi skandinávskými firmami ukázal, že 43 % firem outsourcuje zajišťování kybernetické bezpečnosti. Co se týká využívání veřejných cloudových platforem, údaje z jednotlivých zemí se mírně liší: více než polovina norských firem uváděla, že v dalších dvou letech plánuje převést až 70 % svých činností do veřejných cloudových platforem, v Dánsku a Švédsku to bylo 34 %, ve Finsku 37 % firem (stávající situace viz graf 1).[8] Poptávku po digitalizaci umocnila pandemie Covid-19, závazek budování bezuhlíkové ekonomiky, který skandinávské společnosti berou vážně, a snaha skandinávských zemí stát se světovým technologickým centrem a pionýrem digitálních inovací.

Atraktivitu skandinávského trhu potvrzuje příchod nových investorů do regionu (datová centra zde vybudovaly či aktuálně staví např. Facebook, Google, AWS, Apple, Microsoft), resp. navyšování investic již přítomných investorů (např. Equinix a Interxion). V letech 2020 a 2021 byla ve Finsku, Dánsku, Norsku a Švédsku zřízena více než desítka nových datových center.[9] Na konci roku 2021 bylo v Dánsku v provozu 31 datových center, ve Finsku 23, v Norsku 25 a ve Švédsku 50, další desítka byla ve výstavbě napříč celým regionem.[10] Hybnou silou růstu v tomto segmentu je zejména rozvoj využívání cloudových služeb, big data a IoT jako monitorovací zařízení sloužící pro kontrolu výroby a distribuce elektrické energie z obnovitelných zdrojů, akvakulturu a monitoring rybích populací, chytrá města apod. Růst poptávky po cloud computing souvisí i s rozšiřováním nabídky služeb v této oblasti. Mezi nejaktivnější patří operátoři hyperscale datových center (např. Equinix či GreenMountain). Hlavní destinací investic do datových center bylo v letech 2020 a 2021 Dánsko (cca 30 % všech investic), Norsko, Švédsko i Finsko se nicméně snaží zvýšit svoji atraktivitu a různými daňovými i jinými pobídkami přilákat investory na své území.

Následující analýza je rozdělena do čtyř kapitol. Každá kapitola se věnuje jedné zemi a perspektivám trhu s cloud computing a zajištěním kybernetické bezpečnosti.

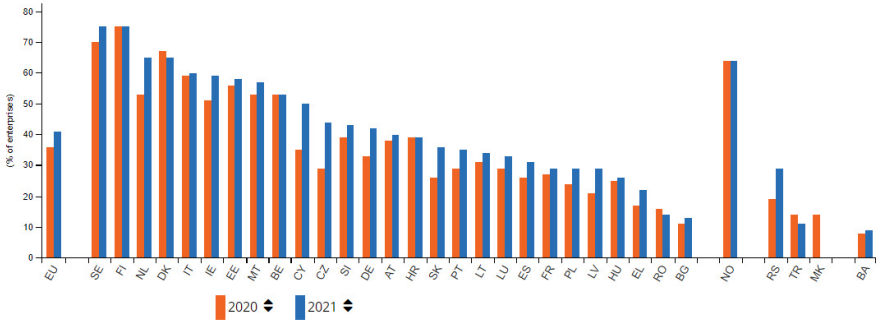
7 PA Consulting, 2022 Nordic IT Sourcing Study (www.paconsulting.com/insights/2022/2022-nordic-it-sourcing-study/).
8 PA Consulting (paconsulting.com/insights/2021/2021-nordic-it-sourcing-study/).
9 Baxtel (baxtel.com/data-center/nordics).
10 S&P Global Market Intelligence (www.vertiv.com/4ae18f/globalassets/documents/analyst-reports/451_reprint_nordicdcmkt_pt2_21oct2021_345291_0.pdf).

Tabulka 5: Srovnání hlavních socio-ekonomických ukazatelů a vývoje v oblasti digitální ekonomiky – ČR, Dánsko, Finsko, Norsko, Švédsko

	ČR	Dánsko	Finsko	Norsko	Švédsko
Počet obyvatel, 2021 (v milionech)	10,7	5,8	5,5	5,4	10,4
Počet obyvatel, odhad pro rok 2030 (v milionech)	10,7	6,0	5,6	6,0	11,1
HDP na hlavu, 2020 (v USD)	22933	61063	48755	67329	52274
HDP na hlavu v paritě kupní síly, 2020 (v USD)	41608	60229	50517	62644	55037
Pozice v žebříčku Doing Business, 2020 (pořadí a skóre)	41 (76,3)	4 (85,3)	20 (80,2)	9 (82,6)	10 (82,0)
Digital Economy and Society Index Ranking (EU-27 + Norsko)	18	1	2	5	3
Vyšší než základní digitální dovednosti (% osob)	26	49	50	51	46
Odborníci a odbornice v oblasti ICT (% osob v zaměstnání ve věku 15-74 let)	4,0	5,5	7,6	5	7,5
Celkové využití pevného širokopásmového připojení (% domácností)	83	85	57	90	84
Připravenost na 5G (přidělené spektrum jako % celkového harmonizovaného spektra 5G)	97	99	99	49	49
Skutečné užívání 5G, 2021 (%)	-	11	11	12	10
Integrace digitálních technologií, Data velkého objemu (% podniků)	9	27	22	19	19
Integrace digitálních technologií, Cloud (% podniků)	20	57	62	58	59
Uživatelé elektronické veřejné správy (% uživatelů internetu)	64	92	91	94	88
Global Cybersecurity Index, 2020 (max 100 bodů)	74,37	92,6	92,7	96,89	94,59

Zdroj: World Bank Indicators, Digital Economy and Society Index 2021, OECD Stats, Mezinárodní telekomunikační unie, statistické úřady příslušných zemí

Graf 1: Využití cloudových služeb v zemích EU (% firem, srovnání roku 2020 a 2021) (SE – Švédsko, FI – Finsko, DK – Dánsko, NO – Norsko[11])



Zdroj: Eurostat (ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises)

Tabulka 6: Skandinávie: Příklady stávajících a zamýšlených investic v oblasti datových center a souvisejících služeb (hyperscale, cloud, colocation, enterprise)

Datové centrum ve výstavbě	Investiční záměr oznámili
Hyperscale	
Švédsko: Facebook, HIVE Blockchain Technologies Dánsko: Yandex, Apple, Facebook	Baidu, Tencent, Xiaomi, Samsung, Huawei
Cloud	
Finsko: Google Dánsko: Google Švédsko: Google, AWS	Alibaba Cloud, IBM Softlayer, Rackspace, OVH, Oracle, Iron Mountain, SAP
Colocation	
Finsko: Equinix, Telia, Hetzner, HermanIT, Ficolo Dánsko: Digiplex, Interion, Global Connect Norsko: Digiplex, Green Mountain, Global Connect, Lefdal Mine, Orange Švédsko: Digiplex, Etix, Hydro 66, Global Connect	Global Switch, China Telecom, GDC, Telehouse KDDI, China Mobile Intl, Cyxtera, Cyrusone
Enterprise	
Finsko: Fujitsu, CGI Švédsko: Ericsson	

Zdroj: ComputerWeekly[12] a webové stránky příslušných firem

[11] Norsko a další čtyři země (Republika Srbská, Turecko, Severní Makedonie a Bosna a Hercegovina) jsou zařazeny na konec grafu, nejsou totiž členskými státy EU.

[12] ComputerWeekly, 10.10. 2021 (computerweekly.com/feature/The-second-coming-The-Nordic-

4. Dánsko

Dánsko tvoří Jutský poloostrov a přilehlé ostrovy v Baltském moři, dále také Grónsko a Faerské ostrovy. Grónsko a Faerské ostrovy mají značnou míru autonomie. V této analýze se věnujeme obchodním příležitostem v centrálním Dánsku, autonomní území jsou vynechána. Evropské území Dánska dosahuje cca poloviny rozlohy ČR (43 tisíc km^2), počet obyvatel stagnuje a dosahuje 5,8 milionu.

Dánsko je jednou z politicky i ekonomicky nejstabilnějších zemí na světě s velmi dobrými ekonomickými vyhlídkami, a to i přes mírný hospodářský pokles spojený s pandemií Covid-19. V průběhu roku 2022 již dánská ekonomika vykazovala mírný růst. Dánsko je členem EU. Nepřijalo sice euro, ale dánská koruna je na euro pevně navázaná a země splňuje všechna kritéria pro přijetí eura tak, aby jej kdykoliv mohla přijmout. O přijetí eura musí rozhodnout lidové referendum. Dánové již hlasovali dvakrát (1992 a 2000) a zatím dvakrát přijetí eura odmítli. Grónsko není členem EU, resp. nevztahují se na něj práva a povinnosti člena EU.

Dánsko je ekonomicky i politicky nediskriminující, má silný systém sociální podpory. To s sebou nese i vysoké daňové zatížení. Pro zahraniční subjekty existuje minimum omezení, např. nemohou ze 100 % vlastnit naleziště ropy a zemního plynu či rekreační bydlení na dánském pobřeží.

4.1 Ekonomická a socio-demografická charakteristika

Dánská společnost je vzdělaná, angličtina je druhým jazykem většiny populace. Významným zaměstnavatelem je veřejný sektor (asi 25 % pracovních sil). V zemi existují zaměstnanecké svazy a odbory, které mají silnou vyjednávací pozici. Za klíčové momenty dánského ekonomického úspěchu jsou považovány digitalizace všech sfér života a ekonomiky, vysoká míra participace žen na trhu práce, integrace uprchlíků do společnosti a ekonomické činnosti a systematická výstavba a modernizace infrastruktury (OECD 2021).

V průběhu pandemie Covid přijala vláda řadu opatření podporujících návrat země k běžnému společenskému

datacentre-market-comes-of-age).

i ekonomickému životu. Pandemii Dánsko zvládlo bez větších obtíží, a to i díky vysoké míře digitálních kompetencí společnosti. Země je exportní ekonomikou, cca 55 % HDP je tvořeno vývozem. Významná část ekonomiky je spojená s námořní přepravou. Hlavními dánskými obchodními partnery jsou USA, Německo, Švédsko a Velká Británie. Dánsko vyváží zejména výrobky s vysokou přidanou hodnotou a služby, high-tech průmyslová výroba je však závislá na dovozu nerostných surovin. V poslední době v Dánsku roste poptávka po IT pracovnících ze zahraničí, IT odborníků z řad Dánů se nedostává.[13]

Dánské vlády se dlouhodobě shodují na podpoře několika sektorů, označovaných za pilíře dánské ekonomiky: sofistikované a čisté technologie, medicína a přírodní vědy, výroba potravin, námořní přeprava a design a inovace.

4.2 Infrastruktura ICT a potenciál pro digitalizaci ekonomiky a společnosti

Dánsko rozvíjí digitalizaci již déle než jedno desetiletí, a tomu odpovídá i rozvinutá institucionální struktura a legislativa, byť v sektoru kybernetické bezpečnosti nedostatky najdeme. Dánsko patří k nejdigitalizovanějším společnostem na světě (na 100 obyvatel připadá 32,7 přístrojů napojených na internet), tam, kde digitalizace výrazněji zaostávala (školství), ji nastartovala pandemie Covid. Dnes nenajdeme v Dánsku sektor, který by byl z digitalizace vyloučen – roste využívání big data, cloudových služeb i umělé inteligence, a to ve veřejném i soukromém sektoru.[14] Společnost napříč věkovými i společensko-ekonomickými skupinami sdílí konsenzus o potřebě pokračovat v digitalizaci. Vláda ve spolupráci s místními úřady zajišťuje pro digitálně méně zdatné obyvatele technologickou podporu a poradenství. Na úrovni obcí byla zřízena technická centra podpory, která slouží všem občanům pro všechny digitální služby. Tyto služby jsou bezplatné.

Rozvoj digitalizace v Dánsku je založen na úzké spolupráci mezi vládou, firmami, univerzitami a občanskou společností. Nejrychleji roste poptávka po zajištění kybernetické bezpečnosti. Naléhavost této poptávky souvisí mj. s tím, že IT systémy dánských firem i úřadů byly opakovaně napadeny.

13 V současné době se kybernetické bezpečnosti věnují v Dánsku dvě univerzity: Technická univerzita v Dánsku a Univerzita v Aalborgu (obě mají magisterský obor kybernetická bezpečnost a každý ročně přijme 60 studentů).

14 Srovnej např. Strategie pro digitální zdraví 2018-2022 (https://sundhedsdatastyrelsen.dk/da/diverse/download); více na Danish Health Data Authority (https://sundhedsdatastyrelsen.dk/da/english).

4 Dánsko

Dánská vláda hodnotí rizika kyberútoků a kybernetické špionáže jako velmi vysoká, a to směrem ke všem dánským entitám a systémům. Podle údajů úřadů se nicméně dánským entitám daří útokům většinou čelit a strategická infrastruktura země zatím nebyla zasažena vážnějším útokem, resp. útoky i pokusy o kybernetickou špionáž se podařilo zhatit. V roce 2020 hlásilo ransomwarové útoky nebo další typy kybernetické kriminality několik hotelových řetězců, dopravní společnosti (např. Maersk), farmaceutické firmy i dánský parlament. Většina útoků pocházela ze zahraničí (KLDR, Rusko, Čína), nicméně dánští hackeři jsou také aktivní.[15] S rozšířením práce z domova v době pandemie Covid se dánské autority obávají, že se počet útoků bude zvyšovat, neboť míra zabezpečení domácích zařízení je výrazně nižší, než u sítí firemních či státních. Další obavy z útoků zvyšuje rozšíření 5G sítí, rostoucí využití IoT i digitalizace a automatizace výrobních procesů. Konečná aukce pro 5G sítě proběhla v roce 2021. Firmy, které získaly podíl na budování 5G sítí, musejí do roku 2023 zajistit přístup 60 % populace k 5G sítím, do roku 2025 pak 75 % obyvatel.

Dánské plány na digitalizaci nejsou jen deklaratorní. Digitální infrastruktura se v Dánsku rozvíjí rychle a s podporou vlády. Státní investice do digitalizace jsou ročně cca 75 milionů dánských korun a tato částka je předvídána každoročně pro období do roku 2025. Vláda také vytvořila celou řadu pobídek pro firmy. Parlament přijal celý systém zákonů upřesňujících, jakým způsobem a v jakých sektorech bude digitalizace probíhat. Od roku 2014 musejí všechny vládní úřady dodržovat normu ISO/IEC 27001 o zásadách informační bezpečnosti. Dánsko respektuje normy kybernetické bezpečnosti zaváděné EU a na posílení kybernetické bezpečnosti spolupracuje s několika zeměmi EU. Společně s Nizozemím se podílí na posilování kybernetické bezpečnosti v rámci NATO a obě země spolupracují i v oblasti posílení interkonektivity maritimních systémů a kybernetické bezpečnosti námořní dopravy.[16]

[15] Danish national strategy for cyber and information security 2022-2024 (en.digst.dk/strategy/the-danish-national-strategy-for-cyber-and-information-security/).

[16] Kybernetické útoky na své počítačové systémy hlásila opakovaně největší dánská kontejnerová přepravní společnost Maersk (Guardian: digitalguardian.com/blog/cost-malware-infection-maersk-300-million nebo safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/).

4.3 Digitalizace ekonomiky a veřejných politik: plány a cíle

Dánsko má propracovaný systém plánů rozvoje, strategií a podpory digitalizace společnosti, ekonomiky i správy věcí veřejných. V roce 2021 Dánsko zavedlo systém mandatorních digitálních služeb a komunikace. Ty zahrnují např. povinnost občanů a firem využívat digitální komunikaci se státními úřady v oblastech jako systém sociální podpory či daňová přiznání.[17] V roce 2022 systém povinné digitální pošty využívalo 92 % občanů a 100 % firem (AfD 2022). Postupně jsou digitalizovány legislativa, politická komunikace i veřejná správa včetně možnosti vydávání digitálních dokladů prostřednictvím aplikací v chytrých telefonech (např. od listopadu 2020 jsou takto vydávány řidičské průkazy).

Průběh dánské digitalizace a vznikající legislativu určuje několik dokumentů:

- - Strategie pro dánský digitální rozvoj 2022-2025,[18]
- Strategie pro dánskou „Tech Diplomacy“ 2021-2023,[19]
- Strategie pro řízení ICT v gesci centrální vlády „A Solid ICT Foundation 2017“,[20]
- Národní strategie pro umělou inteligenci,[21]
- Národní strategie pro kybernetickou a informační bezpečnost 2022-2024,[22]
- Bílá kniha o digitální architektuře veřejného sektoru,[23]
- Strategie pro ICT management v ústřední vládě 2017, a
- Strategie pro digitální zdravotnictví 2018-2022.

Nové dokumenty a legislativa vznikají dle potřeby, někdy však se zpožděním.

4.4 Hlavní aktéři

Hlavní hybatelem digitalizace jsou vláda regionální úřady i municipality. Tito aktéři se v roce 2017 shodli na vytvoření společné digitální architektury.[24]

17 Seznam aktuálně existujících mandatorních digitálních služeb a jejich charakteristika jsou dostupné na stránkách dánské Agentury pro digitalizaci (en.digst.dk/digitisation/).
18 https://en.digst.dk/policy-and-strategy/digital-strategy/
19 Ministerstvo zahraničních věcí, Dánsko (techamb.um.dk).
20 https://en.digst.dk/policy-and-strategy/strategy-for-ict-management/
21 https://en.digst.dk/policy-and-strategy/denmark-s-national-strategy-for-artificial-intelligence/
22 en.digst.dk/strategy/the-danish-national-strategy-for-cyber-and-information-security/
23 https://arkitektur.digst.dk/node/529
24 Agentura pro digitalizaci (https://eforvaltningsdagarna.se/wp-content/uploads/sites/9/FDA-English-eF%C3%B6rvaltningsdagarna-2018-v1.pdf).

4 Dánsko

Vláda vytváří pobídky pro firmy a občany, zajišťuje společně s parlamentem legislativní zázemí digitálního přechodu a zřizuje instituce řídící jednotlivé segmenty digitalizace. Firmy pak postupně, a pandemie Covid tento proces urychlila, digitalizují vnitrofiremní procesy i komunikaci se zákazníky a státem.

Hlavními aktéry digitalizace jsou:

- Agentura pro digitalizaci (spadá pod Ministerstvo financí a koordinuje proces digitalizace mezi vládními úřady, zajišťuje také komunikaci s veřejným sektorem a firmami a zjišťuje systém podpory a vzdělávání v oblasti digitalizace),
- Agentura pro digitální vládnutí (spadá pod Ministerstvo financí a je sdílenou agenturou zajišťující IT servis pro všechny vládní úřady[25]),
- Vládní výbor pro ICT operace (mj. pod něj spadá Fórum pro informační bezpečnost – vyjednávací platforma zahrnující zástupce vlády, odborů, firem a občanské společnosti),
- Agency for Data Supply and Efficiency,
- Data Protection Agency,
- Centrum pro kybernetickou bezpečnost (podléhá dánské Vojenské zpravodajské službě).

Vláda vytvořila několik pobídek a clustrů navazujících na digitalizační cíle. Mezi hlavní platformy sdružující firmy a autority zabývající se digitalizací a kybernetickou bezpečnostní patří CenSec[26], Danish Cyber Security Hub[27] , DigitalLead[28] a FinTech[29] . CenSec je platformou spolupráce mezi firmami, vládou a výzkumem. Soustředí se zejména na rovinu politiky a propojení kybernetické bezpečnosti s národní bezpečností. Cyber Security Hub sdružuje start-upy rozvíjející služby v oblasti kybernetické bezpečnosti.[30] DigitalLead je platformou firem a start-upů zabývajících se kybernetickou bezpečností, umělou inteligenci a IoT. FinTech sdružuje firmy a podporuje start-upy, které se zabývají využitím technologií ve finančních službách. Všechna čtyři uvedená uskupení pravidelně pořádají workshopy a semináře pro veřejnost i firmy z oblasti digitalizace a prezentují obchodní příležitosti v oblasti IT.

Jako poradní platforma vzniklo mezi firmami, vědci, občanskou společností, odbory, municipalitami a regiony v roce 2021 Partnerství pro digitalizaci. Partnerství se podílí na přípravě strategických dokumentů pro digitalizaci země. Další platformou pro diskusi o digitalizaci, včetně např. účasti na připomínkovém řízení k příslušné

25 en.digst.dk
26 censec.dk
27 cyberhub.dk
28 digitallead.dk/english/
29 copenhagenfintech.dk
30 Cyber Hub (cyberhub.dk/danish-cyberstartups-overview/danish-cyberstartups/).

legislativě, je Dánská koalice pro digitální dovednosti a pracovní místa. Sdružuje státní, firemní i nestátní aktéry s cílem zajistit celoživotní digitální vzdělávání.

4.5 Současné trendy a příležitosti

Dánsko vede v mnoha žebříčcích digitalizace i plánů a strategií na prohlubování a rozšiřování tohoto procesu. Největším spotřebitelem IT služeb je stát, kontinuálně však roste i zájem korporátního sektoru. Z tohoto pohledu je dánský trh velmi perspektivní a poskytuje celou řadu obchodních a investičních příležitostí. OECD i další aktéři odhadují, že objem dánského trhu v oblasti digitálních služeb se do roku 2025 zdvojnásobí. Tato analýza se zaměřuje zejména na oblast kybernetické bezpečnosti a cloudových služeb. Právě v těchto oblastech se možnosti a příležitosti rozvíjejí nejrychleji.

Dánská vláda i vnější pozorovatelé mají za to, že digitalizace bude v následujících pěti letech probíhat zejména v sektoru finančních služeb, námořní přepravě a zdravotnictví, zejména zpracování dat pacientů, telemedicíny a diagnostiky. Vysoký je zájem o posílení kybernetické odolnosti komunikace, operací a systémů. Dánská vláda alokovala více, než dvacet milionů dánských korun na posílení kybernetické bezpečnosti všech systémů a sektorů v zemi. Významné investice do kybernetické bezpečnosti jsou očekávány i ze strany domácích firem, které nejen že musejí digitalizovat v souvislosti s požadavky státu, ale také musejí vyhovět požadavkům trhu a změnám, ke kterým došlo v době pandemie Covid.

Větší využití IT nástrojů a technologií je podporováno i v oblastech jako rozvoj bezuhlíkové ekonomiky, environmentálně šetrných systémů a infrastruktury. Roste také využití různých typů cloudových služeb.[31] Ve firmách s minimálně 10 zaměstnanci narostly v letech 2018 až 2020 prakticky všechny typy využití cloud computing: nákup jakýchkoliv cloudových služeb využívaných prostřednictvím internetu (nárůst o 10 %), nákup e-mailu jako cloudové služby (15 %), nákup kancelářského SW jako cloudové služby (16 %), nákup úložiště jako cloudové služby (15 %) a nákup CRM-SW jako cloudové služby (6 %).

Dalšími sektory, kde prudce narůstá digitalizace, a tedy i poptávka po IT službách, jsou doprava (rozvoj autonomních vozidel), námořní přeprava, zdravotnictví (dánské zdravotnictví patří k nejdigitalizovanějším v EU; více viz Danish Health Data

[31] Dánský statistický úřad (www.statbank.dk/ITAV5).

Authority[32]) a finanční služby (bezpečnost finančních služeb, přechod na digitální měnu). Poptávka je také po zjištění IT architektury pro digitální komunikaci napříč sektory a systémy

Dánské firmy i státní autority budují vlastní IT zázemí, nicméně roste i objem outsourcovaných digitálních služeb. Dánské firmy a výzkum jsou nejsilnější v kryptografii, zajištění bezpečnosti sítí a bezpečnosti použití AI. Rozvoj trhu s digitálními službami zpomaluje mj. nedostatečná legislativa definující kybernetickou bezpečnost a kybernetické útoky, banalizace rizik kybernetických útoků, chybějící standardy pro zajištění kybernetické bezpečnosti organizací, nedostatek IT odborníků a neznalost možností cloud computing.

4.6 Vstup na trh

Dánsko je otevřeným, liberálním a inovativním trhem s minimem překážek pro vstup. Dodržuje principy liberalizace obchodu stanovené OECD i WTO. Veškeré registrační a licenční procesy jsou digitalizované, agenda registrací a udělování licencí spadá pod Danish Business Authority[33]. Pro zahraniční investory zřídilo Ministerstvo zahraničí službu „Invest in Denmark". Ta poskytuje zahraničním firmám podporu a bezplatně[34]. Grónsko a Faerské ostrovy mají vlastní systém podpory zahraničních investorů.

Dánsko je k zahraničním investorům a obchodníkům férové, pro zahraniční investory a obchodníky platí stejné podmínky jako pro domácí firmy, jeho instituce jsou hodnocené jako jedny z nejtransparentnějších a nejfunkčnějších na světě. Zákonná opatření jsou publikována na internetových stránkách parlamentu[35], ministerstva publikují příslušné právní úpravy na svých internetových stránkách (zpravidla ve dvou jazycích – dánsky a anglicky).

Všechny investiční a obchodní aktivity musejí splňovat přísné ekologické podmínky a podniky platí zvláštní daň odpovídající ekologické zátěži, kterou produkují konkrétní výrobní procesy. Většina dánských IT firem se hlásí k podpoře budování uhlíkově neutrální ekonomiky.

Obchodní vztahy mezi ČR a Dánskem jsou budovány dlouhodobě, nicméně mezi oběma zeměmi nedochází k obchodům velkého objemu. Česko-dánské obchodní vztahy jsou řízeny v souladu s legislativou EU.

32 sundhedsdatastyrelsen.dk/da/english
33 www.virk.dk
34 www.investindk.com
35 Folketinget (www.ft.dk).

5. Finsko

Finsko je politicky i socio-ekonomicky stabilní a liberální země s vysokým HDP na hlavu. Stejně jako jiné ekonomiky, i finská ekonomika byla zasažena vlnou pandemie COVID a zpomalila. Podle finských dat i dat OECD (2021b) se země již vrací do normálu ve většině sektorů ekonomiky, nejpomaleji dochází k obnově mezi na služby orientovanými SME. Země je členem Evropské unie, po ruském útoku na Ukrajinu země podala přihlášku do NATO. Helsinky prozatímně uzavřely obrannou dohodu s Velkou Británií, která by v případě útoku ze strany Ruska Finsku pomohla. Finsko se však kromě vojenského útoku připravuje i na další hrozby jako hackerské a jiné útoky na strategickou infrastrukturu, krádeže dat ze serverů finských institucí a firem a na kybernetickou špionáž. Není zatím jasné, jak ekonomiku země zasáhne rusko-ukrajinská vláka, resp. ruská odvetná opatření vůči Helsinkám za snahu země vstoupit do NATO.

5.1 Ekonomická a socio-demografická charakteristika

Finsko, podobně jako ostatní skandinávské země, buduje moderní ekonomiku směřující k využití nejmodernějších technologií a digitálních procesů. Jako mateřská země firmy Nokia i dalších významných technologických firem má Finsko generace IT vzdělaných pracovních sil. Finsko je sice nejchudší ze skandinávských zemí a populačně nejmenší (5,5 milionu obyvatel), i tak je však HDP na hlavu více než dvakrát vyšší než v České republice. Země má stabilní příjmy, vyspělou, na služby orientovanou ekonomiku (tvoří 70 % HDP) a vzdělanou populaci. Finové jsou digitálně gramotní a podporují rozvoj a využívání moderních technologií. Podle Finského statistického úřadu[36] využívá internet 93 % lidí a chytrý telefon 88 % lidí.

Finsko není typickou cílovou destinací migrace, jeho společnost a pracovní trh jsou nejintenzivněji ovlivněny pracovní migrací z okolních zemí – Estonska, Ruska a Polska. Největší skupinou obyvatel cizího původu jsou ve Finsku Estonci. Finská společnost má silný integrační potenciál a je velmi otevřená. Finové v posledních dvou dekádách v různých výzkumech

[36] Finský statistický úřad (www.stat.fi/tup/suoluk/suoluk_digitalisaatio_en.html).

veřejného mínění opakovaně potvrzovali spokojenost s politickou i ekonomickou situací v zemi a deklarovali vysokou míru politické důvěry vůči státu (OECD 2021d).

5.2 Infrastruktura ICT a potenciál pro digitalizaci ekonomiky a společnosti

Finsko za poslední dekádu vyvinulo silný sektor datových center se záměrem podpořit růst pracovních míst vázaných na IT infrastrukturu a služby i růst HDP. Již v současnosti patří tzv. širší Helsinky ke skandinávským regionům s nejhustější koncentrací firem zabývajících se kybernetickou bezpečností. Finsko má dobře propracovanou národní strategii kybernetické bezpečnosti, solidní regulační rámec pro cloud computing, služby v oblasti kybernetické bezpečnosti a provozu datových center a aktivně fungující spolupráci mezi firmami i veřejným sektorem. Silné postavení země v datovém průmyslu souvisí s politicky a ekonomicky stabilním prostředím, vzdělanou IT orientovanou pracovní silou (IT zaměstnává cca 7 % pracovních sil), tradicí technologického výzkumu, vývoje a výroby v zemi (Nokia), silnými firemními koalicemi a dohodami podporujícími digitalizaci (bankovní služby) a dobudováním arktického kabelového spojení, které dělá z Finska jeden z nejsilnějších datových mostů mezi Evropou a Asií.[37]

Finský systém digitální identity a digitální identifikace občanů pro služby státu, firem i bankovní platby jsou jedny z nejlepších na světě. Digitální ID pro občany by mělo začít fungovat v roce 2023.[38]

Nejsilnější jsou v procesu přijímání a zavádění cloud computing a opatření kybernetické bezpečnosti státní úřady, banky a velké firmy, největší problém vidíme u SME. Ty nemají ani dostatek zdrojů, ani znalosti, na jejichž základě by mohly komplexně zavádět a efektivní využívat cloud computing a kyberbezpečnostní opatření.

[37] CINIA (www.cinia.fi/en/solutions/international-connectivity/arctic-connect).

[38] Digital and Population Data Services Agency, Finsko (dvv.fi/en/identification) a BiometricUpdate.com (/www.biometricupdate.com/202201/new-national-authentication-service-and-digital-identity-announced-for-finland).

5.3 Digitalizace ekonomiky a veřejných politik: plány a cíle

Finsko je jedním z pionýrů digitalizace, a to jak v sektoru veřejných politik, tak v korporátní sféře. Státní úřady intenzivně pracují na digitalizaci vlastní práce i komunikace s občany a firmami již více než jedno desetiletí, což je znatelné jak na existenci programových a strategických dokumentů a státních investicích, tak na nově schválené legislativě. Zájem o digitalizaci vnitrofiremních i vně-firemních procesů lze ve Finsku zaznamenat jak u velkých firem, tak SME. Zatímco v EU komunikuje digitálně se státem průměrně 52 % obyvatel, ve Finsku je to téměř 90 % (Evropská komise 2021b). Helsinky významně rozvíjejí i digitální komunikaci v regionu; jedná se např. o e-ID (zavedení plánováno v roce 2023) či e-řidičský průkaz (již zaveden) jako dokumenty uznávané na základě dohody ve skandinávských, a pobaltských zemích[39] (významným partnerem v digitalizaci je pro Finsko sousední Estonsko, jehož pionýrské digitální počiny jsou pro Finsko v mnoha ohledech modelem). Plně digitalizovaný je již systém veřejných zakázek.

Země, i v důsledku zkušeností z pandemie Covid, reagovala vytvořením nových strategických dokumentů, resp. inovací starších:

- čtvrtý „Open Government Action Plan" pro období 2019 až 2023,
- Program národní architektury pro digitální služby (2017),
- Vládní zpráva o informační politice a umělé inteligenci (schválená parlamentem v roce 2019),
- Strategie pro obnovu veřejného vládnutí pro období 2020 až 2030 (2020),
- Vládní rozhodnutí o digitální bezpečnosti pro veřejný sektor (2021/Haukka) včetně plánu implementace,[40]
- Klimatická a environmentální strategie pro informační a komunikační technologie (2021),
- Národní strategie pro kybernetickou bezpečnost (2019), a
- Program pro umělou inteligenci 2020 až 2022 s vizí do roku 2025[41] (tzv. AuroraAI Programme).

[39] Více viz Nordic Co-operation (www.norden.org/en/news/more-efficient-co-operation-digitalisation).

[40] Dokumenty včetně příslušných legislativních úprav jsou dostupné v anglickém jazyce na webu Ministerstva financí Finska (vm.fi/en/information-security-and-cybersecurity).

[41] V jakých segmentech plánuje vláda nasadit AI viz webové stránky Ministerstva financí Finska (vm.fi/en/national-artificial-intelligence-programme-auroraai).

5.4 Hlavní aktéři

Hlavním aktérem v procesech digitalizace je stát, dále pak korporátní sektor a platformy umožňující setkávání státních úřadů s firmami, univerzitami i občanskou společností. Státní úřady určují rámce digitalizace v sektoru veřejných politik i v korporátním sektoru. Stát je také významným zákazníkem ICT služeb a s ohledem na digitalizační plány vládních úřadů, stát sám potřebuje fungující legislativu upravující poskytování digitálních služeb a výstavbu digitální infrastruktury. Hlavními hráči v procesech digitalizace jsou:

- Ministerstvo financí a Public sector ICT department,
- Ministerstvo dopravy a komunikací,
- Poradní výbor pro bezpečnou vládní síť,
- Strategická řídící skupina pro digitální bezpečnost ve veřejném sektoru
- Digital and Population Data Service Agency a v jejím rámci Public Sector Digital Security Managment Board (VAHTI), a
- vládní centrum pro ICT Valtori.

Vedle uvedených aktérů se na procesech digitalizace, jejich rozvoji a úpravě podílí Agentura pro regulaci komunikace (TAFICOM), do jejíž gesce spadá bezpečnost informačních sítí a kybernetická bezpečnost a v jejímž rámci bylo zřízeno Národní centrum pro kybernetickou bezpečnost Finska (NCSC-FI)[42]. Dále to jsou platformy vznikající na základě spolupráce korporátního i veřejného sektoru a univerzit: Finnish Information Security Cluster[43] sdružující firmy z oblasti kybernetické bezpečnosti, program Digital Trust Finland[44] a Data Breach Support,[45] ústřední vládní platforma pomáhající jedincům či entitám při zneužití či krádeži osobních dat, či obecněji, obětem digitálních trestných činů.

5.5 Současné trendy a příležitosti

Finské vlády, společnost i korporátní sektor dlouhodobě podporují digitalizaci ve všech společenských a ekonomických oblastech. Roste zájem o multi-cloudové a hybridní cloudové strategie; roste poptávka po příslušné infrastruktuře i po službách a poradenství. Od roku 2019 roste počet ruských

42 www.kyberturvallisuuskeskus.fi/en
43 FISC (www.fisc.fi/about-fisc/).
44 Business Finland (www.businessfinland.fi/en/do-business-with-finland/explore-key-industries/ict-digitalization/digital-trust).
45 Data Breach Support (tietovuotoapu.fi/en/).

hackerských útoků na finské cíle Podle údajů Helsinek se po ruském útoku na Ukrajinu a poté, co země oznámila zájem o vstup do NATO, kybernetické útoky z Ruska zintenzivnily.[46] Od února 2022 tak poptávka po ochraně dat a poradenství v oblasti kybernetické bezpečnosti roste ještě rychleji. V této souvislosti veřejný i soukromý sektor začaly výrazněji preferovat využívání datových center na finském území. V zemi najdeme několik desítek datových center; provozována jsou jak velkými hráči (centrum Google v Hamině), tak lokálními firmami. Největší koncentraci datových center a poskytovatelů cloudových služeb najdeme v oblasti tzv. širších Helsinek.

Na finském trhu se však nedostává IT odborníků. S ohledem na GDPR, existující finskou legislativu i globální politicko-bezpečnostní a energetickou situaci se finské firmy i úřady zdráhají outsourcovat tyto služby a poradenství mimo prostor EU. Ve Finsku se tak pro české firmy otevírá řada příležitosti: služby IaaS, Open Stack platformy pro cloud computing, bezpečnostní software pro chytré telefony, systémy řízení přístupu k administrátorským a jiným privilegovaných účtů (PAM) a Unified Threat Management. Mezi silné stránky finských firem patří šifrování, ochrana osobních dat, předcházení hrozbám a Identity Management Solutions.

Aktuální poptávky ze sektoru datových center a digitalizace uveřejňuje agentura Invest in Finland[47] a jednotlivá regionální obchodní a investiční centra[48] i individuální města.[49] Podporu pro zahraniční obchodníky a investory poskytuje agentura Business Finland[50]. Tato agentura otevřela v roce 2021 projekt „5G Project Initiative“ jehož cílem je podpořit vývoj 5G technologií, které by Finsko mohlo vyvážet.[51]

46 Deník Yle (yle.fi/news/3-12380786; yle.fi/news/3-12443701), Reuters (www.reuters.com/world/europe/finnish-swedish-security-services-warn-russian-meddling-over-expected-nato-bids-2022-04-27/).

47 www.businessfinland.fi/en/do-business-with-finland/invest-in-finland/business-opportunities/data-centers

48 Finské regiony a větší města mají vlastní investiční agentury. Helsinky např. Invest in Helsinki (www.myhelsinki.fi/en/business-and-invest/invest-in-helsinki; www.helsinkipartners.com/what-we-offer/invest-in-helsinki/).

49 Příkladem je zapojení finských měst do evropského projektu AiRMOUR (airmour.eu), v jehož rámci se testuje nasazení dronů při poskytování lékařské péče a zjištění akutních zásahů integrovaného záchranného systému. Samotné Helsinky pak zřídily organizaci Forum Virium (forumvirium.fi/en/), jejímž cílem je umožnit firmám testovat autonomní systémy v praxi městského provozu.

50 www.businessfinland.fi/en/do-business-with-finland/home

51 ComputerWeekly.com (www.computerweekly.com/news/252500568/Business-Finland-rolls-out-5G-industrial-initiative), Business Finland (www.businessfinland.fi/en/do-business-with-finland/invest-in-finland/business-opportunities/ict-digitalization/5g-product-development).

5.6 Vstup na trh

Finsko by se podle vládních vizí mělo stát evropským technologickým centrem, a to zejména v oblasti robotiky, 5G a AI. , Ve srovnání s ostatními skandinávskými státy má Finsko nejnižší korporátní daňové zatížení a nejvyšší daňové zvýhodnění pro výzkum a vývoj v oblasti IT. Finská vláda navíc v roce 2021 vytvořila řadu pobídek pro domácí i zahraniční firmy s cílem podpořit rozvoj IT segmentu ekonomiky (daňové úlevy, daňové prázdniny atd.).

Země je členem EU a je liberální otevřenou ekonomikou, k investorům a obchodníkům ze zemí EU se chová stejně jako k finským entitám. Největší finští obchodní partneři jsou Německo, Švédsko, Dánsko a Estonsko. Více než polovina zahraničního obchodu země směřuje na trh EU. Obchodní vztahy mezi ČR a Finskem jsou budovány dlouhodobě, nicméně mezi oběma zeměmi nedochází k obchodům velkého objemu. Česko-finské obchodní vztahy jsou řízeny v souladu s legislativou EU.

6. Norsko

Norsko se po druhé světové válce stalo jednou z nejrozvinutějších a nejbohatších zemí světa. Norský ekonomický zázrak souvisí se zahájením těžby ropy a zemního plynu, rostoucí cenou obou komodit a moudrým a prozíravým norským přístupem k investování zisků z prodeje fosilních paliv. Norsko je dnes moderní, energeticky soběstačnou ekonomikou s rovnoměrnou distribucí příjmů ve společnosti. Země je také jedním z největších mezinárodních dárců, a to jak prostřednictvím OSN, tak prostřednictvím vlastní rozvojové agentury. Norsko není členem EU, mj. i proto, že se chce vyhnout roli čistého plátce a přelévání financí prostřednictvím fondů EU. Země je však součástí Evropského sdružení volného obchodu a je členem Evropského hospodářského prostoru a Schengenského prostoru.

6.1 Ekonomická a socio-demografická charakteristika

Norská ekonomika kombinuje prvky liberálního trhu s uměřenými vládními intervencemi. Stát kontroluje klíčové strategické sektory jako těžba a zpracování ropy a zemního plynu. Má také podíl v řadě velkých firem. Vedle fosilních paliv má Norsko další energetické zdroje, zejména se jedná o hydroenergii a využití přílivové energie. Patří také k zemím s dostatečnými zásobami minerálů. Mezi klíčové pilíře ekonomiky patří lodní průmysl, těžba a zpracování ropy a zemního plynu a chov ryb. V posledních desetiletích také roste podíl služeb a výzkumu a vývoje na výkonu ekonomiky. Mezi nejrychleji rostoucí oblasti posledních let patří telemedicína, biotechnologie, čisté technologie a ICT.

Norská společnost patří k hodnotově stabilním, vzdělaným a bohatým národům se silným vztahem k životnímu prostředí a vazbou na demokratické a liberální hodnoty. Norové jsou digitálně gramotní a k digitálním procesům otevřenou společností. S tím, jak postupuje digitalizace veřejné politiky a komunikace mezi státem a občany, dbá vláda na digitální vzdělávání. V roce 2014 byl zahájen projekt celoživotního digitálního vzdělávání s cílem zahrnout celou norskou populaci a umožnit jednotlivým generacím se průběžně seznamovat s IT inovacemi

(NMLGM 2021). Navzdory vysoké digitální gramotnosti Norů se na pracovním trhu nedostává IT odborníků. Vláda v roce 2015 přijala zvláštní program podpory ICT studijních oborů, což by mělo během několika let uvést na trh až 1600 nových IT odborníků. Studenti prvních ročníků budou končit studium v letošním akademickém roce, tj. 2021/2022. Z vládních a univerzitních analýz vyplývá, že ani toto navýšení studijních míst nepokryje potřebu – v roce 2022 by na norském pracovním trhu mělo podle odhadů chybět 5 tisíc IT odborníků.

6.2 Infrastruktura ICT a potenciál pro digitalizaci ekonomiky a společnosti

Norsko má výbornou konektivitu; dobudována je síť vysokorychlostních podmořských optických kabelů směrem do západní Evropy (Frankfurt, Londýn, Amsterdam a Paříž) i USA. Budováno je spojení do Kanady. Norsko se může napojit na arktický kabel spojující Finsko s asijskými státy. Pandemie Covid, resp. přechod na práci z domova, digitalizace zdravotnictví[52] a digitalizace komunikace téměř vyčerpaly volné kapacity IT infrastruktury a její technologické možnosti. Vláda tak v roce 2021 zahájila nové investice do IT infrastruktury (NMLGM 2021). V současné době má přístup k vysokorychlostnímu internetu 90 % Norů. Vládní cíl je do dvou let 100 % populace. Jak ukazují světová i severská srovnání (tabulky 2 a 5), patří Norsko k pionýrům digitalizace s dobře připravenou legislativou, technickým zázemí a investičními pobídkami pro budování IT, cloud computing i služeb v oblasti kybernetické bezpečnosti.

6.3 Digitalizace ekonomiky a veřejných politik: plány a cíle

Jak jsme zmínili výše, digitalizační procesy urychlila pandemie Covid.[53] Ta uspíšila také přípravu nových dokumentů, strategií a norem tak, aby vláda podpořila rozvoj digitálních procesů a růst firem v sektoru digitálních operací. Pro firmy, které pracují v oblasti zajištění GDPR, využití umělé inteligence,

[52] Před pandemií byl podíl digitální komunikace lékaři – pacienti asi 3 %, v době pandemie to bylo asi 40 %, dnes se podíl digitální komunikace lékaři – pacienti ustálil na 25 až 30 % (NMLGM 2021).

[53] Analýza rozvoje digitalizace v době pandemie je shrnuta v norské vládní zprávě „Our New Digital World" z roku 2021 (www.regjeringen.no/contentassets/00493dd2f00347098f15274e9302d392/en-gb/pdfs/our-new-digital-world_web_may-2021.pdf).

robotiky, zajištění kybernetické bezpečnosti a cloud computingu, připravila vláda balík podpůrných opatření jako daňové úlevy či administrativní pomoc státních úřadů.

Klíčové dokumenty upravující norské IT cíle jsou:

- Hodnotící zpráva a národní plán digitalizace „Our new digital world“ (2021),
- Strategie „Digital agenda for Norway – ICT for a simpler everyday life and increased productivity“,
- Plán digitalizace veřejné správy „Digital²1“ (2020),[54]
- Národní strategie pro umělou inteligenci (2020),
- Národní strategie pro kybernetickou bezpečnost (2019),
- Strategie pro cloud computing (2016),
- Strategie „Powered by Nature – Norway as a data centre nation“ (2018, revidováno 2021 a doplněno dokumentem, jak v Norsku zřídit datové centrum), [55]
- Strategie „One digital public sector: Digital strategy for the public sector 2019-2025“ (2019),[56] a
- Národní strategie pro e-zdravotnictví (2019).

V současnosti Norsko připravuje nové strategie a nástroje pro ochranu digitální infrastruktury státu. Vedle uvedených dokumentů zveřejňuje vláda plány pro digitalizaci veřejného sektoru v tzv. Digitalisation Circular, což je dokument, který vláda každoročně předkládá parlamentu a veřejnosti. Dokument obsahuje i doporučení digitální transformaci pro regiony a municipality.

6.4 Hlavní aktéři

Systém norských institucí zabývajících se digitalizací a upravujících prostředí IT se v posledních letech výrazně změnil a rozrostl. Byly zřízeny nové agentury, došlo k efektivnějšímu propojení a spolupráci při ochraně digitálního sektoru mezi policií, zpravodajskými službami, armádou a civilními úřady. Hlavními hráči v sektoru digitálních procesů jsou:

- Ministerstvo spravedlnosti a veřejné bezpečnosti (odpovídá za

[54] Dokumenty Digital21 a Digital agenda for the public sector 2019-2025 předpokládají začlenění kybernetické bezpečnosti do všech IT řešení, která bude vláda budovat, a to nejpozději do roku 2025. Konkrétní projekty ve vybraných sektorech ekonomiky a veřejné správy viz Digital Norway (www.digitalnorway.com/prosjekter/eu/).

[55] Norská vláda (www.regjeringen.no/contentassets/a76ebef545ae4e87a5b0761a93fb6ba1/how-to-establish-a-data-center-in-norway.pdf).

[56] Norská vláda (www.regjeringen.no/contentassets/db9bf2bf10594ab88a470db40da0d10f/en-gb/pdfs/digital_strategy.pdf).

národní kybernetickou bezpečnost ve všech civilních oblastech, koordinuje spolupráci v této oblasti mezi orgány a agenturami státu),

- Ministerstvo lokálního vládnutí a modernizace (odpovídá za modernizaci, digitalizaci a rozvoj digitální infrastruktury státu; disponuje Oddělením ICT politik a reformy veřejného sektoru),
- Ministerstvo obrany (odpovídá za národní kybernetickou bezpečnost ve vojenském sektoru),
- Agentura pro digitalizaci (vznikla v roce 2019, kdy po sérii kybernetických útoků vláda reagovala sdružením několika agentur, výrazným navýšením rozpočtu a aktivit pro digitalizaci země a posílením IT bezpečnosti[57]),
- Centrum pro informační bezpečnost (NorSIS), a
- Národní centrum pro kybernetickou bezpečnost (NCSC; jeho součástí je Norwegian Computer Emergency Response Team/ NorCERT).

Vedle ministerstev a státních agentur se na rozvoji digitalizace i kybernetické bezpečnosti podílejí platformy veřejného a soukromého partnerství a sdružení firem. Jedná se zejména o asociaci firem ICT průmyslu ICT-Norway[58], asociaci technologických firem Abelia[59], Data Centre Industry Association[60], a platformu DigitalNorway. Jejím cílem je podporovat digitalizaci norské ekonomiky a je považována za jednu z nejprogresivnějších platforem. DigitalNorway se soustředí se zejména na SME a udržuje spolupráci napříč EU. Je držitelkou řady mezinárodních grantů a projektů.[61]

6.5 Současné trendy a příležitosti

Hybnou silou digitalizace a poptávky po IT službách je stát. Příležitosti se na norském trhu generují v šesti oblastech: 1) budování datových center, 2) digitalizace veřejných politik a ochrana dat občanů, 3) ochrana kritické infrastruktury, 4) ochrana dat korporátního sektoru, 5) multi-cloud computing (46 % firem využívá dva poskytovatele IaaS nebo PaaS, 21 % firem dokonce tři /EY 2019/) a 6) řízení a ochrana IoT (vzdálené řízení a kontrola výroby elektřiny z obnovitelných zdrojů v odlehlých oblastech, řízení a kontrola chovu ryb v severních pobřežních oblastech, maritimní

57 www.digdir.no
58 ICT-Norway (www.ikt-norge.no/english/).
59 Abelia (www.abelia.no/om-Abelia/in-english/).
60 Norsk Datasenter (www.datasenterindustrien.no).
61 Více na DigitalNorway (www.digitalnorway.com/prosjekter/eu/).

průmysl, zemědělství ve vzdálených oblastech).

Vláda podporuje rozvoj cloud computing (Norsko je jedinou skandinávskou zemí, která má pro daný sektor samostatnou strategii) i výstavbu a využití datových center (vláda vypracovala instruktážní materiál pro zahraniční firmy, jak v Norsku postavit a provozovat datové centrum). Pro dané oblasti existují též daňové pobídky a příslušná legislativa. Výsledků těchto pobídek je již několik: v roce 2019 v Norsku otevřel několik datových center Microsoft, Google nakoupil pozemky s cílem vybudovat datová centra, Volkswagen oznámil výstavbu centra pro HPC[62], podobné plány avizovala AQ Compute. Jako důvod nárůstu využívání cloud computing firmy uvádějí potřebu nových digitálních řešení pro rychlejší vstup na trh a rychlejší komunikaci se zákazníky, potřebu obchodních inovací a snížení nákladů. Jako hlavní překážky pro větší využívání cloud computing pak norské firmy uvádějí nedostatek odbornosti v této oblasti, přílišnou složitost migrace dat a bezpečnostní obavy (EY 2019).

Podobně jako u dalších skandinávských zemí, i v Norsku od roku 2019 roste počet kybernetických útoků. Jedná se o krádeže firemních dat či dat norských občanů a snahy paralyzovat norskou energetickou i vládní infrastrukturu. V roce 2021 byly několikrát napadeny webové stránky parlamentu a emailové účty poslanců. V roce 2022 Norsko zahájilo velkou kampaň k posílení kybernetické bezpečnosti a skokově navýšilo státní výdaje do tohoto sektoru. Reagovalo tak mj. na zhoršující se bezpečnostní situaci po ruském útoku na Ukrajinu.

Norský trh s IT službami se překotně rozvíjí a roste podobně, jako v ostatních skandinávských zemích. Zvyšuje se počet start-upů, investic zavedených zahraničních firem i vládní podpora digitálnímu průmyslu a službám. V roce 2021 vznikla Norská asociace průmyslu datových center (Norsk Datasenterindustri), která sdružuje zavedené i nové operátory datových center a firmy zajišťující infrastrukturu datových center a dodávky elektrické energie.

6.6 Vstup na trh

Jak avizujeme v kapitole 3.3, Norsko disponuje celou řadou jasných plánů a strategií pro digitalizaci služeb, výroby i veřejných politik. Vláda vyčleňuje dostatečné rozpočty tak, aby plány byly realizovány. Dokumenty

[62] VW (/www.volkswagenag.com/en/news/stories/2019/06/crashtests-mit-der-kraft-des-wassers.html), GreeByte (www.greenbyte.no/news/volkswagen-group-opens-data-centre-at-green-mountains-location/).

i zákony upravují využívání cloud computing, AI i zavádění opatření pro posílení kybernetické bezpečnosti. Jaká opatření budou zaváděna a v jakých oblastech, vláda jasně uvádí ve strategických dokumentech i zprávách schválených parlamentem.

Od roku 2016 vláda – ve snaze zlepšit investiční prostředí a přilákat zahraniční investory – snižuje daň z příjmu i korporátní daně. V současné době mají zahraniční investoři a obchodníci ze zemí EU a Evropského hospodářského prostoru téměř ve všech sektorech ekonomiky stejné podmínky jako norské firmy. Určitá omezení platí v sektoru železniční dopravy, poštovních službách a těžbě nerostných surovin. Počet a rozsah restrikcí je postupně snižován a trh se výrazně otevírá a liberalizuje.

Hybnou silou poptávky po cloud computing a zajištění kybernetické bezpečnosti je stát a státní pobídky a projekty, i když poptávka soukromého sektoru také roste. Poptávku po IT službách zvýšila pandemie Covid, trvalý přechod části zaměstnanců na home office a opakované kybernetické útoky na veřejné úřady i firmy. V roce 2021 vláda oznámila vytvoření on-line platformy pro výběrová řízení státních úřadů poptávajících cloudové služby. Tato platforma by měla sloužit i jako informační databáze (normy atd.) pro poskytovatele.

Norsko není členem EU, je však součástí Evropského hospodářského prostoru. Hlavním obchodním partnerem Norska jsou státy EU. Obchodní a investiční vztahy mezi ČR a Norskem jsou upraveny Dohodou o Evropském hospodářském prostoru mezi EU a Norskem a pravidly Evropského společenství volného obchodu, jehož je Norsko členem. V souvislosti se současnou situací na energetickém trhu a ve snaze členských zemí EU snížit závislost na dovozu ruského plynu a ropy bude narůstat energetická vazba EU-Norsko. Norsko již deklarovalo, že je ochotno zvýšit vývoz ropy i zemního plynu na trh EU, což postupně přinese do norského státního rozpočtu další finanční zdroje.

7. Švédsko

Švédsko je od roku 1995 členskou zemí EU. Hlavní političtí a ekonomičtí partneři Švédska jsou ostatní severské státy, dále země Pobaltí, Velká Británie, Německo a USA. 52 % švédského exportu směřuje na trh EU, více než 60 % dovozu pochází ze zemí EU. Ruský útok na Ukrajinu vyústil ve významnou politicko-bezpečnostní změnu. Stejně jako Finsko i Švédsko podalo přihlášku do NATO. Prozatímně uzavřelo obrannou dohodu s Velkou Británií, která by v případě útoku ze strany Ruska Švédsku pomohla. Švédsko se však kromě vojenských hrozeb připravuje i na hrozby nevojenské jako hackerské a jiné útoky na strategickou infrastrukturu, krádeže osobních a dalších dat z databází státních institucí a firem a kybernetickou špionáž.

Švédsko patří politicky i socio-ekonomicky k nejstabilnějším, nejtransparentnějšími a nejinovativnějším zemím s největším potenciálem pro rozvoj digitalizace. Švédské vlády opakovaně deklarovaly, že země bude první uhlíkově neutrální ekonomikou na světě. Vládní kroky z posledních let nasvědčují tomu, že země se snaží cíl naplnit. Vláda vytváří příslušné pobídky, přijímá potřebnou legislativu a firmy ze všech oblastí (včetně ICT sektoru) hledají cesty, jak transformovat svoje výrobní a obchodní procesy. Mezi handicapy jinak liberálního, rostoucího, solventního a inovativního trhu patří vysoké zdanění mezd, vysoká DPH a vysoké životní náklady.

7.1 Ekonomická a socio-demografická charakteristika

Švédsko patří mezi bohaté státy s vysokým HDP na hlavu a vzdělanou populací. Ekonomické rozdíly ve společnosti jsou relativně malé, což je mj. dáno progresivním a vysokým zdaněním. Švédský trh je inovativní s rostoucí poptávkou po nových technologiích a digitalizaci. Zvláštní pozornost je věnována digitalizaci finančních služeb a projektům chytrých měst a chytré dopravy. Do těchto oblastí směřuje významná část zahraničních investic. Vlády podporují výzkum a vývoj a budování ekonomiky založené na inovacích. Švédsko před několika lety založilo program „Test Bed

Sweden“[63], v jehož rámci municipality, univerzity, laboratoře či podniky nabízejí domácím i zahraničním firmám a investorům prostor a příležitost pro testování určitého nástroje, zařízení či technologie v praxi (např. v projektu chytré dopravy testují švédská města nejrůznější inovace v městské dopravě, při svozu odpadu anebo distribuci tepla).

Švédové jsou technologicky vyspělí, s vysokou IT gramotností (v zemi je vysoký podíl obyvatel s přístupem k internetu, 98 %); patří ke společnostem s nejvyšším počtem IT zařízení na osobu na světě. Společnost podporuje digitalizaci i automatizaci. V posledních letech se ale začíná projevovat rozdíl mezi Švédy a imigranty. Švédsko bylo tradičně otevřenou zemí ochotnou přijímat migranty z různých oblastí světa, ukazuje se ale, že švédská společnost není schopna příchozí sociálně i ekonomicky dostatečně integrovat. V posledních letech vedlo rostoucí napětí mezi Švédy a migranty k násilným demonstracím, ničení majetku a nedávno i k útokům na školy. V této souvislosti je věnována pozornost i rostoucí kriminalitě mládeže, zejména z okruhu imigrantů.

7.2 Infrastruktura ICT a potenciál pro digitalizaci ekonomiky a společnosti

Mezi zeměmi EU vykazuje Švédsko nejvyšší podíl obyvatel zaměstnaných v IT segmentu (6,1 %). Infrastruktura potřebná pro rozvoj IT je v zemi vysoce rozvinutá a dodávky elektrické energie stabilní. Švédský trh s IT tvoří téměř 40 % severského trhu s IT. Podle odhadu Švédského statistického úřadu poroste trh se službami v oblasti kybernetické bezpečnosti o 2 až 25 % do roku 2024. Za nejperspektivnější segmenty v IT sektoru jsou považovány cloudová bezpečnost, Identity Access Management a digitalizace vybraných sektorů (medicína, finanční služby, veřejné politiky). Vláda ve spolupráci se soukromým sektorem a univerzitami buduje technologické parky, výzkumné ústavy a tzv. „test beds“, tedy platformy či „tržiště“ poskytovatelů nástrojů a technologií, státních institucí (zapojila se např i Švédská centrální banka) a uživatelů ochotných zavádět do testovacího provozu inovace. V zemi jsou tři desítky testovacích center zabývajících se AI, IoT, 5G sítěmi, IT bezpečností a virtuální realitou.

V zemi rose zájem o cloud computing[64], výsledky herního průmyslu, které by

63 swedishtestbeds.com/en/find-testbed/

64 Podle údajů Eurostatu z roku 2022 patří Švédsko k nejvyšším uživatelům cloudových služeb – využívá je více než 75 % firem (ve Finsku a Dánsku se toto číslo pohybuje kolem 40 %).

bylo možno aplikovat ve výrobních procesech, v oblasti vzdělávání či vizualizaci, využití umělé inteligence a strojového učení ve výrobních procesech, medicíně a finančních službách a zpracování velkých dat. Podle údajů Švédského statistického úřadu z roku 2021 roste míra digitalizace nejrychleji v sektoru ICT firem, dále pak v oblasti energetiky, prodeje motorových vozidel a obchodu s nemovitostmi. V sektoru ICT pak nejrychleji roste segment softwaru a IT služeb. Významně se zvýšil i počet firem podnikajících v daném sektoru. V roce 2020 95 % nových společností působilo právě v sektoru softwaru a IT služeb. Ze Švédska pocházejí např. Skype, Spotify, Klarna, Kry či Yubico.

Švédsko směřuje k udržitelné IT infrastruktuře, což je atraktivní jak pro zemi samotnou, tak pro investory; Švédové např. využívají zbytkové teplo z datových center pro vytápění budov. Hledána jsou i další udržitelná řešení a inovace směřující k vybudování bezuhlíkové ekonomiky.

7.3 Digitalizace ekonomiky a veřejných politik: plány a cíle

Digitální sektor tvoří významnou část HDP, v roce 2021 to bylo téměř 5,8 %. Význam digitalizace a IT sektoru se projevuje i v přístupu švédských vlád. Ty přijaly řadu dokumentů (viz níže) deklarujících cíle státu v oblasti IT a zveřejnily i rozpočtové plány, které indikují (a běžící projekty tento trend potvrzují), že veřejné úřady budou investovat do digitalizace chodu státu a zajištění kybernetické bezpečnosti miliony švédských korun (srovnej Evropská komise 2021d). Státní sektor bude v následujících pěti letech jedním z nejvýznamnějších zákazníků IT firem. Bude se jednat o zajištění bezpečnosti informačních systémů a databází, poradenskou činnost, zajištění fyzické infrastruktury nutné pro digitalizaci zdravotnictví, daňový, důchodový a soudní systém včetně přístupu k soudním spisům a záznamům z jednání, katastr nemovitostí, e-ID včetně e-řidičského průkazu atd. Cílem vlády je vytvořit jednu digitální infrastrukturu využívanou všemi vládními úřady a agenturami.

Rozvoj IT vláda podporuje také legislativně – zákony, strategickými plány atd. Klíčové dokumenty představující digitalizační plány Švédska pro období následujících pěti let jsou (chronologicky):[65]

[65] Tam, kde existuje anglický název dokumentu a instituce, jej uvádíme, tam, kde existují jen švédské názvy pro příslušný dokument či instituci, převádíme název do češtiny.

- Národní strategie pro kybernetickou bezpečnost (2017),[66]
- Comprehensive cyber security action plan 2019-2022 (2019, inovován v roce 2021),[67]
- Artificial Intelligence and eHealth, resp. Vision for eHealth (2020; eHealth Agency),
- Promoting public administration´s ability to use AI (2021; Agency for digital government),
- National approach to AI (2018; Agency for digital government),
- A completely connected Sweden by 2025 – Broadband strategy (2021),
- Development for the Digital Age – A new strategy for local and regional governments (2019; Swedish Association of Local Authorities and Regions), a
- Framework for digital collaboration (2020).

7.4 Hlavní aktéři

Hlavním aktérem digitalizace i trhu s IT službami je stát. Ten je významným zaměstnavatelem, tvůrcem norem i vlastníkem mnoha velkých firem. V procesu přípravy strategických dokumentů pro rozvoj ICT má hlavní slovo Ministerstvo pro infrastrukturu.[68] Na přípravě legislativy i praktickém zajišťování digitalizace a souvisejících témat se podílejí také Ministerstvo spravedlnosti, Ministerstvo vnitra a Ministerstvo obrany společně s armádou. Vzniká také celá řada platforem sdružujících vládní úřady, veřejnou správu, soukromý sektor a univerzity.[69]

Hlavními hráči v oblasti politiky IT a digitalizace jsou:

- Ministerstvo infrastruktury,
- Agency for Digital Government,
- e-Health Agency,
- Civil Contingencies Agency,[70]
- Cooperation Group for Information Security (SAMFI),
- Národní centrum pro kybernetickou bezpečnost,[71]
- Centrum pro kybernetickou obranu a informační bezpečnost,[72] a
- Swedish Authority for Privacy Protection dříve Data Protection Authority.[73]

66 Ministerstvo spravedlnosti, Švédsko: government.se/4adab4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy
67 cyberwiser.eu/sites/default/files/Sweden_CyberPlan_March2019.pdf
68 www.government.se/government-of-sweden/ministry-of-infrastructure/
69 Např. Computer Emergency Response Team (www.cert.se).
70 www.msb.se/en/
71 www.cfcs.se
72 www.kth.se/cdis
73 www.imy.se/en/

Jako meziministerská a meziagenturní platforma pro kybernetickou bezpečnost IT systémů a dat vznikla Informationssakerhet.se (NSIT), která mj. poskytuje základní informace o legislativě pro kybernetickou bezpečnost, přehled o vládních opatřeních apod. Vláda také zřídila několik nových meziministerských agentur, úřadů a platforem zaměřujících se na segment IT. Byla posílena tělesa švédské armády podílející se na obraně před kybernetickými hrozbami.

Vznikají také nová sdružení firem pracujících v oblasti digitalizace a IT služeb. Vláda i města zřizují různé projekty a programy s cílem posílit a urychlit digitalizaci a využití chytrých technologií pro dopravu, udržitelnou výrobu elektrické energie či chytrá města. Nejaktivnějšími hráči v této oblasti jsou platformy Cybernode[74] a Swedsoft[75].

7.5 Současné trendy a příležitosti

I když počet obyvatel ve Švédsku mírně roste, zemi chybějí pracovní síly s IT znalostmi. Přitom 60 % všech nových pracovních míst bylo v roce 2021 generováno IT sektorem, resp. s IT svázanými oblastmi (Business Sweden 2022). Švédské firmy IT služby obvykle outsourcují, jen malý podíl švédských firem má vlastní IT specialisty.

Poptávka po IT službách a digitalizaci roste v pěti sektorech: 1) zdravotní péče (technologie pro konektivitu, cloudové služby, komunikace, technologie pro pokročilou analýzu dat), 2) doprava (technologie pro autonomní vozidla, digitální infrastruktura a konektivita, e-commerce), 3) finanční služby (digitální infrastruktura a konektivita, technologie pro pokročilou analýzu dat), 4) IoT a pokročilá analýza dat, a 5) veřejný sektor (digitální interakce, sdílení a zveřejnění vládních dat, digitální podpora rozhodovacích procesů). Strmě roste poptávka po zajištění kybernetické bezpečnosti. Švédský statistický úřad uvádí, že v roce 2021 jen cca 20 % švédských firem mělo vyšší než základní zajištění proti kybernetickým útokům. Další příležitosti generují výzkumná a vývojová centra velkých IT firem. V posledních letech v zemi otevřely svá centra např. Apple, Amazon, Fujitsu, Google, IBM, Microsoft, Nvidia, Samsung či Tata. Velké investice ve Švédsku v oblasti IT ohlásily pro rok 2023 Google a Microsoft.

Roste také poptávka po cloudových službách. V dubnu 2022 poskytovaly ve Švédsku cloudové služby firmy Equinix (AWS, Google Cloud Platform,

74 cybernode.se/en/home/
75 swedsoft.se/en/

Microsoft Azure, Oracle Cloud) a Interxion (AWS, Google Cloud Platform). I když švédští SaaS poskytovatelé preferují švédské IaaS partnery, největším poskytovatelem je ve Švédsku Amazon[76] (služby jako ochrana databází, IoT či umělá inteligence), následován Microsoftem a firmami Hetzner a Rackspace. Mezi významné lokální IaaS poskytovatele patří Zitcom, TDC Hostin, Loopia či Glesys. Mezi nejsilnější švédské SaaS poskytovatele patří iZettle a Klarna (finanční služby), Truecaller a Tele2 (komunikace) a Ericsson. PaaS poskytovatelů je v zemi poskrovnu – patří mezi ně např. Accedo, Bariumlive a Cloudnet.

Vláda uvádí, že v letech 2022 až 2027 by měly zahraniční a domácí investice do IT přesáhnout 4 miliardy USD. Země má dobré komunikační spojení (podmořské kabely, rozsáhlá telekomunikační síť) s ostatními severskými státy i zeměmi EU, což je pro řadu investorů rozhodující.

7.6 4.6 Vstup na trh

Švédský trh je otevřený a nediskriminující, nicméně v zemi najdeme i překážky; jedná se o vyspělý a náročný trh hledající konkurenceschopné inovace splňující kritéria bezuhlíkové ekonomiky. Jedná se také o trh, který je silně ovlivňován státem; ten má podíl v mnoha velkých firmách. V zemi hrají velkou roli odbory, téměř 70 % pracovních sil je organizováno v odborech. Švédská legislativa odpovídá legislativě EU, na firmy i jedince se vztahují pravidla Schengenského prostoru.

Největšími švédskými obchodními partnery jsou Německo, Dánsko, Finsko, Nizozemsko, Francie a Estonsko. Více než polovina zahraničního obchodu země směřuje na trh EU. Obchodní vztahy mezi ČR a Švédskem jsou budovány dlouhodobě, nicméně mezi oběma zeměmi nedochází k obchodům velkého objemu. Česko-švédské obchodní vztahy jsou řízeny v souladu s legislativou EU.

[76] www.business-sweden.com/insights/client-cases/amazon-web-services/

8. Skandinávie: Ochodní události v oblasti ICT

Událost	Kde	Poznámka
Digital Tech Summit	dk	my.eventbuizz.com/event/digital-tech-summit-2022-10651/detail
Homeland Security Conference	dk	
Nordic Fintech	dk	copenhagenfintech.dk
SecTech Sweden Expo	sw	Securityworldmarket.com
Software Technology Exchange Workshop, STEW	sw	swedsoft.se/en/stew/
Software Development Day	sw	softwareday.lindholmen.se/en
Nordic IT Security	sw	nordicitsecurity.com
CyberSecurity Nordic	fi	cybersecuritynordic.messukeskus.com
SLUSH	fi	www.slush.org/events/helsinki/
Teknologia23	fi	teknologia.messukeskus.com
SecTech Norway	no	securityworldmarket.com/sectech/no/en/index.asp

9. Seznam zkratek

5G	pátá generace bezdrátových systémů (5G mobilní síť)
AI	umělá inteligence
AWS	Amazon Web Services
BaaS	Business Process as a Service
EU	Evropská unie
FDI	přímé zahraniční investice
GRC	Governance, Risk and Compliance
HDP	hrubý domácí produkt
HPC	High-Performance Computing
HW	hardware
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ICT	informační a komunikační technologie
IoT	internet věcí
OECD	Organizace pro ekonomickou spolupráci a rozvoj
PaaS	Platform as a Service
PAM	Privileged Access Management
R&D	výzkum a vývoj
SaaS	Software as a Service
SME	malé a střední podniky
SW	software
USD	americký dolar
WBG	Skupina Světové banky
WTO	Světová obchodní organizace

9 Seznam zkratek

Terminologie použitá v této zprávě je v souladu s terminologií použitou v následujících dokumentech a publikacích:

- Iniciativa Průmysl 4.0

(mpo.cz/assets/dokumenty/53723/64358/658713/priloha001.pdf)

- Jirásek, P. et al (2015): Výkladový slovník kybernetické bezpečnosti. Policejní akademie ČR v Praze.

V případě zavedených odborných oborově (ICT) specifických termínů a v případě zavedených názvů projektů a institucí ve skandinávských zemích anglické pojmy nepřekládáme. Cílem je dodržet obsahovou přesnost.

10. Použité zdroje

AFD (Agency for Digitisation, Denmark) (2022): Policy and Strategy. https://en.digst.dk/policy-and-strategy/

Aula, I. et al (2020): Critical Nordic Flows. Collaboration between Finland, Norway and Sweden on Security of Supply and Critical Infrastructure Protection. cyberwiser.eu/sites/default/files/critical-nordic-flows.pdf

Business Finland by Frost & Sullivan (2021): Market Opportunities in Cybersecurity. Future Watch 7/2021.

Centre for Cyber Security (2021): The cyber threat against Denmark 2021.

Copenhagen Economics (2017): Finland´s economic opportunities from data centre investments. A study prepared for Google.

Copenhagen Economics (2020): Inside Finland. Google´s European hyperscale data centres and infrastructure ecosystem. A study prepared for Google.

Cyber Hub (2021): Insight. The Danish Cybertech Ecosystem. Danish hub for cybersecurity.

Danish Ministry of Finance, Local Government Denmark and Danish Regions (2016): A stronger and more secure digital Denmark. The Digital strategy 2016-2020. Kodaň, Agency for Digitalisation.

Dánský statistický úřad: www.dst.dk/en

European Data Flow, Evropská komise (digital-strategy.ec.europa.eu/en/policies/european-data-flow-monitoring)

Equnix (2021): Finland is moving to the cloud. Opportunities and challenges in the digital transformation journey. Report Digital transformation.

EY (2019): EY Norwegian Cloud Maturity Survey 2019. Current and Planned adoption of cloud services. EY.

EY (2020): Nordic IT sourcing & cloud survey 2020. Status and trends in the Nordic IT sourcing market.

Evropská komise (2021a): Digital Public Administration factsheet. Denmark.

Evropská komise (2021b): Digital Public Administration factsheet. Finland.

Evropská komise (2021c): Digital Public Administration factsheet. Norway.

Evropská komise (2021d): Digital Public Administration factsheet. Sweden.

Evropská komise (2021e): Digital Economy and Society Index 2021. https://digital-strategy.ec.europa.eu/en/policies/desi

Government Offices of Sweden (2019): National approach to Artificial Intelligence. Ministry of Enterprise and Innovation.

Government.no (2022): Cloud Computing strategy for Norway. Ministry of Local Government and Regional Development.

MIT Technology Review (2022): The Global Cloud Ecosystem Index 2022. wp.technologyreview.com/wp-content/uploads/2022/04/MITTR-INFOSYS-Cloud_Reort_FNL.pdf

National Board of Trade (2021): The Swedish Market. IT Services. Open Trade Gate Sweden.

NMLGM (2021): Our New Digital World. Norwegian Ministry of Local Government and Modernisation

Nordic Council of Ministers (2018): Data Centre Opportunities in the Nordics. An analysis of the competitive advantages. NCM.

OECD (2021a): OECD Economic Surveys: Denmark 2021. OECD.

OECD/Statistics Finland (2021b): Finland: Road to Recovery after COVID-19, OECD Publishing, Paris.

OECD (2021c): Norway´s strategic proces to capitalise on the potential of new technology.

OECD (2021d): Drivers of Trust in Public Institutions in Finland. OECD Publishing.

Saunavaara, Juha, Antti Laine, Matti Salo (2022): The Nordic societies and the development of the data centre industry: Digital transformation meets infrastructural and industrial inheritance. Technology in Society, Vol. 69, https://doi.org/10.1016/j.techsoc.2022.101931.

US International Trade Administration (2021): Global Artificial Intelligence Market Report.

Použitý denní tisk a zprávy jsou odkazovány přímo v textu pod čarou.