

eGovernment

G-cloud, blockchain a datová ambasáda

Vojtěch Bínek

eGovernment lze definovat jako využívání informačních a komunikačních technologií (ICT) k elektronickému propojování a zveřejňování dat ze státní správy. Jeho cílem je poskytnout občanům a firmám platformu, přes kterou budou moci elektronicky a efektivněji komunikovat se státními úřady. V soukromé a business sféře elektronické propojování dat jenom kvete, státní sféra ale zůstává pozadu. Jaké jsou tedy ty hlavní předpoklady, jež musí být naplněny, aby se koncept eGovernmentu proměnil ve skutečnost?

Škálování intergovatelnosti

V první řadě je třeba zajistit, aby spolu všechny jednotlivé systémy, servery a další prvky, jež mají být součástí sdílené platformy, byly schopny komunikovat. Vzájemná kompatibilita a integrovatelnost jednotlivých systémů a počítačů v nich, neboli modularita, si vyžadují standardizaci a kontinuální vývoj, jež se nedají zajistit jinak než top-down řízením. V případě chybějící vize anebo koordinace jejího naplňování se projekty digitalizace státní správy jednotlivých úseků nutně stávají časem obskurními, čímž dochází k narušení jejich bezpečnosti a potenciálně ke kompromitaci uložených dat. Jedním z nabízejících se řešení problematiky bezpečnosti a zároveň problematiky jednotičiho, modulárního designu systému digitální státní správy je technologie cloudu.

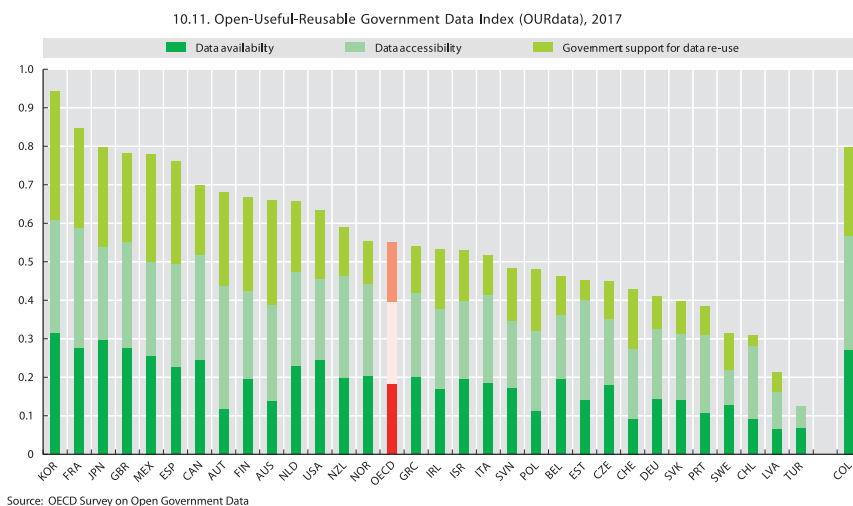
Trend státní správy v cloudu, nazývaný též G-cloud nebo eGC (eGovernment Cloud), umožňuje pojmout celý eGovernment jako službu (as-a-service) a zbavuje tak jednotlivé menší i větší úřady nutnosti provozovat lokální úložiště dat anebo i celá IT oddělení, včetně kompletního digitálního zabezpečení dat. V otázce integrace celého systému eGovernmentu je tak cloud přirozeným řešením. Rovněž je cloud pozitivním krokem k navyšování ekonomické efektivity celého konceptu eGovernmentu: provozování několika datových center využívajících nejmodernější osvědčené postupy pro zálohování, s redundantní infrastrukturou a s nejvyšší bezpečnostní certifikací vyjde vždy levněji než do stejné míry zabezpečovat každý fyzický uzel v síti.

Směrem k ještě silnější integritě eGovernmentu a zároveň řešením problematiky bezpečnosti může být technologie blockchainu, dnes známá především díky kryptoměnám,

jako je Bitcoin. Na rozdíl od cloudu implementace blockchainu do státní správy není na první pohled zrovna intuitivním řešením. Důvodem je decentralizace vlastní struktury – blockchainové databáze ukládají data na každý uzel v síti redundantně tak, aby byl zajištěn nepřetržitý provoz systému, tedy nahlížení a úprava dat. Například Bitcoin byl k začátku července 2017 v provozu po 99,991548808 % času od svého spuštění v roce 2009.

Implementace blockchainu ale neznamená opětovně opouštění pracně budovaných data center pro eGC – decentralizované databáze blockchainu se dnes komerčně využívají primárně buď coby kryptoměny, které nejsou příliš náročné na objem uložených dat, anebo k zajištění autenticity, neměnitelnosti dat uložených v jiných databázích. Velikost blockchainových sítí a kvanta rychle se vrstvících dat totiž mimo jiné poskytují výhodu jedné z nejdokonalejších a nejbezpečnějších šifrovacích metod. Blockchain tedy zatím nenahrazuje

Obr. 1: Graf z aktuální studie OECD, která analyzuje vývoj digitalizace státní správy a inovace ve veřejném sektoru. Vybraný graf znázorňuje dostupnost a použitelnost otevřených dat. ČR je v uvedeném kritériu lehce pod průměrem.



kompletní databáze a úložiště dat, pouze do- dáva neprolomitelnou vrstvu zabezpečení. Do budoucnosti má ale technologie blockchainu potenciál najít i další využití v eGovernmentu a jedním z průkopníků se chystá být Dubaj – do roku 2020, kdy se zde bude konat výstava Expo, chce arabský emirát zavést technologii blockchainu do řady odvětví státní správy.

Diskriminace negramotných

Zaváděním jakýchkoli nových technologií do odvětví tak citlivého, jako je státní správa, se zákonitě vytváří i řada problémů, a to i když je jejich dopad ve výsledku veskrze pozitivní. S nedostatečnou integrací jednotlivých projektů se poji riziko neefektivního ekonomické hospodaření, opakování jednotlivých drahých projektů, které napoprvé nepřinesly kžžený výsledek, bez adresování důvodu, proč se tomu tak stalo, nebo ukončení vývoje a ohrožení bezpečnosti často citlivých dat.

Bezpečnost dat ve státní správě má přitom několik dimenzí. Jedním z vytyčených cílů každého eGovernment projektu je kromě těch již zmínovaných také transparentnost, tedy zveřejňování dat, jež mají být veřejná. Jestliže ale existuje systém, do nějž jsou integrovány úřední, policejní a zdravotnické databáze, z nichž se dají vyčíst veškeré soukromé informace o konkrétních lidech, není přípustné, aby se staly veřejnými. Ať už nedopatřením

obsluhy, s přičiněním hackerů anebo jen jako nedostatečně anonymizovaná součást dat určených k analýze a k vylepšení národního zdravotnického programu nebo k optimalizaci dopravní infrastruktury státu. Rovněž není žádoucí, aby měl celý personál nemocnice možnost prohlížet si o polední pauze kartotéku pacientů s důvěrnými lékařskými zprávami. Neoprávněný přístup k osobním datům je jedním z těch málo adresovaných rizik spojených s komplexní digitalizací společnosti. Blockchain, stejně jako většina technologických řešení, přitom dokáže efektivně chránit data pouze proti jedné z výše popsaných možností – proti hackerům.

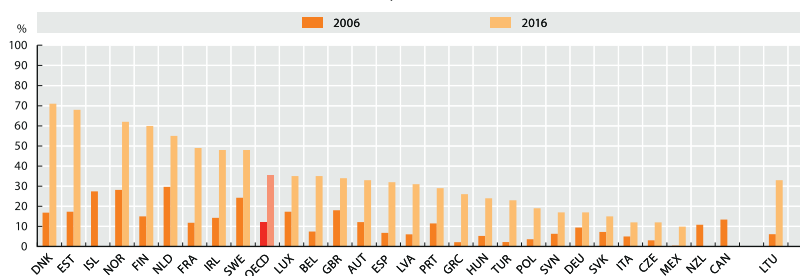
Zbylé příklady se více či méně pojí s dalším nelehce řešitelným problémem digitalizace státní správy, a to s počítačovou gramotností populace. Ačkoli čeští uživatelé jsou na relativně vysoké úrovni, především starším generacím a sociálně znevýhodněným občanům hrozí postupné odsouvání do druhé kategorie, ve které může být jejich přístup ke všem službám státní správy omezen, ať už důsledkem nedostatečného vzdělání, absencí technologických artefaktů, jejichž vlastnictví se pro využití daných služeb předpokládá, anebo i rezignací na snahu držet krok s kontinuálně se měnícím technologickým prostředím. Přirozeně pak takto postižení občané nebudou dostatečně obezřetní při zacházení s čipy, přístupovými údaji a dalšími rekvizitami, jež eGovernment do života občanů přináší, čímž se navíc stanou náchylnějšími k podvodnému zneužití technologicky zdatnějšími kriminálníky.

Estonská datová ambasáda

I přes všechny zatím nevyřešené nedostatky je ale vznik eGovernmentu nepochybně pozitivním vývojem. Při troše štěstí umožní transformovat stát dvacátého století v jeho levnější, transparentnější, efektivnější a bezpečnější verzi. Digitalizace jednotlivých systémů státní správy snižuje časovou náročnost veškerého vyřizování pro občany i firmy, snižuje náklady státu na provoz, zjednodušuje veškerou interní i externí práci s daty a do budoucna představuje výchozí bod, ze kterého může stát růst dále do budoucnosti, zatím asi ani netušenými směry.

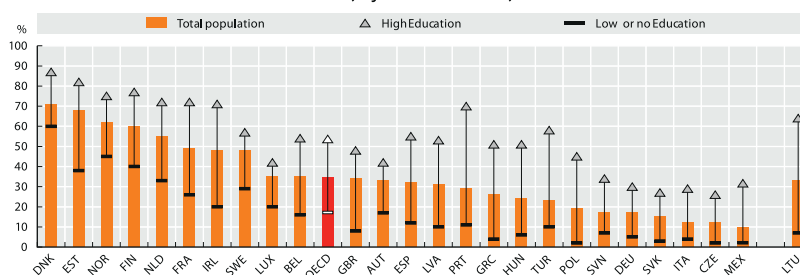
Nejčastěji uváděným příkladem toho, jak může eGovernment už dnes vypadat, je estonský projekt e-Estonia. Občanské průkazy zde nabízejí kromě samozřejmého offline ověřování totožnosti i jeho online verzi, díky které lze autorizovat digitální podpis, mít přístup ke zdravotním a všem dalším centralizovaným

11.5. Individuals using the Internet for sending filled forms via public authorities websites in the past 12 months, 2006 and 2016



Source: OECD, ICT database, OECD, Paris; Eurostat, Information Society database, Eurostat, Luxembourg.

11.6. Individuals using the Internet for sending filled forms via public authorities websites in the past 12 months, by education level, 2016



Source: OECD, ICT database, OECD, Paris; Eurostat, Information Society database, Eurostat, Luxembourg.

Obr. 2: Ze studie OECD jasně vyplývá, jak zatím ČR zaostává v oblasti eGovernmentu. Na grafech je např. vidět, že jen malý zlomek z nás využívá elektronickou komunikaci se státní správou. ČR je vždy na chvostu sledovaných zemí.

státním záznamům anebo k nakupování léků na elektronický recept (jenž na občanský průkaz nahraje lékař), může sloužit pro přístup k osobnímu bankovníctví, jako platební karta i jako karta na přepravu v MHD po celém státě. Výčet není ani zdaleka kompletní a nové aplikace jsou přidávány každým rokem. Pravidelně chytré funkce občanských průkazů využívá 67 % Estonců. Občanský průkaz se váže na zpracovaný koncept e-rezidenta, který umožňuje velmi pohotovou a komplexní komunikaci s úřady. Založit firmu, podat daňové přiznání, převést nemovitosti, požádat o rozvod, ale i volit politickou reprezentaci – vše se odehrává po internetu. Výhod e-rezidenta může do určité míry využívat i člověk, jenž není občanem Estonska. Zajímavý je koncept zejména pro podnikatele a start-upy.

Pro zajištění autenticity a integrity dat využívá estonský eGovernment vlastní technologii blockchainu. Co se ale stane, když Estonsko napadne nepřátelská armáda anebo se stane obětí rozsáhlých hackerských útoků nebo přírodních pohrom? I na takové krize se místní vláda připravuje. Řešením pro zajištění nepřetržitého provozu systému má být právě dokončovaná datová ambasáda v Lucemburku, první svého druhu. Koncept je jednoduchý: nová budova v neznámé lokaci se do konce roku stane legálně plnohodnotnou ambasádou Estonska, namísto sídla velvyslanců ale bude sloužit jako cloudové úložiště dat, primárně pro zálohování a Disaster Recovery dat ze systému e-Estonia, jež jsou dnes

kritická nejen pro fungování občanů a firem, ale i komplexně digitalizované a efektivní státní správy.

Z tohoto pohledu má Česká republika stále co dohánět, což potvrzuje mj. zpráva OECD, podle které si ČR v oblasti digitalizace státní správy vede téměř nejhůře z celého bloku. Zatímco například v Estonsku služeb eGovernmentu k vyplňování a odesílání formulářů využilo v roce 2016 přes sedmdesát procent obyvatel, v ČR to bylo jen něco málo přes deset procent. Zásadně jiná nebyla situace v ČR ani mezi lidmi s vyšším vzděláním nebo s vysokými příjmy, což ukazuje, že problém ČR neleží v nízké přístupnosti nebo v nedostatečném povědomí, ale skutečně v dlouhodobém opomíjení celého trendu digitalizace státní správy na celostátní úrovni. V důsledku zde využitelné digitalizované nástroje státní správy prostě chybí. Česká republika tak v oblasti eGovernmentu rychle zaostává a poškozují tím nejen svou image, ale i limituje potenciál vlastní společnosti. ■

Vojtěch Bínek

Autor článku je Content Specialist ve společnosti Acronis CZ. V článku jsou uvedeny grafy ze studie OECD „Government at a Glance 2017“, kterou lze v různých formátech stáhnout ze stránek OECD iLibrary.