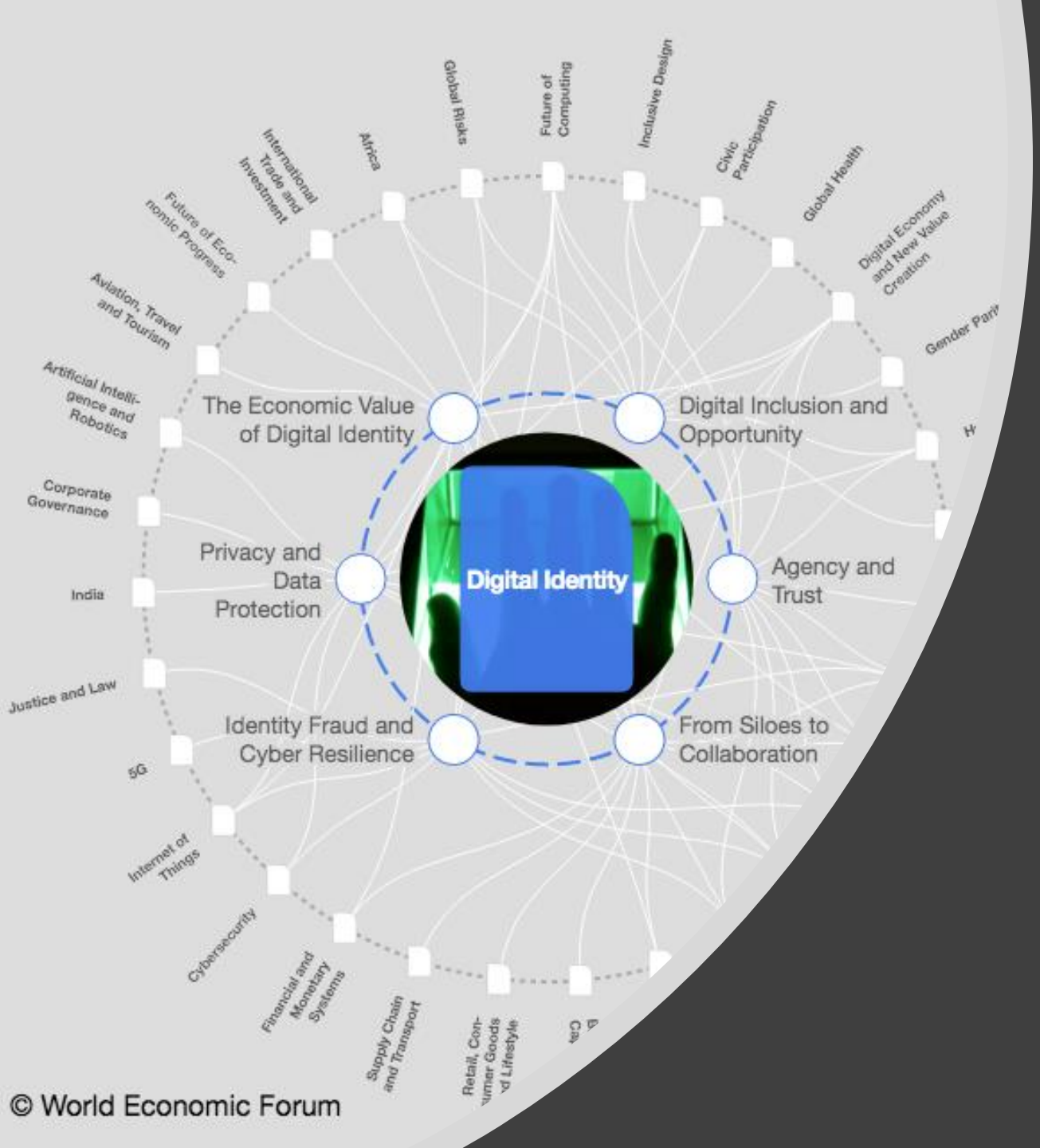

DIGITÁLNA IDENTITA

SITCON spol. s r.o.

Dôverná a overiteľná totožnosť je nevyhnutná.

Keďže digitálna interakcia prináša informácie online bezprecedentnou rýchlosťou, údaje, ktoré tvoria našu identitu, sa široko zdieľajú vytvárajú tak príležitosti, ako aj slabé miesta.

Ak bude navrhnutá správne, digitálna identita môže do roku 2030 poskytnúť krajinám ekonomickú hodnotu ***rovnajúcu sa až 13% HDP, ušetriť 110 miliárd hodín*** *prostredníctvom efektívnejšej elektronickej verejnej správy a podnikom ušetriť až 1,6 bilióna dolárov podľa Globálneho inštitútu McKinsey.*

A pre odhadovanú 1 miliardu ľudí, ktorí nemajú žiadny oficiálny dôkaz totožnosti (nehovoriac o 3,2 miliardách ľudí, ktorí nedokážu efektívne používať identitu na digitálnych kanáloch), má model digitálnej identity založený na spolupráci a na základe používateľov vedeného zdieľanými princípmi rastúci potenciál.

Digitálne začlenenie a príležitosť

Preklenutie priepasti v oblasti digitálnej identity môže posilniť ľudskú dôstojnosť a rozšíriť príležitosti

Podľa Svetovej banky ***viac ako miliarda ľudí nemá právnu totožnosť*** *a približne polovica z nich má bydlisko v subsaharskej Afrike. Takmer 40% celkovej populácie v krajinách s nízkymi príjmami nemá právnu identitu (v porovnaní s menej ako 10% v krajinách so strednými príjmami), zatiaľ čo tento problém má jedna z dvoch žien v krajinách s nízkymi príjmami.*

Vyvíja sa niekoľko snáh o integráciu vylúčených skupín obyvateľstva prostredníctvom digitálnych prostriedkov. Napríklad iniciatíva Svetovej banky ID4D poskytuje krajinám technickú pomoc a odborné znalosti, aby im pomohla implementovať inkluzívne systémy digitálnej identity. Medzitým Agentúra OSN pre utečencov a Svetový potravinový program používajú skenovanie dúhovky na registráciu utečencov a vysídlených osôb a na poskytovanie humanitárnej pomoci. OSN odhaduje, že rozšírenie tohto úsilia by mohlo pomôcť asi 66 miliónom vysídlených ľudí na celom svete.

So zberom biometrických údajov však existujú riziká najmä ak je vláda ochotná ich použiť na zisťovanie a podvádzanie disidentov alebo na vylúčenie ľudí z ich oprávneného prístupu k jedlu a prístrešia. Okrem toho, ak jediná forma identity jednotlivca pochádza z humanitárnej agentúry, môže to skomplikovať uznanie z ich domovskej alebo hostiteľskej krajiny.

Digitálne začlenenie a príležitosť

Gavi, The Vaccine Alliance, používa digitálne zdravotné karty, biometrické údaje, textové správy a platformu mobilnej identity na zlepšenie doručovania vakcín v rozvojových krajinách.

Podľa Medzinárodnej organizácie práce by ***odhadovaným 40 miliónom obetí moderného otroctva*** mohli pomôcť systémy digitálnej identity, ktoré sledujú pracovné podmienky v globálnych dodávateľských reťazcoch. Austin, Texas sa snaží pomáhať ľuďom bez domova, ktorí sa snažia udržať fyzické formy identifikácie a často majú fragmentované údaje o zdraví, vyvíjaním MyPass, riešenia založeného na blockchainoch, ktoré umožňuje prístup k zdravotnej starostlivosti, zamestnaniu alebo bývaniu priložením digitálnych zdravotných záznamov a ďalších údaje na telefónne číslo alebo e-mailovú adresu osoby.

Zatiaľ čo digitálna identita môže lepšie integrovať populáciu, zle navrhnutý systém môže byť zneužití na diskrimináciu. Participatívny dizajn je kľúčom k akémukoľvek systému, ktorý slúži zraniteľným skupinám obyvateľstva. V konečnom dôsledku by každé riešenie malo zodpovedať rozdielom vo veku, digitálnej gramotnosti a prístupu na internet.

Zainteresované strany vo všetkých odvetviach by sa mali zapojiť do výskumu založeného na dôkazoch, ktorý podporujú identitu zameranú na človeka, zapájať občiansku spoločnosť a verejnosť do jej navrhovania a zavádzať prototypy a piloty zaoberajúce sa problémami identity, ktorým čelia zraniteľné skupiny obyvateľstva.

Agentúra a dôvera

Dať ľuďom viac informácií o svojich údajoch by mohlo zlepšiť ich vzťahy s inštitúciami

Biometria, rozpoznávanie tváre a viacfaktorová autentifikácia (overenie používateľa s niekoľkými povereniami) pomáhajú nadviazať online dôveru, ale niečo sa stáva ťažším, keďže sa zvyšuje počítačová kriminalita a komerčné využívanie osobných údajov.

Rovnaká technológia, ktorá zlepšuje overovanie, môže vyčerpávať dôveru. Napríklad umelá inteligencia môže byť zraniteľná voči únosom a diskriminácii. Zatiaľ čo polícia v Naí Dillí bola v roku 2018 schopná použiť rozpoznávanie tváre na sledovanie tisícov nezvestných detí v priebehu niekoľkých dní, tá istá technológia sa môže použiť na sledovanie a útlak.

Ľudia požadujú ***viac údajov o svojich údajoch*** vedieť viac o tom, ako sa používajú, a prispôsobiť ich svojim potrebám. Technologické spoločnosti a vlády skúmajú decentralizované systémy identifikácie, ktoré takto posilňujú jednotlivcov.

Spoločnosti Microsoft, Accenture a Mastercard oznámili plány na investovanie do decentralizovaných modelov. Evernym a Learning Machine vytvárajú autonómne riešenia s otvoreným zdrojovým kódom a vláda Malty vyvinula spôsob, ako môžu vzdelávacie inštitúcie vydávať akademické osvedčenia založené na blockchainoch, ktoré vlastnia študenti a sú prenosné a okamžite overiteľné.

Podľa IDC bude mať do roku 2022 asi ***150 miliónov ľudí identitu založenú na blockchainu****, hoci táto technológia je stále v pomerne ranom štádiu vývoja.*

Agentúra a dôvera

*Vlády alebo banky tradične zohrávajú úlohu **„ukotvenia dôvery“,** hoci nové modely digitálnej identity zahŕňajú nových aktérov. Napríklad spoločnosť Capsule Pharmacy, ktorá sa označuje **„Uber na lieky“,** sa pri vypĺňaní elektronických predpisov na doručenie spolieha na lekárov ako na zdroj dôvery.*

Existuje niekoľko súvisiacich riadiacich snáh, ako je napríklad pan-kanadský trustový rámec a implementácia etickej stratégie AI zo strany Európskej únie. Monopolizácia technologických platforiem používaných pri vyhľadávaní a sociálnych médiách a všadeprítomné zhromažďovanie osobných údajov však komplikujú úsilie o získanie digitálnej dôveryhodnosti. Udalosti, ako nezákonné zhromažďovanie údajov Cambridge Analytica a využívanie údajov používateľov Facebookom na politickú reklamu, nepomáhajú.

Podľa výskumného centra Pew ***49%*** v roku 2018 ***amerických respondentov*** v prieskume nedôverovalo vláde na ochranu osobných údajov a ***51% neverilo spoločnostiam v oblasti sociálnych médií.*** Zatiaľ čo používatelia internetu očakávajú personalizované skúsenosti, očakávajú tiež bezpečnosť a sprostredkovanie svojich osobných údajov niečo, čo sľubuje, že sa stane konkurenčným diferenciátorom medzi spoločnosťami a organizáciami.

Zainteresované strany vo všetkých odvetviach by mali podporovať správcovstvo dobrej identity, umiestňovať používateľa do centra systémov identifikácie, vytvárať mechanizmy riadenia spolupráce a brať do úvahy interakcie medzi ľudskou a nehumánnou identitou.

Od Silos po spoluprácu

Kolaboratívne prístupy k digitálnej identite rozmazávajú tradičné hranice.

Inštitúcie tradične navrhovali systémy digitálnej identity z úzkej perspektívy vlastnej interakcie s používateľmi.

Pre používateľov to znamenalo nepohodlné rozhranie s viacerými často interoperabilnými systémami. Teraz inštitúcie začínajú reagovať na širší digitálny kontext používateľov skúmaním prístupov spolupráce, ktoré presahujú tradičné hranice. Vnútroštátne systémy identifikácie, ktoré sú interoperabilné a škálovateľné, môžu ušetriť peniaze, zlepšiť poskytovanie služieb a podporovať finančné začlenenie. Pre podniky môže tento prístup umožniť zákazníkom viac prehĺbiť dôveru, znížiť náklady a zdieľať zodpovednosť s ostatnými zúčastnenými stranami.

Normy Európskej únie v oblasti eIDAS podporujú harmonizáciu a vzájomné uznávanie vnútroštátnych systémov totožnosti vo všetkých členských štátoch čo je výhodné pre občanov EÚ, ktorí môžu robiť veci ako otvorenie bankového účtu v rámci bloku jednoducho pomocou národného preukazu totožnosti.

V inom príklade Estónsko a Fínsko zabezpečili interoperabilitu príslušných dátových vrstiev svojich identifikačných systémov, aby umožnili bezproblémové cezhraničné zdieľanie údajov o Estóncoch, ktorí žijú vo Fínsku, ale sú registrovaní na výhody a služby doma. Od roku 2018 používalo približne 1 000 organizácií v Estónsku a 81 vo Fínsku svoje vrstvy na výmenu údajov na ľahšie poskytovanie služieb.

Od Silos po spoluprácu

Hospodárska komisia Organizácie Spojených národov pre Afriku a Komisia Africkej únie spolupracujú na zvýšení regionálnej harmonizácie noriem digitálnej identity v rámci procesu rozvoja africkej kontinentálnej zóny voľného obchodu najväčšej zóny voľného obchodu na svete z hľadiska počtu účastníkov.

V rámci súkromného sektora vyvinul juhokórejský mobilný telefónny operátor SK Telecom *„T-Auth“,* ktorého cieľom je zefektívniť online nakupovanie jeho prepojením na mobilné čísla používateľov 99% webových stránok krajiny prijíma túto službu a do konca roku 2016 mala 13 miliónov používateľov mesačne, ktorí uskutočnili *650 miliónov transakcií ročne*, uviedla spoločnosť SK Telecom v správe uverejnenej v roku 2017.

Medzitým vo Švédsku finančné inštitúcie vyvinuli *„BankID“* na účely identifikácie. a prístup k účtu, daňové priznania a podpisovanie dokumentov. BankID má podľa odhadov *8 miliónov aktívnych používateľov* v roku 2018 sa však zistilo, že 14 osôb bolo uznaných vinnými za krádež ekvivalentu približne 160 000 dolárov volaním používateľov, predstieraním, že sú zástupcami banky.

Zainteresované strany vo všetkých odvetviach by mali vytvárať spoločné obchodné modely, spoločné zásady, normy, rámce a systémy identity, ktoré sú skutočne interoperabilné.

Podvody s identitou a kybernetická odolnosť

Zvyšujúce sa množstvo zhromažďovaných a využívaných osobných údajov

Rastúce využívanie digitálnej identity online v kombinácii s obrovským objemom osobných údajov, ktoré čoraz viac zhromažďujú vlády, podniky a všetko od nositeľných zariadení po domáce spotrebiče vytvárajú zraniteľné miesta.

Podľa indexu úrovne porušenia od roku 2013 bolo stratených, alebo odcudzených viac ako *15 miliárd údajových záznamov a 3,4 miliárd kompromitovaných záznamov*.

V prvej polovici roku 2018 to predstavuje 72% nárast v porovnaní s rovnakým obdobím minulého roka.

Medzi významné porušenia právnych predpisov v posledných rokoch patria kompromitované údaje takmer 150 miliónov ľudí v úverovej spravodajskej spoločnosti Equifax. Medzitým sa objavujú nové hrozby podľa Federálneho rezervného systému USA najrýchlejšie rastúci finančný zločin ***„syntetický podvod s totožnosťou“*** zahŕňa použitie falošných informácií na vytvorenie falošného úverového súboru. Objavilo sa niekoľko prístupov k lepšej bezpečnosti identít a zvýšeniu odolnosti vrátane minimálneho zberu a zverejňovania údajov a informovaného súhlasu.

Pomôcť môže aj posilnenie digitálnej gramotnosti a pomoc ľuďom lepšie porozumieť potrebe viacfaktorovej autentifikácie bez hesla.

Podvody s identitou a kybernetická odolnosť

Bezpečnosť je často priamo začlenená do návrhu systémov digitálnej identity.

Napríklad aplikácia belgickej vlády *„itsme“* používa multifaktorové autentifikačné kritériá vrátane biometrie, čísla mobilného telefónu a karty SIM prepojenej s používateľom spolu s osobným kódom banky. V dôsledku porušenia Equifaxu sa spoločnosť spojila s firmou FIS pre finančné technológie s cieľom vytvoriť *OnlyID*, nástroj digitálnej identity, ktorý využíva biometriu na zníženie podvodov, zlepšenie skúseností so zákazníkmi a obnovenie dôvery a lojality značky.

Pokiaľ ide o internet vecí, ktorý spája zariadenia každodenných spotrebiteľov prostredníctvom online pripojenia, Európsky inštitút pre telekomunikačné normy schválil súbor zásad zabezpečenia podľa návrhu, aby zariadenia neboli vopred nastavené pomocou hesiel, čím poskytne kontaktné miesto na podávanie správ a odpovedanie na problémy a včasné aktualizácie softvéru.

Dosiahnutie úplne neomylnej bezpečnosti je nemožné a bezpečnosť je skôr proces ako stav bytia.

Zainteresované strany vo všetkých odvetviach a priemyselných odvetviach by mali podniknúť proaktívne kroky v oblasti navrhovania a politiky na ochranu digitálnej identity a osobných údajov, poskytnúť mechanizmy na riešenie prípadov porušenia ochrany údajov a opätovného získania dôvery používateľov a podporiť školenie v oblasti digitálnych zručností.

Ochrana osobných údajov a ochrana údajov

Ochrana súkromia a osobnej slobody je kľúčom k akejkoľvek dobre navrhnutej digitálnej identite

Digitálna identita síce umožňuje lepší prístup a zvyšuje pohodlie, ale vytvára aj významné problémy týkajúce sa slobody a súkromia.

Napríklad indický biometrický systém digitálnej identity, ktorý sa nazýva *„Aadhaar“,* vyvolal verejnú a právnu diskusiu, ktorá v konečnom dôsledku viedla k tomu, že Najvyšší súd v roku 2018 obmedzil jeho používanie pričom uznával súkromie ako základné právo. V tom istom roku sa ukázalo, že analytická firma Cambridge Analytica získala informácie o miliónoch používateľov Facebooku bez ich vedomia s cieľom vybudovať nástroj politického profilovania a reklamy.

Medzi nedávne reakcie na obavy o ochranu súkromia a údajov patrí všeobecné nariadenie Európskej únie o ochrane údajov, požiadavka v americkom štáte Vermont, aby sa sprostredkovatelia údajov zaregistrovali vo vláde, a kalifornské právne predpisy, ktoré umožňujú obyvateľom odmietnuť predaj svojich údajov. Čína kladie prísne požiadavky na využívanie a prenos údajov mimo krajiny, ktoré dávajú vláde prednosť.

Celkovo 107 krajín zaviedlo právne predpisy na ochranu údajov a súkromia, podľa Konferencie OSN o obchode a rozvoji, hoci viac ako pätina, väčšinou v Ázii a Afrike, stále nepriniesla žiadny súvisiaci pokrok.

Ochrana osobných údajov a ochrana údajov

Nezávislý dohľad zo strany orgánov na ochranu údajov alebo komisárov na ochranu súkromia môže posilniť zodpovednosť a poskytnúť viac spôsobov, ako hľadať prostriedky na riešenie konfliktov záujmov vo veciach ako je národná bezpečnosť a práva jednotlivcov.

Medzitým môžu subjekty, ktoré vydávajú digitálne identity, odradené od zbytočného zhromažďovania osobných údajov a vedúci pracovníci môžu byť vyzvaní, aby sa viac zamerali na súkromie. Generálny riaditeľ spoločnosti Microsoft Satya Nadella vyzval technologické spoločnosti, aby považovali ***súkromie za ľudské právo a urobili z neho globálnu normu***, zatiaľ čo generálny riaditeľ spoločnosti Apple Tim Cook vyzval na ***komplexné zákony o ochrane súkromia*** v USA.

Estónsko, India a Rakúsko využívajú minimálny zber údajov a vo svojich vnútroštátnych systémoch používajú náhodne jedinečné identifikačné čísla a tokenizáciu. Medzičasom začínajúce podniky ako Privitar a BigID vytvárajú nástroje, ktoré organizáciám pomôžu vykonávať analýzu veľkých údajov a zároveň dodržiavať zákony o ochrane údajov.

Napriek všeobecne rastúcemu dôrazu na väčšie súkromie sa súvisiace postoje stále líšia a údaje týkajúce sa identity môžu byť ľahko zneužité alebo vložené do systémov umelej inteligencie, ktoré diskriminujú.

Zainteresované strany vo všetkých odvetviach a priemyselných odvetviach by mali do svojich obchodných stratégií a návrhov začleniť zásady ochrany súkromia a informovaného súhlasu, harmonizovať príslušné nariadenia a začleniť nezávislý dohľad do správy identity.

Ekonomická hodnota digitálnej identity

Digitálna identita sa môže premietnuť do vážnych ekonomických ziskov

V štúdii siedmich krajín uverejnenej v roku 2019 odhadoval Globálny inštitút spoločnosti McKinsey, že poskytovanie digitálnej identity by mohlo viesť do roku 2030 k ***pridanej ekonomickej hodnote až 13% HDP a ušetriť 110 miliónom hodín*** *prostredníctvom služieb elektronickej verejnej správy. Odhaduje sa, že 1,7 miliardy ľudí zostáva bez prístupu k formálnym finančným službám často v dôsledku nedostatku dokumentácie.*

Podľa štúdie by podniky mohli profitovať zo zvýšenej efektívnosti, znížených nákladov a podvodov vďaka digitálnej identite ušetriť až 1,6 bilióna dolárov.

Estónsko napríklad umožňuje verejné služby vrátane zdravotnej starostlivosti, bankovníctva a hlasovania prostredníctvom systému digitálnej identity. V Estónsku sa iba v roku 2014 použilo viac ako 80 miliónov krát overovanie a 35 miliónov krát digitálne transakcie. Odhaduje sa - ***až päť dní ušetrí*** digitálna identita zbytočných nákladov na byrokraciu, a ***zníži náklady rovnajúce sa 2% HDP.***

Medzitým indický systém digitálnej identity *„Aadhaar“* centralizovaným národným prostriedkom na podporu sociálneho začlenenia a prístupu k vládnym službám pokrýval 95% obyvateľstva od roku 2017 a vláde ***ušetril odhadom 9 miliárd dolárov*** znížením podvodov, podľa Deloitte.

Ekonomická hodnota digitálnej identity

Najmä odvetvie cestovného ruchu by malo mať z využívania digitálnej identity ekonomický úžitok.

Keďže medzi rokmi 2016 a 2030 sa medzinárodný letecký prírastok zvyšil o 50%, podľa Svetovej organizácie cestovného ruchu by koncepcia ako ***Digitálna identita známeho cestovateľa****, vyvinutá skupinou vlád a podnikov, mohla zmierniť tlak pomocou biometrických a biografických údajov a rýchle posúdiť riziko a overiť totožnosť.*

Podľa odvetvia OECD môže digitálna identita v odvetví dodávateľského reťazca pomôcť v boji proti ***falšovanému tovaru,*** ktorý predstavuje asi ***3% svetového obchodu***. Spoločnosti vrátane BMW a IBM sú členmi iniciatívy Mobility Open Blockchain Initiative, ktorá využíva blockchain na zníženie používania falšovaných náhradných dielov s cieľom zvýšiť bezpečnosť a zvýšiť transparentnosť.

Digitálnu identitu možno tiež použiť na overenie firiem online. Singapur vytvoril *„CorpPass“*, ktorý má uľahčiť digitálne transakcie medzi podnikmi a vládou, a vlády Britskej Kolumbie, Ontária a Kanady vytvorili *„sieť overiteľných organizácií“* na digitalizáciu vládnych osvedčení pre firmy, ako sú registrácie, povolenia a licencie.

Zainteresované strany v každom odvetví a priemysle by mali investovať do digitálnej identity ako základnej infraštruktúry, navrhovať flexibilné riešenia a odhaľovať viac prípadov použitia identity.

Zdroje

- World Economic Forum
- McKinsey and Comp
- *Gavi, The Vaccine Alliance*
- IDC
- Normy Európskej únie v oblasti eIDAS
- OSN
- OECD
- Deloitte
- *Svetová organizácia cestovného ruchu*