KRYPTOAKTIVA A VEŘEJNÁ POLITIKA

CENTRÁLNÍ EVIDENCE FINANČNÍCH ÚDAJŮ
RIZIKA A HROZBY PRO OBČANY

Kryptoaktiva, datová agregace
a rizika pro fyzickou bezpečnost

AUTOR
Ing. Jan Šincl
pod záštitou ČKMA

OBSAH

EXECUTIVE SUMMARY

Největším rizikem implementace evropské směrnice DAC8 v českém prostředí je možnost spojit identitu, bydliště a několik let kryptoměnové aktivity do profilu, který může při zneužití usnadnit výběr obětí trestných činů.

- **Agregace mění citlivost dat.** Pokud se údaje o člověku spojí napříč poskytovateli, státy a roky, vzniká kvalitativně nový obraz: kdo v minulosti pracoval s významnými objemy kryptoaktiv, kde žije a zda jeho aktivita naznačuje operace mimo regulované poskytovatele.
- **Ochranu nového rizikového systému nelze odmítnout s tím, že by bylo lepší jednou opravit všechny ostatní.** Pokud je obdobný bezpečnostní standard potřebný i u dalších systémů, je to legitimní téma pro širší změnu. Nebylo by však rozumné kvůli tomu rezignovat na vyšší ochranu právě u nově vznikajícího systému, který bude spojovat identitu, bydliště a údaje o aktivitě v kryptoaktivech.
- **U kryptoaktiv může únik skončit fyzickým násilím.** Self-custody umožňuje držet majetek bez banky a převést jej pod nátlakem rychle a prakticky nevratně. Evropské zkušenosti ukazují, že pachatelé před útokem zjišťují majetek, adresu a rodinné vazby oběti.
- **Největší slabina nemusí být technická.** Organizovaná skupina nepotřebuje stáhnout celou databázi. Může jí stačit zkorumpovat nebo jinak získat člověka s legitimním přístupem a nechat ho provádět několik cílených dotazů. Právě proto musí systém zaznamenávat nejen přístup, ale i jeho konkrétní důvod, účel, vyhledávání, kopírování, exporty a neúspěšné pokusy a musí umět odhalovat neobvyklé vzorce dotazů.
- **Česká RIA minula to nejdůležitější.** Hodnocení dopadů nezahrnulo zásah do soukromí mezi kritéria, podle kterých porovnávalo varianty, a bezpečnostní externalitu vznikající koncentrací identity a majetkové aktivity neposoudilo vůbec. Posouzení vlivu na ochranu osobních údajů v důvodové zprávě sice zpracování označuje za rizikové a velkého rozsahu, model hrozeb ani scénář zneužití oprávněného přístupu však neobsahuje. Výsledkem je, že klíčová bezpečnostní otázka se do rozhodování prakticky nedostala.
- **Evropa určuje, co se reportuje. Česko rozhoduje, jak nebezpečná budou data po převzetí.** DAC8 vyžaduje reporting i u českých rezidentů. Nevyžaduje však, aby český stát ponechal prostor pro vytvoření prohledávatelného dlouhodobého profilu každého občana, který vlastní kryptoaktiva. Česká úprava navíc volí desetiletou retenci u poskytovatelů na horní hranici evropského rozpětí, nevyužívá možnost vypustit místo narození a veřejně nepopisuje dobu uchování, přístupový model ani rozsah konsolidace na straně státu.
- **Přeshraniční předávání musí rozlišovat povinnost od volby.** Tam, kde výměnu ukládá DAC8 nebo jiný závazný režim, ji Česká republika musí provést. U nepovinného předávání z vlastního podnětu je však namístě vyžadovat konkrétní právní a daňový důvod a nepřenášet citlivá data jen proto, že technicky mohou být předána. U finančních dat s možnými fyzickými následky má být nutnost předání součástí bezpečnostního posouzení.
- **Ústavní otázka začíná tam, kde existuje méně invazivní cesta.** Ústavní soud pracuje s právem na informační sebeurčení a s principem informačního sebeomezení státu. Pokud lze stejný daňový cíl splnit tak, že stát report přijme, ale nejcitlivější položky segmentuje a jejich spojení s osobou podmíní konkrétním účelem, musí být případná invazivnější plošná analytická dostupnost přesvědčivě odůvodněna.
- **Řešení existuje a nesnižuje rozsah evropského reportingu.** Finanční správa může přijmout celý report, ale oddělit nejcitlivější vrstvu, vázat přístup na konkrétní spis nebo jiný doložený účel, používat nezměnitelné logy, detekci anomálií, princip čtyř očí u exportů a technicky omezit hromadné řazení osob podle majetkové aktivity. Občan má mít možnost zjistit, kdo a proč k jeho údajům přistupoval.

Otázka pro Českou republiku tedy není, zda data budou reportována. Otázka je, zda bude systém navržen tak, aby se z povinně získaných údajů při zneužití nemohl snadno stát nástroj pro výběr obětí.

1. JAK AGREGACE DAT MĚNÍ JEJICH BEZPEČNOST

Moderní finanční regulace produkuje o lidech záznamy, které umožňují jejich identifikaci, ve stále větším množství. Poskytovatelé finančních služeb musí znát své klienty a uchovávat o nich doklady, daňové správy si mezi sebou automaticky vyměňují informace o účtech svých rezidentů a řada majetkových vztahů se povinně zapisuje do veřejných nebo neveřejných rejstříků.

Finanční záznamy pokrývající období například jednoho měsíce nebo roku jsou samy o sobě pouze slabým zdrojem informací. Řeknou nám třeba informace o proběhlých transakcích, ale pravděpodobně z nich nebudeme schopni poskládat obraz toho, jakým majetkem daný člověk momentálně disponuje.

Zásadní změnu do tohoto obrazu však přináší spojování. Unikátní identifikátory, u daňových agend například daňové identifikační číslo, umožňují záznamy spolehlivě přiřadit ke konkrétní osobě napříč zdroji a napříč roky. Z údajů, které samy o sobě nemají příliš vysokou informační hodnotu, vzniká určitý profil daného člověka.

Aktuálním příkladem tohoto tlaku na podrobnější sběr dat o jednotlivcích je evropská úprava oznamování transakcí s kryptoaktivy, která se v České republice právě projednává. Předkládaná legislativa člení oznamované údaje do dvou skupin.

- Identifikační skupina obsahuje jméno, adresu bydliště, stát nebo státy daňové rezidence, DIČ, datum a místo narození.
- Transakční skupina obsahuje u každého druhu kryptoaktiva souhrnné hodnoty a počty transakcí za dané období.[1]

Kromě těchto údajů jsou součástí oznámení také převody na adresy, které nejsou adresami jiného poskytovatele nebo finanční instituce. Zvlášť se pak vykazuje takzvaná oznamovaná maloobchodní platební transakce, tedy platba za zboží nebo služby v hodnotě přesahující 50 000 amerických dolarů.[2]

Nic z toho nám samozřejmě neřekne, kolik daný člověk v současné době vlastní té které kryptoměny.

Bezpečnostní problém ale účetní přesnost nevyžaduje. Útočníkovi zpravidla postačí informace, že konkrétní osoba v posledních letech obchodovala v relativně vysokých objemech. V tom také spočívá rozdíl mezi záznamem a profilem. Záznam popisuje jednu událost v jednom roce u jednoho poskytovatele. Profil vzniká tehdy, když někdo záznamy spojí a může je využít k plánování a provedení násilné činnosti.

Námitka proti výše uvedenému je jednoduchá. Údaje, o kterých je řeč, přece existují už dnes. Každý regulovaný poskytovatel zná totožnost svých klientů, jejich adresu i objem jejich obchodů, protože mu to ukládají pravidla proti praní špinavých peněz. A faktem je, že několik těchto soukromých databází už v minulosti uniklo. Pokud tedy stát vytvoří vlastní úložiště, nepřidá nic nového, jen přesune riziko z jednoho místa na druhé. Níže však nalezneme čtyři vlastnosti centrálního státního úložiště, kterými nedisponuje žádný ze soukromých poskytovatelů:

- **Burza vidí svého klienta a nic víc.** Nemá jak zjistit, co tentýž člověk dělá u konkurence, a nemá k tomu ani oprávnění. Pokud oproti tomu vznikne státní úložiště, které bude přijímat hlášení od všech domácích poskytovatelů najednou, umožní jednoznačné identifikátory, například DIČ, záznamy spolehlivě spojit.
- **Pokud člověk není spokojen se službami poskytovanými soukromým subjektem, může odejít jinam**, zvolit poskytovatele s jinými podmínkami nebo službu zcela přestat využívat. Vůči státu tato volba neexistuje.
- **Stát dostává údaje o vlastních rezidentech také od zahraničních daňových správ.** Žádný domácí poskytovatel takovou informací logicky nedisponuje. V rámci českých reálií je tento fakt o to podstatnější. Závěrečná zpráva o hodnocení dopadů regulace k vládnímu návrhu totiž sama uvádí, že většina tuzemských uživatelů kryptoaktiv využívá poskytovatele sídlící mimo Českou republiku.[3] V takovém úložišti se tedy ocitnou i lidé, kteří u českého poskytovatele účet nikdy neměli.

[1] Důvodová zpráva k vládnímu návrhu zákona, kterým se mění zákon č. 164/2013 Sb., kap. 10.3. Sněmovní tisk 98, PDF str. 62 (dokument str. 60).

[2] Navrhované znění zákona, sněmovní tisk 98, PDF str. 11 a 161. K rozsahu oznamovaných údajů dále příloha VI směrnice Rady (EU) 2023/2226.

[3] Závěrečná zpráva z hodnocení dopadů regulace k návrhu zákona, kterým se mění zákon č. 164/2013 Sb., část A, kap. 1.1. Sněmovní tisk 98, PDF str. 117 (dokument str. 6).

- **Poskytovatel po zániku vztahu maže veškerá data, s výjimkou těch, která uchovat musí.** Naproti tomu stát je drží po dobu, kterou určuje retenční rámec, který si sám stanovuje. Vládní návrh volí u poskytovatelů retenci dat po deset let, tedy na samé horní hranici rozpětí, které evropská směrnice připouští.[4]

Pokud je databáze vytvořena profesionálně a udržuje si vysoké bezpečnostní standardy, je jedno, zda je provozována veřejným nebo soukromým sektorem. Problém tkví v rozsahu škody, kterou způsobí jediné selhání. Pokud uniknou data z jedné soukromé databáze, škody jsou omezeny pouze na klienty dané platformy. Pokud se to stane u souhrnné státní databáze obsahující klienty všech poskytovatelů, rozsah problému je řádově větší. Jak dlouho bude stát oznámené údaje držet, přitom návrh neurčuje. Desetiletá lhůta, kterou stanoví, dopadá na poskytovatele.

Čtyři vlastnosti, které má státní úložiště navíc

Vidí všechny domácí poskytovatele najednou. Nelze se mu vyhnout odchodem ke konkurenci. Dostává údaje i od zahraničních daňových správ. A dobu, po kterou si je ponechá, si určuje samo.

V květnu 2025 oznámila společnost Coinbase, že se útočníci dostali k zákaznickým datům. Podle vlastního sdělení společnosti oslovili zahraniční pracovníky zákaznické podpory Coinbase s nabídkou finanční odměny za předání dat zákazníků platformy.[5] Odcizená data zahrnovala například jméno, adresu, kontaktní údaje, bankovní identifikátory, snímky dokladů totožnosti, informace o zůstatku nebo historii transakcí.[6] Pokud by se něco takového stalo v centralizované státní databázi, následky by byly nedozírné.

Výše uvedený příklad nám ale ukazuje ještě jeden úhel pohledu. I v sebelépe technicky zabezpečeném systému je jeho nejzranitelnějším článkem člověk, který do něj má přístup. Ať už na něj útočníci zvolí metodu cukru v podobě finanční odměny nebo biče v podobě výhružek a násilí, vždy existuje možnost, že daná osoba selže a data vydá třetí straně.

Tvrzení, že stát chrání data hůře než soukromé firmy, není empiricky obhajitelné. Oproti soukromě spravovaným databázím mají však ty státní několik strukturálních zvláštností, které se pojí se samotným postavením státu a které u soukromého správce nenajdeme.

- **Stát nezanikne kvůli jednomu úniku.** Soukromá firma, která opakovaně ztrácí data svých klientů, přichází o klienty a v krajním případě o možnost podnikat. U státního systému tato zpětná vazba chybí, protože povinnost odevzdat údaje trvá bez ohledu na to, jak dobře je stát v minulosti chránil.
- **Šíře záběru bývá výjimečná.** Soukromý poskytovatel má tolik klientů, kolik si jich získal. Státní systém pokrývá z podstaty věci všechny, na které dopadá zákonná povinnost, a nemá horní hranici danou trhem.
- **Odpovědnost je rozptýlená mezi mnoho útvarů a dodavatelů.** Zatímco u soukromé firmy lze zpravidla určit jednoho správce a jednoho odpovědného člověka, u státního informačního systému vstupují do hry provozovatel, integrátoři, správci sítě a externí dodavatelé podpory.

[4] Rozpětí nejméně pěti a nejvýše deseti let stanoví příloha VI směrnice Rady (EU) 2023/2226; viz rozdílovou tabulku ke sněmovnímu tisku 98, PDF str. 244. Desetiletou lhůtu volí navrhovaný § 15zd, tamtéž, PDF str. 18.

[5] Coinbase, Protecting Our Customers - Standing Up to Extortionists, 15. 5. 2025.

[6] Tamtéž. Společnost uvádí, že šlo o klienty představující méně než jedno procento měsíčně aktivních uživatelů; méně než jedno procento uživatelů, kteří v daném měsíci provedli transakci; podle pozdějšího oznámení úřadu generálního prokurátora státu Maine šlo o 69 461 osob. Útočníci požadovali 20 milionů dolarů, společnost odmítla zaplatit a vypsala odměnu ve stejné výši za informace vedoucí k dopadení pachatelů.

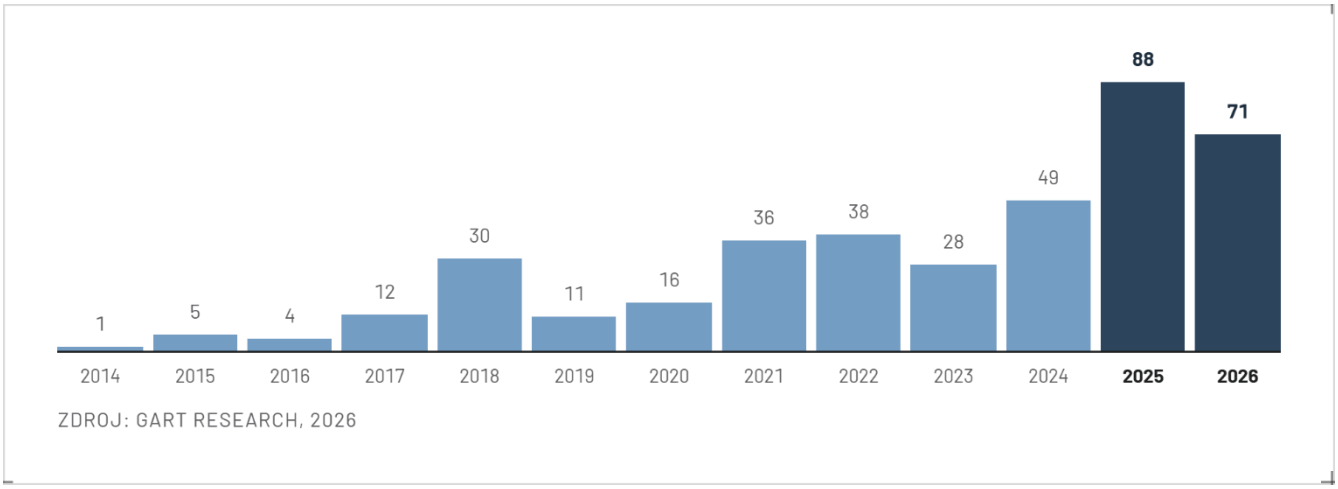
2. ANATOMIE ÚTOKŮ NA DRŽITELE KRYPTOAKTIV

Fyzické útoky na držitele kryptoaktiv tvoří samostatnou kategorii, kterou je možné sledovat teprve několik let a jejíž skutečný rozsah nikdo nezná. Veřejné přehledy vycházejí z medializovaných případů a řada incidentů se do médií nedostane vůbec, protože oběť o útoku mlčí.

Nejdéle vedený veřejný, který zachycuje případy od roku 2014, spravuje Jameson Lopp. Sám u něj výslovně upozorňuje, že seznam není úplný, protože mnoho incidentů není medializováno nebo není veřejně spojeno s kryptoaktivy.[7]

Na tuto práci navazuje Gart Research, který případy strukturuje a doplňuje statistiku. K datu uzávěrky této studie evidoval 389 zdokumentovaných incidentů v 59 zemích. Počet evidovaných případů vzrostl ze 49 v roce 2024 na 88 v roce 2025, tedy o 80 %. Gart Research z Loppova katalogu vychází a Loppův katalog naopak odkazuje na jeho statistiky; oba zdroje proto nejsou na sobě nezávislé.[8]

GRAF 1 **Incidence útoků evidovaných Gart Research v letech 2014 – 2026**[9]



ZDROJ: GART RESEARCH, 2026

Dalším relevantním zdrojem dat k problematice je recenzovaná studie z konference AFT 2024, kterou autoři označují za první komplexní empirickou práci na toto téma. Popisuje pachatele od organizovaných skupin až po známé a rodinné příslušníky, formy útoku od vydírání po vraždu a upozorňuje, že zkušenost s kryptografickým zabezpečením sama o sobě proti fyzickému útoku neochrání. Autoři zároveň upozorňují na dvousečnost pravidel pro rozpoznávání klientů. Data, která slouží k prevenci praní špinavých peněz, se totiž jednoduše stávají vodítkem pro pachatele.[10]

Analytická společnost CertiK, sleduje případy, jež lze nezávisle ověřit z policejních hlášení, soudních dokumentů, médií, svědectví obětí nebo z blockchainových stop. Společnost uvádí, že v prvním pololetí roku 2026 evidovala 52 případů oproti 39 ve stejném období roku 2025. Podstatnější, než celkový nárůst, je struktura těchto případů.[11]

[7] Jameson Lopp, Known Physical Bitcoin Attacks, veřejný katalog vedený od prosince 2014.

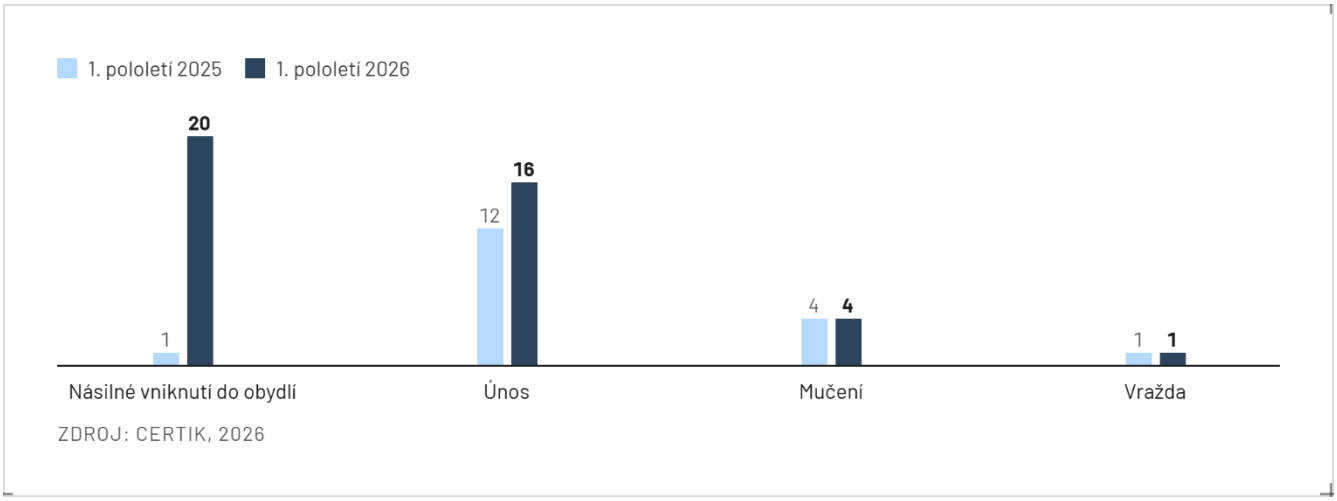
[8] Gart Research, veřejný přehled statistik fyzických útoků. Údaje odpovídají stavu katalogu k datu uzávěrky této studie; poslední případ byl do katalogu doplněn 9. 9. 2026. Katalog se doplňuje i zpětně, čísla se proto v čase mění.

[9] Sloupec pro rok 2026 obsahuje data pouze do 9.9. 2026.

[10] Ordekian, M., Atondo-Siu, G., Hutchings, A., Vasek, M., Investigating Wrench Attacks: Physical Attacks Targeting Cryptocurrency Users, AFT 2024, 16. 9. 2024.

[11] CertiK, Intel3D: Wrench Attacks H1 2026, 23. 7. 2026. Zpráva uvádí nárůst případů vniknutí do obydlí z jednoho v prvním pololetí 2025 na dvacet ve stejném období roku 2026, u únosů z dvanácti na šestnáct, u mučení shodně čtyři a u vražd shodně jeden případ. Zaznamenaná majetková expozice ověřených případů vzrostla z 10,5 milionu amerických dolarů na 124,1 milionu.

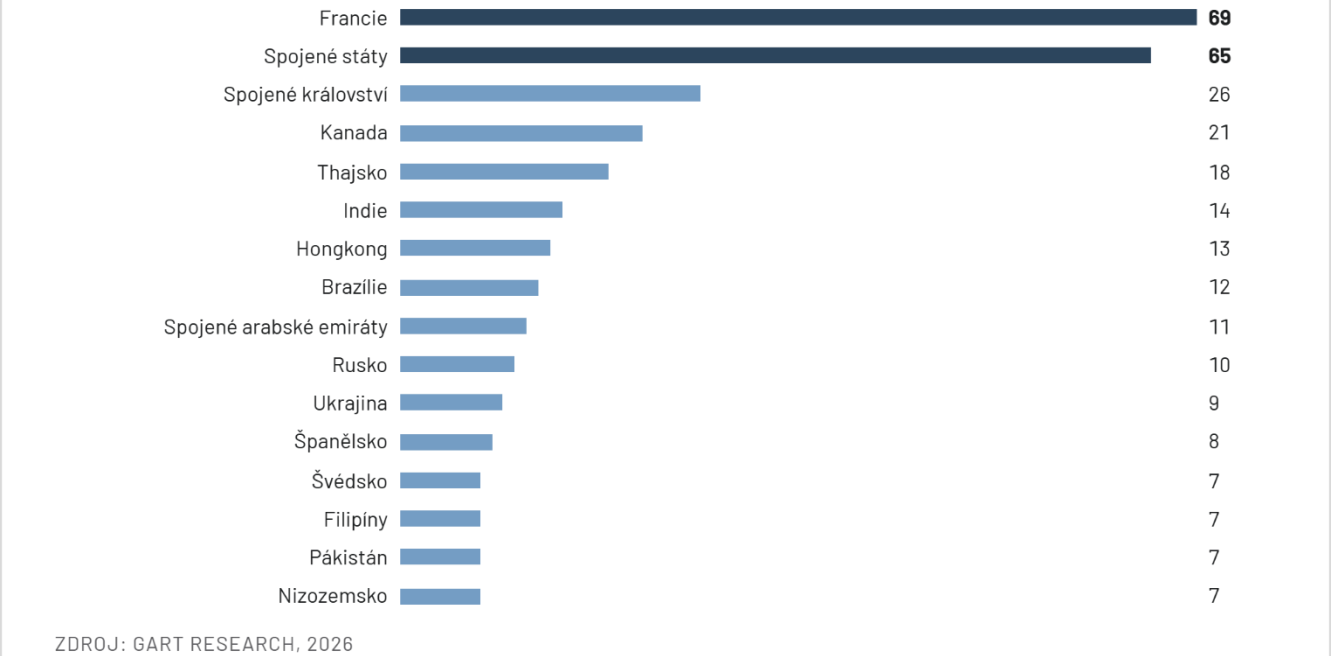
GRAF 2 **Struktura útoků v porovnání prvních pololetí 2025 a 2026**[12]



ZDROJ: CERTIK, 2026

Nárůst z jednoho případu na dvacet se týká právě té kategorie, u níž pachatel musí předem znát bydliště oběti. Stejný směr ukazuje i analýza společnosti Chainalysis, která pracuje s odlišným souborem případů: podíl vniknutí do obydlí u ní vzrostl ze 14 % v roce 2025 na 37 % v první polovině roku 2026 (v roce 2023 činil 26 %) a útoky mířené na rodinné příslušníky nebo blízké osoby se zvýšily z hodnoty blízké nule v roce 2021 na 25 až 30 % počátkem roku 2026.[13]

GRAF 3 **Rozdělení útoků evidovaných Gart Research dle zemí v letech 2014 – 2026**[14]



ZDROJ: GART RESEARCH, 2026

S uvedenými čísly je třeba pracovat opatrně. Jednotlivé databáze používají odlišné definice i odlišná kritéria pro zařazení případu. Přehledy, které přebírají medializované zprávy, vykazují systematicky vyšší počty než ty, které trvají na ověření z policejních nebo soudních zdrojů. Trend posledních let je však jednoznačný. Fyzické útoky na držitele kryptoaktiv existují, jejich počet v posledních letech roste a mění se jejich provedení směrem k pečlivěji připraveným scénářům, které vyžadují znalost bydliště oběti a jejího okolí.

[12] Graf zobrazuje jen vybrané kategorie; jejich součet (18, resp. 41) je nižší než celkový počet případů (39, resp. 52). CertiK řadí případy podle převažujícího donucovacího mechanismu a v roce 2026 zavedl novou kategorii vynuceného převodu, meziroční srovnání kategorií je proto třeba číst opatrně.

[13] Chainalysis, Violent Wrench Attacks Targeting Crypto Holders, 6. 8. 2026. Chainalysis řadí případ podle převažujícího následku, takže případ, který začal vniknutím do obydlí a skončil odvlečením oběti, vykazuje jako únos. Jiné přehledy řadí tytéž případy podle způsobu prvotního vniknutí a docházejí k vyššímu podílu vniknutí do obydlí; zdroj na tento rozdíl sám upozorňuje.

[14] Vybrány země se sedmi a více útoky. Celý přehled je k dispozici na stránkách Gart Research.

Každý útok má dvě fáze a na veřejnost zpravidla prosákne pouze jedna z nich – samotné provedení, tedy vniknutí do bytu, únos nebo nátlak. Předchází jí ale práce, o které se nemluví, protože po ní nezůstávají stopy. Pachatel musí zjistit, kdo má dost majetku, kde bydlí, kdy bývá doma a zda je pravděpodobné, že prostředky dokáže sám převést. Ve veřejně dokumentovaných datech je v posledních letech patrný výrazný nárůst a řada případů vykazuje znaky předchozího cíleného výběru oběti.

> **Číslo, které je třeba číst pozorně**
>
> Vniknutí do obydlí: jeden veřejně oznámený případ v prvním pololetí 2025, dvacet ve stejném období roku 2026. Právě u této kategorie musí pachatel předem znát adresu oběti.
>
> CertiK, Intel3D: Wrench Attacks H1 2026

Nejlepší dostupný popis přípravné fáze pochází ze společného materiálu Metropolitní policie a společnosti TRM Labs z července 2026. Autoři analyzovali sedmnáct případů oznámených v Londýně mezi březnem a prosincem 2024 a cesty, kterými se pachatel k oběti dostal, roztřídili do čtyř skupin.[15]

- **Dobrovolná expozice**, která podle materiálu tvořila 47 % případů. Oběť o svém majetku sama informovala veřejnými příspěvky o držených objemech, obchodní aktivitou, profilem influencera nebo viditelnou vazbou na kryptobyznys. Materiál výslovně upozorňuje na skupiny na Telegramu a Discordu organizované kolem obchodování a osobních setkání, které podle autorů vytvářejí koncentrovanou a snadno zneužitelnou expozici. Jde o nejčastější cestu a zároveň o jedinou, kterou má oběť plně ve svých rukou.
- **Komunitní expozice.** Konference, fóra a uzavřené kanály soustřeďují na jednom místě lidi s nadprůměrným majetkem. Pachatel nemusí znát konkrétní jméno předem, stačí mu vědět, kde hledat.
- **Nedobrovolná expozice.** Sem patří data z úniků, převzetí telefonního čísla nebo odcizené zařízení. Autoři jako doložený příklad uvádějí únik u výrobce hardwarových peněženek Ledger z roku 2020, při kterém se dostalo ven 272 000 záznamů zákazníků včetně fyzických adres.[16] Oběť v tomto případě neudělala nic, čím by na sebe upozornila.
- **Expozice přes okolí.** Útok míří na rodinné příslušníky nebo blízké osoby jako na cestu k hlavnímu držiteli. Tato kategorie v posledních letech výrazně roste, jak ukazuje například statistika Chainalysis zmíněná výše.

Pachatel potřebuje získat odpověď na dvě otázky. Kdo stojí za pozornost a kde ho najít. Většina zdrojů odpovídá jen na jednu z nich. Kupříkladu sociální sítě mohou prozradit, že někdo pravděpodobně něco vlastní. Naopak třeba veřejné registry prozradí adresu, ale o likvidním majetku neřeknou nic. U konsolidovaného úředního souboru tato práce odpadá. Pokud jeden dotaz spojí totožnost, bydliště a kvantifikovanou majetkovou aktivitu za několik let, pachatel už nemusí zjišťovat, zda daný člověk vůbec stojí za pozornost. Zbývá mu ověřit, jestli je oběť fyzicky dosažitelná a jestli je informace stále aktuální.

Z hlediska prevence z toho plyne nepříjemný závěr. Proti dobrovolné expozici se člověk bránit umí, stačí o svém majetku mlčet. Proti zbylým třem cestám se brání obtížně. Ale proti nedobrovolné expozicí z úřední databáze se nedá bránit vůbec. O tom, jak dobře je člověk v takovém případě chráněn, rozhoduje někdo jiný.

[15] TRM Labs a Metropolitan Police Service, Wrench Attacks: A Crypto Crime Response Framework, 30. 7. 2026.

[16] Tamtéž. Akademický rozbor následků tohoto úniku viz Abramova, S., Böhme, R., Anatomy of a High-Profile Data Breach: Dissecting the Aftermath of a Crypto-Wallet Case, USENIX Security 2023.

3. VAROVÁNÍ Z EVROPY

FRANCIE: ZNEUŽITÍ PŘÍSTUPU UVNITŘ DAŇOVÉ SPRÁVY

Francouzský případ je nejbližší analogií k tomu, čím se tato studie zabývá. Je proto potřeba přesně vymezit, co z něj plyne. Analytická společnost Chainalysis ve své zprávě ze srpna 2026 uvádí, že v roce 2024 měla pracovnice francouzské daňové správy v pařížské oblasti odcizit a prodávat složky o movitých držitelích kryptoaktiv. Podle téhož zdroje obsahovaly tyto složky jména, adresy, informace o držených objemech, telefonní čísla a daňové záznamy, které od pracovnice nakupovali kriminální zprostředkovatelé.[17] Podle deníku Le Parisien byla bývalá pracovnice finanční správy mimo jiné obviněna z neoprávněného využívání interních daňových nástrojů. Vyšetřování například popisovalo případ vězeňského dozorce, jehož novou adresu měla pracovnice vyhledat v daňovém systému a který byl následně se svou manželkou doma napaden třemi ozbrojenými muži. Mezi jejími dotazy se objevovali také specialisté a investoři z kryptoměnového prostředí.[18]

Pro českou debatu z toho plyne jedno konkrétní poučení. K úniku nemusí dojít hackerským průnikem do celé databáze. Postačí oprávněný účet, který někdo používá k cíleným dotazům, a odbyt na straně organizovaného zločinu. Takový model je obtížněji zjistitelný než hromadné stažení dat, protože nevytváří žádnou anomálii v objemu přenosů.

NORSKO: VEŘEJNÉ MAJETKOVÉ ÚDAJE A VÝBĚR OBĚTÍ

Norský systém daňových seznamů zveřejňuje u fyzických osob jméno, rok narození, poštovní směrovací číslo s obcí, daňovou obec, čistý zdanitelný příjem, čisté zdanitelné jmění a vyměřenou daň.[19] Policejní ředitelství této severské země v roce 2009 uvedlo, že je pravděpodobné, že jsou daňové seznamy používány při cílení loupeží, výhrůžek, krádeží a podvodů. Popsalo sérii výhrůžných dopisů zaslaných majetným lidem v Oslu, vloupání a pokusů o loupež, které byly přímo spojeny s cíleným vyhledáváním v daňových seznamech. Norské orgány zároveň upozorňovaly, že nejde o důkaz masového rozšíření tohoto jevu, jednalo se jen o několik závažných případů.[20]

Podstatná je reakce, kterou Norsko zvolilo. Od roku 2011 nesmějí být daňové seznamy zveřejňovány v podobě, ve které v nich lze vyhledávat. Od roku 2013 je vyhledávání možné pouze po přihlášení a hledaná osoba se o dotazu dozví. Dnešní pravidla pocházejí z roku 2014. Norská daňová správa u toho uvádí konkrétní rozsah, tedy jméno hledajícího, jeho rok narození, poštovní směrovací číslo s obcí a čas dotazu. Kompletní elektronické seznamy přitom novináři pro žurnalistické účely dostávají dodnes, a to na základě smlouvy o jejich užití. Omezení tedy nemíří na přístup k údajům jako takový, směřuje proti tomu, aby v nich mohl kdokoli anonymně a hromadně vyhledávat.[21]

ŠVÉDSKO: ROZHODUJÍCÍ JE SPOJITELNOST ÚDAJŮ

Švédsko dnes nezveřejňuje čisté jmění tak jako Norsko. Dlouhodobě má ale mimořádně otevřené osobní registry a rozvinutý trh komerčních vyhledávacích služeb, které údaje z různých zdrojů spojují a nabízejí je v jednom rozhraní. Švédská vláda v letech 2023 a 2024 opakovaně uvedla, že kriminální sítě mohou tyto služby využívat k mapování potenciálních obětí.[22] Dozorový úřad pro ochranu osobních údajů k tomu ve svém právním stanovisku uvádí, že tyto služby zpřístupňují například jméno, adresu, věk, velikost domácnosti, držbu vozidel, firemní vazby a údaje o odsouzeních v trestních věcech.[23] Vládní vyšetřování z roku 2024 se touto otázkou zabývalo systematicky a vedlo k návrhu na posílení ochrany osobních údajů zveřejňovaných ve vyhledávacích službách.[24] Švédská zkušenost je pro tuto studii relevantní kvůli mechanismu spojování, který popisuje. Jednotlivé registry byly veřejné po desetiletí, aniž by to působilo problém. Problémem se stala až technická možnost je spojit a prohledávat najednou.

[17] Chainalysis, Violent Wrench Attacks Targeting Crypto Holders, 6. 8. 2026. Tatáž analýza uvádí i únik u francouzské kryptodaňové služby Waltio z ledna 2026, který se týkal přibližně 50 000 uživatelů.

[18] Le Parisien, L'agente du fisc ciblait gardiens de prison et investisseurs en cryptomonnaie pour un mystérieux commanditaire, 6. 1. 2026.

[19] Skatteetaten, Search the tax lists.

[20] Stanovisko norského policejního ředitelství (Politidirektoratet) z dopisu ze dne 19. 11. 2009, citované v dokumentu Stortinget, Dokument 8:15 S (2010–2011). Tentýž dokument cituje i navazující dopis policejního ředitelství ze dne 1. 2. 2010, podle kterého nelze z dostupných informací dovodit, že by se údaje z daňových seznamů využívaly ve velkém rozsahu.

[21] Skatteetaten, informace k vyhledávání v daňových seznamech. Přehled změn od roku 2011 do roku 2014 popisuje Skatteetaten v materiálu k historii daňových seznamů.

[22] Regeringskansliet, tisková zpráva Skyddet för personuppgifter ska förstärkas, 21. 10. 2023, a Kommittédirektiv Dir. 2023:145 ze dne 19. 10. 2023. Tentýž závěr zopakovala vláda v tiskové zprávě Utredning föreslår stärkt skydd för personuppgifter som offentliggörs i söktjänster ze dne 22. 11. 2024.

[23] Integritetsskyddsmyndigheten (IMY), právní stanovisko Klagomål mot söktjänster med utgivningsbevis, IMYRS 2024:1, 14. 5. 2024.

[24] SOU 2024:75, Personuppgifter och mediegrundlagarna, 20. 11. 2024.

4. RIZIKA

LIDSKÝ FAKTOR

Představa úniku bývá spojena s hackerským útokem a následným stažením celé databáze. Pro organizovaný zločin je ale zpravidla hodnotnější jiný model. Stačí získat jednoho člověka, který má do systému legitimní přístup, a nechat ho provádět malý počet cílených dotazů na konkrétní osoby. Tento model má z pohledu pachatele několik výhod. Vyhne se většině kontrol, protože ty bývají navrženy proti hromadné exfiltraci a reagují na neobvyklý objem přenesených dat. Výstup je navíc přesně cílený, takže odpadá práce s tříděním velkého objemu záznamů. Dva případy popsané v předchozích kapitolách odpovídají tomuto vzorci. Ve francouzském případě šlo o pracovnici daňové správy s přístupem k interním nástrojům a datům. U společnosti Coinbase pak o zaměstnance zákaznické podpory, kteří data zkopírovali z nástrojů, se kterými denně pracovali. Ani v jednom případě nemusel útočník prolomit technickou ochranu.

Oba případy nám zároveň dávají návod, jak by mohla vypadat ochrana před tímto nežádoucím typem jednání. Systém musí zaznamenávat nejen to, že k záznamu někdo přistoupil, ale i důvod, spisovou značku nebo účel dotazu. Musí umět rozpoznat vzorec, ve kterém pracovník opakovaně vyhledává majetné osoby bez vazby na svou agendu. A musí být chráněna proti tomu, aby ji obešel právě ten, kdo systém spravuje.

KONCENTRACE HODNOTY

Bezpečnostní inženýrství pracuje s jednoduchým principem. Čím vyšší je informační hodnota soustředěná v jednom systému, tím atraktivnějším cílem se systém stává, a to nezávisle na tom, jak dobře je zabezpečen. Motivace útočníka roste s hodnotou kořisti, zatímco obtížnost útoku roste s kvalitou obrany. Tyto dvě veličiny se pohybují nezávisle na sobě. Neveřejnost systému tento problém neřeší. Utajení chrání před náhodným kolemjdoucím a nechrání před tím, kdo o existenci systému ví a má motiv se do něj dostat. Součástí prostoru pro útok jsou navíc privilegované účty, administrátoři, servisní organizace, testovací prostředí a integrační rozhraní na další systémy.

Rozhodující otázka proto zní, zda centrální systém potřebuje trvale uchovávat a zobrazovat celý agregovaný profil osoby. Pokud data mohou zůstat rozdělená tak, že jejich spojení vyžaduje další oprávněný krok, klesá hodnota systému pro útočníka, aniž by se podstatně snížila jeho použitelnost pro účel, kvůli kterému vznikl.

ROZŠIŘOVÁNÍ ÚČELU SYSTÉMU

Jev, kterému se anglicky říká „function creep“, je běžným typem institucionálního chování. Jakmile už jednou drahý informační systém funguje, začnou se objevovat návrhy využít ho i pro jiné cíle, protože alternativou by bylo postavit další systém za další prostředky. U daňových a majetkových dat se nabízejí především jejich využití pro boj s praním peněz, trestní řízení, exekuční agendu nebo třeba analytické vyhodnocování rizik. Každý jednotlivý návrh může být samozřejmě politicky i věcně obhajitelný. Součet těchto rozšíření ale postupně mění povahu systému, aniž by o této změně kdy proběhlo samostatné rozhodnutí. Omezení účelu zakotvené v zákoně, technicky vynucené oddělení datových domén, minimalizace rolí a to, že pokročilé analytické funkce, které pro původní účel nejsou potřeba, v systému vůbec nevzniknou, jsou v tomto ohledu minimálními požadavky, aby k bezbřehému rozšiřování funkcí systému v budoucnu nedocházelo. Podobný požadavek ostatně vznesl v roce 2023 i evropský inspektor ochrany údajů, když u návrhu evropské úpravy oznamování kryptoaktiv žádal taxativní výčet účelů dalšího zpracování.[25]

NEVRATNOST ÚNIKU

Kybernetická bezpečnost běžně pracuje s obnovitelností. Heslo lze změnit, certifikát revokovat, zranitelný server odpojit a napadený systém obnovit ze zálohy. Většina bezpečnostních postupů z tohoto předpokladu vychází a hodnotí incident podle toho, jak rychle se podaří obnovit původní stav. U historické finanční informace tento předpoklad neplatí. Údaj o tom, co člověk v minulosti nakoupil a kam to převedl, nelze změnit ani po incidentu. Pokud se jednou rozšíří věrohodná informace, že určitá osoba dlouhodobě akumulovala významné množství kryptoaktiv a část z nich odeslala mimo regulované poskytovatele, pozdější prodej ani změna způsobu držení nezpůsobí, že ji pachatelé přestanou považovat za vhodný cíl.

Databázi lze vypnout, zranitelnost opravit a odpovědného člověka potrestat. Uniklé kopie, snímky obrazovky a jednotlivé záznamy, které mezitím změnily majitele, ale stáhnout zpět nelze. Náprava po incidentu tady funguje jen omezeně.

[25] Stanovisko evropského inspektora ochrany údajů 2023/C 199/04 ze dne 3. 4. 2023 k návrhu směrnice Rady, kterou se mění směrnice 2011/16/EU o správní spolupráci v oblasti daní. Úř. věst. C 199, 7. 6. 2023, s. 5.

5. KDO ROZHODUJE O NAŠICH DATECH

Listina základních práv a svobod chrání soukromí ve dvou rovinách. Vedle ochrany před neoprávněným zasahováním do soukromého života zakotvuje samostatně ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o osobě.[26] Nejpodrobněji tuto ochranu rozvedl Ústavní soud v nálezu k plošnému uchovávání provozních a lokalizačních údajů z března 2011, kterým zrušil příslušná ustanovení zákona o elektronických komunikacích a navazující vyhlášku.[27]

Soud v něm pracuje s právem na informační sebeurčení a vychází z toho, že jednotlivec musí mít kontrolu nad tím, které jeho osobní údaje jsou zveřejňovány, uchovávány nebo použity, a v jakém rozsahu a jakým způsobem se dostávají k jiným.[28]

Pro naši problematiku je podstatná pasáž o tom, co vzniká spojováním. Soud dovodil, že z kombinace údajů, které samy o sobě nevypovídají o obsahu komunikace, lze odvodit politické zaměření a osobní sklony člověka a zjistit, s kým a jak často se stýká.[29]

> **Čtyři požadavky evropského inspektora ochrany údajů**
>
> Taxativní výčet účelů dalšího zpracování zakotvený v právním předpisu. Maximální doba uchování a povinný postup výmazu. Vyjasnění, které povinnosti Evropské komise odůvodňují její přístup do centrálního rejstříku. A určení, kdo je správcem osobních údajů.
>
> Stanovisko 2023/C 199/04 ze dne 3. 4. 2023

Nejdůležitější je ovšem důvod, pro který soud úpravu zrušil. Uchovávání takových údajů bylo samo o sobě legitimním požadavkem. Výtka však směřovala k tomu, že úprava zcela nedostatečně stanovila jasná a detailní pravidla, včetně minimálních požadavků na zamezení přístupu třetích osob a postupů k ochraně integrity a důvěrnosti údajů a k jejich likvidaci.[30] Soud také obecně požaduje, aby vnitrostátní úprava s dostatečnou jasností vymezila rozsah a způsob výkonu příslušné pravomoci, a poskytla tak ochranu proti svévoli.[31]

Obdobné problematice se mnohokrát věnoval i Soudní dvůr Evropské unie, jehož rozhodnutí jsou postavena na několik zásadách, které se v této souvislosti často opakují. Údaje mají být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nemají být dále zpracovávány způsobem s těmito účely neslučitelným. Rozsah zpracování má být omezen na to, co je nezbytné. A správce má zavést technická a organizační opatření odpovídající riziku pro práva a svobody dotčených osob.[32]

Soud tyto zásady opakovaně uplatnil i proti unijním a vnitrostátním předpisům. V rozsudku ve věci Digital Rights Ireland z dubna 2014 prohlásil za neplatnou směrnici o uchovávání údajů, mimo jiné proto, že ukládala plošné uchovávání bez dostatečného rozlišení a bez odpovídajících záruk.[33] V listopadu 2022 pak v souvislosti s lucemburským rejstříkem skutečných majitelů zneplatnil ustanovení, které zpřístupňovalo údaje o skutečných majitelích široké veřejnosti. Soud v něm označil takový přístup za závažný zásah do práv na respektování soukromého života a na ochranu osobních údajů podle Listiny základních práv Evropské unie a dospěl k závěru, že tento zásah není omezen na to, co je nezbytně nutné.[34]

Napříč touto judikaturou se opakuje jedna myšlenka. Legitimní cíl sám o sobě neospravedlňuje nejširší možný informační dosah a zásah musí být omezen na

[26] Listina základních práv a svobod, čl. 7 odst. 1 a čl. 10 odst. 2 a 3.

[27] Nález Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011, kterým byla zrušena ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích, a vyhláška č. 485/2005 Sb.

[28] Tamtéž, body 29 až 31.

[29] Tamtéž, bod 44.

[30] Tamtéž, bod 50.

[31] Tamtéž, bod 39.

[32] Nařízení Evropského parlamentu a Rady (EU) 2016/679, zejména čl. 5 odst. 1 písm. b) a c) a čl. 32.

[33] Rozsudek Soudního dvora Evropské unie (velkého senátu) ze dne 8. 4. 2014 ve spojených věcech C-293/12 a C-594/12, Digital Rights Ireland. Za neplatnou byla prohlášena směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, Úř. věst. L 105, s. 54. K plošnosti uchovávání viz bod 57, podle kterého se směrnice „vztahuje všeobecně na každou osobu, každý prostředek elektronické komunikace a na všechny provozní údaje bez jakéhokoli rozlišování, omezení či výjimky v závislosti na cíli boje proti závažné trestné činnosti". K chybějícím zárukám viz bod 62 k absenci předchozí kontroly ze strany soudu nebo nezávislého správního orgánu a bod 66 k nedostatečným zárukám proti zneužití a neoprávněnému přístupu. Souhrnně bod 65.

[34] Rozsudek Soudního dvora Evropské unie (velkého senátu) ze dne 22. 11. 2022 ve spojených věcech C-37/20 a C-601/20, Luxembourg Business Registers a Sovim. Za neplatný byl prohlášen čl. 1 bod 15 písm. c) směrnice Evropského parlamentu a Rady (EU) 2018/843 ze dne 30. května 2018, kterou se mění směrnice (EU) 2015/849 o předcházení využívání finančního systému k praní peněz nebo financování terorismu a směrnice 2009/138/ES a 2013/36/EU, a to v rozsahu, v němž jím byl změněn čl. 30 odst. 5 první pododstavec písm. c) směrnice Evropského parlamentu a Rady (EU) 2015/849 tak, že členské státy musí zajistit, aby informace o skutečných majitelích byly vždy k dispozici jakékoli osobě z široké veřejnosti. Závažnost zásahu konstatuje bod 44, závěr, že zásah není omezen na to, co je nezbytně nutné, bod 76. K porovnání s předchozím režimem, který přístup podmiňoval oprávněným zájmem, viz bod 85.

to, co je k dosažení cíle skutečně nezbytné. Tento požadavek se posuzuje u konkrétní podoby opatření, tedy u toho, jaké údaje jsou dostupné komu a za jakých podmínek.

K oznamování údajů o kryptoaktivech existuje dokument, který se věnuje přímo ochraně osobních údajů. Vydal jej v dubnu 2023 evropský inspektor ochrany údajů k tehdejšímu návrhu směrnice.[35]

Inspektor cíl úpravy podpořil a zároveň však požadoval doplnit záruky ve čtyřech bodech (nejedná se o výčet všech závěrů).

- Další zpracování údajů má být vázáno na taxativní výčet účelů, který bude zakotven v právním předpisu a bude splňovat podmínky pro omezení práv podle obecného nařízení o ochraně osobních údajů.
- Má být stanovena maximální doba uchování a povinný postup výmazu. Záznamy mají být vymazány po jejím uplynutí, případně dříve, pokud pominou důvody, pro které byly uchovávány.
- Má být vyjasněno, které konkrétní povinnosti Evropské komise odůvodňují její přístup do centrálního rejstříku, a má být výslovně uveden účel tohoto zpracování.
- Má být vyjasněno, zda jednotlivé zapojené subjekty vystupují jako samostatní správci, nebo jako společní správci osobních údajů.

První dva body se přímo protínají s tím, co popisují předchozí oddíly. Požadavek na taxativní výčet účelů je odpovědí na postupné rozšiřování účelu a požadavek na maximální dobu uchování s povinným výmazem míří na nevratnost následků úniku. Význam tohoto stanoviska spočívá v tom, že je vznesl dozorový orgán Evropské unie, nikoliv odvětvová asociace nebo některý z odpůrců regulace.

[35] Stanovisko evropského inspektora ochrany údajů 2023/C 199/04 ze dne 3. 4. 2023 k návrhu směrnice Rady, kterou se mění směrnice 2011/16/EU o správní spolupráci v oblasti daní. Úř. věst. C 199, 7. 6. 2023, s. 5.

6. MITIGACE RIZIK

Předchozí kapitoly popisují riziko. Tato shrnuje, co s ním lze udělat při návrhu systému, a to obecně, bez ohledu na konkrétní právní úpravu.

Východiskem je rozlišení, které se v debatách o podobných systémech často stírá. Stát může mít povinnost údaje přijmout, uchovat a použít pro určitý účel. Z této povinnosti ale samo o sobě neplyne, kdo uvnitř státní správy je smí vyhledávat, v jakých kombinacích a bez jakého dalšího kroku. Plný rozsah oznamovaných údajů a plná analytická dostupnost těchto údajů jsou dvě odlišné vlastnosti systému. První z nich bývá dána právním předpisem. Druhá vzniká rozhodnutím o architektuře, které zpravidla nikdo veřejně neprojednává, protože se považuje za technický detail.

Právě zde vzniká prostor, ve kterém lze snížit riziko popsané v předchozích oddílech, aniž by se dotklo splnění právní povinnosti. Následující tuzemské a zahraniční příklady ukazují, jak k tomuto riziku přistoupily obdobné systémy.

Od roku 2018 provozuje Česká republika centrální evidenci účtů, jejímž správcem je Česká národní banka. Systém byl zřízen z podobných důvodů, tedy aby oprávněné orgány dokázaly rychle zjistit, kde má konkrétní osoba účet, bez zdlouhavého obesílání jednotlivých bank.[36]

Pro nás je však podstatné, co daná evidence obsahuje:

- Která instituce účet vede,
- číslo účtu,
- datum jeho vytvoření
- identifikační údaje klienta, disponujících osob a v relevantních případech skutečného majitele.

Zůstatek účtu ani historie transakcí se do evidence neukládají. Detail zůstává u banky a oprávněný orgán si jej vyžádá podle jiného zákona, pokud pro to má důvod.

Přístup je navíc strukturován účelově. Okruh oprávněných žadatelů je vymezen zákonem a zahrnuje zejména orgány činné v trestním řízení, finanční analytický útvar, orgány Finanční a Celní správy a zpravodajské služby. Žádost musí být spojena s konkrétním řízením a žadatelé vedou evidenci podaných žádostí. Kontrolu nad systémem vykonává orgán zřízený Poslaneckou sněmovnou. Přímý přístup k uchovávaným údajům mají pouze určení zaměstnanci České národní banky, kteří bezprostředně zajišťují provoz evidence. Kontrola je zde tedy postavena na parlamentním dohledu; zákon naopak vylučuje, aby se dotčená osoba u České národní banky domáhala přístupu ke svým údajům podle obecného nařízení o ochraně osobních údajů.

Model je tedy postaven na oddělení dvou různých informací. Centrálně se vede pouze údaj o tom, že vztah existuje. Obsah tohoto vztahu zůstává rozptýlený u jednotlivých institucí a spojí se s identitou až v okamžiku, kdy pro to existuje doložený zákonný důvod.

Podobné uspořádání používají i další státy a stojí za to zmínit alespoň dva z nich. Německo provozuje u finanční správy postup pro zjišťování údajů o účtech, který je vázán na konkrétní zákonný účel. Součástí úpravy je vedení evidence provedených dotazů a pravidlo, podle kterého má být dotčená osoba o dotazu zpravidla informována.[37] Estonsko pak používá pro výměnu údajů mezi úřady společnou vrstvu, ve které je každá zpráva podepsána a opatřena časovým razítkem, takže ji odesílatel nemůže zpětně popřít. Občan si přitom může sám ověřit, který úřad se na jeho údaje ptal, a to u těch registrů, které jsou do této služby zapojeny.[38]

Ke stejné rodině opatření patří i norské řešení popsané dříve, kde hledaná osoba vidí, kdo si ji v daňových seznamech vyhledal. Tyto prvky spojuje jedna myšlenka. Dotaz na citlivé údaje nesmí být neviditelnou operací, ale úkonem, který po sobě zanechává stopu a za který je někdo odpovědný.

[36] Zákon č. 300/2016 Sb., o centrální evidenci účtů. Obsah evidence vymezuje § 4, okruh oprávněných žadatelů § 6 odst. 1, vazbu žádosti na konkrétní řízení a spisovou značku § 7 odst. 1, evidenci podaných žádostí § 6 odst. 3 a 4, kontrolní orgán Poslanecké sněmovny § 11 a okruh osob s přímým přístupem u České národní banky § 9 odst. 2. Vyloučení práva na přístup podle obecného nařízení o ochraně osobních údajů stanoví § 18a odst. 2. Evidence je v provozu od 1. 1. 2018.

[37] Postup podle § 93 a § 93b německého daňového řádu (Abgabenordnung). Povinnost upozornit dotčenou osobu předem a vyrozumět ji po provedení dotazu stanoví § 93 odst. 9; tamtéž jsou uvedeny výjimky z této povinnosti.

[38] Estonská vrstva pro výměnu dat mezi informačními systémy veřejné správy, známá jako X-Road. Podepisování a časová razítka zpráv popisuje provozovatel v dokumentaci k zabezpečení; přehled o tom, kdo se na údaje ptal, poskytuje občanům služba Data tracker na portálu eesti.ee, a to u registrů, které jsou do ní zapojeny.

7. JAK ZABEZPEČIT SYSTÉM

Na základě předchozích kapitol, které se věnovaly problematice existence centrálního systému a možným rizikům, která jsou s podobnou centralizací nerozlučně spjata, nalezneme níže seznam principů, kterých by se měl architekt nového systému při jeho návrhu držet. Principy jsou formulovány obecně a následující část této studie je pak přímo aplikuje v českém prostředí.

- **Oddělit příjem dat od analytického přístupu.** Systém může přijmout a uchovat celý zákonem předepsaný rozsah a zároveň omezit, které položky jsou dostupné pro rutinní práci.
- **Segmentovat datové vrstvy.** Identifikační údaje, transakční údaje a analytické funkce mohou být odděleny tak, že jejich spojení vyžaduje samostatné oprávnění.
- **Spojovat údaje až na doložený účel.** Propojení identity s citlivými údaji a historií napříč zdroji má být podmíněno uvedením konkrétního řízení, spisu nebo zákonného důvodu.
- **Omezit okruh osob s přístupem.** Počet zaměstnanců, kteří mohou zobrazit konsolidovaný profil osoby, má být držen na nezbytném minimu a být auditovatelný.
- **Logovat nezměnitelně a včetně důvodu.** Záznam má obsahovat identitu člověka nebo technického procesu, dotčenou osobu, čas, důvod a konkrétní účel, a to i u neúspěšných pokusů. Logy mají být chráněny proti jakékoliv manipulaci.
- **Detekovat neobvyklé vzorce dotazů.** Systém má sám upozornit na chování, které odpovídá modelu popsanému v kapitole 4, tedy na opakované vyhledávání majetných osob bez vazby na spis.
- **Vyloučit hromadné řazení osob.** Sestavení seznamu podle pravděpodobné výše majetku má být technicky znemožněno, pokud pro takovou operaci neexistuje výslovný zákonný účel a zvláštní schválení.
- **Vyžadovat dvojí schválení u exportů.** Citlivé exporty a nestandardní spojení dat mají podléhat principu čtyř očí.
- **Umožnit kontrolu dotčenou osobou.** Občan má mít možnost zjistit, kdo a z jakého důvodu k jeho údajům přistupoval, s možností odkladu pouze tam, kde by to ohrozilo probíhající řízení.
- **Ošetřit dodavatele a testovací prostředí.** Externí vývoj a podpora mají pracovat se syntetickými daty, privilegované přístupy mají být časově omezené a monitorované.
- **Ověřit model před spuštěním.** Posouzení vlivu na ochranu osobních údajů, model hrozeb, penetrační test a nezávislý audit kontrol proti zneužití oprávněného přístupu mají proběhnout před ostrým provozem.

Žádný z těchto principů nesnižuje rozsah údajů, které stát podle práva obdrží. Všechny se naopak zaměřují na to, co se s údaji děje poté, co je stát obdrží, a na cenu, kterou by jejich zneužití mělo pro toho, kdo by se o to pokusil.

8. IMPLEMENTACE DAC8 V ČESKÉM PROSTŘEDÍ

První část této studie popisuje, proč soustředění finančních dat na jednom místě zvyšuje riziko pro ty, jichž se data týkají. Následující kapitoly problematiku zkoumají v kontextu konkrétního českého případu, o kterém se právě rozhoduje v Poslanecké sněmovně.

Podstata návrhu je jednoduchá. Oznamující poskytovatelé služeb souvisejících s kryptoaktivy, typicky české směnárny a burzy, budou každoročně oznamovat Finanční správě údaje o svých uživatelích. U každého uživatele se uvádějí identifikační údaje a k tomu za každý druh kryptoaktiva úhrnné částky nákupů a prodejů, úhrnné počty jednotek a počty transakcí. Hlásí se také úhrnná hodnota převodů na adresy, které podle daného poskytovatele nepatří regulované finanční instituci, tedy typicky převodů do peněženek mimo evidované poskytovatele.[39]

U poslední položky je namístě upřesnění, protože bývá čtena šířeji, než jak je napsána. Oznamuje se úhrnná hodnota a úhrnný počet jednotek takových převodů za období. Cílová adresa v distribuovaném registru mezi oznamovanými údaji není.

Oznamovaným obdobím je kalendářní rok a oznámení se podle navrhovaného § 15zg podává do 30. dubna roku následujícího.[40]

Vláda tento návrh rozeslala poslancům 5. února 2026 jako sněmovní tisk 98. Jde o novelu zákona o mezinárodní spolupráci při správě daní, kterou se do českého práva převádí evropská úprava oznamování údajů o kryptoaktivech a navazující směrnice z dubna 2025.[41] Předpisy měly být přijaty a vyhlášeny do 31. prosince 2025 a používat se od 1. ledna 2026.[42]

Dne 14. července 2026 sněmovna odmítla návrh schválit v prvním čtení ve zrychleném režimu a předala jej výborům. Garančním se stal výbor rozpočtový.[43] Text tedy zatím platným zákonem není a jeho podoba se může ve výborech ještě změnit.

S tímto odmítnutím kontrastuje předpokládaný náběh povinností. Přechodná ustanovení návrhu určují jako první oznamované období rok 2026 a zákon má nabýt účinnosti dnem následujícím po dni vyhlášení.[44] Poskytovatelé tedy mají oznámit údaje za období, které začalo dříve, než sněmovna o návrhu poprvé hlasovala.

Jak bude Finanční správa tato data ukládat, jak dlouho, kdo do nich uvidí a jak se přístupy zaznamenávají, není upraveno na úrovni zákona.[45] K účelům, ke kterým lze získané informace použít, se ale vyjadřuje a okruh těchto účelů rozšiřuje. Informace přijaté z jiného členského státu bylo dosud možné také použít v omezenějším okruhu a se souhlasem státu, který je poskytl. Podle nového ustanovení se souhlasu nevyžaduje, jde-li o clo nebo o výkon působnosti v oblasti legalizace výnosů z trestné činnosti, financování terorismu a provádění mezinárodních sankcí. Změna vychází z evropské úpravy.[46]

Vedle toho obsahuje předložený text tři konkrétní povinnosti, které lze posoudit už dnes.

- **Deset let uchovávání.** Poskytovatelé mají uchovávat doklady k prověřování a zjišťování po dobu deseti let od posledního dne lhůty pro podání oznámení.[47] Tato lhůta dopadá na poskytovatele. Jak dlouho bude údaje držet stát, návrh neurčuje. Horní hranice tak bude pravděpodobně určena dle interních pravidel v návaznosti na obecnější úpravu v daňovém řádu.
- **Zastavení transakcí.** Pokud uživatel neposkytne požadovanou součinnost ani po dvou upomínkách, poskytovatel pro něj neprovede oznamovanou transakci. Opatření nelze uplatnit dříve než šedesát dní od odeslání žádosti a od šedesátého prvního dne je poskytovatel povinen

[39] Obsah oznámení stanoví navrhovaný § 15zf. Sněmovní tisk 98, PDF str. 19 a 20 (dokument str. 17 a 18); úhrnné údaje o transakcích viz odst. 1 písm. h), převody na adresy distribuovaného registru bod 9 téhož písmene, PDF str. 20. Údaje zjišťované o uživateli vymezuje příloha č. 5 návrhu, PDF str. 33 a 209; jejich přehled uvádí též důvodová zpráva, kap. 10.3, PDF str. 62 (dokument str. 60).

[40] Navrhovaný § 15j, podle kterého je oznamovaným obdobím kalendářní rok, PDF str. 13 (dokument str. 11), a navrhovaný § 15zg, který stanoví lhůtu do 30. dubna kalendářního roku následujícího po oznamovaném období, PDF str. 20 (dokument str. 18).

[41] Sněmovní tisk 98, vládní návrh zákona, kterým se mění zákon č. 164/2013 Sb., o mezinárodní spolupráci při správě daní. Rozesláno poslancům 5. února 2026. Transponuje směrnici Rady (EU) 2023/2226 ze dne 17. 10. 2023 a směrnici Rady (EU) 2025/872 ze dne 14. 4. 2025.

[42] Čl. 2 směrnice Rady (EU) 2023/2226, citovaný v rozdílové tabulce k čl. III návrhu, Sněmovní tisk 98, PDF str. 275. Důvodová zpráva k účinnosti uvádí, že transpoziční lhůta uplynula dnem 1. ledna 2026, PDF str. 110 (dokument str. 108).

[43] Poslanecká sněmovna Parlamentu ČR, sněmovní tisk 98, průběh projednávání. První čtení proběhlo 14. 7. 2026 na 27. schůzi; usnesením č. 258. Sněmovna nesouhlasila s projednáváním tak, aby mohla s návrhem zákona vyslovit souhlas již v prvém čtení, a přikázala jej k projednání výborům. Garančním výborem je rozpočtový výbor.

[44] Čl. II bod 5 přechodných ustanovení návrhu a čl. III o účinnosti. Sněmovní tisk 98, PDF str. 36 (dokument str. 34).

[45] Stále tedy existuje možnost, že je toto možno dovodit z jiných předpisů a postupů správce daně.

[46] Čl. I body 38 a 39 návrhu, kterými se mění § 22 odst. 4 a vkládá nový § 22 odst. 5. Sněmovní tisk 98, PDF str. 28 (dokument str. 26); znění s vyznačením změn PDF str. 179. Rozšíření odůvodňuje důvodová zpráva odkazem na DAC8, PDF str. 106 (dokument str. 104).

[47] Navrhovaný § 15zd. Sněmovní tisk 98, PDF str. 18 (dokument str. 16).

je uplatnit.[48] Oznamovanou transakcí je směna i převod, uživatel tedy u daného poskytovatele nemůže nakoupit, prodat ani odeslat své kryptoaktivum, dokud údaje nedodá. Na ostatní služby poskytovatele opatření nedopadá.

- **Místo narození.** Mezi zjišťované a oznamované údaje patří vedle jména, adresy, daňové rezidence, daňového identifikačního čísla a data narození také místo narození.[49]

KDO SE OZNAMUJE A KDO O TOM ROZHODL

Musí česká kryptoburza hlásit Finanční správě i své české klienty, nebo si to Česká republika zvolila sama? Vládní materiály na tuto otázku odpovídají dvěma způsoby, které se navzájem vylučují. Odpověď je přitom v textu směrnice.

Okruh oznamovaných osob vymezuje příloha směrnice ve třech na sebe navazujících definicích. Oznamovaným uživatelem je uživatel kryptoaktiv, který je oznamovanou osobou a je rezidentem členského státu. Oznamovanou osobou je osoba z členského státu jiná než vyňatá osoba. A osobou z členského státu je fyzická osoba nebo entita, která je rezidentem kteréhokoli členského státu podle daňové legislativy tohoto státu.[50]

Řečeno srozumitelněji: kdo je daňovým rezidentem kteréhokoli členského státu, včetně toho, ve kterém je poskytovatel usazen, se oznamuje.

Že nejde o nepřesnost v překladu, ukazuje srovnání se starší úpravou oznamování finančních účtů. Tam táž definice zní osoba, která je rezidentem kteréhokoli jiného členského státu podle daňové legislativy tohoto jiného členského státu.[51] Novější úprava slovo jiného vypustila, a to jen u osob; v téže větě u pozůstalostí zůstalo.

Směrnice totéž uvádí i v odůvodnění, kde stojí, že oznamovací povinnost by se měla vztahovat jak na přeshraniční, tak na vnitrostátní transakce, a to s cílem zajistit účinnost pravidel oznamování, řádné fungování vnitřního trhu, rovné podmínky a dodržování zásady zákazu diskriminace.[52] Stejně úpravu vykládá Evropská komise, která poskytovatelům ukládá sbírat od 1. ledna 2026 údaje o všech uživatelích s rezidencí v Evropské unii, výslovně včetně rezidentů členského státu, ve kterém je poskytovatel usazen.[53]

Odpověď na úvodní otázku tedy zní, že oznamování českých klientů vyžaduje evropská úprava a českou volbou není.

Důvodová zpráva a souhrnná část hodnocení dopadů s tímto závěrem souhlasí. Důvodová zpráva označuje rozšíření za čistě transpoziční opatření[54] a v souhrnu je u položky, zda návrh jde nad rámec požadavků stanovených předpisem Evropské unie, zaškrtnuta odpověď ne.[55] Obecná část důvodové zprávy to říká ještě přímo, když uvádí, že oznamovaným uživatelem je daňový rezident členského státu, a v závorce dodává, že včetně České republiky.[56]

Závěrečná zpráva z hodnocení dopadů regulace však tvrdí opak:

> „směrnice DAC8 ani standard CARF přímo nezavádí oznamování uživatelů, kteří nejsou rezidenty zúčastněného státu, ale jsou daňovými rezidenty státu, který informace předává (tzv. tuzemští rezidenti)"[57]

Toto tvrzení je nesprávné. Platí pro standard CARF, který je svou povahou nástrojem výměny mezi jurisdikcemi. Neplatí pro směrnici, která z tohoto standardu vychází a která okruh oznamovaných osob vymezuje šířeji. Zpráva obě úpravy v jedné větě spojuje a přebírá na obě závěr, který platí jen pro jednu z nich.

Na tomto základě pak zpráva postavila volbu mezi dvěma variantami. Varianta 0 tuzemské rezidenty z oznamování vynechává, Varianta 1 je do něj zahrnuje.

[48] Navrhovaný § 15zb odst. 2 a 3, PDF str. 18 (dokument str. 16). K povinnosti uplatnit opatření od šedesátého prvního dne viz důvodová zpráva, PDF str. 93 (dokument str. 91). Oznamovanou transakcí je podle § 15e směnná transakce a převod, PDF str. 11 (dokument str. 9).

[49] Příloha č. 5 návrhu, PDF str. 33 a 209; k okruhu zpracovávaných identifikačních údajů též důvodová zpráva, kap. 10.3, PDF str. 62 (dokument str. 60).

[50] Směrnice Rady (EU) 2023/2226, příloha VI oddíl IV pododdíl D body 1, 7 a 8. Anglické znění bodu 8: „Member State Person with regard to each Member State means an Entity or individual that is resident in any Member State under the tax laws of that Member State." Český text téhož ustanovení je citován v rozdílové tabulce ke sněmovnímu tisku 98 u čl. I bodu 37, PDF str. 231: osobou z členského státu se rozumí subjekt nebo fyzická osoba, která jsou rezidentem kteréhokoli členského státu.

[51] Směrnice Rady 2014/107/EU (DAC 2), příloha I oddíl VIII pododdíl D bod 3: „Member State Person with regard to each Member State means an individual or Entity that is resident in any other Member State under the tax laws of that other Member State."

[52] Směrnice Rady (EU) 2023/2226, bod 13 odůvodnění.

[53] Evropská komise, informační stránka k DAC8: „Start collecting data on reportable crypto-asset transactions of all EU-resident users, including residents of the Member State where you are established, from 1 January 2026."

[54] Důvodová zpráva, kap. 10.1, PDF str. 60 (dokument str. 58).

[55] Závěrečná zpráva RIA, shrnutí, bod 1, PDF str. 113 (dokument str. 2).

[56] Důvodová zpráva, obecná část, PDF str. 43 (dokument str. 41).

[57] Závěrečná zpráva RIA, část A, kap. 1.1. Sněmovní tisk 98, PDF str. 117 (dokument str. 6).

K tomu, proč se ani jedna z variant nevyřazuje předem, uvádí:

„Vzhledem k tomu, že se žádná z navrhovaných variant nedá vyloučit pro její nerealizovatelnost, pro rozpor s ústavním pořádkem nebo právem Evropské unie, budou všechny navržené varianty dále analyzovány."[58]

Varianta 0 ovšem v rozporu s právem Evropské unie byla. Zpráva tedy porovnávala zvolené řešení s variantou, kterou zákonodárce zvolit nemohl. Co z toho plyne pro kvalitu celého porovnání, rozebírá kapitola 9.

KDE MÁ ČESKÁ REPUBLIKA PROSTOR

Rozsah oznamovaných osob tedy mezi české volby nepatří. Návrh přesto obsahuje dvě volby, u kterých je prostor pro vlastní rozhodnutí státu doložitelný přímo v textu směrnice.

- **Doba uchování dokladů u poskytovatelů.** Směrnice stanoví, že záznamy mají zůstat dostupné nejméně pět a nejvýše deset let. Návrh volí horní hranici tohoto rozpětí. Důvodová zpráva to odůvodňuje shodou s délkou uchování u ostatních agend automatické výměny informací a odkazem na § 148 daňového řádu, podle kterého lze daň stanovit nejdéle do deseti let.[59]
- **Místo narození.** Podle přílohy směrnice nemusí být místo narození oznamováno, pokud poskytovatel není jinak povinen jej získat a oznámit podle domácího práva. Návrh tuto možnost minimalizace nevyužívá a s místem narození pracuje.[60]

U obou jde o rozhodnutí, které zvyšuje množství citlivých údajů v systému nebo prodlužuje dobu, po kterou jsou vystaveny riziku. Ani u jednoho z nich neuvádějí materiály samostatné odůvodnění, které by vycházelo z povahy těchto konkrétních dat. Máme na mysli pochopitelně ve vztahu k posouzení rizik subjektu údajů.

Třetí prostor, a podle této studie největší, leží mimo text zákona. Týká se toho, co se s povinně získanými údaji děje poté, co je stát obdrží, tedy jak se ukládají, jak dlouho, kdo je smí spojovat a za jakých podmínek. Právě tam se rozhoduje o riziku popsaném v první části studie a právě tam návrh mlčí. Této otázce se věnují kapitoly 11 a 12.

KOLIKA OSOB SE ÚPRAVA TÝKÁ

Počet dotčených osob uvádí závěrečná zpráva na jediném místě. Odhaduje jej na základě konzultací se zástupci sektoru a dodává:

„počet tuzemských uživatelů kryptoaktiv se pohybuje až v řádu několika stovek tisíc. Nicméně podle informací ze sektoru poskytovatelů služeb souvisejících s kryptoaktivy většina tuzemských uživatelů kryptoaktiv využívá služeb poskytovatelů služeb usazených mimo ČR"[61]

Povinnosti podle nové úpravy se budou týkat několika desítek subjektů podnikajících v České republice. Očekávaný fiskální přínos zpráva odhaduje v řádu několika desítek milionů korun a celkové výdaje na vývoj a provoz informačních technologií správce daně v rozmezí 25 až 35 milionů korun.[62]

Údaj o tom, že většina tuzemských uživatelů využívá zahraniční poskytovatele, má pro tuto studii jeden podstatný důsledek. Data o této skupině doputují k Finanční správě cestou mezinárodní výměny informací, data o zbytku cestou domácího oznamování. Stát tedy získá obraz o obou skupinách, pokud mají účet u poskytovatele v EU nebo v jurisdikci, která uplatňuje standard CARF. Otázka, jak s tímto obrazem naloží, se proto týká tuzemských držitelů kryptoaktiv jako celku.

[58] Závěrečná zpráva RIA, část A, kap. 2.2, PDF str. 120 (dokument str. 9).

[59] Rozpětí stanoví příloha VI směrnice Rady (EU) 2023/2226; viz rozdílovou tabulku, PDF str. 244. Odůvodnění viz důvodová zpráva, PDF str. 74 a 95.

[60] Příloha VI směrnice Rady (EU) 2023/2226, oddíl II pododdíl C, citovaná v rozdílové tabulce k čl. I bodu 58, PDF str. 268.

[61] Závěrečná zpráva RIA, část A, kap. 1.1, PDF str. 117 (dokument str. 6).

[62] Závěrečná zpráva RIA, část A, kap. 1.1, PDF str. 117 (dokument str. 6).

9. NEKVALITNĚ ZPRACOVANÁ RIA

Předchozí kapitola ukázala, že závěrečná zpráva z hodnocení dopadů regulace postavila proti sobě dvě varianty, z nichž jedna nebyla dostupná. Tato kapitola mapuje, jak zpráva k výběru došla.

Následují čtyři zjištění. První se týká toho, co zpráva vlastně porovnávala. Druhé toho, jaká rizika zvažovala. Třetí toho, podle jakých kritérií varianty poměřovala. Čtvrté toho, jak z těch kritérií sestavila výsledek.

POROVNÁNÍ STOJÍ NA VARIANTĚ, KTEROU ZVOLIT NEŠLO

Jak ukázala kapitola 8, oznamování tuzemských rezidentů vyžaduje evropská úprava. Varianta 0, tedy řešení bez nich, k dispozici nebyla.

Závěrečná zpráva to ovšem netvrdí. V kapitole 2.2 uvádí, že žádnou z navržených variant nelze vyloučit pro rozpor s ústavním pořádkem nebo právem Evropské unie, a obě proto analyzuje dál.[63] Celá kapitola 3, kapitola 4 i závěrečná tabulka tedy porovnávají zvolené řešení s variantou, která zvolena být nemohla.

Pro čtenáře zprávy z toho plynou dva důsledky. Porovnání neukazuje, co by se stalo, kdyby stát rozhodl jinak, protože jinak rozhodnout nešlo. A náklady i přínosy, které zpráva připisuje rozšíření o tuzemské rezidenty, nejsou náklady a přínosy rozhodnutí, nýbrž náklady a přínosy povinnosti, která ze směrnice plyne tak jako tak.

Stojí za zmínku, jak blízko této otázce byla pracovní komise Legislativní rady vlády. Mezi jejími připomínkami je požadavek, aby zpráva v bodě 2.2 uvedla, že varianta bez transpozice by byla v rozporu s právem Evropské unie. Bod 2.2 zpráva obsahuje, ale je v něm napsán opak, tedy že v rozporu s právem Evropské unie není žádná z posuzovaných variant.[64]

HODNOCENÍ RIZIKA JDE JEN JEDNÍM SMĚREM

Závěrečná zpráva obsahuje samostatnou kapitolu nazvanou Zhodnocení rizika a uvádí zde konkrétně dvě. Prvním je riziko daňových úniků a rostoucích nákladů, pokud se současný stav neřeší. Druhým je riziko, že Evropská komise zahájí řízení o porušení práva Evropské unie, pokud nebude přijat žádný transpoziční předpis.[65] Tím kapitola končí. Riziko, které by vzniklo přijetím navrhované úpravy, v ní uvedeno není. Zpráva tedy hodnotí rizika nečinnosti a rizika zvoleného postupu ponechává stranou.

S tím souvisí i pojmenování variant. Varianta 0 je v textu označena jako zachování současného stavu.[66] Její popis ovšem odpovídá něčemu jinému. Tuzemští poskytovatelé by podle něj oznamovali uživatele z jiných států a vynechali by pouze tuzemské rezidenty. Současný stav, ve kterém se neoznamuje nikdo, to není, a řádná transpozice směrnice také ne. Označení tedy navozuje dojem, že jde o variantu nečinnosti, ačkoli jde o variantu neúplné transpozice.

MEZI KRITÉRII CHYBÍ TO, O ČEM JE CELÁ TATO STUDIE

Zpráva porovnává obě varianty podle pěti kritérií.[67]

- zmírnění rizika daňových úniků,
- náklady na straně poskytovatelů služeb souvisejících s kryptoaktivy,
- náklady na straně Finanční správy,
- náklady na straně uživatelů kryptoaktiv,
- narovnání tržního prostředí.

Jediné kritérium, které míří na dotčené osoby, jsou náklady na straně uživatelů. Zpráva je vymezuje takto:

> „Nad stávající povinnosti se jedná především o informaci o daňovém rezidenství, což by vzhledem k okruhu osob, na které by tyto povinnosti měly dopadat (tj. tuzemští rezidenti s tuzemským poskytovatelem služeb), nemělo představovat zvýšené obtíže."[68]

Nákladem uživatele se tedy rozumí to, že bude muset sdělit svou daňovou rezidenci. Skutečnost, že o několika stovkách tisíc lidí vznikne u státu evidence spojující totožnost, bydliště a majetkovou aktivitu, se tím do porovnání variant nedostane. V soustavě pěti kritérií pro ni není místo.

Toto zjištění platí i přesto, že okruh oznamovaných osob určuje směrnice (kapitola 8), a v jistém smyslu je o to závažnější. Pokud okruh oznamovaných osob určuje směrnice, zbývá předkladateli právě prostor v

[63] Závěrečná zpráva RIA, část A, kap. 2.2, PDF str. 120 (dokument str. 9). Totéž ustanovení cituje kapitola 8 této studie.
[64] Stanovisko Pracovní komise Legislativní rady vlády pro hodnocení dopadů regulace, čj. OVA 408/24 ze dne 19. 7. 2024. Vypořádání jednotlivých připomínek uvádí tabulka v dalším oddíle této kapitoly.
[65] Závěrečná zpráva RIA, část A, kap. 1.5 Zhodnocení rizika, PDF str. 120 (dokument str. 9).
[66] Závěrečná zpráva RIA, kap. 2.1, popis Varianty 0, PDF str. 120 (dokument str. 9).
[67] Závěrečná zpráva RIA, kap. 3.1, PDF str. 120 (dokument str. 9).
[68] Závěrečná zpráva RIA, kap. 3.2, náklady na straně uživatelů kryptoaktiv, PDF str. 121 (dokument str. 10).

tom, jak s údaji naloží. Kritérium, které by tento prostor zachytilo, ovšem zpráva nemá, takže otázku, o které Česká republika skutečně rozhodovala, neporovnávala vůbec.

Ochrana soukromí a osobních údajů by měla být v rámci RIA, dle metodiky RIA, posuzována v rámci kapitoly o sociálních dopadech.[69] Vzhledem k tomu, že RIA žádné sociální dopady neuvažuje, byla zřejmě rizika v tomto případě špatně posouzena a identifikována.

Souhrnná část zprávy tento stav jen dokončuje. U položek sociálních dopadů, korupčních rizik i dopadů na bezpečnost nebo obranu státu je zaškrtnuta odpověď ne a v poli pro popis je pomlčka.[70] Tyto pomlčky jsou důsledkem toho, co bylo popsáno výše, jelikož co nebylo mezi kritérii, nemohlo se objevit ani v souhrnu.

Co v hodnocení nešlo zohlednit

Soustava pěti kritérií, podle kterých se varianty porovnávaly, neobsahuje žádné hledisko zásahu do soukromí. Protože okruh oznamovaných osob určuje směrnice, měla zpráva porovnávat varianty nakládání s údaji, tedy dobu uchování, rozsah údajů a přístupový model. Ty v ní chybějí stejně jako kritérium, které by je zachytilo.

Kapitola 9

TABULKA 1 **Hodnocení variant podle pěti kritérií závěrečné zprávy**

	NÁKLADY POSKYTOVATELŮ	NÁKLADY UŽIVATELŮ	NÁKLADY FINANČNÍ SPRÁVY	ZMÍRNĚNÍ RIZIKA ÚNIKŮ	NAROVNÁNÍ TRHU
Varianta 0	**1**	**1**	2	2	2
Varianta 1	2	2	**1**	**1**	**1**

VÝBĚR VARIANTY JE PROSTÝ POČET KRITÉRIÍ

Výsledek porovnání shrnuje jediná tabulka, ve které má nižší číslo význam lepšího hodnocení.[71]

Pod tabulkou následuje závěr, podle kterého je nejvhodnější variantou k realizaci varianta 1. Žádné vážení kritérií tabulka neobsahuje. Varianta 0 je lepší ve dvou kritériích, varianta 1 ve třech, a rozhodl prostý poměr tři ku dvěma.

Ve dvou z těch tří kritérií je přitom hodnocení sporné.

- **Náklady na straně Finanční správy.** Toto kritérium je bodováno ve prospěch varianty 1, přestože text téže zprávy u varianty 1 popisuje zvýšení nákladů. Odůvodnění zní, že zanedbatelné zvýšení nákladů umožní významné zvýšení transparence a navýšení daňových příjmů.[72] Do kritéria pojmenovaného jako náklady se tak dostal přínos, který už je započítán v kritériu zmírnění rizika daňových úniků. Tentýž přínos je tedy v tabulce započten dvakrát.
- **Náklady na straně poskytovatelů.** Zpráva u tohoto kritéria výslovně uvádí, že přesné náklady nelze určit.[73] Kritérium je přesto obodováno.

Poměr tři ku dvěma tedy stojí na jednom kritériu, které je hodnoceno proti vlastnímu textu zprávy, a na jednom, u kterého zpráva sama uvádí, že čísla nemá. A obojí se počítá vůči variantě, která podle kapitoly 8 nebyla dostupná. Očekávaný fiskální přínos v řádu několika desítek milionů korun zpráva odvozuje z odhadu Evropské komise o kapitálových příjmech z operací s bitcoinem v zemích Evropské unie v roce 2020.

Z téhož odhadu pochází i údaj, že Česká republika je mezi členskými státy na šestém místě.[74] Vzhledem k tomu, jak se trh s bitcoinem a potažmo se všemi kryptoaktivy během posledních let proměnil, je tento odhad zastaralý. Na straně nákladů je odhad stejně hrubý.

Částka 25 až 35 milionů korun je uvedena pro vývoj a provoz systému jako celku a další náklady nezohledňuje.

[69] Obecné zásady pro hodnocení dopadů regulace (RIA), výčet posuzovaných dopadů.

[70] Závěrečná zpráva RIA, shrnutí, bod 3, položky 3.5, 3.11 a 3.12, PDF str. 114 (dokument str. 3).

[71] Závěrečná zpráva RIA, kap. 4, Tabulka 1 a navazující závěr, PDF str. 125 (dokument str. 14).

[72] Závěrečná zpráva RIA, kap. 3.4.2, náklady na straně Finanční správy u Varianty 1, PDF str. 124 (dokument str. 13).

[73] Závěrečná zpráva RIA, kap. 3.2, náklady na straně poskytovatelů, PDF str. 121 (dokument str. 10).

[74] Závěrečná zpráva RIA, kap. 1.1, PDF str. 117 (dokument str. 6). Zpráva zde odkazuje na pracovní dokument Rady WK 249/2023 INIT, prezentaci Evropské komise z 10. 1. 2023; údaj je na snímku nazvaném Estimated capital gains from Bitcoin in 2020 across EU countries. Jde o jedinou poznámku pod čarou v části A závěrečné zprávy.

TABULKA 2 **Vypořádání připomínek Komise pro hodnocení dopadů regulace**

PŘIPOMÍNKA KOMISE	STAV	DOKLAD
Uvést dodatečné varianty řešení včetně varianty, při které nedochází k transpozici evropské směrnice	Nezohledněno	Část A obsahuje pouze Variantu 0 a Variantu 1. Varianta bez transpozice doplněna nebyla.
V bodě 2.2 uvést, že varianta bez transpozice by byla v rozporu s právem EU	Nezohledněno	Taková varianta ve zprávě není. Bod 2.2 uvádí, že žádnou z navržených variant nelze vyloučit pro rozpor s právem EU.
Uvést detailnější odhady nákladů na straně poskytovatelů	Nezohledněno	Zpráva uvádí, že přesné náklady nelze určit a nárůst nákladů je obtížné kvantifikovat.
Uvést odhadované přínosy plynoucí z narovnání trhu	Nezohledněno	Narovnání tržního prostředí zůstává hodnoceno pouze slovně.
U variant v části C doplnit variantu se zachováním současného stavu	Nezohledněno	Část C obsahuje pouze Variantu 1 a Variantu 2.
Uvést jednotlivé zdroje dat a správně je citovat v textu (vzneseno dvakrát)	Nezohledněno	Viz následující odstavec.
Specifikovat rizika spojená s absencí implementace	Zohledněno	Doplněno riziko řízení pro porušení práva EU.
Doplnit kritéria nákladů na straně správce daně a uživatelů	Zohledněno	Obě kritéria byla doplněna.

VÝTKY KOMISE PRO HODNOCENÍ DOPADŮ REGULACE

Kvalitu hodnocení dopadů posuzovala též pracovní komise Legislativní rady vlády. K tomuto návrhu vydala v červenci 2024 stanovisko, ve kterém vznesla 22 doporučujících připomínek a schválení podmínila jejich zohledněním.[75] Porovnali jsme proto každou připomínku s finálním textem závěrečné zprávy. Pět z nich bylo zohledněno, pět částečně a dvanáct nikoli. Následující výběr uvádí ty, které se dotýkají otázek řešených v této studii.

Požadavek na řádné uvedení zdrojů vznesla Komise dvakrát. Závěrečná zpráva v rozsahu dvaceti devíti stran však obsahuje pouze pět poznámek pod čarou.

Všechny tři oddíly nazvané konzultace a zdroje dat popisují zdroje obecně. Uvádějí konzultace s útvary Generálního finančního ředitelství, využití blíže neurčených materiálů Organizace pro hospodářskou spolupráci a rozvoj a Evropské komise a neformální konzultace se zástupci sektoru.

Odhad počtu dotčených osob, tedy údaj, o který se opírá posouzení přiměřenosti celého opatření, tak stojí na neformální konzultaci bez uvedení konkrétního zdroje, metodiky a dat.

Materiály tedy vyčíslují náklady informačních systémů správce daně a očekávaný fiskální přínos.

[75] Stanovisko Pracovní komise Legislativní rady vlády pro hodnocení dopadů regulace, čj. OVA 408/24 ze dne 19. 7. 2024. Komise doporučila návrh schválit „za předpokladu zohlednění výše uvedených doporučujících připomínek".

K nákladům poskytovatelů pak uvádějí:

> „Přesné náklady nelze určit, a to i vzhledem k různým možnostem způsobů identifikace, se kterými jsou spojeny různě vysoké náklady. Současně je v tuto chvíli obtížné kvantifikovat nárůst nákladů spojených s povinnostmi poskytovatelů služeb souvisejících s kryptoaktivy ve vztahu k daňovým rezidentům v ČR nad náklady, které těmto provozovatelům budou vznikat ve vztahu k daňovým rezidentům, jiných států z důvodu implementace povinností směrnice DAC8 a standardu CARF."[76]

Náklady poskytovatelů se tedy materiály zabývají pouze v obecné rovině a bez konkrétní snahy o vyčíslení. Posouzení nákladu, který vzniká mimo tento okruh, neobsahují vůbec.

Posouzení bezpečnostní externality by u tohoto typu systému mělo obsahovat alespoň následující položky.

- Odhad hodnoty datového souboru pro útočníka, tedy toho, kolik osob by z něj bylo možné vytřídit jako pravděpodobné cíle a jak přesně.
- Scénář zneužití oprávněného přístupu zevnitř, včetně toho, jaké kontroly by takové jednání odhalily a za jak dlouho.
- Následky kompromitace pro dotčené osoby a jejich domácnosti, včetně toho, že u historické finanční informace není náprava možná.
- Posouzení, zda lze stejného daňového cíle dosáhnout uspořádáním, které hodnotu souboru pro útočníka snižuje.

Žádná z těchto položek se v RIA nevyskytuje.

CO Z TOHO PLYNE

Žádné z těchto zjištění nezpochybňuje cíl úpravy a žádné z nich nezpochybňuje platnost budoucího zákona. Hodnocení dopadů není podmínkou platnosti předpisu. Týkají se toho, zda dokument skutečně splnil svůj účel, tedy zda porovnal dostupné možnosti podle relevantních kritérií.

Čtyři zjištění spolu souvisejí. Zpráva nesprávně popsala, co evropská úprava vyžaduje. Na tom postavila volbu mezi dvěma variantami, z nichž jedna dostupná nebyla. Rizika vážila jen na straně nečinnosti státu. A mezi kritérii neměla žádné, které by zachytilo to, o čem ve skutečnosti rozhodovala. Ve všech čtyřech případech směřuje chyba stejným směrem.

[76] Závěrečná zpráva RIA, kap. 3.2, PDF str. 121 (dokument str. 10)

10. ZÁRUKY PROTI ZNEUŽITÍ JAKO PODMÍNKA ÚSTAVNOSTI

CO ÚSTAVNÍ SOUD VYTKL V ROCE 2011

Ústavní soud v nálezu k plošnému uchovávání provozních a lokalizačních údajů úpravu, která byla popsána v kapitole 5, zrušil zejména proto, že chyběla jasná a detailní pravidla, jak bude s daty nakládáno. A to včetně minimálních požadavků na zamezení přístupu třetích osob, postupů k ochraně integrity a důvěrnosti údajů a k jejich likvidaci.[77]

Pokud stejnou optikou nahlédneme na předložený návrh implementace DAC8 do českých reálií, vypadá výsledek takto. Zákonný text stanoví okruh oznamovaných osob, rozsah oznamovaných údajů, dobu uchování dokladů u poskytovatelů, postup při neposkytnutí součinnosti a sankce. To jsou informace o tom, jak se údaje ke státu dostanou. O tom, jak se s daty bude uvnitř státní správy zacházet, obsahuje předložený text podstatně méně. Důvodová zpráva popisuje účel zpracování, určuje správce a vymezuje kategorie údajů. Opatření, která mají podle ní rizika omezit, jsou obecné procesní záruky daňového řízení, tedy vymezení účelu, nahlížení do spisu, opravné prostředky a povinnost mlčenlivosti.[78]

Konkrétní pravidla, na jejichž absenci Ústavní soud upozorňoval v roce 2011, v projednávaném zákonném textu nenajdeme. Chybí vymezení okruhu osob oprávněných zobrazit konsolidovaný profil, podmínka doloženého účelu u citlivého dotazu, povinnost zaznamenat důvod přístupu, ochrana těchto záznamů proti změně a doba, po kterou bude údaje držet stát[79].

CO SOUDU STAČILO O OSM LET POZDĚJI

Kdyby argumentace této kapitoly skončila u nálezu z roku 2011, byla by neúplná. Tutéž oblast posuzoval Ústavní soud znovu v květnu 2019 a tehdy návrh na zrušení úpravy zamítl.[80]

Rozdíl mezi oběma rozhodnutími je poučný, protože ukazuje, co soudu stačilo. Zákonodárce mezitím doplnil taxativní výčet orgánů oprávněných k přístupu a u každého z nich účel, ke kterému může údaje žádat, zkrátil dobu uchování na šest měsíců, podmínil přístup v trestním řízení odůvodněným soudním příkazem, zavedl povinnost dotčenou osobu o získání jejích údajů informovat a ponechal dohled dvěma nezávislým úřadům.[81] Soud k tomu uvedl, že nynější zákonná úprava je oproti předchozí podrobnější a přísnější a naplňuje požadavky dřívějších nálezů.[82]

Zároveň připomněl, že pochybnosti nad samotným principem plošného sběru vyslovil v roce 2011 jen jako obiter dictum, tedy jako část odůvodnění, která rozhodnutí nenese.[83]

Mezi důvody, pro které soud úpravu v roce 2019 aproboval, je přitom jedna formulace, která k projednávanému návrhu míří přímo. Při hodnocení úrovně zabezpečení soud uvedl, že bez významu nezůstává ani

> „skutečnost, že oprávněné orgány nedisponují žádnou databází údajů, v níž by mohly libovolně vyhledávat"[84]

Z téhož řízení je poučné i svědectví zástupce Ministerstva vnitra: zvažoval se zvláštní úřad, u kterého by se data soustředila, od centrálního uchovávání u jedné instituce se však upustilo kvůli vyššímu riziku zneužití.[85]

U provozních a lokalizačních údajů data zůstávají u operátorů a orgán si o konkrétní údaj žádá. U projednávaného návrhu je situace obrácená, protože správce daně údaje sám přijímá a drží. Právě této otázce se věnují kapitoly 11 a 12.

[77] Nález Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011, bod 50. K obecnému požadavku na jasnost úpravy tamtéž, bod 39.

[78] Důvodová zpráva k vládnímu návrhu, kap. 10.6. Sněmovní tisk 98, PDF str. 66 (dokument str. 64).

[79] Jak již bylo zmíněno, obecná lhůta retence je zřejmě stanovena jinými předpisy a řády.

[80] Nález Ústavního soudu sp. zn. Pl. ÚS 45/17 ze dne 14. 5. 2019, vyhlášen pod č. 161/2019 Sb. Výrok zní, že se návrh zamítá. Nález má jedno odlišné stanovisko.

[81] Tamtéž, bod 73 k výčtu změn provedených zákonodárcem, bod 107 k soudnímu příkazu v trestním řízení, bod 108 k povinnosti informovat dotčenou osobu a bod 126 k dohledu Českého telekomunikačního úřadu a Úřadu pro ochranu osobních údajů.

[82] Tamtéž, bod 121.

[83] Tamtéž, bod 72.

[84] Tamtéž, bod 97.

[85] Tamtéž, bod 36.

INFORMAČNÍ SEBEOMEZENÍ STÁTU

Další nález, o který se tato kapitola opírá, se týká elektronické evidence tržeb. Ústavní soud v něm mimo jiné zrušil § 5 písm. b) zákona o evidenci tržeb, tedy povinnost evidovat platby kartou a další obdobné bezhotovostní platby.[86]

Podstatný je důvod, pro který soud tyto platby z evidence vyňal. Vychází z toho, že takové platby už jednu stopu zanechávají:

> „tržby plynoucí z bezhotovostních převodů – byť se specifikací uvedenou právě pod písmenem b) – jsou obecně poměrně dobře dohledatelné "[87]

Z toho soud dovodil obecnější pravidlo:

> „Stát tak sám musí dodržovat jisté informační sebeomezení, může-li jím zajišťované funkce zabezpečit i jinak "[88]

Ve stejném bodě soud odmítl argument vlády, že širší evidence přispěje k úplnosti analytických informací správce daně, a dodal, že ústavně nekonformní je i stav, kdy stát disponuje údaji, které nezbytně nepotřebuje, i když z toho neplynou přímé negativní důsledky.[89]

Vztaženo k projednávanému návrhu je namístě jedno upřesnění. Jako argument proti oznamování samotnému tento princip použít nelze, protože oznamování vyžaduje evropská úprava a Česká republika o jeho rozsahu většinou nerozhoduje, pakliže se samozřejmě nejedná o něco, co je zcela v rozporu s tuzemským ústavním pořádkem. Použitelný je na to, co následuje po odevzdání údajů.

Otázka pak zní takto. Pokud lze daňového cíle dosáhnout tím, že nejcitlivější položky zůstanou oddělené a jejich spojení s totožností a s historií napříč poskytovateli bude možné až na základě doloženého účelu, proč stát potřebuje uspořádání, ve kterém je takové spojení dostupné rutinně? Materiály na tuto otázku neodpovídají, protože ji nekladou.

Své místo v této úvaze má i údaj, že většina tuzemských uživatelů využívá zahraniční poskytovatele.[90] Data o této skupině doputují k Finanční správě cestou mezinárodní výměny informací a data o zbytku cestou domácího oznamování. Stát tedy bude mít obraz o tuzemských držitelích pocházejících ze zemí EU prakticky v úplnosti.

Evidence tržeb a mezinárodní výměna daňových informací jsou samozřejmě odlišné instituty a soud se k druhému z nich nevyjadřoval. Přenosná je ovšem myšlenka, na které nález stojí. Legitimní daňový cíl sám o sobě neospravedlňuje nejširší možný informační dosah.

KDY VZNIKÁ PROSTOR PRO ÚSTAVNÍ PŘEZKUM

Cílem studie v žádném případě není ústavní přezkum. Je nicméně namístě popsat podmínky, za kterých pro něj vzniká prostor, protože jejich odstranění je v zájmu jak předkladatele, tak dotčených osob.

[86] Nález Ústavního soudu sp. zn. Pl. ÚS 26/16 ze dne 12. 12. 2017, výrok I. Zrušeno bylo mimo jiné § 5 písm. b) zákona č. 112/2016 Sb., o evidenci tržeb, s účinností k 28. únoru 2018.

[87] Tamtéž, bod 96.

[88] Tamtéž, bod 96.

[89] Tamtéž, bod 96.

[90] Závěrečná zpráva RIA, část A, kap. 1.1. Sněmovní tisk 98, PDF str. 117 (dokument str. 6).

Z citované judikatury plyne pět okolností, jejichž souběh tento prostor vytváří.

- **Vysoká intenzita zásahu.** Zpracovávané údaje spojují totožnost, bydliště a kvantifikovanou majetkovou aktivitu a lze je propojovat napříč zdroji i roky. Sám předkladatel je ve svém posouzení označuje za rizikové zpracování osobních údajů vysoce osobní povahy a velkého rozsahu.[91]
- **Absence zákonných záruk pro nakládání s údaji.** Pravidla přístupu, doloženého účelu, zaznamenávání důvodu a ochrany záznamů nejsou obsažena v zákonném textu. Právě doplnění obdobných záruk přitom bylo důvodem, proč soud v roce 2019 návrh na zrušení úpravy uchovávání provozních údajů zamítl.
- **Neodůvodněné volby nad rámec unijního minima.** Směrnice připouští dobu uchování od pěti do deseti let[92] a umožňuje vynechat místo narození.[93] Návrh volí u obou možnost, která dotčené osoby zatěžuje více, a materiály k tomu neuvádějí odůvodnění vycházející z povahy těchto dat.
- **Nevymezená doba uchování na straně státu.** Desetiletá lhůta v návrhu dopadá na poskytovatele. Jak dlouho bude oznámené údaje držet Finanční správa a jak proběhne jejich výmaz, zákonný text neurčuje.
- **Neposouzená bezpečnostní externalita.** Sociální dopady, korupční rizika i dopady na bezpečnost nebo obranu státu jsou v souhrnné části hodnocení dopadů vyhodnoceny jako nulové.[94] Důvodová zpráva sice obsahuje obecný rozbor korupčních rizik, scénář zneužití oprávněného přístupu zevnitř však neřeší. Soustava hodnotících kritérií. Soustava hodnotících kritérií, podle které se varianty porovnávaly, žádné takové hledisko neobsahuje.

Žádná z těchto okolností sama o sobě nezakládá protiústavnost, dohromady by však mohly. Pro předkladatele z toho však plyne praktický závěr. Doplnění záruk do zákonného textu je podstatně levnější než potenciální řízení o návrhu na zrušení ustanovení, po kterém by bylo nutné systém přepracovávat za provozu.

PRÁVNÍ ZÁKLAD SBĚRU ÚDAJŮ ZA ROK 2026

Posledním bodem, vedle výše uvedených otázek o budoucí podobě systému, je okamžitý dopad na konkrétní subjekty. Předpisy měly být přijaty a vyhlášeny do 31. prosince 2025 a používat se od 1. ledna 2026. Sněmovna nesouhlasila se zrychleným projednáním zákona a jeho schválením již v prvním čtení. K datu uzávěrky této studie zákon dosud přijat nebyl. Přechodná ustanovení návrhu přitom počítají s prvním oznamovaným obdobím od 1. ledna 2026.

Poskytovatelé se tak nacházejí v situaci, kterou nezavinili a nemohou ji ovlivnit. Transpozice je totiž zpožděná a k její implementaci dojde až na konci nebo po konci prvního reportovacího období, což vyvolává nejistotu na všech stranách.

Deficit v transpozici vznikl na straně státu a jeho důsledky dnes nesou soukromé subjekty, které jej nezpůsobily.

[91] Důvodová zpráva, kap. 10.4, PDF str. 62 (dokument str. 60).
[92] Rozpětí stanoví příloha VI směrnice Rady (EU) 2023/2226; viz rozdílovou tabulku, PDF str. 244.
[93] Příloha VI směrnice Rady (EU) 2023/2226, oddíl II pododdíl C, PDF str. 268.
[94] Závěrečná zpráva RIA, shrnutí, bod 3, položky 3.5, 3.11 a 3.12, PDF str. 114 (dokument str. 3).

11. TEST PROPORCIONALITY

Předchozí kapitoly shromáždily materiál ke třem otázkám. Kapitola 8 popsala, co v návrhu vyžaduje evropské právo a kde má Česká republika prostor pro vlastní rozhodnutí. Kapitola 9 ukázala, co hodnocení dopadů posoudilo a co ne. Kapitola 10 připomněla měřítko, které na takové zásahy klade Ústavní soud. Zbývá tyto tři vrstvy přiložit k sobě.

Nástrojem bude test proporcionality, standardně využívaný pro posouzení ústavnosti. Zásada proporcionality podle něj zahrnuje tři kritéria. Prvním je způsobilost opatření naplnit sledovaný účel. Druhým je potřebnost, ve které se zkoumá, zda byl z dostupných prostředků vybrán ten, který je k základnímu právu nejšetrnější. Třetím je přiměřenost v užším smyslu, tedy zda újma na základním právu není nepřiměřená ve vazbě na zamýšlený cíl.[95]

Legitimitu cíle naše studie nezpochybňuje. Řádný výběr daní a mezinárodní spolupráce při správě daní jsou legitimní státní cíle.

Jedno vymezení je třeba udělat hned na začátku. Okruh oznamovaných osob určuje evropská úprava, jak ukázala kapitola 8. Test se proto vztahuje na ta rozhodnutí, která Česká republika skutečně učinila. Jsou tři. Doba uchování u poskytovatelů, místo narození a uspořádání systému, ve kterém bude stát s údaji pracovat.

VHODNOST

První kritérium se ptá, zda zvolené opatření může sledovaného cíle dosáhnout. Systematické oznamování údajů o obchodech s kryptoaktivy k lepší správě daní v této oblasti přispět může a předkladatel od něj očekává vyšší transparentnost a fiskální přínos. Tento předpoklad považujeme za věrohodný a v tomto kritériu návrh podle našeho názoru obstojí.

POTŘEBNOST

Druhé kritérium se ptá, zda byl z prostředků, kterými lze cíle dosáhnout, vybrán ten nejšetrnější. U všech tří českých rozhodnutí byl k dispozici šetrnější prostředek.

- **Kratší doba uchování.** Směrnice připouští rozpětí od pěti do deseti let. Návrh volí horní hranici a odůvodňuje to shodou s ostatními agendami automatické výměny informací[96] a odkazem na § 148 daňového řádu, podle kterého lze daň stanovit nejdéle do deseti let. Tento odkaz vysvětluje, proč mohou být údaje užitečné po celou tuto dobu. Nevysvětluje ale, proč musí být drženy v plném rozsahu, a nezvažuje, jaké riziko pro dotčené osoby přinášejí roky šest až deset ve srovnání s jejich přínosem.
- **Vynechání místa narození.** Příloha směrnice tento údaj vynechat umožňuje, pokud poskytovatel není podle domácího práva povinen jej získat a oznámit.[97] Návrh možnost nevyužívá a v materiálech k tomu není uvedeno nic.
- **Uspořádání systému.** Model popsaný v kapitole 12 zachovává plný rozsah přijímaných údajů a omezuje jejich plošnou dostupnost uvnitř státní správy. Cíl tedy zůstává nedotčen a klesá hodnota souboru pro útočníka i pro zneužití zevnitř.

Třetí položka je v tomto kritériu nejdůležitější a zároveň je tou, o které se nikde nerozhodovalo veřejně. Rozsah přijímaných údajů je dán směrnicí, kdežto o tom, kdo je smí spojovat, v jakých kombinacích a za jakých podmínek, rozhoduje architektura systému. To bývá považováno za technický detail a neprojednává se.

Sem míří i závěr kapitoly 10. Ústavní soud v roce 2019 uvedl mezi důvody přiměřenosti úpravy uchovávání provozních údajů skutečnost, že oprávněné orgány nemají databázi, ve které by mohly libovolně vyhledávat. U projednávaného návrhu nikdo nevysvětlil, proč takovou databázi mít musí.

V tomto kritériu jsou materiály nejslabší. U žádné ze tří voleb neuvádějí, proč by šetrnější řešení cíle nedosáhlo.

[95] Nález Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. 3. 2011, bod 37.

[96] Rozpětí stanoví příloha VI směrnice Rady (EU) 2023/2226; viz rozdílovou tabulku, PDF str. 244. Odůvodnění viz důvodová zpráva, PDF str. 74 a 95.

[97] Příloha VI směrnice Rady (EU) 2023/2226, oddíl II pododdíl C, PDF str. 268.

PŘIMĚŘENOST V UŽŠÍM SMYSLU

Třetí kritérium poměřuje újmu na základním právu s přínosem opatření. K takovému poměřování je zapotřebí mít obě strany vah, tedy přínos i újmu.

Materiály odhadují očekávaný fiskální výnos v řádu desítek milionů korun a náklady na vývoj a provoz informačních technologií správce daně v rozmezí 25 až 35 milionů korun.[98] Druhá strana v materiálech chybí. Riziko plynoucí z existence souboru identifikovaných držitelů nebylo oceněno ani kvalitativně, například v podobě kvalitativního zásahu do soukromí a jeho intenzity vůči zájmu na řádném výběru daní. Poměřování, které třetí kritérium vyžaduje, proto na dosavadních materiálech provést nelze.

SHRNUTÍ A CO BY JE ZMĚNILO

Rozdíl mezi druhým a třetím kritériem stojí za zdůraznění. U potřebnosti chybí odůvodnění rozhodnutí, která předkladatel učinil. U přiměřenosti chybí samotný podklad, bez kterého se poměřovat nedá. První nedostatek lze odstranit doplněním textu, druhý vyžaduje posouzení, které dosud nikdo neprovedl.

TABULKA 3 Tři kritéria proporcionality podle dosavadních materiálů

Kritérium	Stav podle dosavadních materiálů	Co by jej doplnilo
Vhodnost	Podle našeho názoru splněno. Systematické oznamování může správu daní v této oblasti zlepšit.	Nic dalšího není třeba.
Potřebnost	Nedoloženo. U tří rozhodnutí, která Česká republika skutečně učinila, byl k dispozici šetrnější prostředek a materiály neuvádějí, proč nebyl použit.	Odůvodnění u desetileté doby uchování, u místa narození a u plošné analytické dostupnosti údajů uvnitř státní správy.
Přiměřenost v užším smyslu	Neprovedeno. Jedna strana vah, tedy bezpečnostní riziko souboru, nebyl oceněna	Ocenění tohoto rizika alespoň kvalitativně a doplnění poměřování.

[98] Závěrečná zpráva RIA, kap. 1.1, PDF str. 117 (dokument str. 6).

12. DOPORUČENÝ MODEL

Bezpečnostního cíle samozřejmě nelze dosáhnout tak, že stát umožní, aby poskytovatel některé povinné položky vůbec neoznamoval. Takový postup by mohl být posouzen jako neúplná transpozice a vystavil by poskytovatele i stát riziku reakce ze strany EU.

Robustnější cesta vede opačným směrem. Poskytovatel odešle celý evropsky předepsaný report a Finanční správa jej v plném rozsahu přijme. Architektura systému pak omezí, které části jsou dostupné pro rutinní práci a které lze otevřít pouze v konkrétním případě. Plný rozsah oznamovaných údajů a plná analytická dostupnost jsou dvě odlišné vlastnosti systému, jak popisuje kapitola 6.

Rozdělení do dvou vrstev může vycházet přímo z toho, k čemu jsou jednotlivé položky při správě daní potřeba.

1. Rutinní daňová vrstva obsahuje údaje nezbytné pro běžné určení daňové povinnosti, tedy zejména informace o zdanitelných dispozicích. Sem patří prodeje do fiat měny a tam, kde je to relevantní, směny mezi kryptoaktivy. Součástí by případně mohly být i nákupy, pokud by byly potřeba pro stanovení daňové povinnosti nebo časového testu.
2. Chráněná vrstva obsahuje položky, které indikují akumulaci nebo samosprávné nakládání s vlastními bezpečnostními klíči. Sem patří odchozí převody a souhrnné převody na adresy, které poskytovatel nezná jako adresy jiného poskytovatele nebo finanční instituce. Právě tato kombinace umožňuje odhad, o kterém pojednávala druhá kapitola týkající se útoků a jejich přípravy.

Přístup do chráněné vrstvy by měl být možný pouze na základě konkrétního řízení, spisu nebo jiného doloženého zákonného účelu. K tomu se pojí další opatření uvedená v kapitole týkající se architektury nového systému. Konkrétně tedy omezení okruhu oprávněných osob, nezměnitelné logování včetně důvodu a účelu, dvojí schválení u exportů a nestandardních spojení, technické znemožnění hromadného řazení osob a možnost dotčené osoby zjistit, kdo k jejím údajům přistupoval.

Přísnější varianta by spočívala v tom, že by některé čistě domácí položky nebyly v operativním státním úložišti dlouhodobě drženy vůbec a v konkrétním případě by byly znovu vyžádány od poskytovatele. Tato varianta si zaslouží samostatný právní rozbor, protože retenční povinnosti nejsou pro všechny datové toky totožné. Základní doporučení této studie je proto konzervativnější a spočívá v přijetí plného reportu se segmentací citlivých položek.

Návrh modelu vychází z toho, že stát citlivé údaje bude mít k dispozici, protože je evropská úprava vyžaduje oznamovat. Mění ovšem ekonomiku jejich zneužití. Pracovník, který by chtěl databázi použít k vyhledávání nových obětí, narazí na to, že nejcitlivější profil se otevře až tehdy, když existuje předem identifikovaná osoba a doložený služební důvod. Postup popsaný v kapitole 4, tedy malý počet cílených dotazů bez vazby na spis, přestává být pohodlnou cestou k získání dat.

Jakkoliv se výše uvedené bezpečnostní návrhy pro stavbu systému snaží o zlepšení nakládání s daty a jejich větší bezpečnost, níže nicméně nalezneme rizika, kterým se vyhnout nelze. Jsou to zejména následující:

1. **Kompromitace celé infrastruktury** – scénář, kdy útočník získá kontrolu nad systémem jako celkem. Pokud jsou vrstvy odděleny jen logicky, útočník s kontrolou nad celým systémem je dokáže propojit sám. Hodnotu takového útoku snižuje jen oddělení, při kterém je propojovací klíč (pseudonymizace) spravován mimo systém a mimo dosah jeho administrátorů.
2. **Zvýšení časových a finančních nákladů** – z logiky věci návrh na větší bezpečnost zvyšuje provozní náklady a zpomaluje část analytické práce. Dotaz do chráněné vrstvy vyžaduje uvedení důvodu a v některých případech druhé schválení.
3. **Citlivost rutinní vrstvy** – i totožnost, bydliště a objemy prodejů do fiat měny prozrazují, kdo s kryptoaktivy pracoval ve větším rozsahu. Rozdělení do vrstev riziko výběru obětí snižuje, ale neodstraňuje; logování, detekce anomálií a zákaz hromadného řazení proto musí platit i pro rutinní vrstvu.
4. **Lidský faktor** – Lidský faktor – základní slabina každého systému. Návrh sice zneužití přístupu ztěžuje a zvyšuje riziko odhalení, od všech zúčastněných však vyžaduje kázeň při provozu. Pokud se doložení účelu stane formalitou vyplňovanou automaticky, opatření ztratí smysl.

Poslední bod považujeme za nejzávažnější. Technická opatření fungují jen tehdy, pokud je doprovází kontrola jejich skutečného dodržování, a právě proto katalog v kapitole 7 obsahuje nezávislý audit před spuštěním a detekci neobvyklých vzorců dotazů.

13. CO JE NYNÍ TŘEBA DOLOŽIT PŘED SCHVÁLENÍM

TABULKA 4 Bezpečnostní koncept systému: co materiály obsahují a co chybí

OBLAST	CO MATERIÁLY OBSAHUJÍ	CO CHYBÍ
Posouzení vlivu na ochranu osobních údajů	Samostatnou kapitolu s vymezením účelu, určením správce, popisem kategorií údajů a vyhodnocením rizikovosti, které zpracování označuje za rizikové a velkého rozsahu.	Model hrozeb, scénář zneužití oprávněného přístupu zevnitř a popis architektury úložiště.
Účely dalšího využití údajů	Rozšíření okruhu účelů, ke kterým lze informace z mezinárodní spolupráce použít bez souhlasu státu, který je poskytl, nově o oblast cel a o legalizaci výnosů z trestné činnosti, financování terorismu a mezinárodní sankce.	Posouzení, co toto rozšíření znamená u datové sady tohoto typu, a taxativní výčet účelů dalšího zpracování.
Doba uchování u správce daně	Nic. Desetiletá lhůta v návrhu dopadá na poskytovatele.	Jak dlouho bude Finanční správa oznámené údaje držet a jak proběhne jejich výmaz.
Korupční rizika	Analýzu včetně kontrolních mechanismů a jejich eliminace.	Rozbor scénáře, ve kterém oprávněný pracovník provádí cílené dotazy bez vazby na spis.
Informování dotčené osoby o incidentu	Povinnost vyrozumět dotčenou osobu při zjištění narušení bezpečnosti, která vyplývá z unijní úpravy.	Lhůta, určení toho, kdo o vyrozumění rozhoduje, a vyjasnění, zda se povinnost vztahuje i na podezření zneužití zevnitř.
Záznamy o přístupech	Zmínku o přístupu zaměstnanců včetně logování náhledů a provedených změn.	Zakotvení v závazném předpisu, obsah záznamu, ochrana proti změně a určení toho, kdo kontroluje administrátory.
Datový tok	Určení specializovaného úřadu jako správce a konstatování, že zapojení zpracovatele se nepředpokládá.	Kde se domácí a zahraniční údaje ukládají a které navazující systémy z nich vytvářejí kopie.
Konsolidace a analytické funkce	Nic.	Zda lze jediným dotazem spojit historii osoby napříč poskytovateli a roky a zda systém umožňuje sestavit hromadné pořadí osob podle majetkové aktivity.
Přístupový model	Nic.	Kolik zaměstnanců má technickou možnost zobrazit konsolidovaný profil osoby a na jaké organizační úrovni.

Tato kapitola shrnuje, co by měly materiály obsahovat, aby na otázky předchozích kapitol odpověděly. Tabulka 4 výše mapuje jednotlivé oblasti, které jsou důležité z hlediska architektury celého systému, co k nim vládní materiály obsahují a co v nich chybí.

Níže pak nalezneme doplňující otázky, které rozšiřují test proporcionality představený v kapitole 11 a následně ještě bezpečnostní koncept navrhovaného systému.

ODŮVODNĚNÍ, CHYBĚJÍCÍ V TESTU PROPORCIONALITY

Okruh oznamovaných osob mezi následující položky nepatří, protože jej určuje evropská úprava. Všechna čtyři doplnění se týkají rozhodnutí, která učinila nebo teprve učiní Česká republika.

- **Proč je retence u poskytovatelů stanovena na deset a ne na pět let.** Doložit, že přínos let šest až deset pro správu daní převažuje nad rizikem pro dotčené osoby; odkaz na shodu s jinými agendami a na maximální lhůtu podle § 148 daňového řádu sám o sobě nestačí.
- **Jak dlouho bude údaje držet stát.** Určit dobu uchování oznámených údajů u správce daně a postup jejich výmazu, které zákonný text neobsahuje.
- **Kritérium, které zachytí dopad na dotčené osoby.** Doplnit do soustavy hodnotících kritérií hledisko zásahu do soukromí a bezpečnostního rizika plynoucího z existence evidence. Jak ukazuje kapitola 9, žádné z pěti kritérií použitých v závěrečné zprávě takové hledisko neobsahuje.[99]
- **Proč návrh nevyužívá možnost vypustit místo narození.** Doložit, k čemu správce daně tento údaj potřebuje, nebo jej z okruhu zjišťovaných a oznamovaných údajů vypustit (viz doporučení 3 v kapitole 14)

BEZPEČNOSTNÍ KONCEPT SYSTÉMU

Zejména druhý řádek v tabulce výše stojí za zvláštní pozornost, protože jde o místo, kde se návrh vyjadřuje k nakládání s údaji, a vyjadřuje se rozšiřujícím směrem.[100] Považujeme za potřebné, aby se předkladatel vyslovil k tomu, jak se okruh účelů bude vyvíjet dál, protože právě postupné rozšiřování účelu patří k rizikům popsaným v kapitole 4.

Odpověď, podle které budou údaje chráněny v souladu s obecným nařízením o ochraně osobních údajů a bezpečnostními standardy, u systému této povahy nestačí. Parlament potřebuje znát bezpečnostní model a rozsah funkcionality, jinak nemá jak posoudit přiměřenost zásahu do soukromí.

[99] Soustavu pěti hodnotících kritérií uvádí Závěrečná zpráva RIA, část A, kap. 3.1, PDF str. 120 (dokument str. 9).

[100] Čl. I body 38 a 39 návrhu, kterými se mění § 22 odst. 4 a vkládá nový § 22 odst. 5. Sněmovní tisk 98, PDF str. 28 (dokument str. 26); znění s vyznačením změn PDF str. 179.

14. DOPORUČENÍ

POSLANECKÉ SNĚMOVNĚ A ROZPOČTOVÉMU VÝBORU

1. Vyžádat si od předkladatele odůvodnění položek uvedených v kapitole 13, následně pak i odpověď na otázku, zda bude systém obsahovat rutinní plošnou konsolidaci údajů o jednotlivci a pokud ano, tak zdůvodnění, proč tomu tak je.
2. Podmínit další projednávání předložením veřejně popsaného bezpečnostního konceptu v rozsahu uvedeném v kapitole 13.
3. Zvážit pozměňovací návrh, který vypustí místo narození z okruhu zjišťovaných a oznamovaných údajů. Výjimka ve směrnici je vázána na to, že poskytovatel není podle domácího práva povinen tento údaj získat a oznámit. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti sice ukládá místo narození zjišťovat a uchovávat, povinnost oznamovat je orgánu veřejné moci v pravidelném hlášení z něj ovšem neplyne.[101]
4. Zvážit zakotvení základních záruk přímo v zákoně, konkrétně podmínku doloženého účelu u dotazu do citlivých údajů, povinnost zaznamenat důvod přístupu, ochranu záznamů proti změně, zákaz sestavování hromadného pořadí osob bez výslovného zákonného účelu a dobu uchování údajů na straně správce daně.

MINISTERSTVU FINANCÍ A FINANČNÍ SPRÁVĚ

1. Doplnit posouzení dopadu na dotčené osoby v rozsahu uvedeném v kapitole 9.
2. Popsat datový tok, přístupový model a retenční model v podobě, kterou lze veřejně posoudit, přičemž citlivé technické detaily veřejné být nemusí.
3. Zpracovat model hrozeb zahrnující scénář zneužití oprávněného přístupu a nechat kontroly proti němu nezávisle otestovat před ostrým provozem.
4. Vypořádat ty výtky Komise pro hodnocení dopadů regulace, které zůstaly bez odezvy.
5. Implementovat model popsaný v kapitole 12.

[101] Zákon č. 253/2008 Sb. vymezuje identifikační údaje v § 5 odst. 1 písm. a) a místo narození mezi ně řadí. Uchovávání po dobu deseti let stanoví § 16, poskytnutí údajů na pokyn Finančního analytického úřadu § 24 a uvedení identifikačních údajů v oznámení podezřelého obchodu § 18 odst. 2. Povinnost pravidelně oznamovat identifikační údaje orgánu veřejné moci zákon neobsahuje.

ZÁVĚR

Moderní stát má legitimní důvody získávat některé finanční informace o svých občanech. Výběr daní, boj proti podvodům a mezinárodní spolupráce bez dat fungovat nemohou a tato studie to nezpochybňuje. Stejně legitimní je ovšem požadavek, aby stát při budování informačních systémů počítal vedle běžného kybernetického útoku také s korupcí, se zneužitím privilegovaného účtu, s postupným rozšiřováním účelu a s tím, jakou hodnotu data získají po propojení s fyzickou identitou konkrétního člověka.

U kryptoaktiv má tento požadavek zvláštní váhu. Dostupný výzkum neumožňuje tvrdit, že centralizovaná databáze automaticky povede k únosu nebo k loupeži. Umožňuje ovšem doložit jednotlivé články rizikového řetězce. Fyzické útoky na držitele kryptoaktiv existují a jejich provedení se posouvá k pečlivěji připraveným scénářům. Výběru oběti předchází zjišťování majetku a bydliště. Osobní a majetkové databáze byly v několika zemích při výběru obětí využity. Pracovník s přístupem může citlivé údaje zneužít a doložené případy z veřejného i soukromého sektoru to potvrzují. A jednou kompromitovanou historickou finanční informaci nelze vzít zpět.

Otázka, kterou tato studie klade, se přitom netýká toho, zda stát údaje o kryptoaktivech dostane. To určuje evropská úprava a Česká republika o tom nerozhoduje. Týká se toho, v jakém uspořádání je bude držet, kdo je bude smět spojovat, jak dlouho a za jakých podmínek. O tom rozhoduje Česká republika sama a veřejně se o tom zatím nejednalo.

Ani riziko postupného rozšiřování účelu v tomto případě nezůstává v rovině obavy. Samotný návrh rozšiřuje okruh účelů, ke kterým lze informace z mezinárodní spolupráce použít bez souhlasu státu, který je poskytl, o oblast cel a o legalizaci výnosů z trestné činnosti, financování terorismu a mezinárodní sankce.[102] Každý z těchto účelů je sám o sobě obhajitelný. Podstatné je, že se okruh rozšiřuje v témže předpisu, který datovou sadu zavádí, a že se tak děje bez posouzení, co to pro tuto konkrétní sadu znamená.

Česká republika se přitom řadí mezi nejbezpečnější země světa. V žebříčku Global Peace Index za rok 2026 jí patří třinácté místo ze 163 hodnocených zemí a území.[103] Tento stav je hodnotou, kterou má veřejná politika chránit, a důvodem k obezřetnosti při rozhodnutích, jejichž následky se projeví až za několik let.

Ústavní soud k tomu má formulaci, která se na projednávaný návrh dá vztáhnout přímo. Stát podle něj musí dodržovat jisté informační sebeomezení, může-li jím zajišťované funkce zabezpečit i jinak.[104] Právě tuto otázku materiály k návrhu zatím nezodpovídají. Evropskou oznamovací povinnost lze splnit a současně usilovat o to, aby nejcitlivější data nebyla plošně využitelná jako nástroj pro třídění obyvatel. Kapitola 12 popisuje, jak by takové uspořádání mohlo vypadat.

Politici a úředníci, kteří rozhodují o rozsahu, architektuře a přístupových pravidlech citlivých databází, rozhodují zároveň o bezpečnosti konkrétních lidí a jejich rodin. U aktiv, která lze pod fyzickým nátlakem převést během několika minut, to platí zvlášť. Heslo lze změnit a server vyměnit. Informaci, která jednou unikla a označila člověka za pravděpodobného držitele významného likvidního majetku, zpět do databáze nevrátíme.

[102] Čl. I body 38 a 39 návrhu, § 22 odst. 4 a 5. Sněmovní tisk 98, PDF str. 28 (dokument str. 26). Blíže viz kapitolu 13 této studie.

[103] Institute for Economics and Peace, Global Peace Index 2026, červen 2026. Žebříček hodnotí 163 zemí a území; Česká republika je na 13. místě se skóre 1,517.

[104] Nález Ústavního soudu sp. zn. Pl. ÚS 26/16 ze dne 12. 12. 2017, bod 96. Viz kapitolu 10 této studie.

O TÉTO STUDII

AUTOR A ZÁŠTITA

Autorem studie je Ing. Jan Šincl. Studie vzniká pod záštitou ČKMA. Za obsah, včetně všech hodnotících soudů, odpovídá autor.

METODIKA

Studie pracuje výhradně s veřejně dostupnými prameny. Právní část vychází z textu sněmovního tisku 98 včetně důvodové zprávy, závěrečné zprávy z hodnocení dopadů regulace a rozdílové tabulky, dále z primárních textů evropských předpisů a z judikatury Ústavního soudu a Soudního dvora Evropské unie. U každého tvrzení opřeného o tyto prameny uvádí poznámka pod čarou konkrétní stránku nebo bod, aby si čtenář mohl údaj ověřit sám.

Empirická část o fyzických útocích na držitele kryptoaktiv vychází z pěti na sobě částečně závislých zdrojů (Lopp, Gart Research, CertiK, Chainalysis, TRM Labs s Metropolitní policií) a ze dvou recenzovaných prací (AFT 2024, USENIX 2023). Studie tyto zdroje nesměšuje do jednoho čísla, protože každý používá jinou definici incidentu i jiná kritéria pro jeho zařazení. Tam, kde se údaje liší, studie rozdíl uvádí a vysvětluje jej.

Porovnání připomínek pracovní komise Legislativní rady vlády s konečným zněním závěrečné zprávy provedl autor tak, že každou z dvaadvaceti připomínek dohledal ve výsledném textu a zařadil ji do jedné ze tří kategorií, tedy zohledněno, zohledněno částečně a nezohledněno.

Studie nepředjímá, jak by o případném návrhu rozhodl Ústavní soud, a ústavní přezkum nepovažuje za cíl, o který by bylo vhodné usilovat.

UZÁVĚRKA DAT

Text vychází ze stavu právní úpravy a z veřejně dostupných dat ke dni 15. září 2026. Statistiky fyzických útoků se v čase mění, protože katalogy incidentů se doplňují i zpětně; údaje uvedené v kapitole 2 proto odpovídají stavu ke dni uzávěrky, nikoli pozdějšímu.

POUŽITÍ NÁSTROJŮ UMĚLÉ INTELIGENCE

Při přípravě studie byly použity nástroje umělé inteligence, a to k rešerši pramenů, k porovnávání dokumentů a k redakčním úpravám textu. Každé tvrzení opřené o pramen bylo následně ověřeno proti primárnímu zdroji a v poznámkách pod čarou je uvedeno místo, kde se údaj nachází. Odpovědnost za obsah nese autor.

GLOSÁŘ

Následující přehled vysvětluje pojmy, které se v textu opakují.

CARF. Crypto-Asset Reporting Framework, standard Organizace pro hospodářskou spolupráci a rozvoj pro oznamování údajů o kryptoaktivech pro daňové účely. Evropská úprava jej přejímá.

DAC8. Označení směrnice Rady (EU) 2023/2226, kterou se rozšiřuje automatická výměna informací v oblasti daní o údaje o kryptoaktivech.

DAC 9. Označení směrnice Rady (EU) 2025/872, která na předchozí úpravu navazuje.

Hodnocení dopadů regulace (RIA). Postup, kterým předkladatel před přijetím předpisu porovnává možné varianty řešení podle předem stanovených kritérií. Výstupem je závěrečná zpráva.

Posouzení vlivu na ochranu osobních údajů. Analýza rizik, kterou správce provádí u zpracování pravděpodobně vysoce rizikového pro práva dotčených osob. V důvodové zprávě je zpracována jako samostatná kapitola.

Oznamující poskytovatel. Poskytovatel služeb souvisejících s kryptoaktivy, kterému návrh ukládá zjišťovat a oznamovat údaje o uživatelích.

Oznamovaná transakce. Podle návrhu směnná transakce nebo převod kryptoaktiva. Zahrnuje tedy nákup, prodej i odeslání mimo poskytovatele.

Oznamované období. Kalendářní rok, za který se údaje oznamují.

Tuzemský rezident. Uživatel, který je daňovým rezidentem České republiky. Jejich zahrnutí do oznamování vyžaduje DAC8; závěrečná zpráva RIA je nesprávně považuje za volbu České republiky (kapitola 8).

Vlastní úschova (self-custody). Držení kryptoaktiv v peněžence, ke které má soukromé klíče pouze jejich držitel, tedy mimo evidovaného poskytovatele.

Rozšiřování účelu. Postupné využívání existujícího informačního systému k dalším cílům, pro které nebyl zřízen. V anglické literatuře function creep.

Fyzický útok na držitele kryptoaktiv. Násilné jednání směřující k tomu, aby oběť pod nátlakem převedla kryptoaktiva. V anglické literatuře wrench attack.

Specializovaný finanční úřad. Úřad určený návrhem jako správce údajů oznamovaných podle nové úpravy.

Evropský inspektor ochrany údajů. Dozorový orgán Evropské unie pro zpracování osobních údajů orgány a institucemi Unie. V roce 2023 vydal k návrhu DAC8 stanovisko.

SEZNAM ZDROJŮ

PRÁVNÍ PŘEDPISY

Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů.

Zákon č. 164/2013 Sb., o mezinárodní spolupráci při správě daní a o změně dalších souvisejících zákonů, ve znění pozdějších předpisů.

Zákon č. 300/2016 Sb., o centrální evidenci účtů, ve znění pozdějších předpisů [online]. [cit. 2026-09-13]. Dostupné z: https://www.zakonyprolidi.cz/cs/2016-300

Zákon č. 112/2016 Sb., o evidenci tržeb, ve znění pozdějších předpisů.

Zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů.

Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů [online]. [cit. 2026-09-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/2008-253

NĚMECKO. Abgabenordnung, § 93 a § 93b [online]. [cit. 2026-09-13]. Dostupné z: https://www.gesetze-im-internet.de/ao_1977/__93.html

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů) [online]. [cit. 2026-09-13]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679

Směrnice Rady (EU) 2023/2226 ze dne 17. října 2023, kterou se mění směrnice 2011/16/EU o správní spolupráci v oblasti daní (DAC8) [online]. [cit. 2026-09-13]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32023L2226

Směrnice Rady 2014/107/EU ze dne 9. prosince 2014, kterou se mění směrnice 2011/16/EU, pokud jde o povinnou automatickou výměnu informací v oblasti daní (DAC 2) [online]. [cit. 2026-09-15]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32014L0107

Směrnice Rady (EU) 2025/872 ze dne 14. dubna 2025, kterou se mění směrnice 2011/16/EU o správní spolupráci v oblasti daní (DAC 9) [online]. [cit. 2026-09-13]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32025L0872

JUDIKATURA

ÚSTAVNÍ SOUD. Nález ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10 [online]. [cit. 2026-09-13]. Dostupné z: https://nalus.usoud.cz/Search/GetText.aspx?sz=Pl-24-10

ÚSTAVNÍ SOUD. Nález ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17. Vyhlášen pod č. 161/2019 Sb. [online]. [cit. 2026-09-15]. Dostupné z: https://nalus.usoud.cz/Search/GetText.aspx?sz=Pl-45-17

ÚSTAVNÍ SOUD. Nález ze dne 12. 12. 2017, sp. zn. Pl. ÚS 26/16 [online]. [cit. 2026-09-13]. Dostupné z: https://www.usoud.cz/fileadmin/user_upload/Tiskova_mluvci/Publikovane_nalezy/2017/Pl._US_26_16_na_web_vcetne_vsech_disentu.pdf

SOUDNÍ DVŮR EVROPSKÉ UNIE. Rozsudek ze dne 8. dubna 2014, spojené věci C-293/12 a C-594/12, Digital Rights Ireland [online]. [cit. 2026-09-13]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:62012CJ0293

SOUDNÍ DVŮR EVROPSKÉ UNIE. Rozsudek ze dne 22. listopadu 2022, spojené věci C-37/20 a C-601/20, Luxembourg Business Registers a Sovim [online]. [cit. 2026-09-13]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:62020CJ0037

ÚŘEDNÍ A LEGISLATIVNÍ DOKUMENTY ČESKÉ REPUBLIKY

VLÁDA ČESKÉ REPUBLIKY. Vládní návrh zákona, kterým se mění zákon č. 164/2013 Sb., o mezinárodní spolupráci při správě daní, ve znění pozdějších předpisů. Sněmovní tisk 98/0, 10. volební období. Praha, 5. 2. 2026. Obsahuje důvodovou zprávu, závěrečnou zprávu z hodnocení dopadů regulace a rozdílovou tabulku [online]. [cit. 2026-09-13]. Dostupné z: https://www.psp.cz/sqw/text/tiskt.sqw?O=10&CT=98&CT1=0

POSLANECKÁ SNĚMOVNA PARLAMENTU ČESKÉ REPUBLIKY. Sněmovní tisk 98, průběh projednávání [online]. [cit. 2026-09-13]. Dostupné z: https://www.psp.cz/sqw/historie.sqw?O=10&T=98

ÚŘAD VLÁDY ČESKÉ REPUBLIKY, Pracovní komise Legislativní rady vlády pro hodnocení dopadů regulace. Stanovisko k návrhu zákona, kterým se mění zákon č. 164/2013 Sb., čj. OVA 408/24, 19. 7. 2024 [online]. [cit. 2026-09-13]. Dostupné z: https://ria.vlada.cz/wp-content/uploads/408_24.pdf

ÚŘAD VLÁDY ČESKÉ REPUBLIKY. Obecné zásady pro hodnocení dopadů regulace (RIA), znění účinné od 1. 1. 2025 [online]. [cit. 2026-09-13]. Dostupné z: https://ria.vlada.cz/wp-content/uploads/2025_01_01_OZ_RIA.pdf

ÚŘAD VLÁDY ČESKÉ REPUBLIKY. Obecné zásady pro hodnocení dopadů regulace (RIA), znění účinné od 1. 2. 2023 [online]. [cit. 2026-09-13]. Dostupné z: https://ria.vlada.cz/wp-content/uploads/OZ-RIA_FINAL_1.2.2023.pdf

ČESKÁ NÁRODNÍ BANKA. Centrální evidence účtů [online]. [cit. 2026-09-13]. Dostupné z: https://www.cnb.cz/cs/statistika/centralni-evidence-uctu/

DOKUMENTY ORGÁNŮ EVROPSKÉ UNIE A ZAHRANIČNÍCH ORGÁNŮ

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ. Shrnutí stanoviska evropského inspektora ochrany údajů k návrhu směrnice Rady, kterou se mění směrnice 2011/16/EU o správní spolupráci v oblasti daní. Stanovisko 2023/C 199/04 ze dne 3. 4. 2023. Úř. věst. C 199, 7. 6. 2023, s. 5 [online]. [cit. 2026-09-13]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52023XX0607(01)

RADA EVROPSKÉ UNIE. Presentation by the European Commission. Pracovní dokument WK 249/2023 INIT, spis 2022/0413 (CNS). Brusel, 10. 1. 2023 [online]. [cit. 2026-09-13]. Dostupné z: https://data.consilium.europa.eu/doc/document/WK-249-2023-INIT/en/pdf

EVROPSKÁ KOMISE. DAC8: Administrative cooperation in the field of taxation. Informační stránka Generálního ředitelství pro daně a celní unii [online]. [cit. 2026-09-15]. Dostupné z: https://taxation-customs.ec.europa.eu/taxation/tax-transparency-cooperation/administrative-co-operation-and-mutual-assistance/directive-administrative-cooperation-dac/dac8_en

SKATTEETATEN. Skattelistene [online]. [cit. 2026-09-13]. Dostupné z: https://www.skatteetaten.no/person/skatt/skatteoppgjor/skattelistene/

STORTINGET. Representantforslag om offentliggjøring av skattelister. Dokument 8:15 S (2010–2011) [online]. [cit. 2026-09-13]. Dostupné z: https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Representantforslag/2010-2011/dok8-201011-015/?lvl=0

REGERINGSKANSLIET. Skyddet för personuppgifter ska förstärkas. Tisková zpráva, 21. 10. 2023 [online]. [cit. 2026-09-13]. Dostupné z: https://www.regeringen.se/pressmeddelanden/2023/10/skyddet-for-personuppgifter-ska-forstarkas/

SVERIGES REGERING. Ett förstärkt skydd för personuppgifter på tryck- och yttrandefrihetsområdet. Kommittédirektiv Dir. 2023:145, 19. 10. 2023 [online]. [cit. 2026-09-13]. Dostupné z: https://www.regeringen.se/rattsliga-dokument/kommittedirektiv/2023/10/dir.-2023145

REGERINGSKANSLIET. Utredning föreslår stärkt skydd för personuppgifter som offentliggörs i söktjänster. Tisková zpráva, 22. 11. 2024 [online]. [cit. 2026-09-13]. Dostupné z: https://www.regeringen.se/pressmeddelanden/2024/11/utredning-foreslar-starkt-skydd-for-personuppgifter-som-offentliggors-i-soktjanster/

STATENS OFFENTLIGA UTREDNINGAR. Personuppgifter och mediegrundlagarna. SOU 2024:75. Stockholm, 20. 11. 2024 [online]. [cit. 2026-09-13]. Dostupné z: https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2024/11/sou-202475/

INTEGRITETSSKYDDSMYNDIGHETEN. Klagomål mot söktjänster med utgivningsbevis. Rättsligt ställningstagande IMYRS 2024:1, 14. 5. 2024 [online]. [cit. 2026-09-13]. Dostupné z: https://www.imy.se/publikationer/klagomal-mot-soktjanster-med-utgivningsbevis/

NORDIC INSTITUTE FOR INTEROPERABILITY SOLUTIONS. X-Road Security [online]. [cit. 2026-09-13]. Dostupné z: https://x-road.global/security

ESTONIAN INFORMATION SYSTEM AUTHORITY. Usage of personal data [online]. [cit. 2026-09-13]. Dostupné z: https://www.eesti.ee/en/security-and-defense/safety-and-security/usage-of-personal-data/

OECD. International Standards for Automatic Exchange of Information in Tax Matters: Crypto-Asset Reporting Framework and 2023 update to the Common Reporting Standard. Paříž: OECD Publishing, 2023. DOI 10.1787/896d79d1-en.

ODBORNÉ STUDIE A ANALYTICKÉ ZPRÁVY

ORDEKIAN, Marilyne, ATONDO-SIU, Gilberto, HUTCHINGS, Alice a VASEK, Marie. Investigating Wrench Attacks: Physical Attacks Targeting Cryptocurrency Users. In: 6th Conference on Advances in Financial Technologies (AFT 2024). LIPIcs, sv. 316, čl. 24, s. 24:1–24:24. 16. 9. 2024. DOI 10.4230/LIPIcs.AFT.2024.24 [online]. [cit. 2026-09-13]. Dostupné z: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.AFT.2024.24

ABRAMOVA, Svetlana a BÖHME, Rainer. Anatomy of a High-Profile Data Breach: Dissecting the Aftermath of a Crypto-Wallet Case. In: 32nd USENIX Security Symposium. Anaheim, srpen 2023, s. 715–732 [online]. [cit. 2026-09-13]. Dostupné z: https://www.usenix.org/conference/usenixsecurity23/presentation/abramova

TRM LABS a METROPOLITAN POLICE SERVICE. Wrench Attacks: A Crypto Crime Response Framework. 30. 7. 2026 [online]. [cit. 2026-09-13]. Dostupné z: https://www.trmlabs.com/reports-and-whitepapers/wrench-attacks-crypto-enabled-violent-targeting

CERTIK. Intel3D: Wrench Attacks H1 2026. 23. 7. 2026 [online]. [cit. 2026-09-13]. Dostupné z: https://www.certik.com/certik-report/intel3d/intel3d-wrench-h1-2026

CHAINALYSIS. Violent Wrench Attacks Targeting Crypto Holders. 6. 8. 2026 [online]. [cit. 2026-09-13]. Dostupné z: https://www.chainalysis.com/blog/violent-crypto-wrench-attacks-2026/

GART RESEARCH. Cryptocurrency Physical Attacks Statistics. Průběžně aktualizovaný přehled [online]. [cit. 2026-09-13]. Dostupné z: https://gart.io/stats

LOPP, Jameson. Known Physical Bitcoin Attacks. Veřejný katalog vedený od prosince 2014 [online]. [cit. 2026-09-13]. Dostupné z: https://github.com/jlopp/physical-bitcoin-attacks

INSTITUTE FOR ECONOMICS AND PEACE. Global Peace Index 2026. Sydney, červen 2026 [online]. [cit. 2026-09-15]. Dostupné z: https://www.economicsandpeace.org/wp-content/uploads/2026/06/Global-Peace-Index-2026-Report.pdf

ZPRAVODAJSKÉ A PODNIKOVÉ ZDROJE

COINBASE. Protecting Our Customers - Standing Up to Extortionists. 15. 5. 2025 [online]. [cit. 2026-09-13]. Dostupné z: https://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists

CONSTANT, Julien. L'agente du fisc ciblait gardiens de prison et investisseurs en cryptomonnaie pour un mystérieux commanditaire. Le Parisien, 6. 1. 2026 [online]. [cit. 2026-09-13]. Dostupné z: https://www.leparisien.fr/faits-divers/lagente-du-fisc-ciblait-gardiens-de-prison-et-investisseurs-en-cryptomonnaie-pour-un-mysterieux-commanditaire-06-01-2026-WYVSPSJXYFCUFND23GKKJR3D6Y.php

PŘÍLOHA 1 – VYBRANÉ PŘÍPADY Z LOPPOVA KATALOGU

GRIVESNES, SOMME, FRANCIE — 24. 6., 26. 6. A 17. 7. 2026

Pár koupil dům po bohatých důchodcích, kteří byli kryptomilionáři. Na darkwebu unikl daňový výměr předchozích majitelů spolu se starou adresou, tedy tou, kde teď bydlí noví vlastníci. Tři útoky během necelého měsíce. Dva útočníci odsouzeni v srpnu 2026 v Amiens.

https://www.ici.fr/hauts-de-france/somme-80/grivesnes/somme-un-couple-sequestre-chez-lui-et-cible-de-plusieurs-intrusions-pour-de-la-cryptomonnaie-qu-il-ne-possede-pas-9784554

VÍDEŇ, RAKOUSKO — 26. 11. 2025

Syn charkovského místostarosty, který studoval ve Vídni, byl napaden krajany, mezi nimiž měl být i jeho spolužák; byl mučen, aby vydal přístup ke svým peněženkám, okraden a upálen ve vlastním automobilu.

https://www.oe24.at/oesterreich/chronik/wien/feuer-mord-in-wien-zwei-festnahmen/658860793

ZOERSEL, BELGIE — 10. 1. 2026

Dva ozbrojení muži vnikli do domu, zbili a spoutali šedesátiletou lékařku. Motivem byl zisk kryptoměn, které ale žena nevlastnila.

https://www.gva.be/regio/antwerpen/regio-antwerpen/zoersel/gangsters-zoeken-naar-cryptomunten-en-binden-bewoonster-60-vast-in-zoersel-virtuele-munten-steeds-vaker-beoogde-buit/122929883.html

SUNNYVALE, KALIFORNIE, USA — 22. 12. 2025

Útočníci se vydávali za kurýry rozvážkové služby a k tomu využili přístup k účtu oběti. Díky aplikaci sledovali mužovu polohu a věděli, kdy si objednává jídlo, tedy kdy je doma a kdy může kurýra čekat. Muž se útoku nakonec ubránil.

https://www.sfchronicle.com/crime/article/crypto-wrench-attack-home-invasion-22088091.php

MONTREAL, KANADA — 28. 1. 2026

Rodina muže pracujícího v kryptoprůmyslu byla terčem celkem čtyř pokusů o vniknutí do domu během několika týdnů, při jednom dokonce padl výstřel. Případ ukazuje, že jakmile se někdo na seznamu ocitne, jedním útokem to končit nemusí.

https://www.journaldemontreal.com/2026/05/07/violations-de-domicile-une-famille-montrealaise-prise-pour-cible-pour-de-la-cryptomonnaie

Těchto pět případů jsme vybrali pro ilustraci různých cest, kterými se pachatelé k informacím o oběti dostávají; nejde o reprezentativní vzorek. Záminkou pro útok mohou být uniklá zastaralá data nebo účet u rozvážkové služby, útočník může být někdo známý nebo kompletně cizí člověk, útoky mohou být jednorázové nebo se opakovat, důležité je jedno, jakmile útočník získá informace, může je zneužít mnoha způsoby.

Více případů naleznete na:
https://github.com/jlopp/physical-bitcoin-attacks