EVROPSKÁ
KOMISE

V Bruselu dne 9.10.2024
COM(2024) 451 final

ZPRÁVA KOMISE EVROPSKÉMU PARLAMENTU A RADĚ

o prvním pravidelném přezkumu fungování rozhodnutí o odpovídající ochraně týkajícího se rámce EU–USA pro ochranu údajů

1. PRVNÍ PRAVIDELNÝ PŘEZKUM – SOUVISLOSTI, PŘÍPRAVA A POSTUP

Ve svém rozhodnutí ze dne 10. července 2023 (dále jen „rozhodnutí o odpovídající ochraně“) Komise došla k závěru, že rámec EU–USA pro ochranu údajů poskytuje odpovídající úroveň ochrany osobních údajů předávaných z Evropské unie organizacím ve Spojených státech amerických[1]. Rozhodnutí o odpovídající ochraně vyžaduje, aby Komise prováděla pravidelné přezkumy, přičemž k prvnímu by mělo dojít po uplynutí jednoho roku ode dne oznámení rozhodnutí o odpovídající ochraně členským státům. Tato zpráva završuje tento první přezkum.

Jak požaduje 211. bod odůvodnění rozhodnutí o odpovídající ochraně, tento první přezkum, který byl proveden po prvním roce fungování nového rámce, se zaměřil na ověření, zda byly všechny prvky stanovené v rámci provedeny a zda účinně fungují. Přezkum se týkal všech aspektů fungování rámce, a to i s ohledem na právní vývoj, k němuž došlo po přijetí rozhodnutí o odpovídající ochraně.

Při přípravě přezkumu Komise shromáždila informace od příslušných zúčastněných stran, zejména od nevládních organizací s odbornými znalostmi v oblasti digitálních práv a ochrany soukromí[2], organizací certifikovaných podle rámce EU–USA pro ochranu údajů prostřednictvím jejich oborových sdružení[3], jakož i od orgánů USA zapojených do provádění rámce. Kromě toho Komise shromáždila zpětnou vazbu od široké veřejnosti prostřednictvím zvláštní výzvy k předložení faktických podkladů na portálu „Podělte se o svůj názor“[4].

Ve dnech 18. a 19. července 2024 se ve Washingtonu D.C. konalo přezkumné jednání. Zahájili je komisař EU pro spravedlnost a spotřebitele Didier Reynders a ministryně obchodu USA Gina Raimondová.[5]

Za EU prováděli přezkum zástupci Generálního ředitelství Evropské komise pro spravedlnost a spotřebitele spolu s pěti zástupci určenými Evropským sborem pro ochranu osobních údajů (EDPB) z řad různých vnitrostátních úřadů pro ochranu osobních údajů a evropský inspektor

[1] Prováděcí rozhodnutí Komise (EU) 2023/1795 ze dne 10. července 2023 podle nařízení Evropského parlamentu a Rady (EU) 2016/679 o odpovídající úrovni ochrany osobních údajů poskytované rámcem EU–USA pro ochranu údajů.

[2] Komise zaslala devíti nevládním organizacím (Human Rights Watch, American Civil Liberties Union, Consumer Federation of America, Center for Digital Democracy, New America Open Technology Institute, Access Now, Electronic Frontier Foundation, Electronic Privacy Information Center, Center for Democracy and Technology) dotazník, který se týkal zejména relevantního vývoje právního rámce USA, dohledových a donucovacích mechanismů a fungování nápravných mechanismů. Útvary Komise a zástupci EDPB se s těmito nevládními organizacemi setkali rovněž on-line dne 9. července 2024.

[3] Komise zaslala devíti oborovým sdružením (Software & Information Industry Association, U.S. Chamber of Commerce, Information Technology Industry Council, the Software Alliance, Centre for Information Policy Leadership, Interactive Advertising Bureau, United States Council for International Business, Computer and Communications Industry Association, Engine) dotazník, který se týkal zejména zkušeností společností certifikovaných podle rámce EU–USA pro ochranu údajů, především procesu certifikace, kroků přijatých k dodržování zásad rámce EU–USA pro ochranu údajů, mechanismů řešení žádostí a stížností jednotlivců atd.

[4] Obdržená zpětná vazba je k dispozici na této adrese: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-EU-US-Data-Privacy-Framework-report-of-the-Commission-on-how-the-framework-is-functioning_cs.

[5] Přezkumné jednání bylo uspořádáno podle témat, přičemž každý bod programu byl uveden krátkou prezentací příslušného orgánu USA, zástupce EU nebo organizace, po níž následovalo podrobné jednání s otázkami a odpověďmi. První den byly projednávány „obchodní aspekty“ rámce (tj. uplatňování a prosazování požadavků vztahujících se na společnosti certifikované podle rámce EU–USA pro ochranu údajů), druhý den se hovořilo o záležitostech týkajících se přístupu vlády k osobním údajům.

ochrany údajů[6]. Za USA se jednání zúčastnili zástupci Ministerstva obchodu, Ministerstva zahraničí, Federální obchodní komise, Ministerstva dopravy, Úřadu ředitele národních zpravodajských služeb (ODNI), Ministerstva spravedlnosti, Generálního inspektora pro zpravodajskou komunitu a členové Výboru pro dohled nad ochranou soukromí a občanských svobod (PCLOB). Kromě toho během příslušných přezkumných jednání poskytli informace zástupci organizací nabízejících služby nezávislého řešení sporů a Americké arbitrážní asociace. Při přezkumu byly rovněž využity informace, jež přinesly prezentace společností certifikovaných podle rámce EU–USA pro ochranu údajů, které se týkaly toho, jak společnosti plní požadavky rámce.

Dalším zdrojem informací pro zjištění Komise byly veřejně dostupné materiály, jako jsou například soudní rozhodnutí, prováděcí předpisy a postupy příslušných orgánů USA, zprávy a studie nevládních organizací, zprávy o transparentnosti vydané společnostmi certifikovanými podle rámce EU–USA pro ochranu údajů, výroční zprávy nezávislých orgánů dohledu a také zprávy ze sdělovacích prostředků.

2. ZJIŠTĚNÍ

2.1 Obchodní aspekty

2.1.1 Proces certifikace

Aby mohla americká společnost přijímat osobní údaje předávané z EU na základě rámce EU–USA pro ochranu údajů, musí u Ministerstva obchodu provést certifikaci a následně každoročně opětovnou certifikaci s cílem stvrdit dodržování konkrétních požadavků na ochranu údajů („zásady rámce EU–USA pro ochranu údajů“). Certifikovaná společnost musí podléhat vyšetřovacím a donucovacím pravomocem Federální obchodní komise nebo Ministerstva dopravy, veřejně deklarovat svůj závazek dodržovat zásady rámce EU–USA pro ochranu údajů, zveřejnit svou politiku ochrany soukromí a tyto požadavky plně provést[7]. Před dokončením certifikace Ministerstvo obchodu ověří, zda společnost splnila všechny požadavky na certifikaci[8].

Na přezkumném jednání Ministerstvo obchodu vysvětlilo, že v tomto prvním roce fungování rámce EU–USA pro ochranu údajů byl důraz kladen na zavedení procesu certifikace, včetně vývoje specializovaných IT nástrojů, aktualizace postupů, spolupráce se společnostmi a provádění dalších osvětových činností. Ke dni konání přezkumného jednání získalo certifikaci podle rámce EU–USA pro ochranu údajů více než 2 800 společností. To znamená, že certifikace podle rámce EU–USA pro ochranu údajů získalo více společností než v rámci předchozího štítu na ochranu soukromí v prvním roce jeho fungování[9]. Podle informací poskytnutých Ministerstvem obchodu tvoří 70 % účastníků malé a střední podniky a velký počet společností rámce EU–USA pro ochranu údajů (47 %) působí v informačním, komunikačním a technologickém odvětví. Kromě toho je 60 % společností certifikováno výhradně pro údaje z jiných oblastí než lidských zdrojů, 2,5 % společností je certifikováno

[6] Zástupci Komise a EDPB se sešli 12. června a 10. července 2024, aby se na přezkum připravili, projednali obdržené podklady a určili, u kterých aspektů je třeba dalšího sběru informací či objasnění.
[7] Oddíl I.2 přílohy I rozhodnutí o odpovídající ochraně.
[8] Příloha III rozhodnutí o odpovídající ochraně.
[9] Ve stejném období získalo certifikaci podle štítu na ochranu soukromí 2 400 společností.

výhradně pro údaje v oblasti lidských zdrojů a 37,5 % společností je certifikováno pro údaje v oblasti lidských zdrojů i údaje z jiných oblastí.

Ministerstvo obchodu přijalo nezbytné postupy pro vyřizování žádostí společností. Společnosti musí své žádosti o certifikaci podávat na internetových stránkách Ministerstva obchodu věnovaných rámci EU–USA pro ochranu údajů (https://www.dataprivacyframework.gov/). Ty obsahují informace o tom, jak se připojit k rámci EU–USA pro ochranu údajů[10], a o povinnostech společností podle rámce[11]. Za všechny aspekty týkající se řízení a správy rámce EU–USA pro ochranu údajů, včetně procesu certifikace a sledování souladu, je na Ministerstvu obchodu zodpovědný zvláštní tým pod vedením ředitele pro rámec ochrany osobních údajů. Každá žádost je přidělena konkrétnímu pracovníkovi, který zůstává odpovědný za příslušnou společnost po celou dobu certifikačního procesu.

Za účelem certifikace dle rámce předkládají společnosti žádost včetně návrhu politiky ochrany soukromí. Ministerstvo obchodu zkoumá, zda je v souladu s příslušnými požadavky rámce EU–USA pro ochranu údajů. Pokud chtějí organizace certifikovat různé subjekty v rámci skupiny podniků (např. různé dceřiné společnosti), Ministerstvo obchodu si vyžádá a přezkoumá buď jednu komplexní politiku ochrany soukromí, která jasně označuje všechny subjekty, na něž se má vztahovat, nebo samostatné politiky pro každý subjekt. Ministerstvo obchodu rovněž ověřuje u nezávislého odvolacího mechanismu[12] uvedeného v žádosti, zda se u něj organizace skutečně zaregistrovala. U společností, které si vyberou panel orgánu pro ochranu údajů (např. proto, že zpracovávají údaje v oblasti lidských zdrojů), Ministerstvo obchodu kontroluje, zda uhradily předepsané poplatky za využití panelu. V případě potřeby Ministerstvo obchodu rovněž ověří, zda žadatel spadá do pravomoci Federální obchodní komise nebo Ministerstva dopravy (a je tedy způsobilý k připojení se k rámci EU–USA pro ochranu údajů).

Pokud jsou splněny všechny podmínky, informuje Ministerstvo obchodu organizaci, že může na svých internetových stránkách zveřejnit svou politiku ochrany soukromí odkazující na rámec EU–USA pro ochranu údajů. Jakmile je politika ochrany soukromí zveřejněna, Ministerstvo obchodu potvrdí certifikaci a zařadí společnost na seznam organizací rámce EU–USA pro ochranu údajů na svých internetových stránkách. Pokud jde o osobní údaje z EU, rámce EU–USA pro ochranu údajů se lze dovolávat ode dne, kdy Ministerstvo obchodu zařadí organizaci na tento seznam[13].

Jak bylo vysvětleno na přezkumném jednání, kontroly, které dosud Ministerstvo obchodu provedlo, vedly k zamítnutí 33 žádostí, protože nesplňovaly požadavky rámce EU–USA pro ochranu údajů. Obecně platí, že Ministerstvo obchodu spolupracuje s danou společností na odstranění případných nedostatků. Pokud Ministerstvo obchodu zjistí jakékoli nedostatky, upozorní společnost na nutnost jejich odstranění a na to, že neposkytne-li společnost ve stanovené lhůtě odpověď či nedokončí-li autocertifikaci v souladu s postupy Ministerstva obchodu, bude její žádost považována za zrušenou. Pokud není prvotní certifikace dokončena/změněna do dvanácti měsíců, Ministerstvo obchodu k ní již nepřihlíží.

[10] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931).

[11] https://www.dataprivacyframework.gov/key-requirements.

[12] Mechanismy řešení sporů v soukromém sektoru, pomocí nichž jsou stížnosti a nesrovnalosti každého jednotlivce bezplatně prošetřeny a urychleně vyřešeny.

[13] Oddíl I bod 3 přílohy I rozhodnutí o odpovídající ochraně.

Termín pro každoroční opětovnou certifikaci je uveden pro každou společnost v seznamu organizací rámce EU–USA pro ochranu údajů. Za účelem připomenutí povinnosti společnosti požádat o opětovnou certifikaci vytvořilo Ministerstvo obchodu systém s upozorněními na končící platnost certifikace. Organizace obdrží upomínku měsíc před termínem konce platnosti, dále dva týdny před termínem a poté jeden den před termínem. Organizace, které nechaly svou certifikaci propadnout, jsou ze seznamu organizací rámce EU–USA pro ochranu údajů vyřazeny. Jak je popsáno v příloze III rozhodnutí o odpovídající ochraně, má Ministerstvo obchodu na svých internetových stránkách zvláštní oddíl, v němž jsou uvedeny organizace ze Spojených států, které již nejsou aktivními účastníky, a to s uvedením příslušných důvodů, proč byly dotčené společnosti ze seznamu vyřazeny (např. vypršení platnosti nebo vystoupení z rámce) („seznam neaktivních organizací“). Pokud jsou organizace vyřazeny ze seznamu organizací rámce EU–USA pro ochranu údajů, protože nechaly vypršet dobu platnosti své certifikace, Ministerstvo obchodu je kontaktuje, aby ověřilo, zda hodlají certifikaci zrušit, nebo zda mají zájem provést opětovnou certifikaci; v druhém případě ministerstvo ověřuje, zda během doby po vypršení platnosti uplatňovaly společnosti na osobní údaje získané podle rámce EU–USA pro ochranu údajů zásady tohoto rámce, a ujasní si se společnostmi, jaké kroky podniknou k vyřešení přetrvávajících problémů, které zpozdily opětovnou certifikaci. Pokud společnosti oznámí Ministerstvu obchodu, že chtějí od rámce EU–USA pro ochranu údajů odstoupit, vyžaduje od nich Ministerstvo obchodu, aby potvrdily, zda údaje získané podle rámce EU–USA pro ochranu údajů vrátí nebo vymažou, nebo zda je budou uchovávat a nadále na ně uplatňovat zásady rámce EU–USA pro ochranu údajů (to je třeba každoročně potvrdit), nebo zda je zachovají a zavedou jinou ochranu (například standardní smluvní doložky přijaté Evropskou komisí).

Ze zpětné vazby od oborových sdružení a společností vyplývá, že společnosti s certifikací podle rámce EU–USA pro ochranu údajů zavedly řadu opatření k zajištění souladu se zásadami rámce EU–USA pro ochranu údajů. Například v zájmu dodržení zásady *odvolání, prosazování a odpovědnost* prováděly organizace interní kontroly buď sebehodnocením, nebo externě se zaměřením na dodržování předpisů. Zástupci dvou nezávislých odvolacích mechanismů ze soukromého sektoru, kteří se zúčastnili přezkumného jednání, vysvětlili, že je prováděna také externí kontrola dodržování politik ochrany soukromí, a jeden z nich vysvětlil, že jsou rovněž prováděny audity a namátkové kontroly zaměřené například na zásady *přístupu*, *volby* a *dalšího předávání*. Kromě toho certifikované společnosti vyvinuly interní programy dodržování předpisů a mechanismy dohledu, vyškolily zaměstnance, zavedly mechanismy umožňující jednotlivcům uplatňovat jejich práva, provedly posouzení dopadů na ochranu soukromí a přezkoumaly stávající smlouvy.

2.1.2 Sledování dodržování zásad, nepravdivá tvrzení o účasti a prosazování

V rámci EU–USA pro ochranu údajů odpovídá Ministerstvo obchodu za monitorování dodržování zásad rámce EU–USA pro ochranu údajů prostřednictvím různých nástrojů, včetně kontrol *ex-officio* (z vlastní iniciativy), kontrol *ad hoc* na místě a dotazníků o dodržování zásad. Součástí této činnosti je i vyhledávání nepravdivých tvrzení o účasti v rámci, například vyhledáváním na internetu, a jejich řešení[14].

[14] Viz příloha III rozhodnutí o odpovídající ochraně. Nepravdivá tvrzení mohou vzniknout například tehdy, pokud společnost tvrdí, že se účastní rámce EU–USA pro ochranu údajů, a přitom proces certifikace buď nikdy nezahájila, nebo jej zahájila, ale nedokončila, případně nechala svou certifikaci propadnout.

Při sledování dodržování zásad ze strany společností účastnících se rámce EU–USA pro ochranu údajů se Ministerstvo obchodu v uplynulém roce spoléhalo především na *ad hoc* vyhledávání na internetu a kontroly (sociálních) médií. Ministerstvo obchodu konstatovalo, že v tomto prvním roce nezjistilo žádné problémy s dodržováním zásad rámce EU–USA pro ochranu údajů a nepostoupilo žádnou společnost Federální obchodní komisi nebo Ministerstvu dopravy k případným donucovacím opatřením. Zřídilo také specializované kontaktní místo, které usnadňuje spolupráci s úřady pro ochranu údajů a přijímá stížnosti od jednotlivců a postoupené případy od jiných orgánů (např. úřadů pro ochranu údajů nebo Federální obchodní komise). V uplynulém roce však nebyly zaznamenány žádné postoupené případy ani stížnosti. Zatímco první rok fungování rámce EU–USA pro ochranu údajů byl zaměřen na vytvoření rámce a certifikačního procesu, Ministerstvo obchodu na přezkumném jednání vysvětlilo, že plánuje provádět kontroly dodržování předpisů automatizovaně, aby mohly být systematičtější, a v současné době k tomu vyvíjí potřebné IT nástroje.

Komise uznává, že v tomto prvním roce muselo Ministerstvo obchodu zaměřit své úsilí na vytvoření rámce a certifikačního procesu. Do budoucna je důležité, aby Ministerstvo obchodu zvýšilo své úsilí o monitorování a kontrolu dodržování zásad, což je nezbytné pro zajištění trvale vysoké úrovně dodržování rámce a odhalování případů vyžadujících další donucovací opatření, včetně možných nepravdivých tvrzení společností o účasti. V tomto ohledu Komise vítá skutečnost, že Ministerstvo obchodu potvrdilo svůj záměr vyvinout a používat (automatizované) nástroje k účinnějšímu a systematičtějšímu odhalování problémů s dodržováním zásad a nepravdivých tvrzení, a domnívá se, že by to mělo být součástí širšího úsilí o větší využívání různých nástrojů, které má k dispozici (např. namátkové kontroly, dotazníky ověřující dodržování zásad, žádosti o informace atd.), včetně ověřování souladu s konkrétními požadavky v rámci EU–USA pro ochranu údajů[15].

Organizace rámce EU–USA pro ochranu údajů spadají do působnosti Federální obchodní komise a Ministerstva dopravy. Během přezkumného jednání Ministerstvo dopravy potvrdilo, že má zavedeny všechny postupy pro přijetí příslušných donucovacích opatření. Vysvětlilo také, že k rámci EU–USA pro ochranu údajů se připojilo jen velmi málo společností spadajících do jeho působnosti (tj. několik zprostředkovatelů letenek, ale žádné letecké společnosti). Federální obchodní komise potvrdila, že systematicky kontroluje porušování rámce EU–USA pro ochranu údajů při každém svém vyšetřování, které se týká ochrany soukromí. Federální obchodní komise dosud neobdržela žádný postoupený případ od jiných orgánů. Obdržela několik stížností zmiňujících se o rámci EU–USA pro ochranu údajů, nicméně dvě z nich se týkaly společností na „seznamu neaktivních organizací“, dvě se týkaly společností, které se rámce neúčastnily, a jedna se netýkala osobních údajů předávaných z EU. K okamžiku vypracování této zprávy nevydala Federální obchodní komise žádná rozhodnutí o vymáhání dodržování rámce EU–USA pro ochranu údajů, nicméně potvrdila, že v současné době je vyšetřováno několik společností, které mají certifikaci podle rámce EU–USA pro ochranu údajů.

Komise oceňuje skutečnost, že Federální obchodní komise při všech svých šetřeních týkajících se ochrany soukromí systematicky kontroluje porušování rámce EU–USA pro ochranu údajů. Vzhledem k tomu, že trvalá účinnost rámce EU–USA pro ochranu údajů je závislá na jeho důsledném prosazování, očekává se, že Federální obchodní komise bude dále uplatňovat své

[15] Například v souvislosti s dalším předáváním, a to díky využití možnosti podle zásady 3 písm. b) rámce EU–USA pro ochranu údajů vyžádat si shrnutí nebo reprezentativní kopii příslušných ustanovení o ochraně soukromí ve smlouvách o dalším předávání.

vyšetřovací pravomoci na základě rámce, a to i proaktivním prováděním kontrolních akcí zaměřených na dodržování konkrétních požadavků rámce EU–USA pro ochranu údajů a/nebo v určitých odvětvích.

2.1.3 Vyřizování stížností

Rámec EU–USA pro ochranu údajů poskytuje jednotlivcům v EU různé možnosti nápravy v případech nedodržování zásad rámce EU–USA pro ochranu údajů ze strany certifikovaných organizací[16]. Mimo jiné se snaží o řešení formou přímého kontaktu s organizací rámce EU–USA pro ochranu údajů, která musí dotčené osobě poskytnout odpověď do 45 dnů. Jednotlivci mohou také podat stížnost k nezávislému odvolacímu mechanismu určenému organizací k prošetřování a řešení stížností. V závislosti na okolnostech může jít buď o orgán pro alternativní řešení sporů, nebo o úřad pro ochranu osobních údajů[17]. V případě, že žádný z ostatních dostupných způsobů nápravy nevyřeší stížnost subjektu údajů uspokojivým způsobem, mohou fyzické osoby jako poslední možnost využít závazné rozhodčí řízení u panelu rámce EU–USA pro ochranu údajů.

2.1.3.1 Postoj společností ke stížnostem

Z odpovědí oborových sdružení a společností na dotazníky zaslané Komisí vyplývá, že společnosti s certifikací podle rámce EU–USA pro ochranu údajů obdržely od jednotlivců jen velmi málo stížností (pokud vůbec nějaké) týkajících se nedodržování zásad rámce EU–USA pro ochranu údajů. Společnosti zároveň zavedly různé mechanismy a nástroje, které umožňují jednotlivcům uplatňovat svá práva a podávat stížnosti, a to i prostřednictvím webových formulářů, e-mailu a telefonu.

2.1.3.2 *Nezávislé odvolací mechanismy*

Ze zpětné vazby získané během přezkumného jednání a z informací poskytnutých oborovými sdruženími vyplývá, že počet stížností předložených nezávislým mechanismům řešení je velmi nízký. Mezi nezávislé odvolací mechanismy, které si společnosti vybraly, patří BBB National Programs, JAMS, TRUSTe a VeraSafe. Rámec EU–USA pro ochranu údajů vyžaduje, aby nezávislé odvolací mechanismy zveřejňovaly výroční zprávu se souhrnnými statistikami o využívání jejich služeb řešení sporů. V době přijetí této zprávy již všechny dotčené nezávislé odvolací mechanismy zveřejnily své výroční zprávy[18].

---

[16] Viz oddíl 2.4 rozhodnutí o odpovídající ochraně.

[17] Organizace [rámce EU–USA pro ochranu údajů] jsou povinny spolupracovat s úřadem pro ochranu osobních údajů na šetření a vyřešení stížnosti, buď pokud se týká zpracování údajů v oblasti lidských zdrojů shromážděných v kontextu zaměstnaneckého vztahu, nebo pokud se příslušná organizace dobrovolně podřídila dohledu úřadů pro ochranu osobních údajů.

[18] ANA – https://www.ana.net/content/show/id/accountability-dpf-consumers;
BBB National Programs – https://assets.bbbprograms.org/docs/default-source/eu-privacy-shield/dpf_periodicalreport_072024.pdf; ICDR – AAA – https://go.adr.org/rs/294-SFS-516/images/Data%20Privacy%20Framework%20IRM%20Program%20Report%202023-2024%20FINAL.pdf?version=0 ;
Insights association – https://www.insightsassociation.org/Portals/INSIGHTS/Insights%20Association%20DPF%20Services%20Program%202024%20Annual%20Report_Final_1.pdf;
JAMS – https://www.jamsadr.com/files/Uploads/Documents/2024-Annual-Report-DPF-Cases.pdf;
Privacy Trust DPF Services – https://privacytrust.com/fserve/PrivacyTrust_Dispute_Resolution_Report_2023_2024.pdf ;
TRUSTe Dispute Resolution – https://trustarc.com/wp-content/uploads/2024/07/2024-Independent-Recourse-Mechanism-Annual-Report.pdf;

Na přezkumném jednání navíc společnosti BBB a VeraSafe podrobně představily svou činnost za poslední rok. V porovnání s předchozími rámci zaznamenaly nárůst počtu účastníků z řad podniků, kteří si vybrali jejich služby, a zmínily, že obdržely několik stížností, ačkoli naprostá většina z nich byla nezpůsobilá. Například společnost BBB obdržela 87 stížností od osob z EU, přičemž pouze dvě z nich byly způsobilé k řešení. Společnost BBB uvedla, že stížnosti jsou v průměru vyřizovány do pěti pracovních dnů, tyto dvě stížnosti byly však nakonec uzavřeny, protože na ně dotyčné osoby nereagovaly. Společnost VeraSafe obdržela 26 stížností, z nichž šest bylo způsobilých k řešení. Dvě z nich – týkající se žádostí o přístup a výmaz – byly vyřešeny, dvě se nadále projednávají a dvě byly vzaty zpět nebo uzavřeny kvůli tomu, že dotčená osoba nereagovala. Oba nezávislé odvolací mechanismy uvedly, že se snaží odpovídat na stížnosti v jazyce dotčené osoby.

Společnosti v rámci EU–USA pro ochranu údajů, které zpracovávají údaje v oblasti lidských zdrojů předávané z EU, si musí zvolit jako své nezávislé odvolací mechanismy pro tyto údaje unijní úřady pro ochranu údajů, přičemž pro jiné typy osobních údajů předávaných na základě rámce EU–USA pro ochranu údajů si společnost v rámci EU–USA pro ochranu údajů může zvolit unijní úřady pro ochranu údajů jako své nezávislé odvolací mechanismy dobrovolně. Ve skutečnosti byla v době provádění přezkumu pro toto řešení rozhodnutá více než polovina společností certifikovaných v rámci EU–USA pro ochranu údajů[19], což je třeba ocenit. Po přijetí rozhodnutí o odpovídající ochraně přijal EDPB jednací řád „neformálního panelu úřadů EU pro ochranu údajů“. Tomuto panelu přísluší poskytování závazného poradenství americkým organizacím v případě nevyřešených stížností fyzických osob na nakládání s osobními údaji, které byly předány z Evropské unie na základě rámce EU–USA pro ochranu údajů. Podle jednacího řádu je panel tvořen jedním úřadem pro ochranu údajů, který působí jako hlavní úřad pro ochranu údajů, a dalšími určenými úřady pro ochranu údajů, které provádí společnou kontrolu[20]. Poskytuje závazné poradenství do 60 dnů od obdržení stížnosti týkající se rámce EU–USA pro ochranu údajů. EDPB rovněž zveřejnil vzorový formulář pro podávání stížností úřadům pro ochranu údajů[21], jakož i „často kladené dotazy pro evropské fyzické osoby“[22] a podniky[23] týkající se rámce EU–USA pro ochranu údajů. K době provádění přezkumu neobdržel panel žádné stížnosti.

2.1.3.3 Závazný rozhodčí mechanismus

Ministerstvo obchodu vybralo k řízení závazného rozhodčího mechanismu Mezinárodní středisko pro řešení sporů (ICDR), mezinárodní divizi Americké arbitrážní asociace (AAA). Po přijetí rozhodnutí o odpovídající ochraně vybralo Ministerstvo obchodu společně s Komisí jedenáct rozhodců se zkušenostmi v oblasti ochrany soukromí a z různých prostředí, mimo jiné

Verasafe – https://verasafe.com/wp-content/uploads/2020/06/VeraSafe-DPF-Dispute-Resolution-Program-Annual-Report-2024.pdf.

[19] Krátce po datu přezkumného jednání bylo na internetových stránkách rámce EU–USA pro ochranu údajů uvedeno, že 1 511 z 2 892 účastníků má jako odvolací mechanismus úřad EU pro ochranu osobních údajů.

[20] Dne 17. dubna 2024 přijal EDPB podle rámce EU a USA pro ochranu osobních údajů jednací řád „neformálního panelu úřadů EU pro ochranu údajů“. Je k dispozici zde: https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf.

[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_en.

[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_en.

[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_en.

z oblasti rozhodčího řízení, soudnictví, akademické obce a občanské společnosti[24]. Kromě toho byla přijata pravidla rozhodčího řízení[25] pro panel rámce EU–USA pro ochranu údajů a kodex chování rozhodců[26], které jsou k dispozici na internetových stránkách ICDR. K době provádění přezkumu nebyl ještě rozhodčí mechanismus žádným jednotlivcem z EU spuštěn.

2.1.4 Poradenství, spolupráce a zvyšování povědomí

Po vstupu rámce EU–USA pro ochranu údajů v platnost uskutečnilo Ministerstvo obchodu různé osvětové aktivity: uspořádalo putovní prezentace, webové semináře a konference; oslovilo oborová sdružení a přímo komunikovalo s více než 3 000 společností s cílem poskytnout informace o rámci EU–USA pro ochranu údajů. Zveřejnilo také pokyny, mimo jiné ve formě často kladených otázek a odpovědí, a to pro jednotlivce i pro unijní a americké podniky[27]. EDPB vypracoval formuláře stížností a často kladené otázky určené jednotlivcům i podnikům. Podobně Komise při přijímání rozhodnutí o odpovídající ochraně zveřejnila otázky a odpovědi a informační přehled o rámci EU–USA pro ochranu údajů[28].

Z přezkumného jednání zároveň vyplynulo, že je třeba vyvíjet více úsilí při zvyšování informovanosti jednotlivců a poskytování pokynů společnostem. Z podnětů získaných od společností a nezávislých odvolacích mechanismů a z velmi malého počtu stížností lze dovodit, že jednotlivci si nemusí být vždy vědomi svých práv a/nebo mechanismu jejich uplatňování. Během přezkumného jednání vyjádřilo Ministerstvo obchodu zájem spolupracovat s úřady EU pro ochranu údajů, aby se zvýšilo povědomí o rámci mezi jednotlivci v EU. Komise takové iniciativy podporuje a podniká rovněž kroky k lepšímu informování jednotlivců, mimo jiné tím, že na svých internetových stránkách zveřejňuje další informace o rámci EU–USA pro ochranu údajů, například odkazy na příslušné pokyny přijaté EDPB, Ministerstvem obchodu a dalšími orgány USA.

Pokud jde o pokyny k zásadám rámce EU–USA pro ochranu údajů, zástupci EDPB se během přezkumného jednání dohodli, že budou v nadcházejících měsících spolupracovat, aby blíže vysvětlili pojem „údaje v oblasti lidských zdrojů“ podle rámce EU–USA pro ochranu údajů a konkrétní povinnosti, které se na zpracování těchto údajů vztahují. Prozkoumávalo se, které prvky by měly být do těchto pokynů zahrnuty. Tyto pokyny by se například mohly zabývat určitými praktickými scénáři, kde by údaje zaměstnanců byly zpracovávány podle rámce EU–USA pro ochranu údajů (např. poskytovatelem cloudu) a bylo by vysvětleno, které povinnosti rámce EU–USA pro ochranu údajů by byly pro tyto scénáře relevantní. Mohly by rovněž obsahovat doporučení, aby si společnosti, které získávají údaje o zaměstnancích z EU (ale nemusí je nutně používat v rámci pracovněprávního vztahu), zvolily jako svůj nezávislý odvolací mechanismus panel úřadu pro ochranu osobních údajů. Díky tomu by se takové osoby mohly obracet na orgán, který je „v blízkosti jejich domova“ a v případě potřeby se lépe orientuje v platných vnitrostátních předpisech, jež se vztahují na údaje v oblasti lidských zdrojů.

[24] https://go.adr.org/DPF_Arbitrator_Bios.html.
[25] https://go.adr.org/rs/294-SFS-516/images/IC.DR-AAA_EU-US_DPF_AnnexI_Arbitration_Rules.pdf.
[26] https://go.adr.org/rs/294-SFS-516/images/Code_of_Conduct_for_Arbitrators_Appointed_to_EU-US_DPF_AnnexI_Arbitrations.pdf.
[27] Viz např. https://www.dataprivacyframework.gov/US-Businesses.
[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.

Kromě toho by zřejmě bylo užitečné poskytnout více pokynů (rovněž založených na informacích od oborových sdružení), pokud jde o požadavky rámce EU–USA pro ochranu údajů na další předávání. Ministerstvo obchodu dále uvedlo, že by stálo za to prozkoumat, zda by pro některá odvětví byly užitečné dodatečné pokyny k uplatňování zásad rámce EU–USA pro ochranu údajů při jejich činnosti, např. v oblasti zdravotnického výzkumu a finančních služeb.

Komise oceňuje, že obě strany jsou připravené vypracovat pokyny, a předpokládá, že práce na výše uvedených tématech bude brzy zahájena.

Obecněji řečeno, bylo zavedeno několik mechanismů k zajištění výměny a spolupráce mezi americkými orgány a úřady pro ochranu osobních údajů, mimo jiné byla určena specializovaná kontaktní místa v rámci Federální obchodní komise a Ministerstva obchodu, která se zabývají dotazy a případy postoupenými ze strany orgánů pro ochranu údajů.

2.1.5 Relevantní vývoj v právním systému USA

Od přijetí rozhodnutí o odpovídající ochraně došlo v právním rámci USA v oblasti ochrany soukromí k řadě změn. Týkají se vývoje legislativy, regulace a judikatury. Obecně svědčí o větším sbližování přístupů EU a USA k určitým potenciálním problémům v oblasti ochrany soukromí, mimo jiné i díky zavedení podobných právních pojmů. Některé z těchto vývojových trendů stále probíhají a je třeba je dále sledovat.

Na federální úrovni vydal prezident několik prezidentských dekretů, které se týkají používání osobních údajů. Zejména prezidentský dekret č. 14117 ze dne 28. února 2024[29] zakazuje nebo omezuje transakce, v nichž figurují určité kategorie citlivých osobních údajů (např. zdravotní údaje, biometrické identifikátory, lidská genomická data) se subjekty v některých „problematických zemích“[30]. Podle přijatého příkazu má ministr spravedlnosti k upřesnění jeho provádění navrhnout předpisy, které v době přijetí této zprávy ještě nebyly vydány. Na vývoj bezpečné, chráněné a důvěryhodné umělé inteligence se dále zaměřuje prezidentský dekret č. 14110 ze dne 30. října 2023 o umělé inteligenci[31]. Požaduje, aby několik federálních agentur vypracovalo bezpečnostní normy a pokyny týkající se umělé inteligence, včetně konkrétních rizik umělé inteligence pro soukromí a technik pro zachování soukromí.

Pokud jde o legislativní činnost, v minulých letech byly v Kongresu předloženy na federální úrovni návrhy zákonů o ochraně soukromí, přičemž k červenci 2024 přijalo komplexní zákony o ochraně soukromí dvacet amerických států a v osmi z nich vstoupily tyto zákony v platnost: Kalifornie, Colorado, Oregon, Virginie, Connecticut, Utah, Texas a Florida. Kromě toho sedmnáct států USA přijalo právní předpisy, které se zabývají automatizovaným zpracováním

[29] https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

[30] Mezi ně patří na základě návrhu ministra spravedlnosti v rámci předběžného oznámení o navrhovaných předpisech ze dne 3. května 2024 Čína, Kuba, Hongkong a Macao, Írán, Severní Korea a Venezuela. Viz https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and

[31] https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

(nebo alespoň některými jeho formami) a obecně umožňují výjimky pro určité druhy rozhodování na základě „profilování“[32].

Pokud jde o vývoj judikatury, několik zástupců občanské společnosti poukázalo na nedávný rozsudek Nejvyššího soudu ve věci *Loper Bright Enterprises v. Raimondo* ze dne 28. června 2024. Tímto rozsudkem byla změněna předchozí judikatura soudních precedentů týkající se doktríny *Chevron*, podle níž soudy v případě nejasností v předpise uplatňovaném regulační agenturou uplatňují zásadu domněnky rozumného výkladu právního předpisu ze strany agentury. Některé nevládní organizace vyjádřily zejména obavy ohledně dopadu tohoto rozhodnutí Nejvyššího soudu na pravomoc Federální obchodní komise vydávat předpisy v oblasti ochrany soukromí, přičemž uznávají, že na její donucovací pravomoci nemusí mít žádný nebo jen omezený dopad. Na přezkumném jednání Federální obchodní komise uvedla, že na vyvozování konkrétních důsledků tohoto rozsudku je ještě brzy. Současně vysvětlila, že normotvorba u Federální obchodní komise vychází – na rozdíl od jiných správních orgánů – ze zákona o Federální obchodní komisi, a doktrína *Chevron* je pro ni méně relevantní. Nedávný rozsudek proto může mít v této oblasti omezený dopad.

Dále Federální obchodní komise informovala o nedávném vývoji v přístupu k automatizovanému zpracování a umělé inteligenci. Mimo jiné jde o společné prohlášení proti diskriminaci a zaujatosti v automatizovaných systémech, přijaté společně s dalšími donucovacími orgány[33], jakož i o několik donucovacích opatření, v nichž se Federální obchodní komise zaměřuje mimo jiné na transparentnost, spravedlnost automatizovaného zpracování a možnost jednotlivců napadnout výsledky. Nejvýznamnějším případem v tomto ohledu je rozhodnutí Federální obchodní komise ve věci společnosti *Rite Aid* z března 2024, na jehož základě byl této společnosti uložen pětiletý zákaz používání technologie rozpoznávání obličeje pro účely bezpečnosti[34]. Federální obchodní komise zejména zjistila, že společnost *Rite Aid* nepřijala přiměřená opatření, aby zabránila chybným výsledkům a informovala spotřebitele o použité technologii. Obecněji řečeno, Federální obchodní komise se na přezkumném jednání zaměřila na své současné priority a zejména na oblasti, které si podle ní zaslouží aktivnější přístup k prosazování. Patří sem ochrana citlivých údajů (např. zdravotních

[32] Ač se v různých státech vymezení pojmu „profilování“ liší, obecně se profilováním rozumí jakákoli forma automatizovaného zpracování osobních údajů za účelem hodnocení, rozboru nebo odhadu osobních aspektů týkajících se ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa nebo pohybu identifikované nebo identifikovatelné fyzické osoby. Spotřebitelé obvykle mohou s profilováním vyslovit nesouhlas. Následující státy vypracovaly právní předpisy týkající se profilování: Colorado (Colo. Rev. Stat. Ann. § 6-1-1306), Connecticut (Conn. Gen. Stat. Ann. § 42-518), Delaware (Del. Code Ann. tit. 6, § 12D-104), Florida (Fla. Stat. Ann. § 501.705), Indiana (Ind. Code Ann. § 24-15-3-1), Kentucky (Ky. Rev. Stat. Ann. § 367.3615), Maryland (Maryland Online Data Privacy Act of 2024, přijatý dne 9. května 2024), Minnesota (Minn. Stat. Ann. § 325O.07), Montana (Mont. Code Ann. § 30-14-2808), Nebraska (Neb. Rev. Stat. Ann. § 87-1107), New Hampshire (N.H. Rev. Stat. Ann. § 507-H:4), New Jersey (N.J. Stat. Ann. § 56:8-166.8), Oregon (Or. Rev. Stat. Ann. § 646A.574), Rhode Island (Rhode Island Data Transparency and Privacy Protection Act, přijatý dne 29. června 2024), Tennessee (Tenn. Code Ann. § 47-18-3304), Texas (Tex. Bus. & Com. Code Ann. § 541.051) a Virginia (Va. Code Ann. § 59.1-577).

[33] https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

[34] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v.

údajů, biometrických údajů, zeměpisné polohy)[35], ochrana dětí[36] a nezletilých na internetu a bezpečnost údajů.[37]

Komise bude i nadále pozorně sledovat tento a další vývoj v USA, zejména další kroky směřující k vytvoření komplexního federálního zákona o ochraně soukromí a možný dopad nedávné judikatury Nejvyššího soudu na úlohu Federální obchodní komise v oblasti ochrany soukromí.

Komise oceňuje informace Federální obchodní komise o jejích nedávných činnostech v oblasti prosazování a současných prioritách, které do značné míry odpovídají trendům a prioritám v oblasti prosazování ochrany údajů v Evropě. Federální obchodní komise se také aktivně účastní sítě založené Komisí v březnu 2024, která sdružuje země využívající rozhodnutí EU o odpovídající ochraně[38]. Toto větší sbližování by mělo podpořit a usnadnit užší spolupráci mezi orgány prosazujícími ochranu soukromí na obou stranách Atlantiku, zejména v otázkách souvisejících s fungováním rámce EU–USA pro ochranu údajů.

2.2 Aspekty přístupu orgánů veřejné moci USA k osobním údajům předávaným v rámci EU–USA pro ochranu údajů a použití těchto údajů těmito orgány

Rozhodnutí o odpovídající ochraně obsahuje podrobné posouzení pravidel pro shromažďování a používání osobních údajů předávaných z EU společnostem s certifikací podle rámce EU–USA pro ochranu údajů orgány veřejné moci USA, zejména pro účely prosazování trestního práva a národní bezpečnosti. Jak potvrdily orgány USA během přezkumného jednání, pokud jde o právní rámec pro přístup k údajům pro účely prosazování práva nebo pro regulační účely v prvním roce platnosti rámce EU–USA pro ochranu údajů, od přijetí rozhodnutí o odpovídající ochraně nedošlo k žádnému významnému vývoji. Z tohoto důvodu se níže uvedená zjištění týkají pouze vývoje v oblasti národní bezpečnosti.

Závěry rozhodnutí o odpovídající ochraně týkající se přístupu zpravodajských služeb k údajům se opírají o analýzu podmínek a omezení, které se vztahují na operace signálového zpravodajství podle několika příslušných právních předpisů – zejména § 702 zákona o dohledu nad zahraniční informační službou (dále jen „zákon FISA“) a prezidentského dekretu č. 12333[39] – které byly doplněny a podpořeny prezidentským dekretem č. 14086 o posílení záruk

[35] Viz např. nedávný příkaz Federální obchodní komise proti společnosti X-Mode ve věci prodeje a sdílení citlivých informací o poloze (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) a proti společnosti Monument ve věci zpřístupňování citlivých zdravotnických údajů třetím stranám pro marketingové účely (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] Federální obchodní komise například nedávno oznámila vyšetřování vedoucí k žalobě na společnost TikTok a její mateřskou společnost ByteDance kvůli údajnému porušování zákona o ochraně soukromí dětí. Obě společnosti údajně nedodržely povinnost informovat před shromažďováním a používáním osobních údajů dětí mladších třinácti let jejich rodiče a získat jejich souhlas (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

[37] Viz přehled nedávných činností v oblasti prosazování v Novinkách Federální obchodní komise za rok 2023 v oblasti ochrany soukromí a zabezpečení dat: https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307.

[38] Viz https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307. Výsledkem jednání v březnu 2024 bylo rozhodnutí uspořádat řadu tematických zasedání. První z nich se konalo v červenci 2024 a týkalo se především vývoje nástrojů, které mohou malým a středním podnikům pomoci při dodržování zákonů o ochraně soukromí.

[39] Dalšími opatřeními, která lze podle zákona FISA v souvislosti s údaji předávanými z EU přijmout, jsou individualizované elektronické sledování (§ 105 zákona FISA), fyzické prohlídky (§ 302 zákona FISA), použití zařízení pro zaznamenávání informací o odchozí komunikaci sledovaného zařízení nebo zařízení pro

pro signálové zpravodajství Spojených států (prezidentský dekret č. 14086), který přijal prezident USA dne 7. října 2022. Ochranná opatření stanovená v prezidentském dekretu č. 14086 se vztahují na všechny činnosti amerického signálového zpravodajství bez ohledu na to, na jakém právním základě a kde se tyto činnosti provádějí, a chrání údaje osob, které nejsou občany USA (včetně Evropanů)[40]. Prezidentský dekret č. 14086 rovněž zavedl nový nápravný mechanismus, jehož prostřednictvím se mohou jednotlivci v EU dovolávat těchto závazných ochranných opatření a domáhat se jejich dodržování.

V následujících oddílech jsou popsány kroky, které orgány USA podnikly od přijetí rozhodnutí o odpovídající ochraně s cílem dosáhnout souladu s prezidentským dekretem č. 14086, a také příslušný vývoj ve vztahu k výše uvedenému právnímu rámci.

2.2.1 Relevantní vývoj s ohledem na právní rámec USA

2.2.1.1 Provádění prezidentského dekretu č. 14086 zpravodajskými službami

Omezení a záruky zavedené prezidentským dekretem č. 14086 doplňují omezení a záruky stanovené v § 702 zákona FISA a prezidentském dekretu č. 12333. Jsou závazné pro všechny zpravodajské služby a byly dále implementovány prostřednictvím politik a postupů přijatých jednotlivými službami.

V rámci prvního přezkumu americké orgány potvrdily, že v prezidentském dekretu č. 14086 nedošlo po jeho přijetí k žádným změnám. Kromě toho bylo vysvětleno, že prezident USA nevyužil pravomoc dle § 2(b)(i)(B) a 2(b)(ii)(C) prezidentského dekretu č. 14086 k aktualizaci seznamu legitimních cílů, pro které lze uplatnit signálové zpravodajství, ani seznamu účelů, pro které lze hromadně shromažďované údaje používat[41]. Za účelem stanovení konkrétnějších zpravodajských priorit, pro které lze údaje ze signálového zpravodajství skutečně shromažďovat, zavedl prezidentský dekret č. 14086 zvláštní postup. Je zejména nutná konzultace s úředníkem úřadu ODNI pro ochranu občanských svobod (dále také jako „úředník ODNI CLPO“), a to proto, aby se u každé priority posoudilo, zda 1) podporuje jeden nebo více legitimních cílů uvedených v prezidentském dekretu; 2) nebyla navržena tak, aby vedla ke sběru dat signálového zpravodajství pro zakázaný cíl uvedený v prezidentském dekretu, či zda takový sběr nebyl předpokládán, a 3) byla zavedena po náležitém zvážení soukromí a občanských svobod všech osob[42]. Úřednice ODNI CLPO během přezkumného jednání potvrdila, že přezkoumala priority navržené ředitelem národního zpravodajství v rámci národních zpravodajských priorit pro rok 2023, dospěla k závěru, že jsou v souladu s výše uvedenými požadavky, a sdělila svůj závěr řediteli národního zpravodajství, který následně předložil priority ke schválení prezidentovi. Úřednice ODNI CLPO rovněž poskytla školení o požadavcích prezidentského dekretu č. 14086 těm složkám zpravodajské komunity, které se podílejí na vytváření zpravodajských priorit.

zaznamenávání informací o příchozí komunikaci sledovaného zařízení (§ 402 zákona FISA) a shromažďování obchodních záznamů od určitých společností (běžných dopravců, veřejných ubytovacích zařízení, půjčoven vozidel nebo skladů, § 501 zákona FISA). Tyto různé právní základy jsou podrobně rozebrány v rozhodnutí o odpovídající ochraně (142.–152. bod odůvodnění).

[40] Další informace viz oddíl 3.2.1.2 rozhodnutí o odpovídající ochraně.

[41] Mezi tyto legitimní cíle/účely patří například ochrana před špionáží, sabotáží, atentáty nebo jinými zpravodajskými činnostmi prováděnými cizí vládou, organizací nebo osobou, jejich jménem nebo s jejich pomocí; ochrana před terorismem, braním rukojmí a držením osob v zajetí ze strany cizí vlády, organizace nebo osoby nebo jejich jménem.

[42] Ustanovení § 2(b)(iii) prezidentského dekretu č. 14086.

Kromě toho americké orgány v uplynulém roce přijaly další praktické kroky k provádění prezidentského dekretu č. 14086 v rámci své každodenní činnosti. Zpravodajské služby zejména zavedly další interní politiky a pokyny týkající se uplatňování prezidentského dekretu, například interní postupy (prostřednictvím požadavků na interní oprávnění, dokumentované kontroly přístupu, aby k informacím měly přístup pouze osoby, které byly řádně vyškoleny a mají potřebné požadavky pro plnění úkolů, atd.), aby zajistily, že v souvislosti s cíleným i hromadným shromažďováním informací budou dodržovány požadavky na nezbytnost a přiměřenost[43]. Kromě toho bylo zaměstnancům různých zpravodajských služeb (např. NSA, CIA, FBI) poskytnuto školení o prezidentském dekretu č. 14086, a to mimo jiné každoroční a *ad hoc* školení organizované úředníkem ODNI CLPO a povinná školení pro všechny nové zaměstnance nastupující do úřadu ODNI.

Komise oceňuje řadu opatření přijatých k provádění prezidentského dekretu č. 14086 a zajištění souladu s ním. S přibývajícími zkušenostmi s praktickým uplatňováním záruk prezidentského dekretu by Komise uvítala možnost projednat v budoucích přezkumech konkrétní příklady uplatňování prezidentského dekretu v praxi (při respektování příslušných hledisek důvěrnosti).

2.2.1.2 Opětovné schválení § 702 zákona FISA

Paragraf 702 zákona FISA dovoluje cílené sledování osob, které nejsou občany USA, o nichž se lze důvodně domnívat, že se nacházejí mimo území USA, za účelem získávání zahraničních zpravodajských informací. Získávání probíhá na základě osvědčení každoročně předkládaných a schvalovaných Soudem pro uplatňování zákona FISA (FISC). Tato osvědčení určují konkrétní kategorie zahraničních zpravodajských informací, které mají být shromažďovány. Dne 21. července 2023 úřad ODNI informoval, že existují tři schválená osvědčení podle § 702 zákona FISA, která se týkají následujících kategorií zahraničního zpravodajství: 1) zahraniční vlády a související subjekty, 2) boj proti terorismu a 3) boj proti šíření zbraní[44]. Osvědčení musí rovněž obsahovat postupy pro cílené sledování a minimalizaci, které jsou schváleny Soudem pro uplatňování zákona FISA[45]. Cílené sledování spočívá zejména v tom, že se od amerických společností, které spadají pod pojem „poskytovatel služeb elektronických komunikací“ podle zákona FISA, požaduje, aby poskytly údaje o elektronických komunikacích v případě komunikací odeslaných „selektorům“ nebo od nich, které identifikují konkrétní komunikační účet, např. telefonní číslo nebo e-mailovou adresu. Vláda USA zveřejnila různé materiály k § 702 zákona FISA, jejichž cílem je informovat veřejnost o fungování programů sledování, platných požadavcích a ochraně soukromí, jakož i o úloze Soudu pro uplatňování zákona FISA[46].

Vzhledem k doložce o ukončení platnosti měl § 702 zákona FISA vypršet na konci roku 2023, pokud jej Kongres opětovně neschválí. Po dočasném opětovném schválení beze změn přijal Kongres 19. dubna 2024 zákon o reformě zpravodajských služeb a zajištění bezpečnosti Ameriky (Reforming Intelligence and Securing America Act, RISAA), na jehož základě se opětovně schvaluje platnost § 702 zákona FISA na dobu dvou let a zavádí několik změn.

[43] Viz https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguardsin-executive-order-14086, zveřejněno dne 3. července 2023.
[44] https://www.intelligence.gov/ic-on-the-record-database/results/1307-release-of-documents-related-to-the-2023-fisa-section-702-certifications.
[45] Tyto postupy omezují shromažďování údajů s ohledem na konkrétní účel zahraničního zpravodajství, limitují přístup k databázím, v nichž jsou uloženy informace získané podle § 702 zákona FISA (včetně kontroly přístupu), a určují hranice pro používání, uchovávání a šíření těchto informací.
[46] https://www.intel.gov/foreign-intelligence-surveillance-act.

Obecně je možné je rozdělit do dvou kategorií: 1) změny v rozsahu sledovacích činností povolených podle § 702 zákona FISA a 2) institucionální a procedurální změny.

Změny v rozsahu sledovacích činností povolených podle § 702 zákona FISA

Zákon RISAA zavedl tři hlavní změny v rozsahu sledovacích činností, které lze provádět podle § 702 zákona FISA.

Za prvé byl definitivně zakázán sběr „abouts“[47]. To se týká sběru komunikací, u nichž se selektor podle § 702 (např. e-mailová adresa) nenachází v položce komunikace „komu“ nebo „od“, ale obsahuje odkaz na takový selektor v komunikaci (např. e-mailové komunikace, které nejsou odeslány na vybranou e-mailovou adresu nebo z ní, ale obsahují vybranou e-mailovou adresu v textu nebo těle e-mailu). Ačkoli bylo takové shromažďování vyloučeno již na základě novely zákona FISA v roce 2018, zákon FISA stále umožňuje obnovit sběr „abouts“ v budoucnu, a to na základě zvláštního schvalovacího postupu, na němž se podílí Soud pro uplatňování zákona FISA a Kongres. Poslední novela zavedená zákonem RISAA tuto možnost odstranila.

Za druhé, definice zahraničních zpravodajských informací byla rozšířena tak, aby zahrnovala informace týkající se boje proti drogám[48]. Během přezkumného jednání americké orgány vysvětlily, že toto opatření bylo zavedeno s ohledem na současnou fentanylovou krizi a rostoucí hrozbu pro národní bezpečnost ze strany mezinárodních obchodníků s drogami a výrobců drog. V tomto kontextu bylo potvrzeno, že tento pojem spadá pod několik legitimních cílů uvedených v prezidentském dekretu č. 14086, tj. pochopení nebo vyhodnocení schopností, záměrů nebo aktivit zahraničních organizací, které představují aktuální nebo potenciální hrozbu pro národní bezpečnost USA nebo jejich spojenců; pochopení nebo posouzení přeshraničních hrozeb, které mají dopad na globální bezpečnost, včetně rizik pro veřejné zdraví a ochrana před hrozbami přeshraniční trestné činnosti[49].

Za třetí, zákon RISAA rozšířil definici „poskytovatele služeb elektronických komunikací“, čímž se rozšířil okruh společností, které mohou být nuceny poskytovat informace podle § 702 zákona FISA[50]. Definice nyní zahrnuje „ostatní poskytovatele služeb, kteří mají přístup k zařízení, které je nebo může být používáno k přenosu nebo ukládání drátových nebo elektronických komunikací“, přičemž výslovně vylučuje veřejná ubytovací zařízení, obydlí, společenská zařízení a stravovací zařízení. V dopise Kongresu označilo Ministerstvo spravedlnosti tuto změnu za technickou změnu, která má pokrýt „extrémně malý“ počet technologických společností, které podle nedávných rozhodnutí Soudu pro uplatňování zákona FISA a Odvolacího soudu pro uplatňování zákona FISA nespadaly do předchozí definice poskytovatele služeb elektronických komunikací[51]. Tímto dopisem se Ministerstvo spravedlnosti zavázalo zúžit rozsah působnosti tím, že tuto definici použije výhradně na typ poskytovatele služeb, který byl předmětem sporu vedoucího k rozhodnutí Soudu pro uplatňování zákona FISA. V důsledku toho jsou dotčené společnosti uvedeny v utajované příloze pro Kongres. Několik nevládních organizací, včetně těch, které poskytly zpětnou vazbu

[47] Paragraf 22 zákona RISAA.
[48] Paragraf 23 zákona RISAA.
[49] Paragraf 2(b)(ii)(A)(2), (3) a (10) prezidentského dekretu č. 14086.
[50] Paragraf 25 zákona RISAA.
[51] https://www.justice.gov/opa/media/1348621/dl?inline. Viz rozhodnutí Soudu pro uplatňování zákona FISA z roku 2022 (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) a rozhodnutí Odvolacího soudu pro uplatňování zákona FISA, který toto rozhodnutí potvrdil (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

v rámci přezkumu, vyjádřilo z tohoto rozšíření obavy a tvrdilo, že by se mohlo vztahovat na mnoho amerických podniků (protože mnoho z nich poskytuje určitý druh služeb a má přístup ke komunikačnímu vybavení). Vzhledem k těmto obavám byla s podporou zpravodajské komunity v návrhu zákona o povolení zpravodajských služeb na fiskální rok 2025 navržena další změna, která je v současné době projednávána v Kongresu. Na základě této změny – pokud ji Kongres schválí – budou společnostmi spadajícími do definice poskytovatele služeb elektronických komunikací pouze ty, které jsou uvedeny ve výše zmíněných rozhodnutích Soudu pro uplatňování zákona FISA. Návrh zákona rovněž předpokládá, že každá směrnice určená takové společnosti by musela být nahlášena Soudu pro uplatňování zákona FISA, aby tento mohl přezkoumat, zda společnost skutečně spadá do dané oblasti působnosti. Ve svém dopise Kongresu se Ministerstvo spravedlnosti zavázalo, že bude každých šest měsíců podávat Kongresu zprávu o uplatňování aktualizované definice, aby Kongres mohl vykonávat příslušný dohled nad užším uplatňováním definice.

Důležité je, že na přezkumném jednání bylo americkými orgány a výborem PCLOB potvrzeno, že na veškeré shromažďování a používání údajů podle § 702 zákona FISA se nadále plně vztahují všechny záruky prezidentského dekretu č. 14086, a to i po těchto změnách. Ačkoli tedy zákon RISAA poněkud rozšiřuje okruh společností, které mohou obdržet příkaz, neomezuje výkon práv. Přesto bude důležité sledovat další vývoj (legislativní a zpravodajský) a mít informace o uplatňování těchto nových pravidel v praxi. Jde mimo jiné například o dopad rozšíření definic zahraničních zpravodajských služeb a poskytovatelů služeb elektronických komunikací na počet cílů podle § 702 zákona FISA (jak je každoročně sdělováno úřadem ODNI, viz níže o transparentnosti). V tomto ohledu by měla být zvláště informativní budoucí zpráva navazující na nedávnou zprávu výboru PCLOB o § 702 zákona FISA (viz níže).

Institucionální a procedurální změny

Pokud jde o institucionální a procedurální změny, zákon RISAA zakotvil několik postupů, které se již v praxi uplatňovaly, a zavedl nové záruky. Některé z nich se týkají pouze amerických osob, avšak několik změn zvyšuje ochranu amerických i neamerických osob, jejichž údaje mohou být shromažďovány podle § 702 zákona FISA[52], a jsou proto pro fungování rámce EU–USA pro ochranu údajů relevantní.

Za prvé byla zavedena řada dalších požadavků na odpovědnost, dohled a podávání zpráv. Zejména personál FBI musí být nyní každoročně proškolen o pravidlech, která se vztahují na dotazy na informace získané podle § 702 zákona FISA[53]. FBI je rovněž povinna podávat Kongresu zprávy o svých dotazovacích činnostech (např. o počtu dotazů využívajících „technologie hromadných úloh“, tj. provádění více dotazů v rámci jednoho) a o odpovědnostních opatřeních zavedených k zajištění souladu se zákonnými požadavky na dotazování (§§ 11–12 zákona RISAA). Kromě toho je generální inspektor Ministerstva spravedlnosti pověřen vypracováním zprávy o dodržování požadavků na dotazování ze strany FBI (§ 9 zákona RISAA). Obecněji řečeno, za účelem zvýšení transparentnosti řízení před

[52] Kromě toho zákon RISAA zavedl některé změny týkající se tradičního individualizovaného elektronického sledování podle § 105 zákona FISA (na základě příkazu Soudu pro uplatňování zákona FISA vydaného v případě, že je splněn standard zdůvodněného zjištění). Žádost zpravodajské služby ministru spravedlnosti o vydání příkazu k individualizovanému elektronickému sledování nyní vyžaduje čestné prohlášení o splnění podmínek podle § 105 zákona FISA (§ 6 písm. a) zákona RISAA). Možná doba trvání elektronického sledování cizích mocností nebo jejich zprostředkovatelů byla prodloužena ze 120 dnů na jeden rok (§ 6 písm. g) zákona RISAA).

[53] Paragraf 2(d) zákona RISAA.

Soudem pro uplatňování zákona FISA jsou nyní úřad ODNI a ministr spravedlnosti povinni do 180 dnů dokončit přezkum zrušení stupně utajení rozhodnutí Soudu pro uplatňování zákona FISA (§ 7 zákona RISAA). Kromě toho musí být uchovávány a Kongresu předávány přepisy všech výslechů před Soudem pro uplatňování zákona FISA a Odvolacím soudem pro uplatňování zákona FISA (který rozhoduje o odvoláních ve věci dohledu nad zahraničním zpravodajstvím) (§ 8 zákona RISAA).

Za druhé, zákon RISAA zavedl další omezení pro FBI při používání údajů shromážděných podle § 702 zákona FISA. Paragraf 2 písm. d) zákona RISAA stanoví, že k dotazu pomocí „hromadné technologie" lze přistoupit toliko poté, co udělí souhlas právník FBI, nenastanou-li naléhavé okolnosti. Kromě toho je nyní úřadu FBI zakázáno automaticky prověřovat neomezené informace získané podle § 702 zákona FISA a namísto toho musí zajistit, aby analytici výslovně zvolili vyhledávání podle takových informací. Zákon RISAA rovněž zakázal úřadu FBI provádět dotazy, které jsou určeny výhradně k vyhledávání a získávání důkazů o trestné činnosti (pokud neexistuje důvodné přesvědčení, že by mohly pomoci zmírnit nebo odstranit ohrožení života nebo vážnou újmu na zdraví, nebo pokud je to nezbytné pro splnění povinnosti zveřejnit informace v soudním řízení)[54]. FBI navíc nesmí do analytických úložišť vkládat nezminimalizované údaje, pokud není cílová osoba relevantní pro stávající vyšetřování v oblasti národní bezpečnosti[55].

Za třetí byla pozměněna některá ustanovení týkající se postavení a úlohy *amici curiae* před Soudem pro uplatňování zákona FISA[56]. *Amici* jsou jmenováni jako odborníci, kteří pomáhají Soudu pro uplatňování zákona FISA (a Odvolacímu soudu pro uplatňování zákona FISA) v otázkách souvisejících se soukromím a občanskými svobodami nebo pomáhají objasnit technologické otázky při projednávání konkrétní žádosti vlády. Zatímco dříve zákon FISA vyžadoval, aby *amici* měli odborné znalosti v oblasti soukromí a občanských svobod, shromažďování zpravodajských informací, komunikačních technologií nebo v jiných relevantních oblastech, nyní v zásadě vyžaduje odborné znalosti v oblasti soukromí / občanských svobod a shromažďování zpravodajských informací. Soud pro uplatňování zákona FISA měl již dříve možnost jmenovat osobu s funkcí *amicus* v každém případě, který považoval za vhodný, a byl povinen tak učinit, pokud se zabýval novým nebo důležitým výkladem právního předpisu. Po opětovném schválení je nyní Soud pro uplatňování zákona FISA rovněž povinen jmenovat osobu *amicus* pokaždé, když je požádán o schválení osvědčení podle § 702 zákona FISA a doprovodných postupů (např. postupů pro cílené sledování), neshledá-li, že by to nebylo vhodné nebo by to pravděpodobně vedlo k nepřiměřenému zdržení[57]. Kromě toho může Soud pro uplatňování zákona FISA nyní namísto jmenování pouze jednoho rozhodnout o jmenování jednoho nebo více *amici*. Rovněž se upřesňuje, že informace, které mají *amici* poskytnout, musí být „omezeny na řešení konkrétních otázek určených soudem", byť oblasti, k nimž se *amici* mohou vyjádřit, jsou i nadále široké (tj. právní argumenty a informace týkající se ochrany soukromí a občanských svobod osob ve Spojených státech, shromažďování zpravodajských informací a komunikačních technologií nebo jakékoli jiné relevantní oblasti).

[54] Paragraf 3(a) zákona RISAA.

[55] Paragraf 3(b) zákona RISAA. Pokud je to nutné z důvodu naléhavých okolností, může ředitel FBI rozhodnout o výjimce z tohoto ustanovení, která musí být oznámena Kongresu.

[56] K zamezení pochybností je třeba uvést, že tyto změny nemají vliv na postavení a úlohu zvláštních advokátů před Soudem pro přezkum ochrany údajů, jak potvrdily Spojené státy na přezkumném jednání.

[57] Paragraf 5(b) zákona RISAA.

A konečně, § 18 zákona RISAA zřizuje „komisi pro reformu zákona FISA“ – složenou mimo jiné z členů Kongresu, předsedy výboru PCLOB, hlavního náměstka ředitele národního zpravodajství a náměstka ministra spravedlnosti a dalších členů, které jmenuje Kongres[58] – která má doporučit další reformy zákona FISA.

Komise bude pozorně sledovat další vývoj v souvislosti s § 702 zákona FISA, a to i v kontextu dohledových činností výboru PCLOB (viz níže), práce komise pro reformu a nadcházejícího přezkumu zákona FISA po dvou letech.

2.2.1.3 Sledovací činnosti v praxi: čísla a trendy

Z výroční statistické zprávy úřadu ODNI o transparentnosti využívání pravomocí zpravodajské komunity v oblasti dohledu nad národní bezpečností za kalendářní rok 2023 (zveřejněné v dubnu 2024)[59] vyplývá, že počet cílů podle § 702 zákona FISA se zvýšil z 245 073 v kalendářním roce 2022 na 268 590 v kalendářním roce 2023. Zpráva vysvětluje, že výkyvy v počtu cílů mohou souviset s řadou důvodů, včetně změn operačních priorit, událostí ve světě, technických možností, chování cílů a změn v telekomunikačním odvětví. Zpráva rovněž uvádí, že na základě § 402 zákona FISA (zařízení pro zaznamenávání informací o odchozí komunikaci sledovaného zařízení a zařízení pro zaznamenávání informací o příchozí komunikaci sledovaného zařízení) nebyla zaměřena žádná neamerická osoba (v roce 2021 to byla jedna osoba a v roce 2022 žádná osoba), přičemž podle § 501 FISA (přístup k obchodním záznamům běžných dopravců, půjčoven vozidel nebo fyzických skladů) bylo vydáno šest příkazů (v roce 2021 i v roce 2022 to bylo jedenáct příkazů) pro šest cílů (v roce 2021 jich bylo třináct, v roce 2022 jich bylo 11), které se týkaly 5 412 jedinečných identifikátorů (v roce 2021 jich bylo 23 157 a v roce 2022 jich bylo 55 431) použitých ke sdělení informací shromážděných na základě těchto příkazů.

Výroční zpráva Ministerstva spravedlnosti o zákonu o dohledu nad zahraničním zpravodajstvím určená Kongresu uvádí, že v kalendářním roce 2023 bylo u Soudu pro uplatňování zákona FISA podáno 327 žádostí o provádění elektronického sledování a/nebo fyzických prohlídek pro účely zahraničního zpravodajství podle § 105, resp. 302 zákona FISA[60]. Celkový počet cílových osob se pohyboval mezi 500 a 999. Pokud jde o tzv. National Security Letters, zpráva uvádí, že bylo vydáno 10 115 žádostí (s výjimkou žádostí pouze o informace o účastnících) o informace o osobách mimo USA, které se týkaly 3 033 různých osob mimo USA[61].

Několik společností s certifikací podle rámce EU–USA pro ochranu údajů (např. Google, Meta) využívá možnosti, kterou jim dává americké právo, a zveřejňuje zprávy o transparentnosti, které informují o počtu žádostí dle zákona FISA a dle National Security Letters, jež obdržely v daném vykazovaném období. V době přípravy této zprávy ještě nebyly k dispozici statistické údaje o žádostech na základě zákona FISA z července 2023 a pozdějších. Společnost Google například oznámila, že v období od července do prosince 2023 obdržela 500 až 999 žádostí na

[58] Ustanovení § 18 výslovně vyžaduje zastoupení osob mimo Kongres.
[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.
[60] https://www.justice.gov/nsd/media/1350236/dl?inline.
[61] Tyto údaje zůstaly ve srovnání s předchozím vykazovaným rokem (2022) do značné míry stabilní. Pro srovnání, v roce 2022 bylo u Soudu pro uplatňování zákona FISA podáno 317 konečných žádostí o provádění elektronického sledování nebo fyzických prohlídek pro účely zahraničního zpravodajství. Celkový počet osob, ohledně nichž byl vydán příkaz k elektronickému sledování, se pohyboval mezi 0 a 499. FBI v roce 2022 podala 9 103 žádostí na základě National Security Letters o informace o osobách mimo USA (s výjimkou žádostí pouze o informace o účastnících). Zdroj: https://irp.fas.org/agency/doj/fisa/2022rept.pdf.

základě National Security Letters, které se týkaly 2 000 až 2 499 účtů[62]. Společnost Meta oznámila, že ve stejném vykazovaném období obdržela 0 až 499 žádostí na základě National Security Letters, které se týkaly 500 až 999 účtů[63]. V posledních letech zůstává jejich počet poměrně stabilní. V zájmu dalšího zvýšení transparentnosti některé společnosti (např. Google) aktivně zveřejňují National Security Letters, které obdržely, jakmile jsou zrušena omezení týkající se nezveřejňování informací[64].

2.2.1.4 Další vývoj

V souvislosti s přípravou přezkumu vzneslo několik nevládních organizací dotazy týkající se nových forem získávání údajů ze strany zpravodajských služeb USA prostřednictvím nákupu údajů od komerčních subjektů, zejména zprostředkovatelů údajů. Vysvětlily, že ačkoli údaje shromážděné na tomto základě musí být stále zpracovávány v souladu s ostatními požadavky, včetně například prezidentského dekretu č. 12333[65], takové získávání probíhá mimo rámec FISA a prezidentského dekretu č. 14086.

V této souvislosti je třeba připomenout, že jakýkoli druh dobrovolného sdílení údajů s třetími stranami podléhá podle rámce EU–USA pro ochranu údajů několika podrobným podmínkám. Za prvé, certifikovaná organizace nemůže sdílet údaje s třetí stranou (která nejedná jako zprostředkovatel/zpracovatel), aniž o tom informuje dotčené osoby a aniž jim nabídne možnost volby[66]. Za druhé, v souladu se *zásadou odpovědnosti za další předávání* lze další předávání provádět pouze 1) pro omezené a přesně stanovené účely, 2) na základě smlouvy mezi organizací rámce EU–USA pro ochranu údajů a třetí stranou a 3) pouze tehdy, pokud tato smlouva stanoví povinnost, aby třetí strana poskytla stejnou úroveň ochrany, jakou zaručují zásady[67].

Kromě toho, jak bylo rovněž projednáno na přezkumném jednání, Federální obchodní komise podnikla donucovací kroky proti zprostředkovatelům údajů, kteří prodávají citlivé údaje spotřebitelů. Například v případu ve věci společnosti *X-Mode* a jejího nástupce, společnosti *Outlogic*, vydala Federální obchodní komise dne 9. ledna 2024 příkaz, který společnosti zakazuje prodej geolokačních údajů třetím stranám a přikazuje vymazání údajů, které používala a sdílela nezákonně. Šetření Federální obchodní komise mimo jiné zjistilo, že společnost plně neinformovala jednotlivce o používání a prodeji jejich geolokačních údajů, nezavedla opatření umožňující jednotlivcům ukončit své sledování, dopustila použití údajů k potenciálně diskriminačním účelům a nezavedla omezení pro používání těchto informací třetími stranami[68]. Komise očekává, že stejný přístup zaujme Federální obchodní komise v případě, že by společnosti s certifikací rámce EU–USA pro ochranu údajů sdílely údaje v rozporu s výše uvedenými ustanoveními.

[62] https://transparencyreport.google.com/user-data/us-national-security.
[63] https://transparency.meta.com/reports/government-data-requests/country/US/.
[64] https://transparencyreport.google.com/user-data/us-national-security.
[65] Viz například § 2.4 prezidentského dekretu č. 12333 o technikách sběru.
[66] Viz 40. bod odůvodnění rozhodnutí o odpovídající ochraně.
[67] Viz 38. bod odůvodnění rozhodnutí o odpovídající ochraně.
[68] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.

Nakonec je třeba zmínit, že v květnu 2024 vydal úřad ODNI rámec politiky zpravodajské komunity pro komerčně dostupné informace[69]. Tento rámec stanoví řadu zásad a požadavků, kterými by se zpravodajské služby měly při získávání a využívání informací v souvislosti s obchodní transakcí řídit, včetně minimalizace rizik pro soukromí a občanské svobody.

2.2.2 Nezávislý dohled

Činnost amerických zpravodajských služeb podléhá dohledu různých orgánů, včetně úředníků pro ochranu soukromí a občanských svobod, generálních inspektorů, Kongresu a výboru PCLOB. Prezidentský dekret č. 14086 konkrétně stanoví, že každá zpravodajská služba musí mít právní úředníky na vyšší úrovni a úředníky pro dohled a dodržování předpisů, kteří zajistí dodržování platných právních předpisů USA. Tuto funkci dohledu plní úředníci s určenou funkcí v oblasti dodržování předpisů, jakož i úředníci pro ochranu soukromí a občanských svobod a generální inspektoři[70]. Jsou povinni provádět pravidelný dohled nad činnostmi v oblasti signálového zpravodajství a zajišťovat nápravu jakéhokoli nedodržení předpisů. Zpravodajské služby musí těmto úředníkům umožnit přístup ke všem relevantním informacím, aby mohli vykonávat své funkce dohledu, a nesmějí podnikat žádné kroky, které by bránily jejich dohledovým činnostem nebo je nepřiměřeně ovlivňovaly.

Přezkumného jednání se zúčastnil generální rada Úřadu generálního inspektora zpravodajské komunity (ICIG) v rámci úřadu ODNI, který má komplexní pravomoc nad celou zpravodajskou komunitou a je oprávněn vyšetřovat stížnosti nebo informace týkající se údajného nezákonného jednání nebo zneužití pravomocí. Potvrdil, že Úřad generálního inspektora zpravodajské komunity v rámci svých dohledových činností systematicky kontroluje dodržování prezidentského dekretu č. 14086. Odkázal také na nedávné dohledové činnosti ostatních generálních inspektorů zpravodajské komunity, které jsou podrobně popsány v pravidelných zprávách. Například ve své pololetní zprávě Kongresu za období duben–září 2023[71] informoval generální inspektor agentury NSA o hodnocení vnitřního kontrolního rámce agentury NSA pro rozhodování o cíleném sledování a žádostech. Došel k závěru, že tento rámec řádně funguje a vyhovuje požadavkům zákonů, směrnic a politik k ochraně občanských svobod a soukromí. Stejná zpráva se rovněž zmiňuje o vyšetřování, které odhalilo zneužití nástroje pro signálové zpravodajství k neoprávněným účelům jedním ze zaměstnanců agentury NSA.

[69] https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf. Zpravodajské služby jsou povinny dodržovat tento rámec od srpna 2024.

[70] Každá zpravodajská služba má generálního inspektora, který je ze zákona nezávislý a odpovídá za provádění auditů a vyšetřování činností prováděných příslušnou službou pro účely národní bezpečnosti. Inspektoři mají přístup ke všem relevantním (i utajovaným) materiálům a v případě potřeby mohou být předvoláni a podávat svědectví. Generální inspektoři předávají případy podezření na trestné činy k trestnímu stíhání a předkládají vedoucím služeb doporučení k nápravě. Jejich doporučení jsou sice nezávazná, ale jejich zprávy, včetně následných opatření (nebo jejich absence), jsou zpravidla zveřejňovány a zasílány Kongresu. V tomto ohledu viz poznámka pod čarou 136 rozhodnutí o odpovídající ochraně týkající se úlohy generálního inspektora.

[71] https://oig.nsa.gov/reports/Article/3609957/semiannual-report-to-congress-1-april-2023-to-30-september-2023/.

Výbor PCLOB je na základě prezidentského dekretu č. 14086[72] pověřen specifickými dohledovými funkcemi[73]. Předseda výboru PCLOB a jeho tři členové se zúčastnili přezkumného jednání a informovali, že výbor PCLOB v dubnu 2023 poskytl zpravodajským službám poradenství ohledně jejich návrhů politik a postupů provádějících prezidentský dekret č. 14086 a byl taktéž konzultován ohledně jmenování soudců a zvláštních advokátů Soudu pro přezkum ochrany údajů. Výbor rovněž zahájil projekt dohledu, jehož cílem je 1) přezkoumat provádění aktualizovaných politik a postupů přijatých zpravodajskými službami, aby se zajistil jejich soulad s prezidentským dekretem, a 2) každoročně přezkoumat fungování nového nápravného mechanismu (viz níže)[74]. Členové výboru PCLOB potvrdili, že výbor plánuje provést oba přezkumy v blízké budoucnosti. Pokud jde o nápravu, vysvětlili, že v případě neexistence stížností se přezkum výboru PCLOB zaměří na politiky a postupy zavedené za účelem vytvoření mechanismu.

Pokud jde o další dohledové činnosti, výbor PCLOB vydal 28. září 2023 zprávu o § 702 zákona FISA[75]. Tato zpráva navazuje na dřívější zprávu z roku 2014 a obsahuje aktualizované faktické a právní informace o fungování programů sledování podle § 702 zákona FISA. Zpráva rovněž obsahuje doporučení ohledně dodržování příslušných požadavků zpravodajskými službami a návrhy pro Kongres na další posílení některých aspektů § 702 zákona FISA v souvislosti s jeho opětovným schválením (včetně kodifikace legitimních cílů sledovacích činností uvedených v prezidentském dekretu č. 14086).[76] Během přezkumného jednání výbor PCLOB informoval, že očekává, že brzy obdrží odpovědi zpravodajských služeb týkající se provádění jeho doporučení, které budou zahrnuty do budoucí navazující zprávy. K dalším probíhajícím projektům dohledu patří projekt zaměřený na boj proti domácímu terorismu a jeho dopad na soukromí a občanské svobody a na shromažďování údajů z otevřených zdrojů nebo komerčně dostupných údajů ze strany FBI[77].

Nevládní organizace konzultované v rámci přezkumu vyjádřily obavu, že v souvislosti s vypršením funkčního období několika členů výboru PCLOB v blízké budoucnosti by mohlo dojít ke ztrátě usnášeníschopnosti výboru PCLOB. Funkční období konkrétně vypršelo předsedkyni, přičemž období, během něhož může nadále vykonávat funkci, končí v lednu 2025; volná je ještě jedna další pozice, třetí se uvolní rovněž v lednu příštího roku. Členové během přezkumného jednání vysvětlili, že neočekávají, že by výbor PCLOB ztratil schopnost usnášet se, protože na místo, které je v současné době volné, již vznikla nominace (a čeká se

[72] Výbor PCLOB je nezávislým úřadem, kterému jsou svěřeny povinnosti v oblasti protiteroristické politiky a jejího provádění s ohledem na ochranu soukromí a občanských svobod. Má přístup ke všem relevantním (i utajovaným) informacím, může provádět výslechy a vyslechnout svědectví. Může vydávat doporučení pro donucovací a zpravodajské orgány a pravidelně podává zprávy Kongresu a prezidentovi. Jeho zprávy jsou v nejvyšší možné míře zveřejňovány.

[73] https://documents.pclob.gov/prod/Documents/EventsAndPress/834a1977-f420-4b2a-ae93-8a522b2c7c74/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL)%20-%20Completed%20508%20-%2010202022.pdf.

[74] https://www.pclob.gov/OversightProjects/Details/1115.

[75] https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.

[76] Komise poznamenává, že některá z těchto doporučení, včetně doporučení o shromažďování údajů nebo doporučení o posílení úlohy odborníků Soudu pro uplatňování zákona FISA (*amici*), byla začleněna jako součást zákona RISAA.

[77] https://www.pclob.gov/OversightProjects.

na potvrzení Senátem)[78]. Zdůraznili také, že i kdyby výbor ztratil usnášeníschopnost, neovlivnilo by to jeho schopnost pokračovat v provádění projektů dohledu. Nicméně vzhledem k důležité úloze výboru PCLOB při přezkumu provádění prezidentského dekretu č. 14086 bude Komise pečlivě sledovat stav budoucích volných pracovních míst a nominací/jmenování.

2.2.3 Nápravná opatření

Prezidentským dekretem č. 14086, doplněným nařízením ministra spravedlnosti, byl zřízen nový nápravný mechanismus pro vyřizování a řešení kvalifikovaných stížností fyzických osob týkajících se činností amerického signálového zpravodajství[79]. Každá fyzická osoba v EU je v souvislosti s osobními údaji předanými do USA oprávněna podat nápravnému mechanismu stížnost týkající se údajného porušení právních předpisů USA upravujících činnosti v oblasti signálového zpravodajství (např. prezidentský dekret č.14086, § 702 zákona FISA, prezidentský dekret č. 12333), které nepříznivě ovlivňuje její zájmy v oblasti soukromí a občanských svobod. Fyzické osoby mohou podat stížnost u úřadu pro ochranu údajů v členském státě EU, ten ji prostřednictvím sekretariátu EDPB předá nápravnému mechanismu. Tento mechanismus se skládá ze dvou úrovní: počáteční šetření stížností provádí úředník ODNI CLPO a proti jeho rozhodnutí se fyzické osoby mohou odvolat k nezávislému Soudu pro přezkum ochrany údajů. Po dokončení přezkumu úředníkem ODNI CLPO nebo Soudem pro přezkum ochrany údajů jsou fyzické osoby prostřednictvím vnitrostátního orgánu informovány, že „v přezkumu buď nebylo zjištěno žádné dotčené porušení, nebo že [úředník ODNI CLPO /] Soud pro přezkum ochrany údajů vydal rozhodnutí, ve kterém je stanovena povinnost zajistit vhodnou nápravu“. Rozhodnutí úředníka ODNI CLPO a Soudu pro přezkum ochrany údajů jsou pro zpravodajské služby závazná.

Od přijetí rozhodnutí o odpovídající ochraně byly podniknuty další kroky, aby byl nápravný mechanismus plně funkční.

Pokud jde o zřízení Soudu pro přezkum ochrany údajů, dne 14. listopadu 2023 bylo jmenováno osm soudců (tj. o dva soudce více, než je minimální počet požadovaný podle prezidentského dekretu č. 14086, jak je doplněno v nařízeních ministra spravedlnosti v § 28 C.F.R. § 201.3 písm. a))[80]. Byli jmenováni na základě kritérií stanovených v prezidentském dekretu č. 14086 a v souladu s postupem v něm stanoveným, mimo jiné po konzultaci s výborem PCLOB[81]. Patří mezi ně bývalí soudci federálního obvodního soudu a odvolacího soudu, bývalý ministr spravedlnosti USA a bývalý člen výboru PCLOB. V souladu s požadavkem prezidentského dekretu má alespoň polovina soudců předchozí soudní praxi. Kromě toho byli v dubnu 2024 jmenováni dva zvláštní advokáti – právníci s odbornými znalostmi v oblasti ochrany soukromí i národní bezpečnosti –, kteří mají zastupovat zájmy jednotlivců před Soudem pro přezkum ochrany údajů. Na přezkumném jednání bylo potvrzeno, že všichni soudci a zvláštní advokáti získali nejvyšší stupeň bezpečnostní prověrky, a proto mohou mít při plnění svých úkolů pro Soud pro přezkum ochrany údajů přístup k utajovaným materiálům. Soud pro přezkum ochrany údajů rovněž zveřejnil řadu často kladených otázek s dalšími informacemi o své úloze, nezávislosti a fungování[82].

[78] https://documents.pclob.gov/prod/Documents/EventsAndPress/deb9cd13-12af-4250-998e-a520a2419a6b/PCLOB%20nominee%20press%20release%206-13-24.pdf.
[79] 176.–194. bod odůvodnění rozhodnutí o odpovídající ochraně.
[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.
[81] Paragraf 3(d)(A) prezidentského dekretu č. 14086.
[82] https://www.justice.gov/opcl/dprc-resources.

Pokud jde o vyřizování stížností, úřad ODNI přijal dne 6. prosince 2022 směrnici o zpravodajské komunitě č. 126, která podrobně upravuje různé aspekty procesu vyšetřování a vyřizování stížností (stanoví lhůty, zřizuje zabezpečené elektronické úložiště a komunikační kanály, zavádí požadavek na spolupráci úředníka pro ochranu občanských svobod a složek zpravodajské komunity s výborem PCLOB v rámci každoročního přezkumu nápravného mechanismu atd.)[83]. Tato směrnice je použitelná v rámci celé zpravodajské komunity USA a byla doplněna dalšími interními postupy přijatými jednotlivými zpravodajskými službami, které se týkají jejich spolupráce s úředníkem ODNI CLPO v souvislosti s vyřizováním stížnosti (např. vytvoření zabezpečeného úložiště pro sdílení stížností a odpovídajících dokumentů a bezpečná komunikace mezi příslušnými službami). Rovněž Soud pro přezkum ochrany údajů vydá v nadcházejících měsících podrobnější pravidla pro vyřizování stížností a další procesní aspekty.

V Evropské unii i Spojených státech byla přijata řada dalších opatření, jejichž cílem bylo informovat veřejnost a usnadnit podávání a vyřizování stížností. Mimo jiné byla přijata informativní poznámka EDPB o novém nápravném mechanismu[84], vzorový formulář stížnosti (který musí všechny úřady pro ochranu údajů nechat přeložit a zveřejnit ve svých úředních jazycích)[85] a jednací řád, který upravuje spolupráci mezi vnitrostátními orgány dohledu a sekretariátem EDPB[86]. Stejně tak úřad ODNI zveřejnil často kladené dotazy a informační list o novém nápravném mechanismu a zapojil se do osvětové činnosti[87].

V uplynulém roce navíc EDPB a příslušné orgány USA úzce spolupracovaly na několika operativních aspektech. Jak bylo potvrzeno během přezkumného jednání, zavedly zejména šifrovaný komunikační kanál pro předávání stížností vnitrostátními orgány v EU sekretariátu EDPB, sekretariátem EDPB úředníkovi ODNI CLPO a také Úřadu pro ochranu soukromí a občanských svobod (úřad OPCL) Ministerstva spravedlnosti a mezi úředníkem ODNI CLPO a dalšími orgány na straně USA (např. Soudem pro přezkum ochrany údajů). Kromě toho úřednice ODNI CLPO vysvětlila, že pokud jde o vyřizování stížností, byly zavedeny další interní postupy pro její spolupráci s jednotlivými zpravodajskými službami.

Nakonec úřad OPCL, který poskytuje administrativní podporu Soudu pro přezkum ochrany údajů, rovněž informoval, že Soud pro přezkum ochrany údajů pracuje v rámci vlastní vyhrazené rozpočtové položky a má k dispozici potřebné vybavení pro plnění svých úkolů, včetně zabezpečených počítačů a notebooků, telefonů atd. Kromě toho, jak požaduje prezidentský dekret č. 14086, Ministerstvo obchodu přijalo nezbytná opatření, mimo jiné zřídilo šifrovaný komunikační kanál s úředníkem ODNI CLPO, aby mohlo vést záznamy o všech obdržených kvalifikovaných stížnostech. Ministerstvo obchodu bude pravidelně kontaktovat úředníka ODNI CLPO ohledně toho, zda byly odtajněny informace týkající se

[83] https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf

[84] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_en.

[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_en.

[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_en.

[87] https://www.dni.gov/files/CLPT/documents/Fact_Sheets/The_Role_of_the_ODNI_CLPO_FAQs.pdf a https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.

jednotlivých stížností. V takovém případě o tom Ministerstvo obchodu vyrozumí dotčenou osobu, aby jí umožnilo získat přístup k těmto informacím.

Do doby konání přezkumného jednání neobdržely orgány dohledu EU žádné stížnosti, takže nový nápravný mechanismus ještě nebyl spuštěn.

3. ZÁVĚR

Na základě informací shromážděných během tohoto prvního přezkumu dospěla Komise k závěru, že orgány USA zavedly nezbytné struktury a postupy k zajištění účinného fungování rámce pro ochranu údajů. V této souvislosti Komise vysoce oceňuje velmi dobrou spolupráci s americkými orgány při provádění přezkumu.

Tento první přezkum se přirozeně zaměřil na ověření, zda jsou zavedeny všechny základní prvky rámce, nicméně zkušenosti s praktickým uplatňováním záruk, které se vztahují jak na zpracování údajů certifikovanými společnostmi, tak na přístup k údajům ze strany orgánů veřejné moci, jsou po pouhém roce fungování nutně omezené. Komise proto bude v následujících měsících a letech pečlivě sledovat příslušný vývoj a věnovat zvláštní pozornost 1) nadcházejícím zprávám výboru PCLOB o provádění prezidentského dekretu č. 14086 a fungování nápravného mechanismu v oblasti signálového zpravodajství, zejména Soudu pro přezkum ochrany údajů; 2) případným dalším změnám § 702 zákona FISA a 3) nominaci a jmenování členů výboru PCLOB na místa, která se uvolní.

Pro zajištění trvalého a účinného fungování je dále dle Komise důležité, aby:

- Ministerstvo obchodu – v souladu s tím, co zaznělo na přezkumném jednání – více využívalo různé nástroje, které rámec EU–USA pro ochranu údajů nabízí ke sledování dodržování zásad ze strany společností a odhalování nepravdivých tvrzení o účasti,
- Federální obchodní komise dále rozvíjela svůj proaktivní přístup k vyšetřování a prosazování dodržování zásad rámce EU–USA pro ochranu údajů certifikovanými společnostmi a
- Ministerstvo obchodu, Federální obchodní komise a úřady EU pro ochranu údajů vypracovaly společné pokyny k hlavním požadavkům podle zásad rámce EU–USA pro ochranu údajů, např. k údajům v oblasti lidských zdrojů a dalšímu předávání.

S ohledem na tento výsledek přezkumu a v souladu s 211. bodem odůvodnění rozhodnutí o odpovídající ochraně považuje Komise za vhodné provést další pravidelný přezkum po třech letech. Bude tak možné získat více zkušeností s praktickým používáním rámce EU–USA pro ochranu údajů a zohlednit výše uvedený nadcházející vývoj. Z tohoto důvodu bude Komise v souladu s čl. 3 odst. 4 rozhodnutí o odpovídající ochraně konzultovat s EDPB a výborem zřízeným podle čl. 93 odst. 1 obecného nařízení o ochraně osobních údajů periodicitu budoucích přezkumů.