Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Evropské informační systémy a jejich využití v ČR při ochraně vnějších hranic

Bc. Tomáš PŠENICA

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Tomáš Pšenica

Veřejná správa a regionální rozvoj – c.v. Litoměřice

Název práce

Evropské informační systémy a jejich využití v ČR při ochraně vnějších hranic

Název anglicky

European information systems and their use in the Czech Republic in the protection of external borders

---

Cíle práce

Cílem diplomové práce je analýza evropských policejních systémů na ochranu hranic. Dílčím cílem je analýza zavádění a používání evropských policejních informačních systémů při ochraně vnějších hranic, zejména na českých mezinárodních letištích. Dalším cílem je zhodnocení jejich efektivity při hraniční kontrole za použití počítačových aplikací v boji proti ilegální migraci osob.

Metodika

Teoretická část se zabývá analýzou a popisem evropských policejních systémů používaných při ochraně vnějších hranic a kontrole osob na českých mezinárodních letištích. V diplomové práci budou popsány jednotlivé systémy, charakterizován jejich význam a přiblíženo jejich použití přímo v praxi.

Praktická část bude zaměřena na zavádění jednoho zvoleného systému do praxe na území České republiky a bude analyzován jeho přínos. Dále budou provedeny řízené rozhovory s několika zaměstnanci vybraných členských zemí k ověření důležitosti a přínosu interoperability policejních systémů při odhalování nelegální migrace osob. Na základě zjištěných poznatků bude provedena SWOT analýza.

Přínosem diplomové práce bude ověření důležitosti používání evropských bezpečnostních informačních systémů a aplikací na ochranu hranic.

Doporučený rozsah práce

70

Klíčová slova

Cizinecká policie ČR, Evropská unie, informační technologie, hraniční kontrola, policejní informační systémy, nelegální migrace, ochrana hranice, schengenský prostor

---

Doporučené zdroje informací

BALABÁN, Miloš a Bohuslav PERNICA. Bezpečnostní systém ČR: problémy a výzvy. Praha: Univerzita Karlova v Praze, nakladatelství Karolinum, 2015. 10 s. ISBN 978-80-246-3150-9.

HRABÁLEK, M. Ochrana hranic EU a role agentury FRONTEX v ní. Praha: Masarykova universita, 2012. 155 s. ISBN 978-80-210-5988-7.

Nařízení Evropského parlamentu a Rady (ES) č. 1987/2006 ze dne 20. prosince 2006 o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II).

Nařízení Evropského parlamentu a Rady (EU) 2019/818 ze dne 20. května 2019, kterým se zřizuje rámec pro interoperabilitu mezi informačními systémy EU v oblasti policejní a justiční spolupráce, azylu a migrace a kterým se mění nařízení (EU) 2018/1726, (EU) 2018/1862 a (EU) 2019/816.

PIKNA, Bohumil. Vnitřní a vnější bezpečnost a ochrana základních práv (na pozadí boje s mezinárodním terorismem). Praha: Linde, 2002. 473 s. ISBN 80-7201-383-1.

ŠTEINBACH, Miroslav. Zákon o Policii České republiky: komentář. Praha: WoltersKluwer, 2019. Komentáře WoltersKluwer. 280 s. ISBN 978-80-7598-193-6.

VLÁČIL, Jiří. Právo na vstup a pobyt na území členských států Evropské unie. Praha: Univerzita Karlova, Právnická fakulta, 2016. 154 s. ISBN 978-80-87975-52-7.

VLČKOVÁ, Alena. Zákon o pobytu cizinců na území ČR. Praha: Eurounion s.r.o., 2003. 415 s. ISBN 80-7317-024-8.

VOKUŠ, Jiří. Policie České republiky: Police of the Czech Republic : pomáhat a chránit. 1. vyd. Praha: Policejní prezidium České republiky, 2010. 84 s. ISBN 978-80-254-6098-6.

Zároveň další interní materiály Policie České republiky.

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Karel Kubata, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 4. 7. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 04. 11. 2023

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Evropské informační systémy a jejich využití v ČR při ochraně vnějších hranic" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Suchodole 25. března 2024 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Karlu Kubatovi, Ph.D. za jeho cenné rady a připomínky a odbornou pomoc při vedení práce a v neposlední řadě hlavně za jeho vstřícnost. Dále bych chtěl poděkovat plk. Ing. Jindřichu Domanjovi, bez jehož zásluh v podobě poskytnutí důležitých informací a rozsáhlých materiálů k dané problematice by tato práce nevznikla v takto podrobném rozboru. Mé poděkování si zaslouží i plk. Mgr. Petrovi Malovcovi, Ph.D., za jeho podporu a nasměrování při výběru tohoto tématu.

Evropské informační systémy a jejich využití v ČR při ochraně vnějších hranic

Abstrakt

Diplomová práce se zabývá evropskými policejními informačními systémy na ochranu vnějších hranic, konkrétně pak použitím na českých mezinárodních letištích za účelem efektivního provádění hraniční kontroly, odhalování nelegální migrace a přeshraniční trestné činnosti, případně terorismu.

Teoretická část práce je zaměřena na centralizaci a propojenost policejních systémů používanými bezpečnostními složkami evropských států při ochraně vnějších hranic Schengenského prostoru. Práce se také věnuje výčtu těchto systémů a jejich základnímu významu, včetně popisu.

Praktická část se zaměřuje na budování jednoho ze systémů a jeho začleňování do policejní práce na českých mezinárodních letištích. Dále pak ověřováním důležitosti a přínosu interoperability policejních systémů při odhalování nelegální migrace osob.

Klíčová slova: Cizinecká policie ČR, Evropská unie, informační technologie, hraniční kontrola, policejní informační systémy, nelegální migrace, ochrana hranice, Schengenský prostor

European information systems and their use in the Czech Republic in the protection of external borders

Abstract

The diploma thesis deals with European police information systems for the protection of external borders, specifically their use at Czech international airports for the purpose of effective border control, detection of illegal migration and cross-border crime or terrorism.

The theoretical part of the thesis is focused on the centralization and interconnection of police systems used by the security forces of European countries in the protection of the external borders of the Schengen area. The thesis also deals with the enumeration of these systems and their basic meaning, including a description.

The practical part focuses on developing one of the systems and its integration into police work at Czech international airports. Furthermore, by verifying the importance and contribution of the interoperability of police systems in detecting illegal migration of persons.

Keywords: border control, illegal migration, information technology, European Union, border protection, foreign police service, police information systems, Schengen

Obsah

1 Úvod

V současné době procházejí ICT technologie významným rozvojem, zejména v oblasti bezpečnosti ochrany států. S postupem času a globálním vývojem neustále roste důležitost odhalování a potírání nelegální migrace osob a úsilí v boji proti ní. Najít k této problematice volně dostupné informace je téměř nemožné z důvodu absence publikací, které by se tomuto tématu věnovaly. A proto se tato diplomová práce zaměřuje na technologie, které jsou využívány především na vnějších hranicích Schengenského prostoru, zejména pak na českých mezinárodních letištích, čímž se podílejí na její ochraně.

Migrace jednotlivců a skupin lidí stále narůstá, ať už se jedná o turismus, hledání pracovních příležitostí nebo zlepšení životních podmínek. S tímto nárůstem se také zvyšuje počet pokusů o obcházení různých právních omezení týkajících se legálního vstupu a pohybu osob a tyto pokusy jsou stále sofistikovanější. Proto je nezbytné bojovat proti těmto nelegálním aktivitám prostřednictvím pokročilých počítačových systémů, které jsou vzájemně propojeny. Tím se zvyšuje jejich efektivita a usnadňuje se práce při potírání tohoto typu zločinného jednání.

Teoretická část diplomové práce je zaměřena na výčet a popis evropských bezpečnostních systémů a aplikací, které se používají při ochraně vnějších hranic České republiky a kontrole osob, které vstupují a vystupují z našeho území, potažmo z území Evropské unie. Dále je analyzována důležitost propojenosti těchto systémů, takzvaná interoperabilita.

V praktické části, která je pojata jako případová studie, se autor práce zaměřuje na přínosy evropských informačních systémů, dále hodnotí rozdíly mezi životním cyklem běžného informačního systému a životním cyklem bezpečnostních systémů policie. Součástí je analýza projektu systému Entry/Exit, který je v současné době ve fázi finalizace před spuštěním testovacího provozu. Jako další je provedena analýza dat vytěžování stěžejních informačních systémů při ochraně vnějších hranic na největším českém mezinárodním letišti v Praze. K ověření získaných informací autor provedl řízené rozhovory se třemi pracovníky různých evropských zemí a v závěru práce je vyhotovena SWOT analýza, ve které jsou shrnuty zjištěné poznatky.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem této diplomové práce je analýza evropských policejních systémů na ochranu hranic a přiblížení jejich implementace a používání při ochraně vnějších hranic, zejména na českých mezinárodních letištích. Dílčím cílem je zhodnocení jejich efektivity při hraniční kontrole v boji proti nelegální migraci osob. Dalším cílem je přiblížení problematiky ochrany vnějších hranic Evropské unie za pomocí informačních technologií.

2.2 Metodika

Diplomová práce je rozdělena na teoretickou a praktickou část. Teoretická část je věnována výčtu a popisu jednotlivých evropských policejních systémů a aplikací pomáhající při ochraně vnějších hranic České republiky a kontrole osob, které nejenom vstupují na naše území, potažmo území Evropské unie, ale i toto území opouštějí a přibližuje jejich použití přímo v praxi.

Praktická část je zaměřena na zavádění systému Entry/Exit do praxe na území České republiky a bude analyzován jeho přínos. Dále budou provedeny řízené rozhovory s několika zaměstnanci vybraných členských zemí. Na základě zjištěných poznatků bude provedena SWOT analýza a bude vyhodnocen přínos používání evropských policejních systémů všemi členskými státy.

V diplomové práci je použita analytická metoda, která umožní přiblížení problematiky použití informačních technologií při ochraně a kontrole hranic. A metoda syntézy, ve které diplomová práce přiblíží úlohu cizinecké policie při ochraně vnějších státních hranic a ochraně před nelegální migrací osob za pomoci informačních systémů. V práci autor dále použil empirických metod z vlastní praktické činnosti.

3 Teoretická část

3.1 Informatika a Informační systém

3.1.1 Informace

Základním centrem dění informatiky je informace. Pochází z latinského slova informatio, resp. informare, což znamená *„uváděti ve tvar, dodávati tvar, podobu tvořit, zobrazovat“*. Informaci tedy můžeme chápat jako obsah, která je sdílená s vnějším světem a na kterou reagujeme. Základem informace jsou znaky, pomocí kterých dochází k výměně informací, a to nazýváme komunikací, která probíhá mezi minimálně dvěma účastníky skrze systémy znaků.[1]

3.1.2 Informatika

V literatuře se setkáme s různými definicemi pojmu informatika, často jde i o různé názory. Pro tuto práci informatiku chápeme jako vědu o informacích, která se zabývá vyjádřením, zpracováním a přenášením informací v přirozených (lidé a společnost) i umělých (počítače) systémech.[2]

3.1.3 Informační systém

Jako každý obor se i informatika snaží definovat předmět své oblasti, svůj systém. Tento systém se skládá z:[3]

- účelu systému, resp. cílové chování systému,
- struktury systému, tj. prvky systému a vazby mezi nimi,
- vlastností prvku, které jsou významné pro celkové chování systému,
- vlastností vazeb mezi prvky systému,
- okolí systému, což jsou prvky, které nepatří do systému, ale významně ovlivňují chování systému,
- případných subsystémů, tj. relativně malé samostatné celky uvnitř systému.

---

[1] GÁLA Libor, POUR Jan, TOMAN Prokop. *Podniková informatika. Třetí aktualizované vydání.* Praha: Grada Publishing, a. s., 2015. ISBN 978-80-247-5457-4. s. 13-14.
[2] GÁLA Libor, POUR Jan, TOMAN Prokop. *Podniková informatika. Druhé, přepracované a aktualizované vydání.* Praha: Grada Publishing, a. s., 2009. ISBN 978-80-247-2615-1. s. 21.
[3] GÁLA Libor, POUR Jan, TOMAN Prokop. *Podniková informatika. Druhé, přepracované a aktualizované vydání.* Praha: Grada Publishing, a. s., 2009. ISBN 978-80-247-2615-1. s. 23-24.

Cílem informačního systému je zajistit zpracování informací a jejich přenesení v rámci nějakého systému, je tvořen lidmi, nástroji a metodami, které dělíme na základní části:

- vstup (input) – prvky, které jsou předmětem zpracování,
- zpracování (processing) – transformace prvků do požadovaného výstupu,
- výstup (output) – výsledné prvky schopné přenést informaci příjemci (uživateli),

tyto části dále rozšiřujeme o prvky řízení (control) a zpětné vazby (feedback).

Informační systémy rozdělujeme v podniku podle organizačních úrovních na:[4]

- provozní úroveň – IS, které zpracovávají rutinní podnikovou agendu, jako např. výrobní zakázky, nákup, prodej, příjem plateb atd.,
- znalostní úroveň – IS podporuje růst znalostní základny organizace, spadají sem klientské aplikace (CRM, ERP atd.),
- řídící úroveň – IS pomáhá při rozhodování prostřednictvím reportingu (např. generování výstupních sestav ekonomických výsledků),
- strategická úroveň – IS pomáhá k identifikaci dlouhodobých trendů uvnitř i vně organizace a schopnost reagovat na změny.

3.1.4 Životní cyklus informačních technologií

Životní cyklus informačních technologií neboli proces řízení rozvoje aplikace. Jednotlivé fáze životního cyklu aplikace se rozdělují následovně:[5]

- plánování a příprava,
- analýza a návrh,
- implementace,
- migrace,
- provoz a užití,

[4] SODOMKA Petr, KLČOVÁ Hana. *Informační systémy v podnikové praxi. Druhé aktualizované a rozšířené vydání.* Brno: Computer Press, a. s., 2010. ISBN 978-80-251-2878-7. s 73-75.
[5] GÁLA Libor, POUR Jan, TOMAN Prokop. *Podniková informatika. Třetí aktualizované vydání.* Praha: Grada Publishing, a. s., 2015. ISBN 978-80-247-5457-4. s. 199-213.

- rozvoj a optimalizace.

O životním cyklu aplikace hovoříme proto, že se jednotlivé fáze neustále opakují z důvodu přechodu na vyšší úroveň aplikace, která je často založena na nových aktuálních technologiích, které odpovídají novým potřebám uživatelů. Jednotlivé fáze se rozdělují na jednotlivé úlohy a dílčí činnosti.

Plánování a příprava aplikace

Významnou částí této fáze je vstupní analýza a plánování projektu tak, aby byly dané jasné cíle a požadovaná funkcionalita a rozhodnutí, že z počáteční fáze záměru bude realizace. Jakmile dojde ke schválení projektového záměru, přistupujeme k další úloze, a to je výběr dodavatele aplikace. Následuje úvodní studie na projekt, která přesně definuje cíle projektu a zohledňuje aktuální aplikační architekturu daného podniku. Výsledkem jsou nároky na zdroje finanční, technologické a personální. Na studii následně navazuje smlouva.

Analýza a návrh aplikace

Tato fáze zahrnuje komplex činností, které jsou spojené s analýzou potřeb a aktuálního stavu podniku, včetně návrhu řešení. Jedná se o větší úroveň detailu, což znamená jaké funkce má obsahovat, jaká data má zpracovávat a jaké procesy podporovat v podniku. Tato fáze obsahuje nejenom analýzu podnikových procesů, stávajících databází, stávajících aplikací, ale také návrh změn v procesech podniku, návrh databází a aplikace.

Implementace aplikace

Implementaci v praxi chápeme jako technologickou realizaci aplikace, ale zároveň se může jednat i o celý postup řešení aplikace. Může se jednat o tzv. kastomizaci typového softwaru nebo vývoj (dovývoj) nestandardních programových modulů. Jako jedno z řešení lze použít prototypy jako cestu důkladnější analýzy skutečných potřeb uživatelů, a tím eliminovat riziko vzniku omylů při definování funkcionality aplikace. Do této fáze spadá i akceptační řízení, která se vztahují k dílčím řešením i k celkovému projektu aplikace. Tato procedura obsahuje přípravu a instalaci testovaných modulů.

Migrace

Migrace navazuje na fázi akceptačních protokolů a konkretizuje tzv. plán migrace, což je zavedení projektu do provozu. Jedná se o organizačně a pracovně náročnou činnost.

Aby byla tato fáze úspěšná, je potřeba detailní specifikace plánu a harmonogram migrace. Tato fáze na základě úspěšného průběhu končí předávacím řízením mezi zákazníkem a dodavatelem, kde dojde k odsouhlasení žádoucí funkcionality a provozuschopnosti aplikace. Jedná se o formální ukončení projektu. Následné úpravy spadají do tzv. změnových řízení.

Provoz a užití aplikace

Tato fáze se týká běžného provozu a konzultačních služeb ve formě help desk (service desk). Mohou vznikat operativní zásahy do provozu i formulace nových požadavků na aplikaci.

Další rozvoj a optimalizace aplikace

Poslední fází životního cyklu aplikace je její další rozvoj, což znamená vytvoření zcela nového projektu, čemuž předchází analýza již existujících nových požadavků v rámci změnového řízení. V této fázi vzniknou návrhy na realizaci dílčích úprav aplikace, které vyústí v zadání nového projektu.

3.2 Policejní informační systémy

V policejní praxi se používají nejen běžné informační systémy, jako v každém podniku, ale také spousta bezpečnostních systémů, které mají velký podíl na odhalování páchané protiprávní činnosti všeho druhu. Zároveň usnadňují pracovníkům policie jejich jinak složitou, v mnoha případech, mravenčí práci. Problém těchto systémů je, že každý systém řeší pouze jednotlivou problematiku zvlášť a ve většině případů nejsou mezi sebou propojené.

Dále je důležité zmínit, že všechny tyto systémy jsou ovlivňovány příslušnými právními normami, které předcházejí jejich tvorbě a upravují jejich budování a následný provoz. Což je zásadní rozdíl mezi ostatními (např. podnikovými) IS, protože značně omezují jejich programátory, na rozdíl od programátorů, kteří „budují“ běžné IS. Dále striktně omezují jejich provoz, kdy přesně udávají, kde a za jakých podmínek budou uchovávaná jejich data, kdo a za jakých okolností má k těmto datům přístup a kdo za provoz daného systému odpovídá, aby se co nejvíce minimalizovalo riziko zneužití těchto často dosti citlivých dat. Všechny tyto aspekty ovlivňují vývoj a provoz těchto systémů a činí jednotlivé projekty časově náročné a zároveň mnohem dražší oproti ostatním systémům.

Policie ČR rozděluje IS na informační systémy a sbírky, na manuální a elektronické IS, IS s osobními údaji ve smyslu zákona č. 110/2019 Sb. a bez osobních údajů, na IS s informacemi použitelnými pro trestní řízení a na ostatní, kam spadá např. ekonomické, personální, analytické, evidenční, případně distribuční aj. *„Policie dále využívá vedle běžných programů i specializované prostředky – počítačové programy, které nemají charakter IS. Přesto slouží k vyhodnocení dat, nalezení a zobrazení vztahů, vazeb nebo shody získaných údajů. Tyto informace bývají ve velkém množství dat skryty, prostému lidskému vnímání nejsou zřejmé, případně jejich vzájemná souvislost se nejlépe ukáže při grafickém znázornění.“*[6]

3.3 Právní úprava a základní pojmy

Níže jsou uvedeny základní pojmy, včetně jejich znaků, které jsou důležité pro orientaci a přehled v dané problematice s hlavním zaměřením na ochranu hranic. Normy, kterými se řídí fungování jednotlivých informačních systémů, budou zmíněny dále, v jednotlivých kapitolách týkající se konkrétního systému.

V roce 2007 vstoupila Česká republika do Schengenského prostoru, ve kterém z důvodu volného pohybu osob došlo ke zrušení jejích vnitřních hranic s okolními schengenskými státy. Díky této události bylo nutné zavést nové informační systémy, které by řešily výměnu informací mezi všemi schengenskými státy a zároveň docházelo k efektivnější hraniční kontrole. Tato změna však zachovala každému státu možnost definovat podmínky, za kterých bude umožněn vstup na jeho území dle mezinárodního práva.[7]

3.3.1 Právní rámec

Ochranu státních hranic upravuje zejména **zákon č. 191/2016 Sb.**, o ochraně státních hranic České republiky a o změně některých zákonů, ve znění pozdějších předpisů a dále **Nařízení Evropského parlamentu a Rady (EU) číslo 399/2016 ze dne 9. března 2019**, kterým se stanoví kodex Unie o pravidlech upravujících přeshraniční pohyb osob (Schengenský hraniční kodex), v platném znění.

---

[6] DOSTÁL, Petr. *Policejní informační systémy a jejich využití v trestním řízení.* Brno, 2008. Bakalářská práce. Masarykova univerzita. Vedoucí práce prof. JUDr. Vladimír Kratochvíl, CSc. s. 8.
[7] VLÁČIL, Jiří. *Právo na vstup a pobyt na území členských států Evropské unie.* Praha: Univerzita Karlova, Právnická fakulta, 2016. ISBN 978-80-87975-52-7. s. 29.

Samotné použití informačních systémů při hraniční kontrole je dané zákonem, a to zejména zákonem č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, ve znění pozdějších předpisů a dále pak blíže specifikováno vnitřními předpisy Policie, které stanoví, jakým způsobem a za jakých podmínek který systém využít, aby byl dodržen legální postup.[8]

3.3.2 Základní pojmy

a) Bezpečnostní sbor

Pojem bezpečnostní sbor je ukotven v ustanovení § 1 odst. 1 zákona č. 361/2003Sb., o služebním poměru příslušníků bezpečnostních sborů. *„Tento zákon upravuje právní poměry fyzických osob, které v bezpečnostním sboru vykonávají službu (dále jen "příslušník"), jejich odměňování, řízení ve věcech služebního poměru a organizační věci služby (dále jen "služební vztahy"). Bezpečnostním sborem se rozumí Policie České republiky, Hasičský záchranný sbor České republiky, Celní správa České republiky, Vězeňská služba České republiky, Generální inspekce bezpečnostních sborů, Bezpečnostní informační služba a Úřad pro zahraniční styky a informace. “*[9]

b) Schengenský prostor

„Schengen vlastně přestavuje právní instrument zakotvující hlavně volný pohyb osob v plném významu této zásady Unie na teritoriu Schengenu, který do této doby nebyl hmatatelněji a účinněji právně ošetřen. Schengenský systém tak posloužil jako model pro celou významnou oblast Unie s tím, že kontroly osob na vnitřních hranicích byly postupně zrušeny a těžiště přesouváno na kontroly vnějších hranic. “[10]

c) Schengenský hraniční kodex

Zahrnuje definice společných pravidel týkajících se základních podmínek pro překročení vnějších hranic, provádění hraničních kontrol a odepírání vstupu. V preambuli

[8] KRAJČÍK, Vladimír. *Informační systémy I.* Ostrava: Vysoká škola podnikání, 2005. ISBN ISBN 80-86764-24-9. s. 66.
[9] TOMEK, Petr. *Zákon o služebním poměru příslušníků bezpečnostních sborů: s komentářem, poznámkami a judikaturou*. Olomouc: ANAG, 20. října 2019. Právo (ANAG). ISBN 978-80-7554-234-2. s. 24.
[10] PIKNA, Bohumil. *Evropský prostor svobody, bezpečnosti a práva – Prizmatem Lisabonské smlouvy.* Praha: Linde, 2012. ISBN 978-80-7201-889-5. s. 170.

zdůrazňuje, že ochrana hranic není pouze zájmem členského státu, který ji vykonává, ale je v zájmu všech členských států jako celku (bod 6).[11]

d) Vnitřní hranice

„Vnitřními hranicemi jsou:

a) *společné pozemní hranice členských států, včetně říčních a jezerních hranic,*

b) *letiště členských států pro vnitřní lety,*

c) *námořní, říční a jezerní přístavy členských států pro pravidelná trajektová spojení. “*[12]

e) Vnější hranice

„Pozemní hranice členských států, včetně říčních a jezerních hranic, a jejich námořní hranice a letiště, říční přístavy, námořní přístavy a jezerní přístavy, pokud nejsou vnitřními hranicemi. “[13]

f) Hraniční kontrola

Hraniční kontrola představuje prověření cizince na hraničním přechodu v souvislosti s jeho plánovaným nebo již uskutečněným překročením státních hranic. Tato systematická, kontrolní a pečlivě naplánovaná činnost je realizována Službou cizinecké policie v souladu s mezinárodními dohodami, právními předpisy a interními normativními akty.[14]

g) Dlouhodobý pobyt

Dlouhodobým pobytem se rozumí setrvání na území cizího státu po dobu přesahující 90 dní, s možností jeho prodloužení na žádost a případně následně získání povolení k trvalému pobytu po uplynutí stanovené doby. Mezi pobytové tituly patří dlouhodobé vízum, povolení k dlouhodobému pobytu a povolení k přechodnému pobytu pro rodinné příslušníky občanů EU, na které se vztahuje pobytová karta.[15]

---

[11] HRABÁLEK, M. *Ochrana hranic EU a role agentury FRONTEX v ní.* Praha: Masarykova universita, 2012. ISBN 978-80-210-5988-7. s. 76.

[12] Nařízení Evropského parlamentu a Rady (EU) 2016/399 ze dne 9. března 2016, čl. 2/1. In: EUR-Lex. Dostupné z WWW: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016R0399.

[13] Nařízení Evropského parlamentu a Rady (EU) 2016/399 ze dne 9. března 2016, čl. 2/2. In: EUR-Lex. Dostupné z WWW: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016R0399.

[14] KURŽEJA, Jan. *Cizinecká policie a evropské právo.* Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-272-0. s. 33.

[15] ČIŽINSKÝ, Pavel. *Cizinecké právo*. Praha: Linde, 2012. ISBN: 978-80-7201-887-1. s. 30.

h) Nelegální migrace

Nelegální migraci je nutné chápat nejen jako neoprávněný vstup na území státu nebo jeho neoprávněné opuštění, ale též jako neoprávněný pobyt na území nebo pobyt v rozporu s účelem, pro který bylo vydáno pobytové oprávnění. Tato oblast je charakterizována vysokou dynamikou a obtížnou prognózou vývoje, což vyžaduje flexibilní a konzistentní přístup jak v rámci potírání nelegální migrace, tak při navracení cizinců, kteří nelegálně pobývají na našem území.[16]

i) Biometrická zařízení

Biometrická zařízení využívají měření biologických prvků, například lidských charakteristik, k provádění různých funkcí. Patří sem zachytávání informací o zdraví a kondici jednotlivců nebo ověřování totožnosti uživatelů. Tato technologie nabízí široké spektrum využití a lze ji implementovat různými způsoby.[17] Tato zařízení je možné nalézt například na letištích, vládních budovách a donucovacích orgánech.

j) Biometrická data

Biometrická data jsou jednou z metod ověřování a identifikace uživatelů. Do biometrických dat zařazujeme otisky prstů, rysy obličeje, duhovku, hlas, tvar ucha, dynamiku stisku kláves a další. V současné době se nasazení biometrie dotýká většiny používaných aplikací.[18]

„Pomocí biometrie je možné potvrdit nebo stanovit totožnost jednotlivce na základě toho, „kdo je“, spíše než „co vlastní“ (např. občanský průkaz) nebo „co si pamatuje“ (např. heslo).“ [19]

---

[16] MINISTERSTVO VNITRA. *Často kladené otázky* [online] 2021 Ministerstvo vnitra České republiky [cit. 2023-08-25]. Dostupné z WWW: https://www.mvcr.cz/migrace/clanek/migrace-casto-kladene-dotazy-casto-kladene-dotazy.aspx.

[17] Cs.theastrologypage.com. *Co je to biometrické zařízení? - definice z techopedie* [online]. [cit. 2023-09-03]. Dostupné z WWW: https://cs.theastrologypage.com/biometric-device.

[18] Ali, A., Baghel, V.S. & Prakash, S. *A novel technique for fingerprint template security in biometric authentication systems*. Vis Comput 39, 6249–6263 (2023). [cit. 2023-12-18]. Dostupné z WWW: https://doi-org.infozdroje.czu.cz/10.1007/s00371-022-02726-5.

[19] A. K. Jain, A. Ross and S. Prabhakar, *"An introduction to biometric recognition,"* in IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, Jan. 2004, doi: 10.1109/TCSVT.2003.818349. [cit. 2023-12-21]. Dostupné z WWW: https://ieeexplore-ieee-org.infozdroje.czu.cz/stamp/stamp.jsp?tp=&arnumber=1262027&isnumber=28212.

k) Azyl

Mezinárodní ochrana je zastřešujícím pojmem pro azyl a doplňkovou ochranu. Jde o ochranu, která může být poskytnuta cizincům pobývajícím na území České republiky, kteří se nemohou vrátit do své země. A to z důvodů přesně uvedených v zákoně č. 325/1999 Sb., o azylu, ve znění pozdějších předpisů.[20]

„Institut azylu byl znám již v dávné minulosti, kdy měl ale nejprve náboženskou povahu a byl udělován pachatelům trestných činů, nikoliv osobám politicky pronásledovaným. Postupně se ale ustálil azyl území, udělovaný politicky pronásledovaným osobám.“ [21]

l) Dublinská úmluva

Jedná se o dohodu mezi členskými státy EU, která definuje princip, že žadatel o azyl by měl podat svou žádost v prvním členském státu EU, do kterého vstoupí. [22] Tento princip má zabránit tzv. azylovým turistům, kteří by chtěli podat žádost v několika zemích najednou.

m) SWOT analýza

Jedná se o strategický nástroj, který se používá pro analýzu interních a externích faktorů, které ovlivňují organizaci nebo projekt. Při jejím využívání se zaměřujeme na silné a slabé stránky, na příležitosti a hrozby, neboli Strenghts, Weaknesses, Opportunities a Streats.[23]

---

[20] POLITICKÝ SLOVNÍK. *Mezinárodní ochrana: Azyl a doplňková ochrana* [online] 2021 Politický slovník [cit. 2023-08-25]. Dostupné z WWW: http://www.politicky-slovnik.cz/mezinarodni-vztahy/azyl-a-mezinarodni-ochrana/.

[21] POŘÍZEK, Pavel, JÍLEK, Dalibor, ed. *Společný evropský azylový systém: transpozice směrnic*. Brno: Kancelář veřejného ochránce práv, 2008. ISBN 978-80-254-3615-8. s. 20.

[22] Lott G. *The Dublin Convention and the Introduction of the 'First Entry Rule' in the Allocation of Asylum Seekers in Europe.* Contemporary European History. 2023;32(3):459-474. doi:10.1017/S0960777321000746. [cit. 2023-12-21].

[23] MLADÝ PODNIKATEL. *Co to je SWOT analýza? A k čemu slouží?* [online]. [cit. 2024-01-08]. Dostupné z WWW: https://mladypodnikatel.cz/co-to-je-swot-analyza-t2797.

3.4 Evropské policejní informační systémy

V této části práce budou rozebrány hlavní evropské policejní systémy, které jsou, anebo v blízké budoucnosti budou využívány českou policií při zabezpečování ochrany vnějších hranic na mezinárodních letištích.

Je nutné zmínit, že evropské systémy nejsou jediné, které Služba cizinecké policie používá při ochraně vnějších hranic České republiky. Ve své gesci má i spoustu jiných, některé z nich sama vyvíjí za pomoci ověřených externích firem. Převážně se jedná o specifické „dotazovací nástroje“, pomocí kterých se dotazuje do jiných příslušných databází, které není možné z důvodů veřejnosti práce zmiňovat. Díky této kombinaci se celý proces kontroly osob značně zefektivní. A zároveň je větší šance odhalit trestné činnosti, nejenom přímo páchané, ale i spáchané příslušnou osobou v minulosti. Včetně spojení jiných přečinů. A to jak na území České republiky, tak potažmo v celém Schengenském prostoru.

Momentálně existují tři klíčové centrální systémy, které hrají rozhodující roli v oblastech bezpečnosti a migrace:[24]

- **SIS – Schengenský informační systém**,
- **VIS – Vízový informační systém**,
- **Eurodac**.

Každý z těchto evropských IS se skládá z:

- centrální součásti (CS-SIS, CS-VIS, CS-Eurodac), kterou provozuje a rozvíjí evropská agentura eu-LISA,
- národní součásti (NS-SIS, NS-VIS, NS-Eurodac), kterou provozuje a rozvíjí každý členský stát EU včetně ČR.

Centrální součást každého evropského informačního systému zahrnuje aplikační programové rozhraní (API), což je klíčový prvek pro automatizovanou komunikaci mezi systémy. Toto API poskytuje centrální služby nebo operace, které jsou následně využívány národními součástmi příslušných evropských informačních systémů. Detaily týkající se rozhraní centrálních systémů a poskytovaných služeb či operací jsou podrobně popsány v dokumentu známém jako Interface Control Document (ICD). Tímto způsobem se zajišťuje

[24] DOMANJA, Jindřich. Úvod do interoperability. PDF. Policie ČR, 2021.

jednotný standard, což umožňuje efektivní a bezproblémovou výměnu dat a informací mezi jednotlivými národními a centrálními součástmi, tedy:

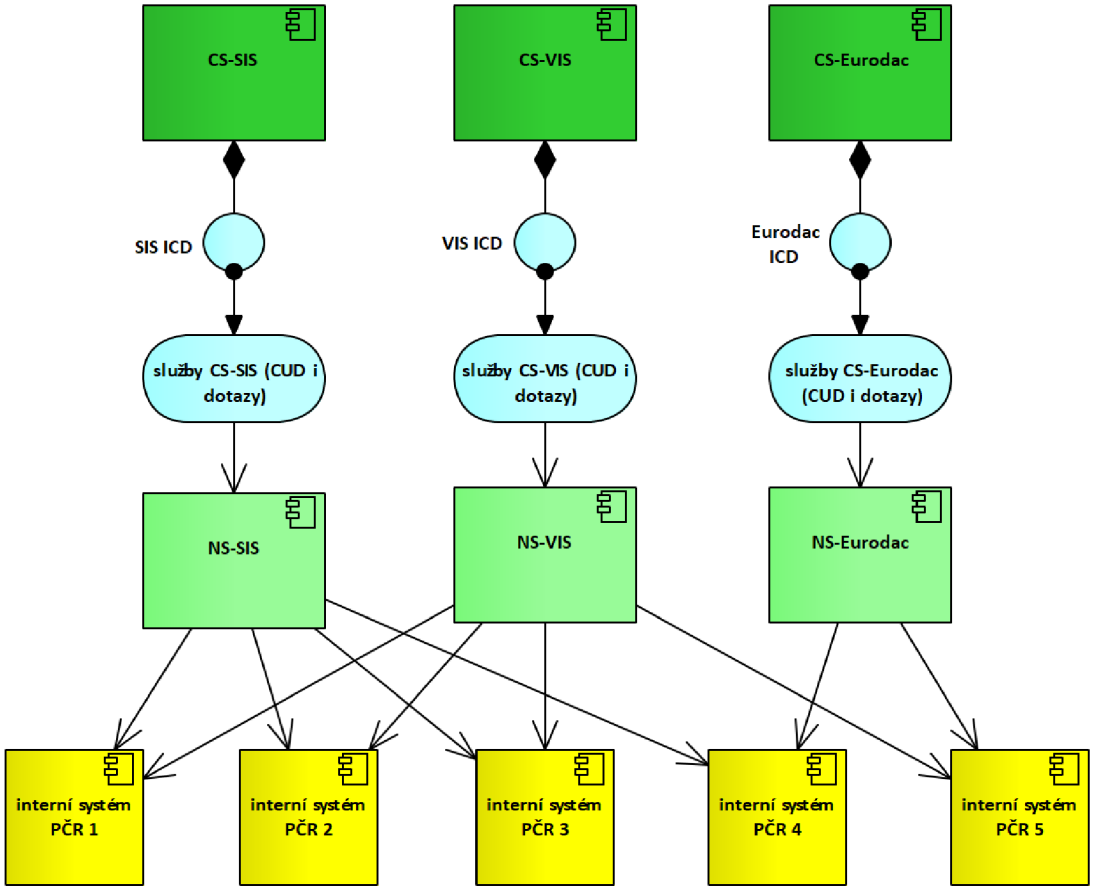
- NS-SIS komunikuje s CS-SIS způsobem definovaným v SIS ICD,
- NS-VIS komunikuje s CS-VIS způsobem definovaným ve VIS ICD,
- NS-Eurodac komunikuje s CS-Eurodac způsobem definovaným v Eurodac ICD.

SIS ICD, VIS ICD i Eurodac ICD obsahují popis dvou základních kategorií služeb (operací):

- dotazy – jak alfanumerické, tak biometrické,
- příkazy – tzv. CUD, tj. Create, Update, Delete neboli vytvoření, úprava či smazání záznamu.

Národní součásti evropských informačních systémů aktivně využívají poskytované centrální služby, které zahrnují operace CUD (Create, Update, Delete) i dotazy. Následně provádějí další zpracování v souladu s definovanými postupy a poskytují je vnitřním systémům Policie České republiky, které slouží jak jako zdrojové, tak dotazovací systémy. Je důležité zdůraznit, že vnitřní systémy PČR nekomunikují přímo s centrálními součástmi evropských informačních systémů. Ověřování, manipulace s daty a další interakce probíhají vždy skrze národní součást konkrétního evropského informačního systému, což zajišťuje dodržování standardů interoperability a bezpečnosti.

Obrázek 1 - Současný stav evropských systémů



Zdroj: (Policie České republiky, Úvod do Interoperability)

Schengenský informační systém (SIS), Vízový informační systém (VIS) a Eurodac jsou klíčové systémy pro výměnu důležitých informací o osobách v rámci Schengenského prostoru. SIS slouží k bezpečnostním opatřením a monitorování osob a věcí, zatímco VIS uchovává informace o krátkodobých schengenských vízech a Eurodac eviduje otisky prstů žadatelů o azyl.

V reakci na migrační krizi v roce 2015 se začaly budovat další tři systémy. Plánuje se vytvoření Evropského systému vstupu/výstupu (EES), který bude evidovat vstupy a výstupy cestující ze třetích zemí do a ze Schengenského prostoru. Stejně tak bude zaveden Evropský systém pro cestovní povolení (ETIAS), který zavádí agendu cestovních povolení (pro občany třetích zemí bez vízové povinnosti) od podání žádosti po kontrolu na hranicích i na území. Posledním systémem, který vznikne v důsledku této reakce, bude Evropský trestní rejstřík třetích zemí (ECRIS-TCN). Tento systém bude sloužit k výměně informací

o trestných činech mezi členskými státy EU, týkajících se občanů třetích zemí. Bližší specifikace výše zmíněných systémů bude provedena v textu níže.

Tyto nové systémy jsou navrženy s cílem posílit bezpečnostní opatření a spolupráci mezi členskými státy EU v reakci na dynamické výzvy týkající se migrace a bezpečnosti. Můžeme říci, že se jedná o revoluční krok směrem k modernizaci schengenských vnějších hranic. Již od roku 2013 hovoříme o konceptu „inteligentní hranice“, což má představovat souhrn legislativních opatření na základě konzultací s Evropským parlamentem. [25]

3.4.1 KODOX

Nejedná se o evropský informační systém, nýbrž o čistě českou aplikaci vyvinutou externí dodavatelskou firmou ve spolupráci s českou policií. Ta jej nechala vybudovat na základě svých potřeb přizpůsobit se migračním problémům a zároveň bezpečnostním požadavkům na ochranu vnějších hranic České republiky na českých mezinárodních letištích. Je důležité ho zmínit, protože systém KODOX je momentálně stěžejní systém pro hraniční kontrolu osob v České republice. Tento systém se neustále vyvíjí a přizpůsobuje aktuálním podmínkám a požadavkům Služby cizinecké policie. Navíc se s tímto systémem počítá i v budoucnosti, kdy i nadále bude pro Službu cizinecké policie důležitým prvkem, přes který bude využívat služby Interoperability při hraniční kontrole osob.

Systém se řídí interními nařízeními Policie ČR a slouží k podpoře procesu hraniční kontroly od konce roku 2011.

IS KODOX je využíván Ředitelstvím služby cizinecké policie za účelem hraniční kontroly, jehož servery jsou provozovány ICP Praha – Ruzyně. Představuje důležitý nástroj nepřetržitého odbavovacího procesu na mezinárodních letištích ČR v souladu se zachováním bezpečnosti ochrany Schengenského prostoru. *„IS KODOX plní také roli klienta „KONTROLA“ národní součásti Vízového informačního systému (NS-VIS ČR) s dotazováním a kontrolou otisku prstů do systému CS-VIS (Centrální součást Vízového informačního systému). Provoz a správu zabezpečuje Ředitelství služby cizinecké policie.“*

[25] THALES. *The Schengen Entry/Exit System: biometrics to facilitate smart borders* [online]. [cit. 2023-12-02]. Dostupné z: WWW https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/eborder/entry-exit-systém.

IS KODOX zpracovává data z mnoha dalších národních a mezinárodních IS. Porovnává cestovní doklady s biometrickými daty, od vizuální kontroly (např. kontrola pravosti optickým expertním systémem) po kontrolu elektronickou (např. kontrola pravosti důvěry certifikátů vydavatele nebo porovnání biometrických prvků).

„IS KODOX umožňuje ověření platností víz a dalších informací prostřednictvím centrálních databází a datových fondů a rovněž zajišťuje provádění bezpečnostní prověrky kontrolovaných osob v informačních systémech dle legislativních nařízení.“ [26]

3.4.2 SIS – Schengenský informační systém

SIS představuje novou generaci informačního systému, který podporuje agendu pátrání, eviduje hledané osoby a věci. Jedná se o jediný evropský systém, který uchovává data jak o občanech třetích zemí, tak o občanech EU. Obsahuje alfanumerická i biometrická data (fotografie, otisky prstů) o osobách a současně evropské zatýkací rozkazy, což usnadňuje práci justičním orgánům, kterým tímto odpadá nutnost zasílat tyto dokumenty členským zemím poštou.[27]

Hlavním cílem tohoto IS je zajistit vysokou úroveň bezpečnosti v rámci Schengenského prostoru tím, že umožňuje vnitrostátním orgánům prověřovat záznamy o osobách nebo věcech. Centrální databáze je umístěna ve Štrasburku a záloha databáze je umístěna v blízkosti Salcburku.

Architekturu SIS tvoří tyto části:[28]

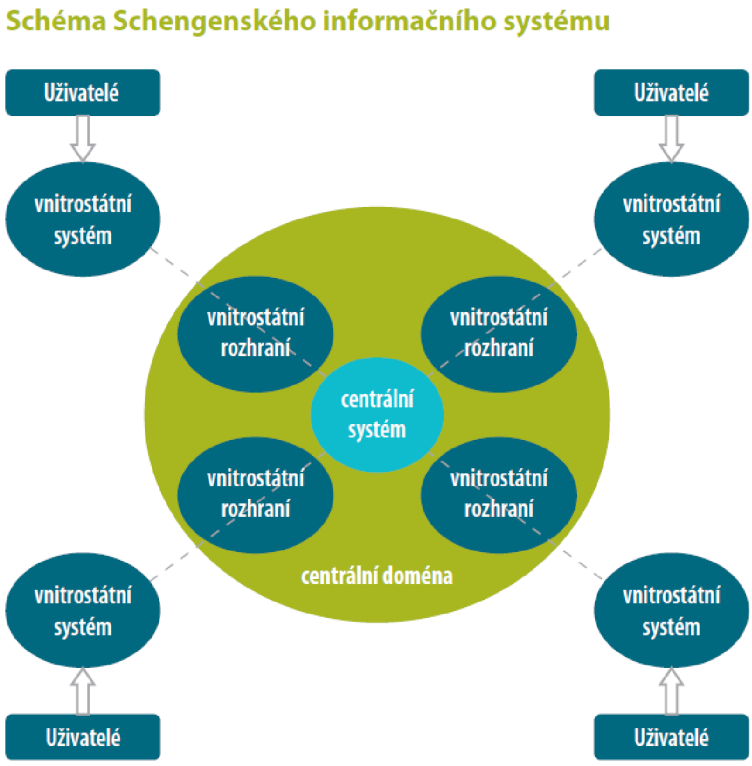
- centrální část (CS-SIS),
- vnitrostátní systém (N.SIS), který komunikuje s centrálním systémem,
- komunikační infrastruktura, která zajišťuje šifrovanou virtuální síť mezi systémy CS-SIS a N.SIS.

[26] PŠENICA, Tomáš. *Informační systémy ochrany vnějších hranic české republiky*. Příbram, 2021. Bakalářská práce. VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE. Vedoucí práce Mgr. Petr Malovec, Ph.D. s. 38.
[27] Nařízení Evropského parlamentu a Rady (EU) 2018/1860 ze dne 28. listopadu 2018. In: EUR-Lex. Dostupné z WWW: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32018R1860&qid=1702894686796.
[28] Commission Nationale de l'Informatique et des Libertés. *SIS II: Schengen Information System II* [online]. červen 2021 [cit. 2023-11-30]. Dostupné z WWW: https://www.cnil.fr/en/sis-ii-schengen-information-system-ii.

Databáze obsahuje záznamy o hledaných osobách na základě evropského zatýkacího rozkazu, pohřešované osoby, jinak důležité osoby (svědci), dále vozidla, plavidla, letadla nebo kontejnery za účelem specifických kontrol a věci spojené s páchání závažné trestné činnosti. V roce 2019 bylo obsaženo v databázi SIS 91 milionů záznamů a byla předmětem 6,6 miliardy dotazů ze strany všech členských států.

Provoz toho systému upravuje Nařízení Evropského parlamentu a Rady (EU) 2018/1860 ze dne 28. listopadu 2018 o využívání Schengenského informačního systému při navracení neoprávněně pobývajících státních příslušníků třetích zemí, Nařízení Evropského parlamentu a Rady (EU) 2018/1861 ze dne 28. listopadu 2018 o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti hraničních kontrol, o změně Úmluvy k provedení Schengenské dohody a o změně a zrušení nařízení (ES) č. 1987/2006, Nařízení Evropského parlamentu a Rady (EU) 2018/1862 ze dne 28. listopadu 2018 o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti policejní spolupráce a justiční spolupráce v trestních věcech, o změně a o zrušení rozhodnutí Rady 2007/533/SVV a o zrušení nařízení Evropského parlamentu a Rady (ES) č. 1986/2006 a rozhodnutí Komise 2010/261/EU.

Obrázek 2 - Schéma SIS



Zdroj: (Evropská komise, GŘ pro vnitřní věci)

3.4.3 VIS – Vízový informační systém

VIS vznikl za účelem společné vízové politiky, kdy umožňuje schengenským státům výměnu údajů o vízech.[29] Podporuje agendu krátkodobých (a v budoucnu i dlouhodobých) víz od podání žádosti o vízum po kontrolu na hranicích i na území. Je pouze pro občany třetích zemí. Obsahuje alfanumerická i biometrická data.[30]

Hlavním smyslem VIS jsou rozhodnutí o zamítnutí, prodloužení, zrušení, jakož i ověřování a identifikace žadatelů a držitelů víz. Účelem je převážně:

- usnadnit postup žádosti o vízum,
- zabránit žádostem o více víz,
- usnadnit boj proti podvodům,
- usnadnit kontroly na vnějších hraničních přechodech a na území členských států,
- pomáhat při identifikaci jakékoli osoby, která nemusí nebo již nemusí splňovat podmínky pro vstup, pobyt nebo pobyt na území členských států,
- usnadnit aplikaci nařízení Dublin II pro určení země Evropské unie odpovědné za kontrolu žádosti o azyl podané občanem z cizí země a za kontrolu uvedené žádosti,
- přispět k prevenci ohrožení vnitřní bezpečnosti kteréhokoli z členských států.

Architektura VIS je tvořena:[31]

- Centrálním částí (CS-VIS),
- vnitrostátní částí (NS-VIS), která komunikuje s centrálním systémem.

VIS zaznamenává v průměru více než 1,5 milionů žádostí o víza měsíčně. V roce 2019 bylo v prvních 9 měsících zpracováno více než 3,5 milionů dotazů z hraničních kontrol

[29] EUROPAN COMMISSION. *VIS – Visa Information System* [online] European Commission [cit. 2023-12-01]. Dostupné z WWW: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en.
[30] Nařízení Evropského parlamentu a Rady (ES) č. 767/2008 ze dne 9. července 2008. In: EUR-Lex. Dostupné z WWW: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32008R0767&qid=1702894545050.
[31] Commission Nationale de l'Informatique et des Libertés. *Visa Information Systém (VIS)* [online]. červen 2021 [cit. 2023-11-30]. Dostupné z WWW: https://www.cnil.fr/en/visa-information-system-vis.

v první kontrolní linii. Informace obsažené ve VIS jsou uchovávány po dobu maximálně pěti let. S vloženými informacemi může v rámci VIS nakládat pouze vkladatelská země.

Provoz tohoto systému upravuje Nařízení Evropského parlamentu a Rady (ES) č. 767/2008 ze dne 9. července 2008 o Vízovém informačním systému (dále jen „VIS“) a o výměně údajů o krátkodobých vízech mezi členskými státy (nařízení o VIS).

3.4.4 EURODAC

Eurodac je databáze EU, která podporuje agendu azylu a imigrace. Funguje pouze pro občany třetích zemí a jako podpora dublinských dohod, které jsou postaveny na podstatě podání žádosti o azyl v první bezpečné zemi, do které žadatel přicestoval. Eurodac obsahuje pouze biometrická data (otisky), v budoucnu bude obsahovat i alfanumeriku.[32] Kromě biometrických dat obsahuje i referenční číslo vkladatelského státu. Toto číslo umožňuje vkladatelskému státu propojit data v systému.[33]

Architektura je tvořena:[34]

- Centrální databází otisků prstů, který se skládá z centrální jednotky a záložního plánu a systému,
- Komunikační infrastrukturou mezi centrálním systémem a členskými státy, která zajišťuje šifrovanou virtuální síť.

Jedná se o vůbec první nadnárodní biometrický systém na světě, který funguje nepřetržitě od roku 2003. Od té doby prošel řadou aktualizací a jeho rozšiřováním. První v roce 2009, kdy byla navýšena kapacita databáze z 1,6 milionů na 2,8 milionů záznamů. Další následovala v roce 2015 (Eurodac Recast) zavedením přesnějšího algoritmu shody a navýšením kapacity databáze zprvu na 3,6 milionů záznamů a poté na 5 milionů záznamů. V současné době databáze je na úrovni 7 milionů záznamů, a přesto zajišťuje vysoký stupeň přesnosti při vyhledávání typu „one-to-many“.

---

[32] Nařízení Evropského parlamentu a Rady č. 603/2013 ze dne 26. 6. 2013. In: EUR-Lex. Dostupné z WWW: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32013R0603&qid=1702894396285.
[33] van der Ploeg, I. The illegal body: `Eurodac' and the politics of biometric identification. Ethics and Information Technology 1, 295–302 (1999). [cit. 2023-12-18]. Dostupné z WWW: https://doi-org.infozdroje.czu.cz/10.1023/A:1010064613240.
[34] Nařízení Evropského parlamentu a Rady č. 603/2013 ze dne 26. 6. 2013. In: EUR-Lex. Dostupné z WWW: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32013R0603&qid=1702894396285.

Díky unikátnímu workflow se Eurodac liší od mnoha jiných systémů AFIS (Automatic Fingerprint Identification System).[35]

V roce 2021 bylo v databázi Eurodac přes 5,8 milionů souborů údajů o otiscích prstů a systém zpracoval přes 855 tisíc transakcí.[36]

Provoz toho systému upravuje Nařízení Evropského parlamentu a Rady č. 603/2013 ze dne 26. 6. 2013 o zřízení systému EURODAC (dále jen „EURODAC“) pro porovnávání otisků prstů za účelem účinného uplatňování nařízení EU č. 604/2013.

3.4.5 Analýza současných problémů a nutnost reagovat

Vzhledem k dynamickým změnám v bezpečnostní situaci v Evropské unii se ukázalo, že stávající funkcionality SIS, VIS a Eurodac nedokáží kompletně pokrýt všechny bezpečnostní potřeby. V reakci na tuto výzvu bylo na úrovni EU rozhodnuto o realizaci následujících aktivit, které mají za cíl odstranit aktuální bezpečnostní mezery:[37]

a. výrazná úprava (rozšíření funkcionalit) stávajících systémů SIS, VIS a Eurodac – tzv. SIS Recast, VIS Recast a Eurodac Recast,
b. vybudování nových evropských IS – EES, ETIAS a ECRIS-TCN,
c. vybudování nástrojů interoperability, které zajistí provázanost a účinnější využívání všech šesti evropských IS, mj. za účelem odhalování vícenásobných totožností, zvýšení efektivity hraničních kontrol a snadnější využívání evropských IS pro účely prevence, odhalování a vyšetřování teroristických a jiných závažných trestných činů.

[35] Pozn. autora: Sytém AFIS se v ČR využívá pro sběr otisků prstů u žadatelů o azyl a je propojen se systémem Eurodac.
[36] THALES. Thales. *Eurodac: the European Union's first multinational biometric system* [online]. 2023, 24.5. 2023 [cit. 2023-12-02]. Dostupné z: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/eurodac.
[37] DOMANJA, Jindřich. Úvod do interoperability. PDF. Policie ČR, 2021.

Mezi hlavní problémy evropských informačních systémů, které si vyžadují reakci patří:

- problém s vyhlašováním celoevropských pátrání po neznámých osobách, věcech a objektech, a s neefektivním využíváním biometrických údajů – nutnost rozšíření SIS (SIS recast),
- absence jednotného a systematického přístupu k vydávání dlouhodobých víz a povolení k pobytu, a efektivního využívaní fotografií v celém vízovém procesu – nutnost rozšíření VIS (VIS Recast),
- absence systematického shromažďování dat o osobách v rámci azylového a imigračního procesu – nutnost rozšíření Eurodacu (Eurodac Recast),
- absence systematického evidování vstupů a výstupů třetizemců do a z EU, včetně evidence délky pobytu – nutnost zřízení nového systému EES,
- absence informací o nevízových třetizemcích v době, než přicestují na vnější hranici – nutnost zřízení nového systému ETIAS,
- absence systematického shromažďování údajů o odsouzených třetizemcích – nutnost zřízení nového systému ECRIS-TCN,
- neefektivní odhalování zneužité totožnosti napříč evropskými systémy a nesnadného přístupu orgánů vymáhající právo do databází evropských informačních systémů – nutnost zřídit nástroje interoperability.

Nově budované informační systémy v rámci interoperability jsou:

- **Entry/Exit**,
- Systém **ETIAS**,
- **ECRIS-TCN**.

Tyto systémy budou fungovat na obdobné architektuře jako SIS, VIS a Eurodac. To znamená, že centrální část bude provozovat agentura eu-LISA, národní součást každý členský stát samostatně. Komunikace mezi národní a centrální součástí bude zajištěna prostřednictvím příslušného ICD.[38]

[38] DOMANJA, Jindřich. Úvod do interoperability. PDF. Policie ČR, 2021.

3.4.6 ETIAS – Evropský systém pro cestovní informace a povolení

ETIAS je předcestovní autorizační systém, který spravuje agendu cestovních povolení pro občany třetích zemí, kteří jsou osvobozeni od vízové povinnosti, od podání žádosti po kontrolu na hranicích i pozdější kontroly na území Schengenského prostoru. Obsahuje jen alfanumerická data.[39]

Hlavním cílem systému je ověření, zda občan třetí země splňuje vstupní požadavky v případě, že cestuje do Schengenského prostoru. Takovýto občan musí před cestou zažádat skrze online aplikaci o cestovní povolení. Díky tomu dochází k posouzení rizik nelegální migrace, kontroly bezpečnosti nebo veřejného zdraví.[40] ETIAS za tímto účelem bude porovnávat vložená data mj. se záznamy v SIS. V případě shody mezi osobními údaji může dojít ke třem situacím. První zahrnuje automatické zamítnutí žádosti (vstupu na území), ve druhém případě může dojít k situaci, kdy musí být žádost vyřešena manuálně národní jednotkou příslušného členského státu, který rozhoduje, zda vydat cestovní povolení či nikoliv. Ve třetím případě může nastat skutečnost, že se jedná o hledanou osobu za účelem zatčení nebo předání, anebo záznamem pro skrytou nebo zvláštní kontrolu, což by nemělo být překážkou pro vydání cestovního povolení. Systém povolení vydá a následně bude vyžadovat po příslušném členském státě opatření v souladu s rozhodnutím Rady 2007/533/SVV.

Architektura je tvořena:[41]

- centrální částí, zahrnující seznam zájmových osob,
- vnitrostátní částí, která komunikuje s centrálním systémem a ústředními přístupovými body ostatních členských států,
- komunikační infrastrukturou, která zajišťuje šifrovanou virtuální síť mezi systémy,

---

[39] Nařízení Evropského parlamentu a Rady (EU) 2018/1240 ze dne 12. září 2018. In: EUR-Lex. Dostupné z WWW: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32018R1240&qid=1702894199558.

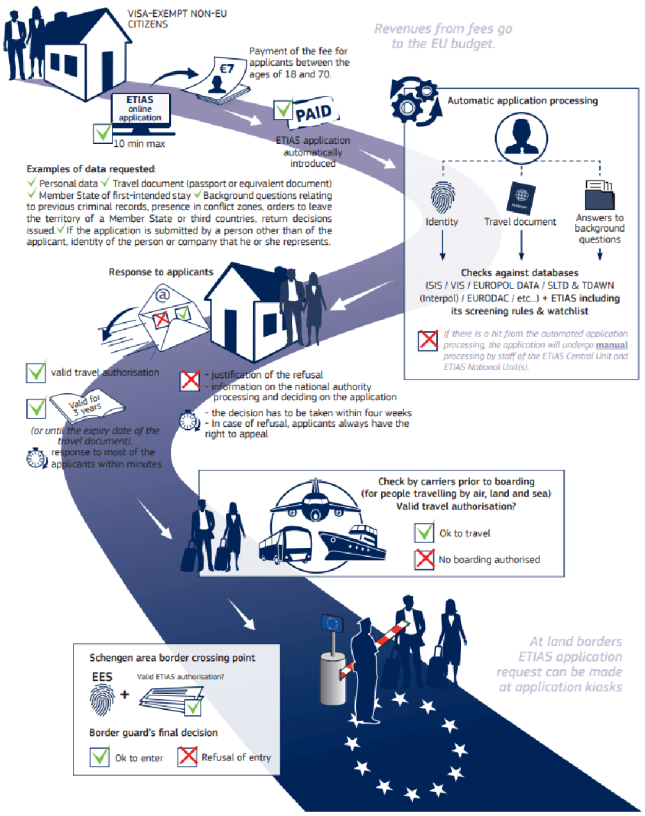
[40] Rada evropské unie. *Evropský systém pro cestovní informace a povolení (ETIAS): Rada přijala nařízení* [online]. 2018 [cit. 2023-12-02]. Dostupné z WWW: https://www.consilium.europa.eu/cs/press/press-releases/2018/09/05/european-travel-information-and-authorisation-system-etias-council-adopts-regulation/.

[41] Nařízení Evropského parlamentu a Rady (EU) 2018/1240 ze dne 12. září 2018. In: EUR-Lex. Dostupné z https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32018R1240&qid=1702893480081.

- zabezpečenou komunikační infrastrukturou mezi centrálním systémem a ostatními IS interoperability a údaji Europolu,
- veřejnými internetovými stránkami a aplikací pro mobilní zařízení,
- e-mailovými službami,
- zabezpečeným uživatelským účtem pro žadatele,
- nástrojem pro verifikaci uživatelů,
- nástrojem pro udělení/odvolání souhlasu s uchováním údajů,
- přístupem pro dopravce,
- centrálního uložiště údajů pro účely hlášení a statistik.

ETIAS bude využívat hardwarové a softwarové prvky systému EES v maximální možné míře.

Obrázek 3 - ETIAS – jak to funguje



Zdroj: (Evropská komise)

Níže zmíněné informace vycházejí z Nařízení Evropského parlamentu a Rady (EU) 2018/1240 ze dne 12. září 2018, kterým se zřizuje Evropský systém pro cestovní informace a povolení (ETIAS) a kterým se mění nařízení (EU) č. 1077/2011, (EU) č. 515/2014, (EU) 2016/399, (EU) 2016/1624 a (EU) 2017/2226.

3.4.7 EES – Systém vstupu a výstupu

EES představuje jednotný informační systém, který podporuje agendu hraniční kontroly – kontroluje, zda osoba má platné vízum (ve VIS) či cestovní povolení (v ETIAS) a zaznamenává rozhodnutí policisty o vstupu, výstupu či odepření vstupu osoby. Zároveň kontroluje, zda osoba, která na území vstoupila, opustila území v legislativně definované lhůtě. Je pouze pro občany třetích zemí překračujících vnější hranice, kteří nemají trvalý pobyt na území členských států. Obsahuje alfanumerická i biometrická data.[42]

Oproti VIS, který se týká pouze občanů s vízovou povinností, je cílem EES vytvořit databázi pro všechny ostatní. V duchu „bona fide“ bude EES zaměřen na prevenci a odhalování teroristických či jinak závažných trestných činů. Vyšetřujícím orgánům bude umožňovat konzultaci přeshraničních pohybů a přístup k datům o cestovní historii. Důvodem existence EES je i mimo jiné očekávaný nárůst cestování občanů třetích zemí. Důležitou součástí systému je biometrie, která kombinuje čtyři otisky prstu a portrét pro rozpoznávání obličeje při vstupu na území. Záznamy k osobě v EES také nahradí razítka udělovaná do cestovního dokladu, čímž eliminuje jejich padělání. Výrazné zefektivnění hraniční kontroly bude probíhat i skrze eGates a samoobslužných kiosků a to nejen na letištích, ale i u námořních terminálů a pozemních hraničních přechodů.

Architektura EES je skládá z:[43]

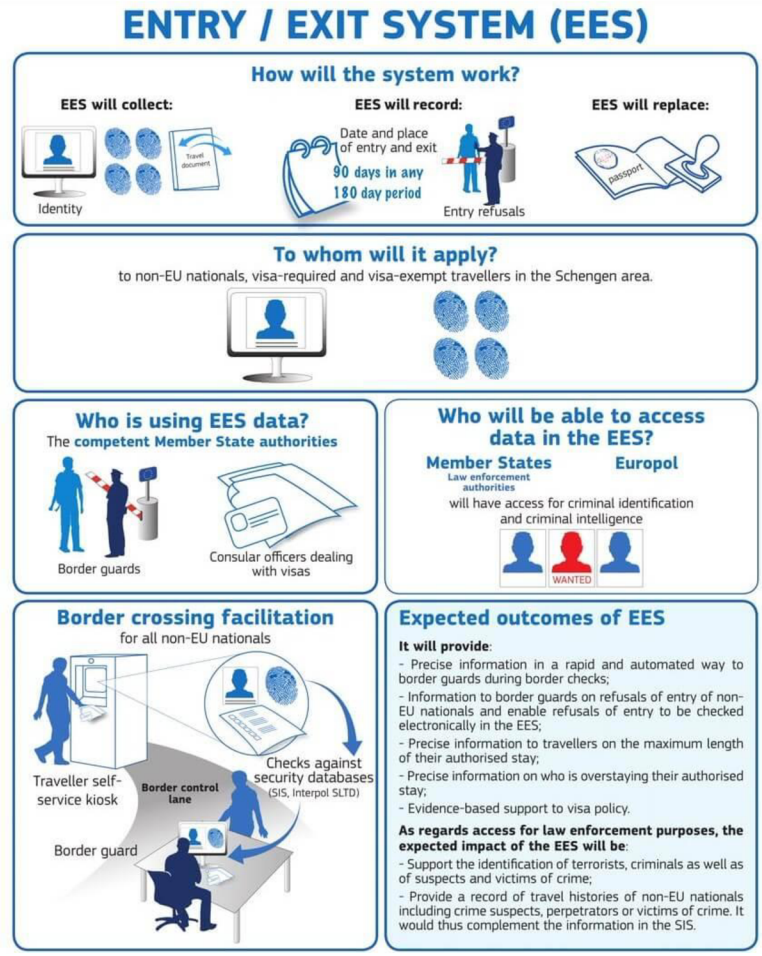
- Centrální části,
- vnitrostátní části, která komunikuje s centrálním systémem,

[42] Nařízení Evropského parlamentu a Rady (EU) 2017/2226 ze dne 30. listopadu 2017. In: EUR-Lex. Dostupné z WWW: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32017R2226&qid=1702893339440.

[43] THALES. *The Schengen Entry/Exit System: biometrics to facilitate smart borders* [online]. [cit. 2023-12-02]. Dostupné z: WWW https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/eborder/entry-exit-systém.

- komunikační infrastrukturou, která zajišťuje šifrovanou virtuální síť mezi systémy,
- zabezpečeného komunikačního kanálu mezi centrálním systémem EES a centrálním systémem VIS,
- webové služby pro uživatele, která slouží ověření počtu dnů strávených v Schengenském prostoru,
- centrálního uložiště dat.

Obrázek 4 - Entry/Exit systému



Zdroj: (schengenvisainfo.com)

Provoz toho systému upravuje Nařízení Evropského parlamentu a Rady (EU) 2017/2226 ze dne 30. listopadu 2017, kterým se zřizuje Systém vstupu/výstupu (dále jen „EES“) pro registraci údajů o vstupu a výstupu a údajů o odepření vstupu, pokud jde o státní příslušníky třetích zemí překračující vnější hranice členských států, kterým se stanoví

podmínky přístupu do systému EES pro účely vymáhání práva a kterým se mění Úmluva k provedení Schengenské dohody a nařízení (ES) č. 767/2008 a (EU) č. 1077/2011.

3.4.8 ECRIS-TCN – Evropský informační systém rejstříku trestů

ECRIS-TCN doplní současný systém ECRIS, který spravuje agendu rejstříku trestů, o databázi občanů třetích zemí odsouzených u trestních soudů EU. A dojede k centralizaci dat. Obsahuje alfanumerická i biometrická data.

Cílem systému je zajistit přístup k detailním informacím soudcům, státním zástupcům a dalším orgánům činným v trestním řízení o trestní historii daného občana, což je klíčové v boji proti přeshraniční kriminalitě. Rozšíření systému ECRIS o „TCN“ z důvodu připravenosti implementování do interoperability.[44]

Provoz toho systému upravuje Nařízení Evropského parlamentu a Rady (EU) 2019/816 ze dne 17. dubna 2019, kterým se zřizuje centralizovaný systém pro identifikaci členských států, jež mají informace o odsouzeních státních příslušníků třetích zemí a osob bez státní příslušnosti (ECRIS-TCN), na doplnění Evropského informačního systému rejstříků trestů, a kterým se mění nařízení (EU) 2018/1726.

3.5 Interoperabilita informačních systémů

Problém výše uvedených systémů je jejich izolovanost a oddělenost, neboť byly vyvíjeny a implementovány nezávisle na sobě bez možnosti vzájemného sdílení a porovnávání uložených dat.[45] Ať z důvodů historických, legislativních, ochrany osobních údajů nebo jiných. Toto se ukázalo jako bezpečnostní riziko na případu občana asijského původu, jenž v roce 2013 na konzulátu v jeho zemi zažádal o schengenské vízum, které legálně získal. Na základě čehož byl zaveden do VIS, včetně otisků prstů. Poté pod jeho pravou identitou přicestoval do Evropy a poté cestoval do další země, kde požádal místní imigrační agenturu o azyl, avšak už pod padělanou identitou, a byl ztotožněn v EURODACu, a kdyby se bývala data z EURODACu porovnala s daty ve VIS, zjistilo by se, že se jedná o zneužitou totožnost a útoku by se zřejmě předešlo, protože by byl podle Dublinské úmluvy

[44] EU-LISA. *European Criminal Records Information System – Third Country Nationals* [online]. 2019 [cit. 2023-12-02]. Dostupné z: https://www.eulisa.europa.eu/Publications/Information%20Material/Leaflet%20ECRIS-TCN.pdf.
[45] Jurnal Kajian Ilmu Hukum dan Syariah. Volume 8, Number 2, 2023. P-ISSN: 2502-8006 E-ISSN: 2549-8274. [cit. 2023-12-21]. DOI: https://doi.org/10.22373/petita.v8i2.214.

vrácen do státu prvotního vstupu a následně s největší pravděpodobností deportován zpět do své vlasti. Místo toho ale řešili jeho případ imigrační úřady země, do které přicestoval pod falešnou identitou a tam měl čas a možnosti se připravit na teroristický útok, který následně spáchal. Poté, co vyšly najevo všechny okolnosti předcházející jeho činu, se urychlila myšlenka na realizaci interoperability evropských informačních systémů, aby se v co největší míře takovýmto věcem zamezilo.

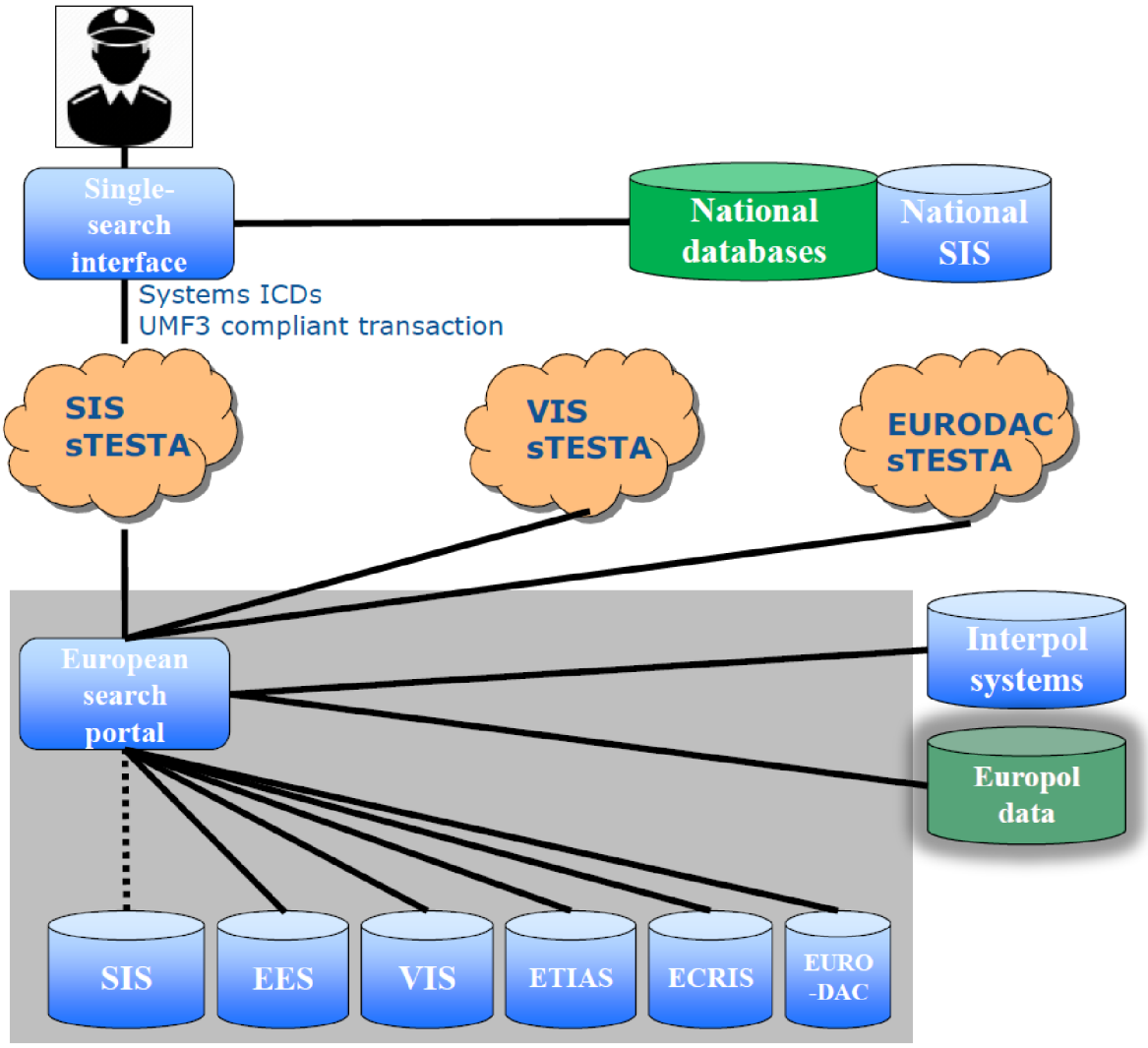
V důsledku toho přijala Evropská unie v květnu 2019 dvě nařízení: Nařízení Evropského parlamentu a Rady (EU) 2019/817 ze dne 20. května 2019, kterým se zřizuje rámec pro interoperabilitu mezi informačními systémy EU v oblasti hranic a víz a mění nařízení Evropského parlamentu a Rady (ES) č. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 a (EU) 2018/1861 a rozhodnutí Rady 2004/512/ES a 2008/633/SVV a Nařízení Evropského parlamentu a Rady (EU) 2019/818 ze dne 20. května 2019, kterým se zřizuje rámec pro interoperabilitu mezi informačními systémy EU v oblasti policejní a justiční spolupráce, azylu a migrace a kterým se mění nařízení (EU) 2018/1726, (EU) 2018/1862 a (EU) 2019/816, které pomohou:[46]

- s odhalováním bezpečnostních hrozeb,
- se zamezením zneužívání totožnosti,
- k lepšímu zabezpečení vnějších hranic,
- s řešením a eliminací nelegální migrace.

Interoperabilita informačních systémů usnadní vzájemné doplňování, umožní efektivní ověřování totožnosti osob a přispěje k účinnějšímu potírání podvodného zneužívání totožnosti. Zároveň nová nařízení nemění existující přístupová práva uvedená v právním základu pro jednotlivé evropské informační systémy. Evropský vyhledávací portál bude informovat o případech, kdy byly k danému vyhledávání nalezeny relevantní údaje nebo propojení. Nicméně každému orgánu zobrazí pouze údaje, ke kterým již má oprávnění podle předchozích právních předpisů, na jejichž základě byly jednotlivé databáze zřízeny.

[46] RADA EVROPSKÉ UNIE. *Interoperabilita mezi informačními systémy EU* [online] [cit. 2023-11-22]. Dostupné z WWW: https://www.consilium.europa.eu/cs/press/press-releases/2019/02/05/interoperability-between-eu-information-systems-council-presidency-and-european-parliament-reach-provisional-agreement.

Obrázek 5 - Ukázka propojenosti systémů



Zdroj: (Evropská komise)

3.5.1 Nové nástroje interoperability

K výše uvedeným problémům se přidává ještě problém s peer-to-peer architekturou zmíněných systémů z hlediska ekonomické výhodnosti, udržitelnosti a spravovatelnosti, neboť vyžaduje samostatné rozhraní pro každý systém, s nímž je komunikováno a v případě změny rozhraní jednoho systému jsou nutné úpravy ve všech dotčených systémech, což je velice nevhodné v takovémto měřítku.

Všechny výše uvedené problémy a nedostatky mají být překonány komponentami interoperability, které vyplývají z nařízení o interoperabilitě. Jsou jimi čtyři hlavní komponenty:[47]

- **CIR** – ukládá na jednom místě údaje o totožnosti ze všech systémů kromě SIS, tj. z EES, VIS, ETIAS, ECRIS-TCN, EDAC,
- **sBMS** – porovnává biometrické údaje (otisky i fotka obličeje) napříč všemi systémy kromě ETIAS, tj. SIS, EES, VIS, ECRIS-TCN, EDAC,
- **MID** – uchovává linky (propojení) mezi totožnostmi v různých systémech, které patří stejné osobě,
- **ESP** – slouží jako jednotný back-endový systém pro přístup ke všem výše uvedeným centrálních systémů a navíc k systémům Europolu a Interpolu.

CIR – The Common Identity Repository

Představuje sdílené úložiště pro identifikační údaje, údaje o cestovních dokladech a biometrická data osob zapsaných v EES (Entry-Exit System), VIS (Visa Information System), ETIAS (European Travel Information and Authorization System), Eurodac a ECRIS-TCN (European Criminal Records Information System for Third-Country Nationals). Bude mít kapacitu uchovávat záznamy o až 300 milionech jednotlivců a nahradí centrální systémy EES, VIS, ETIAS, Eurodac a ECRIS-TCN v uchovávání příslušných dat. Každý soubor v CIR by měl obsahovat alespoň jeden biometrický identifikátor (kormě ETIAS) a základní data o totožnosti osoby, což odpovídá informacím na čipu biometrického pasu.

Hlavním účelem CIR bude usnadňovat a pomáhat při správné identifikaci osob. Dále bude přístupný národním orgánům v případě přírodní katastrofy, nehody nebo teroristického útoku za účelem identifikace neznámých osob nebo neidentifikovaných lidských pozůstatků. Zároveň bude podporovat fungování MID a bude zjednodušovat přístup národních orgánů

[47] PICUM. *Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status*. PDF. [online]. 2019 [cit. 2023-11-29]. Dostupné z WWW: https://picum.org/wp-content/uploads/2019/11/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf.

a Europolu k EES, Eurodac, ETIAS a VIS za účelem prevence, odhalování nebo vyšetřování teroristických činů nebo vážných trestných činů.

sBMS – The shared Biometric Matching Service

BMS bude uchovávat biometrické údaje z pěti EU databází (mimo ETIAS). Zároveň se tato komponenta stane centrální infrastrukturou nahrazující centrální systémy EES, VIS, SIS, Eurodac a ECRIS-TCN, co se týče uchovávání biometrických šablon a umožňování vyhledávání pomocí biometrických dat.

BMS bude komunikovat s CIR a centrální databází SIS. Zatímco obličejové snímky a otisky prstů zůstanou v základních systémech, šablony vytvořené z těchto dat se přenesou do BMS. BMS bude sloužit k překrývání a porovnávání šablon, které neidentifikují jednotlivce, ale umožňují identifikaci podle shody s daty v jednom či více systémech.

Bez BMS by provedení biometrického porovnávání pomocí CIR a MID nebylo možné, protože distribuce biometrických dat do různých systémů by vyžadovala vyhledávání ve všech ostatních systémech k detekci existence dat o téže osobě.

MID – The Multiple-Identity Detector

MID má za úkol kontrolovat, zda jsou vkládaná či aktualizovaná identifikační data o totožnosti osoby přítomná ve více systémech (Eurodac, VIS, EES, ETIAS a ECRIS-TCN), včetně SIS. MID bude aktivován při vytváření nebo aktualizaci dat v EES, VIS nebo ETIAS, při vytváření nebo aktualizaci dat v SIS a při vytváření nebo změně záznamu v ECRIS-TCN. Ve všech těchto případech se využije BMS k porovnání biometrických dat napříč databázemi EU, a CIR a SIS k provedení stejného porovnání údajů o totožnosti osoby a cestovních dokladů.

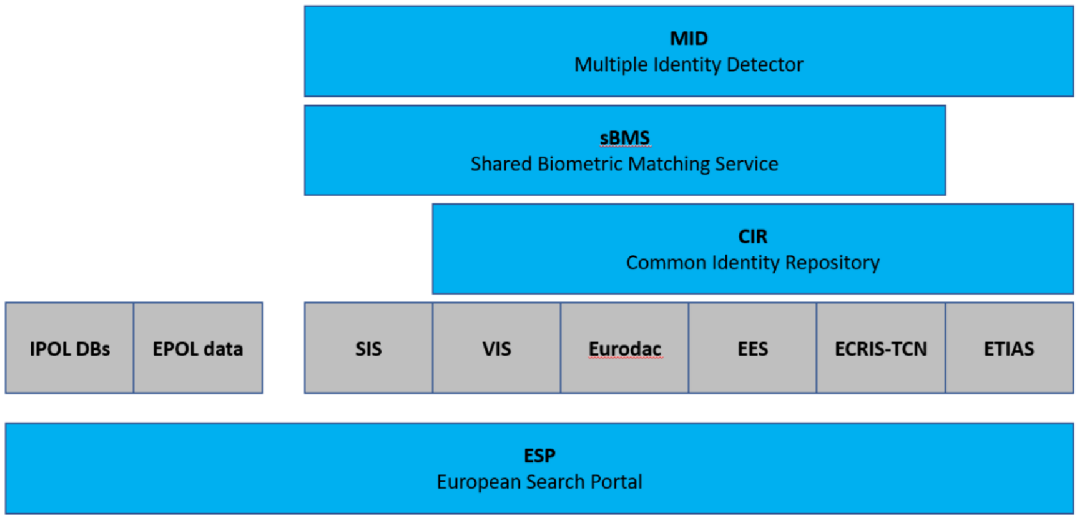
ESP – European Search Portal

ESP se bude skládat z centrální infrastruktury, zahrnující vyhledávací portál umožňující simultánní dotazování v EES, VIS, ETIAS, Eurodac, SIS, ECRIS-TCN, a také údajů Europolu a Interpolu. Zahrnuje též zabezpečené komunikační kanály mezi ESP, národními a EU orgány, ostatními relevantními databázemi a informačními systémy. Umožní vyhledávání pomocí alfanumerických nebo biometrických údajů a stane se výchozím "způsobem přístupu" pro ověřené uživatele ke všem připojeným databázím

a informačním systémům. Zároveň zjednoduší vyhledávání v příslušných databázích a informačních systémech.

Dle nařízení o IO nesmí ESP poskytovat informace, ke kterým uživatel nemá oprávnění přístupu podle platného práva Unie a národních předpisů, čímž je zajištěno bezpečné nakládání s osobními údaji uvedenými v evropských databází a případné jejich zneužití.

Obrázek 6 - Ukázka rozsahu komponent interoperability



Zdroj: (Policie České republiky, Úvod do Interoperability)

Komunikace mezi centrálními a národními součástmi evropských IS zpravidla pracují na bázi komunikačního vzoru Request – Response, čehož se týká drtivá většina obsahu ICD. Request (požadavek) jde od klienta na server. Response (odpověď) jde od serveru ke klientovi. Pokud však NS-IO žádá prostřednictvím ESP, vystupuje v roli klienta**.** Při určování role „server/klient“ je stěžejním faktorem, v jaké fázi procesu se nacházíme. Vždy je důležité určit pro daný proces, jaký systém je klientem a jaký serverem (kdo komu poskytuje data), neboť jeden systém může být klientem pro jeden systém a serverem pro systém druhý.

Všechny uvedené nástroje interoperability budou budovány na centrální úrovni, což znamená, že jejich implementace, provoz a rozvoj budou kompetenci agentury eu-LISA

a nikoli členských států. Podle nařízení o interoperabilitě má každý členský stát povinnost zajistit mimo jiné:[48]

- připojení ke komunikační struktuře ESP a CIR,
- začlenění stávajících vnitrostátních systémů a infrastruktur do ESP, CIR a MID,
- organizaci, správu, provoz a údržbu své stávající infrastruktury a jejího s nástroji interoperability.[49]

Vzhledem ke skutečnosti, že nařízení o interoperabilitě nařizuje pouze povinnost členských států připojení se ke službám ESP a CIR a neříká už jakým způsobem, nabízí se vícero možností. ČR si zvolila variantu samostatné národní komponenty interoperability (NS-IO), která bude komunikovat se službami ESP a CIR. Z důvodu přihlížení k těmto problémům:

- národní bezpečnost,
- ekonomická efektivnost,
- gesce,
- testování,
- administrativa.

V detailnějším pohledu lze národní součást interoperability ještě více rozdělit na takzvanou:

- „Evropskou interoperabilitu – Gateway“ (připojení k ESP a CIR) – kdy dochází ke komunikaci mezi národním a centrálním systémem,
- „Národní interoperabilitu“ - kdy dochází ke komunikaci mezi národními systémy (dotazovací služby, logování, autentizace).

[48] DOMANJA, Jindřich. Úvod do interoperability. PDF. Policie ČR, 2021.
[49] Nařízení Evropského parlamentu a Rady (EU) 2019/817 ze dne 20. května 2019. In: EUR-Lex. Dostupné z WWW: https://eur-lex.europa.eu/legal-ontent/CS/TXT/?uri=CELEX%3A32019R0817&qid=1702893022208.

3.5.2 Praktický příklad využití interoperability

V této části bude obecně a zjednodušeně popsán krok po kroku dotaz z českého policejního systému např. KODOX do jednoho z evropských informačních systémů pomocí interoperability.

1. Koncový uživatel (fyzická osoba) zadá dotaz do front-endového dotazovacího systému.
2. Dotazovací systém volá dotazovací službu NS-IO.
3. NS-IO přijme požadavek na provedení dotazu.
4. NS-IO provede kontrolu oprávněnosti požadavku.
5. NS-IO provede kontrolu priority požadavku.
6. NS-IO požadavek zaloguje v souladu s nařízením o IO.
7. NS-IO kontroluje splnění definovaných byznys pravidel.
8. NS-IO přepošle dotaz do cílových IS v souladu s příslušným dotazovacím profilem a byznys pravidly.
9. Dotázané cílové systémy paralelně realizují požadované dotazy a vrátí odpověď do NS-IO.
10. NS-IO příjme odpovědi od dotázaných systémů.
11. NS-IO odpovědi zaloguje v souladu s nařízením o IO.
12. NS-IO zašle odpovědi zpět front-endovému dotazovacímu systému, který požadavek inicioval.[50]

Podobným způsobem bude probíhat veškerá komunikace mezi národními systémy policie do centrální součásti interoperability tak, aby byly vráceny relevantní odpovědi při dodržení všech zákonných pravidel.

V předložené práci jsou použity zdroje, které nepodléhají žádnému stupni utajení.

[50] DOMANJA, Jindřich. Úvod do interoperability. PDF. Policie ČR, 2021.

4 Praktická část

4.1 Přínosy evropských informačních systémů pro PČR

Tato kapitola je pojata jako případová studie a bude se zabývat přínosy používání evropských policejních informačních systémů a nástrojů interoperability pro Policii České republiky. Toto řešení přinese policii bezesporu spoustu výhod, už vzhledem ke stávající situaci, kdy je většina jejích systémů vzájemně neprovázaných, jak bylo již zmíněno v teoretické části této práce.

Jmenovanými přínosy jsou:

1. **Efektivita** – integrace do evropských policejních systémů umožní rychlou výměnu informací mezi členskými státy. To povede k efektivnějšímu sledování a řešení trestné činnosti, zejména pokud jde o přeshraniční zločiny, což může být klíčové a rychlé reakce na možné hrozby.

2. **Bezpečnostní spolupráce** – využívání evropských policejních systémů umožní lepší spolupráci mezi policejními složkami členských států. Tím se zvýší celková bezpečnost a zlepší se schopnost odhalování a prevence trestné činnosti a teroristických činů.

3. **Efektivnější vyšetřování** – sdílení informací a přístup k evropským databázím usnadní vyšetřování mnohých trestných činů. Orgány mohou rychleji identifikovat podezřelé osoby a více spolupracovat v boji proti trestné činnosti.

4. **Lepší ochrana vnějších hranic EU/ČR** – integrace policejních systémů umožní účinnější sledování a kontrolování pohybu osob přes hranice. Což je zásadní pro prevenci nelegální migrace a dalších potenciálních hrozeb, jež by mohly překročit národní hranice a odhalování přeshraniční trestné činnosti.

5. **Přístup k moderním technologiím** – zavádění evropských policejních systémů přinese přístup k moderním technologiím a analytickým nástrojům, které usnadní sběr a vyhodnocování dat.

6. **Standardizace postupů** – evropské policejní systémy mohou přispět k vytvoření a udržování standardizovaných postupů v oblasti policie, což může usnadnit koordinaci mezi členskými zeměmi a zlepšit interoperabilitu.

7. **Jednotné rozhraní** – zajistí, že systémy budou komunikovat a vyměňovat si data bez problémů a odpovědi na dotazy budou pro všechny stejné (jednotné), bez ohledu na to, odkud pocházejí nebo v jakém formátu jsou. Data budou tedy navzájem kompatibilní. To zvýší rychlost a účinnost výměny informací, což bude mít za následek lepší spolupráci a koordinaci při zajišťování bezpečnosti a v boji proti trestné činnosti na celoevropské úrovni.

8. **Zlepšení spolupráce** – používání stejných nebo interoperabilních policejních systémů zvýší možnosti spolupráce mezi různými policejními složkami a bezpečnostními agenturami v rámci celé EU. Což posílí schopnost reagovat na hrozby nejen české policii, ale celkově celému evropskému společenství.

9. **Vlastní vzdělávání – začleňování** evropských policejních systémů a interoperability bude mít celou řadu přínosů, které posílí bezpečnost, spolupráci a schopnost policie čelit moderním bezpečnostním výzvám na úrovni Evropské unie. To díky předávání informací a nástrojů od dodavatelů technologií, předávání znalostí od orgánů EU, vzájemná inspirace s kolegy ze zahraničí apod.

V detailnějším pohledu vyplývá, že větší část výše zmíněných přínosů přímo odráží model cílového stavu IT PČR, který Ministerstvo vnitra ČR shrnuje deseti body ve svém dokumentu „Základní charakteristika cílového stavu infrastruktury IT PČR“.[51]

4.2 Životní cyklus projektů evropských informačních systémů

V této kapitole případové studie bude analyzován cyklus evropských informačních systémů. Poté bude konkrétněji aplikován na projektu EES. V závěru této kapitoly bude provedeno porovnání s obecným cyklem „běžného“ informačního systému, jehož analýza byla popsána v kapitole 3.1.4 této práce.

[51] MINISTERSTVO VNITRA. *Základní charakteristika cílového stavu infrastruktury IT PČR.* PDF. [online]. [cit. 2024-01-18]. Dostupné z WWW: https://www.zakazky.mvcr.cz/document_78965/99b65d7a7d74d2fd3bad33f188c75473-priloha-c-2-zakladni-charakteristika-cilove-infrastruktury-it-pcr-pdf.

4.2.1 Obecné shrnutí cyklu evropských informačních systémů

Proces tvorby evropských informačních systémů je rozdělen do několika fází, stejně jako každý jiný infomační systém. V zásadě se téměř neliší od fází „běžného“ informačního systému, s výjimkou tvorby legislativy, podle které se evropské systémy musí řídit. Hlavní rozdíl najdeme v délce realizace projektů. U běžných projektů se doba realizace pohybuje maximálně do 5 let. Avšak u projektů evropských systémů se tato doba pohybuje kolem 15 let, což je značně neefektivní. Například vývoj systému SIS trval přes 10 let. A můžeme říci, že Evropa je v tomto směru nepoučitelná, protože při pohledu na jeden z posledních projektů, konkrétně systém EEE uplynulo už více než 15 let od první myšlenky na vytvoření tohoto systému s plánovaným spuštěním 6. 10. 2014 a dodnes není stále v provozu.

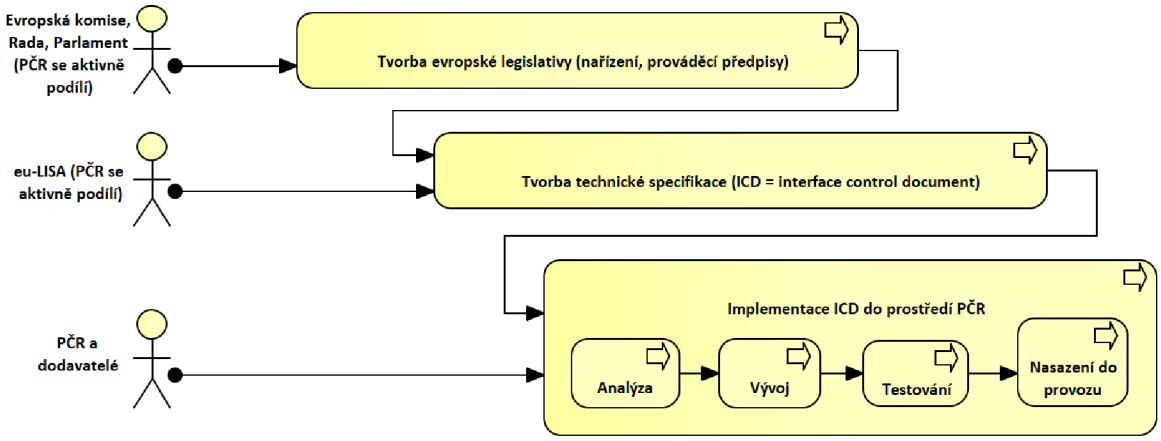
Jednotlivé fáze cyklu evropských informačních systémů jsou:

- Analýza potřeb a požadavků na úrovní EU a členských států.
- Projednání na příslušných pracovní skupinách (např. PS Hranice, PS Víza, SCIFA).
- Tvorba evropské legislativy:[52]
    - schválení zákona,
    - projednání o legislativním návrhu – Evropský parlament s dotčenými výbory (např. Výbor pro občanské svobody, spravedlnost a vnitřní věci),
    - první čtení v Evropském parlamentu,
    - první čtení v Radě,
    - druhé čtení v Evropském parlamentu,
    - druhé čtení v Radě,
    - dohodovací výbor a třetí čtení v Evropském parlamentu a Radě,
    - třetí čtení v Evropském parlamentu a Radě,
    - přijetí/odmítnutí návrhu.
- Definování nákladů, rozpočtu, určení odpovědnosti subjektů (členské státy, evropské agentury např. eu-LISA, EUROPOL).

[52] EVROPSKÝ PARLAMENT. *Řádný legislativní postup* [online]. [cit. 2024-02-28]. Dostupné z WWW: https://www.europarl.europa.eu/infographic/legislative-procedure/index_cs.html.

- Návrh systému High level architektury, pro technologické řešení HW, topologie.
- Realizace projektů v členských státech (provoz, support, odstavení systému, nahrazení novou generací systému, sloučení s jiným systémem).

Obrázek 7 – Schéma cyklu evropských informačních systému



Zdroj: (Vlastní zpracování)

4.2.2 Příklad na systému Entry/Exit

1. **Legislativa:**
   - 2017/2226 ze dne 30. listopadu 2017, kterým se zřizuje Systém vstupu/výstupu (dále jen „EES“) pro registraci údajů o vstupu a výstupu a údajů o odepření vstupu, pokud jde o státní příslušníky třetích zemí překračující vnější hranice členských států, kterým se stanoví podmínky přístupu do systému EES pro účely vymáhání práva a kterým se mění Úmluva k provedení Schengenské dohody a nařízení (ES) č. 767/2008 a (EU) č. 1077/2011.
2. **Technická specifikace:**
   - Entry/Exit ICD verze 7.X (2/2024).
3. **Projektový tým**
   - 8 osob.
4. **Smluvní zajištění**
   - Rámcová dohoda.

5. **Finanční zajištění**

   - Čerpání finančních prostředků z fondů EU (ISF = Internal Security Fund):

     1. Národní projekt EES I – Implementace systému EES ISF/13/01, (100 % cofinancovaný ze strany EU).
     2. Národním projektu EES II. - Pořízení technologií ISF/13/02.

Příprava podkladů až po schválení financování trvalo 12 měsíců (projektový záměr, ICT příloha, žádost o podporu).

6. **Projektové řízení – subjekty, s nimiž je zapotřebí zajišťovat koordinaci**

   - Evropská komise,
   - eu-LISA,
   - dodavatel a subdodavatelé systému Entry/Exit,
   - dotčené útvary PČR – ŘMPS, ŘSCP, NCIKT, ŘLZ,
   - dotčené orgány mimo PČR: Odbor azylové a migrační politiky MVČR.

4.2.3 Zhodnocení proti obecnému cyklu informačního systému

Fáze cyklu evropských informačních systémů se téměř neliší od životního cyklu jiných informačních systémů. Prokazatelný rozdíl je v jeho první fázi konkrétně ve fázi schvalování, kde u evropských informačních systémů je tento proces rozšířen nad běžný rámec schvalování o tvorbu a následné schválení příslušné právní legislativy, které následný provoz systému podléhá. Nejvýznamnějším rozdílem je délka realizace, která je v průměru více jak třikrát delší a rozdíl od běžných projektů informačních systémů.

4.3 Projekt Entry/Exit

Systém Entry/Exit je jeden z nově budovaných systémů EU. V rámci projektu je řešeno i jeho začlenění do národní komponenty interoperability. Původní zadavatel je evropská agentura eu-LISA, která odpovídá za centrální část systému. Aby byl zajištěn nepřetržitý a bezproblémový provoz a všechny části systému byly stále dostupné, bude centrální část systému, jež je umístěna ve Štrasburku ve Francii a zálohu umístěnou v záložním operačním středisku v Sankt Johann im Pongau v Rakousku, která v případě výpadku jakékoliv služby zajistí plnohodnotný přístup všem uživatelům. Vybudování připojení k národnímu jednotnému rozhraní (NUI), pomocí kterého mají povinnost všechny

členské státy EU se připojit, je v kompetenci každého členské státu. Ovšem za dodržení všech podmínek stanovených v ICD.

4.3.1 Základní informace o projektu

Dne 30. listopadu 2017 bylo vydáno evropské nařízení, kterým se má zřídit systém Entry/Exit pro zaznamenání vstupních a výstupních údajů a informací o odmítnutí vstupu státních příslušníků třetích zemí, kteří překračují vnější hranice členských států. Zároveň toto nařízení představuje klíčový prvek revidovaného legislativního balíčku o inteligentních hranicích.

Systém EES bude provozován na vnějších hranicích členských států, které podepsali Schengenskou dohodu. Systém bude ukládat informace o datu, čase a místě vstupu a výstupu překročení vnější hranice členských států státních příslušníků třetích zemí, kdy tento záznam nahradí povinnost udělovat razítka do pasů státních příslušníků třetích zemí. Dále bude vypočítávat délku jejich pobytu a generovat výstrahy o překročení povolené délky pobytu. Navíc systém EES bude evidovat údaje o státních příslušnících třetích zemí, jímž byl krátkodobý pobyt zamítnut.

V rámci projektu bude vybudován:

- zabezpečený komunikační kanál s centrální částí systému VIS,
- zabezpečená komunikační infrastruktura pro propojení NUI a EES,
- centrální uložiště statistik s rozhraním, pomocí kterého budou moci přistupovat pověření pracovníci,
- webová služba, pomocí které si budou moci státní příslušníci třetích zemí ověřit platnost předpokládaného vstupu a výstupu, a dopravcům umožní ověřit data o vízech státních příslušníků třetích zemí.

Každý členský stát má povinnost propojit své systémy správy hranic do národního jednotného rozhraní pomocí zabezpečené infrastruktury.

Cílem EES je zlepšení správy vnějších hranic, zabránění přistěhovalectví a usnadnění sledování migračních toků. Systém EES má zároveň přispět k identifikaci všech osob, které

splňují, nebo již nesplňují podmínky délky povoleného pobytu na území členských států. Stejně jako by měl přispívat k prevenci, odhalování a vyšetřování páchané trestné činnosti.

4.3.2 Národní projekt EES – základní informace

Projekt je zaměřen na implementaci Systému vstupu/výstupu (EES), včetně integrace se systémy stávající vnitrostátní pohraniční infrastruktury, jejich připojení k národnímu jednotnému rozhraní.

Zahájení realizace projektu: 1. 1. 2020.
Plánované ukončení projektu: 30. 04. 2024.
Doba trvání v měsících: 52 (včetně prodloužení z dříve maximální délky 36 měsíců).
Výše podpory z NP ISF: 100 %/ 75 % způsobilých výdajů projektu.
Celkové náklady projektu: 134 697 659,00 Kč z fondů EU ISF.
Vítězný dodavatel: Vítkovice IT Solutions a. s..

Cíl projektu

„Cílem projektu je vybudování národní části Systému vstupu/výstupu pro registraci údajů o vstupu a výstupu a údajů o odepření vstupu, pokud jde o státní příslušníky třetích zemí překračující vnější hranice členských států, včetně integrace se systémy stávající vnitrostátní pohraniční infrastruktury a jejich připojení k národnímu jednotnému rozhraní.“[53]

4.3.3 Implementace systému

Pro připojení České republiky k centrálnímu systému EES je nutné vybudovat Centrální přístupový bod EES, což bude samostatná aplikace provozovaná v rámci prostředí Národní součásti systému Entry/Exit (NS-EES). Jejím cílem je, aby od prvotního spuštění zajistila nahlížení a vyhledávání záznamů v EES pro orgány vymáhající právo (LEA). Zároveň bude navržena tak, aby v budoucnu mohla být využita i pro dotazy do ostatních evropských informačních systémů, jako je ETIAS, VIS a EURODAC. Toho bude docíleno tím, že Centrální přístupový bod nebude používat pouze dotazovací služby vyplývající z Entry/Exit ICD, ale v rámci projektu interoperability budou používat univerzální dotazovací službu z European Search Portal ICD, která bude zprostředkována národní

[53] Policie ČR. *Národní programy Fondů EU v oblasti vnitřních věcí (ISF a AMIF)* [online]. [cit. 2024-01-18]. Dostupné z WWW: https://www.policie.cz/clanek/narodni-programy-fondu-eu-v-oblasti-vnitrnich-veci-isf-a-amif.aspx?q=Y2hudW09MTk%3d.

komponentou interoperability. Centrální přístupový bod bude založen na architektuře webové aplikace klient/server s použitím příslušného komunikačního protokolu. Aplikace bude uživatelům k dispozici prostřednictvím webového serveru v rámci intranetové počítačové sítě Policie ČR jako tenký klient, případně jako specifický klient dle specifických potřeb určitých uživatelů.

Obecná role systému vychází z Nařízení evropského parlamentu a rady (EU) 2017/2226 ze dne 30. listopadu 2017 a základní rámec funkcionality Centrálního přístupového bodu EES definuje dokumentace Entry/exit Interface Control Document (EES-ICD).

V první fázi projektu bude Centrální přístupový bod EES složen z:

- GUI klient,
- rozhraní pro nahlížení a vyhledávání datových záznamů EES,
- rozhraní pro správu systému.

Systém Centrálního přístupového bodu se bude skládat z těchto základních částí:

- **základní webový kontejner** – jádro aplikace, které bude řídit veškeré transakce,
- **rozhraní pro správu dotazů a požadavků** – rozhraní pro řízení správné obsluhy odpovědí,
- **autentizační a autorizační modul** – systém pro autentifikaci a autorizace přistupujících uživatelů,
- napojení na rozhraní NS EES – datový konektor mezi NS EES a NUI,
- **lokální cache datových vět** – bude ukládat všechny požadavky a odpovědi, které budou zadány přes Centrální přístupový bod, mechanismus, který zajistí opakované pokusy o doručení odpovědí,
- **webový klient** – převede většinu funkcí do vizuální podoby pro použití uživatelem, bude k dispozici pro prohlížeče MS Edge a Google Chrome,
- **transakční auditovací modul** – systém bude logovat veškeré významné události po dobu tří let.

Systém bude pracovat se čtyřmi typy uživatelů:

- **Dotazovatel** – uživatel, který si zažádá o data do systému EES a může si zobrazit výsledky schválených a dodatečně nezamítnutých urgentních požadavků.
- **Operátor** – uživatel, jehož úkolem je schvalovat a zamítat požadavky dotazovatelů.
- **Auditor** – uživatel s oprávněním do auditních logů.
- **Administrátor** – uživatel s administrátorskými právy ke službě CAP.

V rámci projektu budou provedeny následující testy:

1. **Automatické testy** – testy budou probíhat v rámci vývoje za účelem ověřování funkcionalit a různých kombinací scénářů.
2. **Manuální testy** – testy budou probíhat v rámci vývojové fáze a i následné testovací fáze a budou sloužit k ověření funkcionalit grafického klienta.
3. **Penetrační testy** – tyto testy budou prováděny zadavatelem za použití sestavených postupů dodavatelem systému.

4.3.4 Závěrečná fáze projektu

V poslední fázi projektu přes spuštěním bude probíhat osazování nakoupeného hardware z rámcových smluv přímo na místech budoucího využití. V České republice se jedná zejména o mezinárodní letiště, mimo letiště v Praze se jedná o letiště v Karlových Varech, Pardubicích, Brně a Ostravě. Dále bude následovat připojení těchto zařízení do společné infrastruktury, nastavení dle požadavků technické dokumentace a implementace do systému. V dalším kroku proběhnou veškerá systémová nastavení a následně test funkčnosti těchto periférií se systémem v reálném prostředí. Vzhledem k velikosti projektu a počtu potřebných zařízení, včetně otestování výše zmíněných kritérií se i této fázi jedná o velice náročný a dlouhý proces. Až po úplném dokončení dojde k fyzickému předání do testování zadavatelem, tedy Policii ČR.

Do budoucna se počítá dalším rozšiřováním, zejména v rámci zmíněné interoperability a využívaní dotazovací služby ESP, což bude vždy dále řešeno samostatnou detailní analýzou a následnou úpravou posledního stavu systému.

Po samotném spuštění systému do provozu se začnou na úrovni Evropské unie evidovat vstupy a výstupy do Schengenského prostoru všech občanů třetích zemí. Čímž dojde k nahrazení udělování přechodových razítek do cestovního dokladu a tím dojde k efektivnější kontrole při překračování povolené délky pobytu, či počtu vstupů na udělené vízum. Zároveň se začne uchovávat biometrie (otisky prstů a fotografie jejich obličejů) těchto osob, což ztíží manipulaci s těmito daty při páchání nelegální migrace a usnadní tím policii odhalování takových činů.

K výše zmíněnému je nutno uvést, že text neobsahuje celistvé a konkrétní informace k technickému zabezpečení projektu. Uváděné informace byly vybírány s ohledem na povahu citlivosti údajů o bezpečnostních systémech a jejich možnému zneužití anebo obejití zabezpečení vnějších hranic EU.

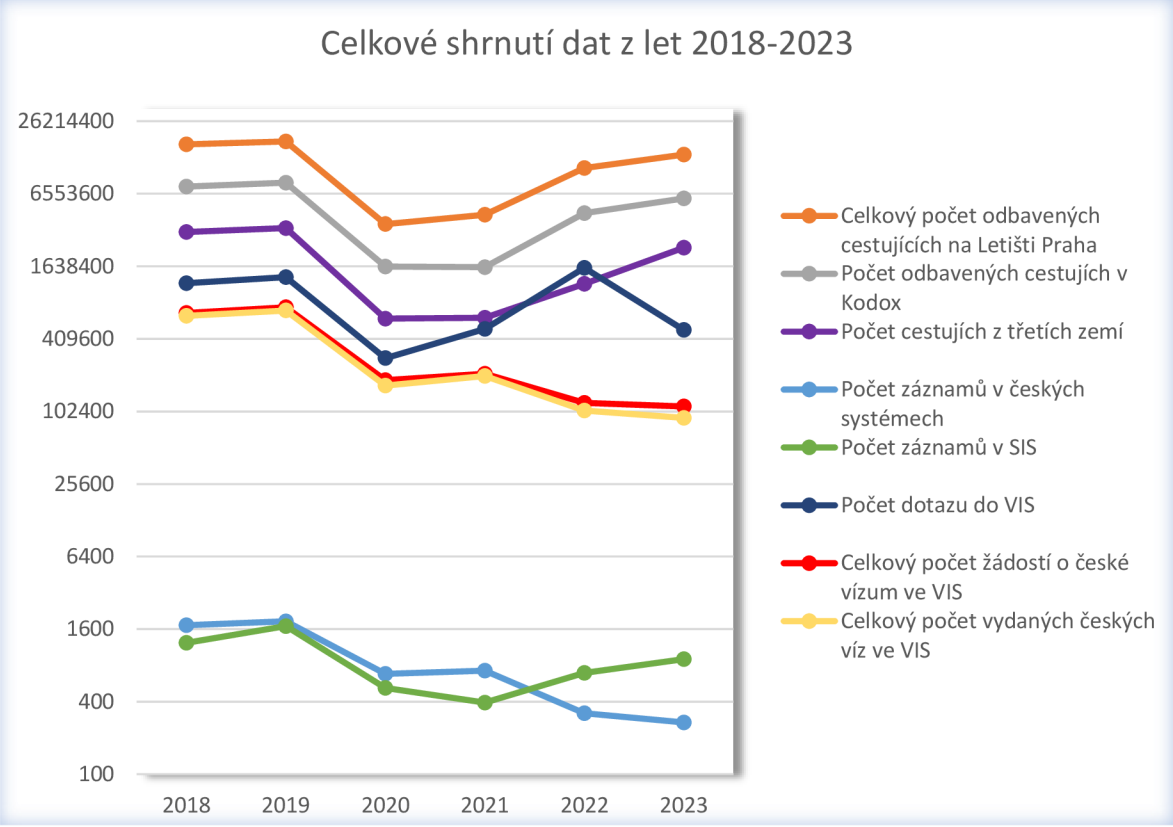
4.4 Analýza statistických dat již používaných systémů

V této části případové studie budou analyzována data využívání evropských informačních systémů při odhalování nelegální migrace, která je sledována od roku 2007, kdy Česká republika vstoupila do Schengenského prostoru. Aby bylo možné podat co nejrelevantnější informace, bylo pro srovnání zvoleno největší české letiště v Praze, které tvoří vnější vzdušnou hranici Schengenského prostoru. Z důvodu negativního vlivu Covid-19 na celkovou migraci osob jsou v práci zpracovány údaje za posledních 6 let.

4.4.1 Celkové shrnutí

Dle dat Letiště Praha a.s. bylo za léta 2018-2023 ročně odbaveno od 4 388 000 do 17 810 000 osob (viz. Graf 1). Pomocí systému Kodox při hraničních kontrolách na vnější schengenské hranici bylo ročně zkontrolováno od 1 613 000 do 8 102 000 osob. Což tvoří v průměru cca 43 % z počtu odbavených cestujících na Letišti Praha a. s. (viz. Graf 1). Z tohoto počtu bylo 60-70 % občanů EU (viz. Graf 1). V českých informačních systémech (Patros, ENO, IS Opatření) bylo ročně zjištěno od 269 do 1 858 osob (viz. Graf 1). V systému SIS bylo v rámci lustrací ročně zjištěno od 390 do 1 695 záznamů (viz. Graf 1). Do systému VIS by provedeno pomocí Kodox od 282 000 do 1 591 194 dotazů (viz. Graf 1). Přes systém VIS bylo podáno od 112 553 do 748 369 žádostí o české vízum a bylo vydáno od 90 511 do 703 460 víz Českou republikou (viz. Graf 1).

Graf 1 - Celkové shrnutí dat z let 2018-2023



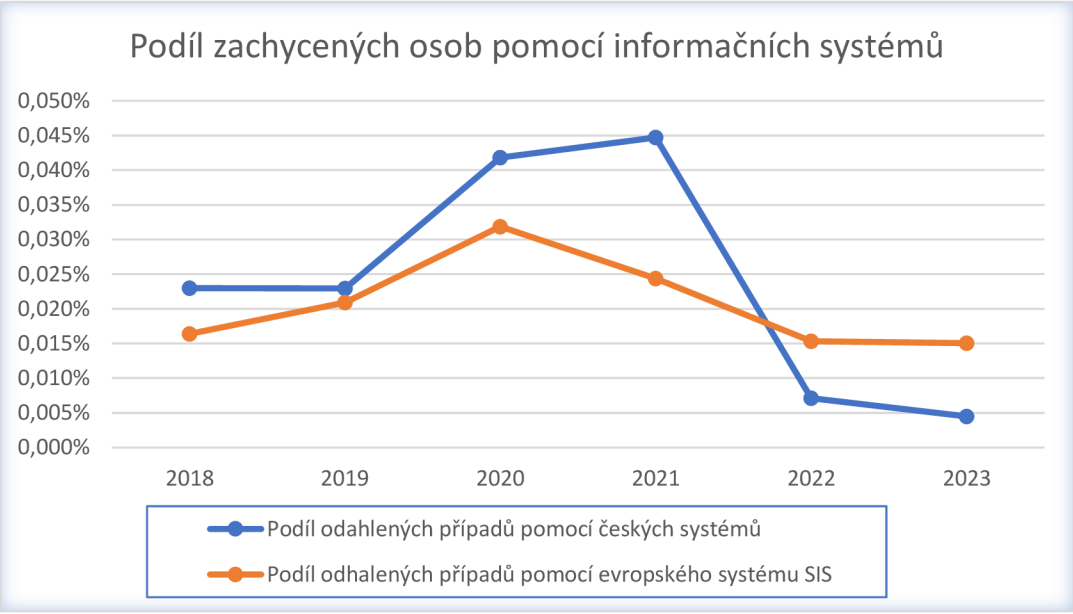
Zdroj: (Vlastní zpracování z tiskových konferncí a tiskových zpráv Policie ČR)

Při celkovém pohledu na analyzovaná data je patrné, že jsou z velké části ovlivněna šířením onemocnění Covid-19 a navázanými bezpečnostními opatřeními. Přesto je znatelný rostoucí počet cestujících a s ním zvyšující se počet zachycených osob, kteří na naše území vstupují anebo z něj vystupují. Data také ukazují, že všechny používané systémy mají své místo v procesu hraniční kontroly a značným způsobem se podílejí na počtu odhalených osob. Je ovšem na místě brát v potaz, že je každý navržený k jinému účelu, včetně rozdílnosti uložených a vytěžovaných dat. Navíc tato data odrážejí aktuální potřeby a tím, že se jedno z čísel zmenší, nutně neznamená neefektivitu systému. To samé platí naopak a tak se čísla u jednotlivých systémů mohou měnit.

V detailnějším pohledu na data z informačních systémů, zejména při zobrazení v procentuálního podílu odhalených osob z celkového počtu cestujících odbavených na vnější hranici Schengenského prostoru, v našem případě na letišti v Praze (viz. Graf 2) vyplývá, že v současné době jediný evropský informační systém SIS používaný v první kontrolní linii značnou měrou doplňuje funkci národních systémů v procesu hraniční kontroly osob. Při srovnání rozdílu odhalených osob je nutné vzít v potaz, že data „českých

informačních systémů“ zahrnují data z několika národních systémů, kdežto v druhém případě se jedná pouze o jediný systém, konkrétně evropský systém SIS. V porovnání těchto dvou výstupů vyplývá, že už v prvním srovnávaném roce 2018 měl nižší podíl odhalených osob oproti českým systémům. V následujícím roce 2018 až 2019 počty odhalených osob pomocí SIS stoupaly, oproti českým systém, kde počty zůstaly téměř stejné. Od roku 2019 všechna čísla začala výrazně růst až do roku 2020. V roce 2020 se do statistik začalo promítat šíření nemoci Covid-19 a podíl zachycených osob pomocí českých systémů se začal mírně zvyšovat oproti systému SIS, kde čísla klesala, a to až do roku 2022. Tato skutečnost byla příčinou vydaných opatření k zastavení šíření pandemie a projevil se zákaz vstupu příslušníků cizích zemí a naopak se zvýšil počet českých občanů vracejících se domů. Ale i přes to všechno podíl systému SIS zůstává vyšší. Naopak v letech 2022 a 2023, kdy počty odhalených osob klesají, u evropského systému SIS zůstává procentuální průměr stejný. Na základě těchto dat lze konstatovat, že systém SIS významnou měrou doplňuje používané národní systémy, je efektivním prostředkem při odhalování hledaných osob v mezinárodním kontextu a pomáhá Cizinecké policii chránit vnější hranici Schengenského prostoru.

Graf 2 - Podíl zachycených osob pomocí IS

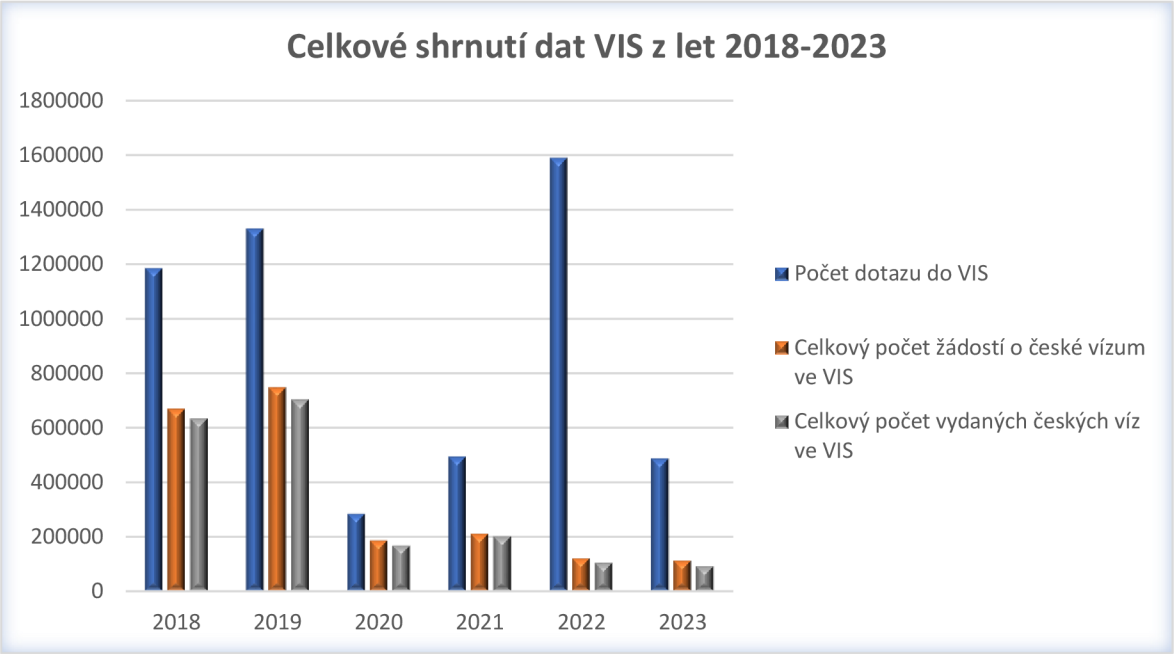


Zdroj: (Vlastní zpracování z tiskových konferncí a tiskových zpráv Policie ČR)

Je žádoucí provést samostatné zhodnocení u systému VIS, který odráží především potřeby občanů než bezpečnostních složek. Bezpečnostním složkám slouží hlavně jako informační nástroj o zamítnutí, prodloužení, zrušení víz, případně k ověřování a identifikaci žadatelů a držitelů víz bez ohledu na místo podání nebo státní příslušnost. Analyzovaná data

tedy prezentují ohromné množství dat, jaké mohou být do evropských systémů vkládána, když vezmeme v potaz použití alfanumerických a biometrických údajů. S přihlédnutím ke skutečnosti, že počty obsahují pouze data České republiky. Pomůže nám to pochopit, jak velkému zatížení musí technické zabezpečení systémů čelit.

Graf 3 - Celkové shrnutí dat VIS za léta 2018-2023



Zdroj: (eu-LISA)

Závěrem je možné říci, že všechny bezpečnostní systémy plní svou funkci a přispívají tak velkou mírou k odhalování osob při páchání přestupků a trestních činů nejen v oblasti nelegální migrace osob. Důležitým faktorem, který ovlivňuje a bude ovlivňovat efektivitu a účinnost evropských systémů, je ochota členských států využívat tyto systémy v co největší míře a sdílet co nejvíce informací. I přesto je možné říci, že v rámci zabezpečení hranic plní svou roli a přispívají k efektivnější kontrole.

4.5 Řízené rozhovory

K doplnění zjištěných poznatků bylo provedeno výzkumné šetření pomocí řízených strukturovaných rozhovorů s policejními IT pracovníky tří evropských zemí, kteří se podílejí na projektech interoperability, případně i přímo na projektech nově budovaných systémů, jež byly popsány v předchozích kapitolách této práce. Konkrétně byli osloveni pracovníci z České republiky, Slovenska a Belgie. Tyto rozhovory jsou přílohami 1, 3 a 5 této práce.

Řízené rozhovory se skládají z části úvodu, vlastních otázek a informovaného souhlasu účastníka výzkumu. Otázky byly sestaveny pro potřeby ověření a doplnění výzkumného šetření. Celkově bylo zvoleno 14 otázek, s jednou volnou otázkou k doplnění celkové problematiky. Průměrná doba rozhovorů byla v průměrné délce 60 minut. Rozhovory byly poskytnuty po předchozí domluvě a byly se souhlasem nahrávány pro následné zpracování.

4.5.1 Výstup z rozhovorů

Následující výstup obsahuje klíčové oblasti, které vyplynuly z rozhovorů s respondenty.

Všichni tři oslovení respondenti mají shodné informace o účelu IO, ale vnímají slabinu v implementaci, která spočívá v tom, že neexistuje jedno autoritativní místo, které by vše řídilo centrálně. Naopak vnímají, že každý členský stát bude preferovat vlastní přístup a tím pádem může vznikat různá praxe v různých členských státech. Dále se shodují v potřebě změny v dosavadním způsobu práce díky zavádění nových technologií a nároků kladených na koncové uživatele, kdy bude potřeba změna procesu. V otázce nákladů implementace systémů IO a jejich provoz respondenti vnímají jejich vyšší prioritu oproti jiným národním požadavkům a velkou výhodou je spolufinancování z fondů EU. Nevýhodou však je složitost a posouvání termínů. Respondenti shodně zhodnotili vysokou míru zabezpečení na centrální úrovni včetně logování a důraz na dostupnost systémů pro koncové uživatele. Na otázku fungování systémů v praxi s ohledem na vytyčené cíle, včetně Smart Borders odpověděli pouze dva respondenti, neboť třetí respondent neměl dostatečné informace. Respondenti popisují, že z jejich pohledu dojde k vyššímu zabezpečení hraniční kontroly, ale na úkor efektivnosti z důvodu vyššího náporu a tím pádem dojde k prodloužení času hraniční kontroly. Zároveň vnímají potřebu dalšího vzdělávání se a překonání počáteční nedůvěry koncových uživatelů. Evropa ale není připravená na zavedení IO, v tom se shodují všichni oslovení respondenti. Jedním z důvodu je nedokončená legislativa a příručka pro koncové uživatele. Termín spuštění všech komponent a IO je dle respondentů ve fázi odhadů a to z důvodu zpožďování projektu. Na otázku nutné organizační změny každý stát předpokládá jiný přístup. Respondent z SK předpokládá personální posílení. Respondent z ČR předpokládá ustanovení specialisty za každý útvar. A respondent z BE očekává zřízení

nového útvaru. Rizika při zavádění evropských systémů respondenti popisují každý ze svého úhlu pohledu. Avšak se shodují v oblasti náročnosti jak finanční, tak časové a koordinační.

4.6 SWOT analýza

SWOT analýzu autor práce použil za účelem ucelení zjištěných poznatků vycházejících z řízených rozhovorů a výsledků analýzy evropských informačních systémů jejich evropské integrace.

Obrázek 8 - SWOT analýza

SWOT analýza - evropské informační systémy

	Pozitivní	Negativní/Škodlivé
INTERNÍ	**Silné stránky**	**Slabé stránky**
	STRENGTHS	**WEAKNESSES**
	1 zefektivnění hraničních kontrol (str. 55 kap. 4.4.1)	1 nákladnost (příloha č. 5)
	2 dostupnost dat/údajů napříč Evropou (str. 39-42, kap. 3.5.1)	2 časová náročnost vývoje systému (příloha č.3)
	3 zabezpečení dat a přístupu k nim, včetně logování (str. 57 kap. 4.5.1)	3 prodloužení času na odbavení při hraniční kontrole (str. 57 kap. 4.5.1)
	4 dostupnost systémů (str. 48, kap. 4.3)	4 technické zabezpečení/množství dat (příloha č.3 a str. 56, kap. 4.4.1)
	5 zabezpečení komunikační infrastruktury (příloha č.3)	5 implementace (str. 57 kap. 4.5.1)
	6 záloha v různých regionech (str. 48, kap. 4.3)	6
	7 technická podpora od externích subjektů 24/7 (příloha č.1)	7
EXTERNÍ	**Příležitosti**	**Hrozby**
	OPPORTUNITIES	**THREATS**
	1 propojení různorodých agend, nejen národních (příloha č.3)	1 nepřipravenost evropského společenství (str. 57 kap. 4.5.1)
	2 zrychlení hraničních kontrol (str. 57 kap. 4.5.1)	2 nepřipravenost evropské legislativy (str. 57 kap. 4.5.1)
	3 propojení policejních databazí všech evropských států (Nařízení o IO)	3 absence finální technické specifikace nástrojů IO (příloha č.3)
	4 zavedení moderních technologií (str. 57 kap. 4.5.1)	4 nutnost rozšíření personálních stavů (str. 57 kap. 4.5.1)
	5	5 roztříštěnost či nedostupnost potřebných informací (příloha č.3)
	6	6 angažování velkého množství subjektů (příloha č.3)
	7	7 nejednotnost členských států (příloha č.3)
	8	8 zvýšení pracovního zatížení pracovníků (str. 57 kap. 4.5.1)

2024, vytvořil Tomáš Pšenica

Zdroj: Vlastní zpracování

4.7 Výsledky a diskuse

Na začátku všeho stála myšlenka inteligentní hranice (Smart Borders), která by zvýšila bezpečnost Schengenského prostoru. Stála na využívaní nových technologií a vzájemné spolupráci členských států Evropské unie. Důvodem byla snaha o centralizaci dat ze systémů a eliminaci bezpečnostního rizika, které vznikalo díky izolovanosti a oddělenosti systémů v různých regionech (kap. 3.5). Vznikla tak myšlenka velmi komplexního projektu Interoperability.

Každý nově implementovaný systém používaný nejen při hraniční kontrole, je implementován na základě aktuálních potřeb bezpečnostních složek a globálních problémů.

A tím větší či menší mírou přispívá k vyšší efektivnosti zavedených kontrol. Celoevropsky užívané systémy mají nespornou výhodu v provázanosti dat, na které je možné okamžitě reagovat v jakémkoli státě EU.

Na základě dat (kap. 4.4.1) předkládané práce vyplývá, že i přes šíření nemoci Covid-19 dochází ke stálému nárůstu počtu odbavených osob na mezinárodním letišti v Praze. Narůstá i počet zachycených případů díky zmíněným informačním systémům v předkládané práci. Z dat znázorněných v kapitole 4.4.1 plyne jednoznačná důležitost informačních systémů, které zajišťují ochranu vnějších hranic a hrají v jejím procesu nezastupitelnou roli. Bez těchto systémů by docházelo k tomu, že na území České republiky by se mohly vyskytovat osoby, které se do Schengenského prostoru dostaly neoprávněně a mohly by být hledané v jiných státech, případně by mohli představovat bezpečnostní riziko. V této problematice hraje důležitou roli právě interoperabilita, která má zajistit propojenost různých databází členských států a měla by nastavit standardy komunikace při vytěžování ukládaných dat a přístupu k nim. Interoperabilita bude pouze backendovým systémem, který bude rozšiřovat stávající systémy a stane se součástí kritické infrastruktury, čemuž budou muset odpovídat dostatečná zabezpečení.

Jak již bylo řečeno výše projekt interoperability představuje komplexní řešení, které bude mít dopady do mnoha oblastí, především do oblasti personální (navýšení počtu zaměstnanců, změny pracovních návyků a s tím související zvyšující se nároky na vzdělávání a celkové změny mindsetu), technologické (zabezpečení, logování) a finanční. Takto rozsáhlý projekt je sice financován z velké části z evropských fondů, ale z důvodu protahování termínů dochází i k jeho prodražování, což má dopad i do financování členských států. Zároveň tento typ projektu má vždy přednost před projekty národními, protože by hrozilo mezinárodní fiasko (viz. provedené řízené rozhovory). Stále častěji dochází k tomu, že evropské a nadnárodní systémy v mnoha případech nahrazují národní systémy.

Při porovnávání cyklu běžného informačního systému a evropského informačního systému (kap. 4.2.1 a 4.2.3) tvoří největší rozdíl fáze schvalování. V případě evropského informačního systému je nutné vytvoření právního rámce, který je často časově náročný. Rozdílná je i doba realizace obou typů informačních systémů, kdy u běžného IS se jedná o dobu maximálně 5 let, kdežto u evropského IS může být až 15 let.

Pro zajištění bezproblémové výměny dat a informací mezi národními a centrálními součástmi evropských systémů je důležitý dokument Interface Control Dokument, ve kterém jsou popsány všechny detaily ohledně centrálních systémů a poskytování jejich služeb a přesných popisů přístupů k nim, což zajistí jednotný standard pro každý systém (kap. 3.4).

Provedené rozhovory potvrdily výsledky práce, že je potřeba reagovat na současnou situaci a zvýšit ochranu vnějších hranic Schengenského prostoru, což se ale ukazuje jako náročný a zdlouhavý proces, který je velice nákladný a jeho prodlužováním se ještě více prodražuje. Vše se tak děje, protože do celého procesu vstupuje velké množství subjektů, kde každý řeší svou problematiku a neexistuje žádný zastřešující orgán, který by zmíněnou problematiku řídil komplexně. Dále se při samotné realizaci ukazuje rozpolcení a nejednotnost členských států při zásadních otázkách projektů a jejich neochota spolupracovat na společném postupu.

Výsledky SWOT analýzy prokázaly hlavní myšlenku inteligentních hranic, kde mezi silné stránky patří zejména zefektivnění hraničních kontrol, což v praxi bude znamenat důkladnější prověřování osob. Neméně důležité je zajištění dostupnosti dat napříč Evropou, ve které interoperabilita propojí data evropských systémů pomocí jejích služeb (CIR, MID, sBMS, ESP). Další silnou stránkou je vysoká míra zabezpečení, která pokrývá všechny oblasti technického zabezpečení systémů bezpečnostních složek jako například logování, síťová konektivita, fyzická a objektová bezpečnost a záloha v různých regionech. Současně je komunikační (síťové) zabezpečení na evropské úrovni řešeno zabezpečenou sítí TESTA-ING, která se následně pomocí firewallů propojuje s národními sítěmi členských států. Za silnou stránku označujeme i dostupnost systémů, kdy jsou výše zmíněné evropské systémy uloženy 1:1 na různých místech v různých regionech, aby v případě jakéhokoliv výpadku, byla dostupná plnohodnotná záloha. Díky tomu, že jsou tyto systémy provozovány na evropské úrovni, je možné nastavit backup systémů v odlišných geografických regionech Evropy. Velkou výhodou pro zajištění dostupnosti 24/7 bude spolupráce s externí společností, jelikož stav dostatečně kvalifikovaného personálu ve státní správě, která tyto systémy používá, je nedostatečný.

SWOT analýza poukázala i na slabé stránky, mezi které řadíme celkovou nákladnost na vybudování jednotlivých evropských systémů v řádech sta milionů. Nejedená se však o něco nestandartního. V případě takto komplexních projektů, ještě navíc nadnárodních, se

jedná o běžný náklad. Ovšem v situaci, kdy dochází k nedodržování termínu, což se v těchto evropských projektech děje, náklady raketově rostou. Další nevýhodou takto komplexních projektů je jejich časová náročnost, která je umocněná velkým množstvím zainteresovaných subjektů, které je těžké napříč EU zkoordinovat a sjednotit. Ačkoliv jedním z cílů inteligentních hranic bylo zrychlení provádění hraniční kontroly, tak se ukazuje, že tohoto cíle nebude dosaženo, protože vyšší zabezpečení značí důkladnější kontrolu a tím pádem více času na každou prověřovanou osobu. Vzhledem k tomu, že systémy budou uchovávat velké množství dat, je nutné počítat s vysokými požadavky na technické zabezpečení (hardware). Další nevýhodou je upřednostnění implementace nadnárodních projektů před těmi národními, navíc je implementace náročná z pohledu splnění vysokých požadavků na funkčnost dle ICD dokumentace.

Za největší hrozby SWOT analýza ukázala v oblasti nepřipravenosti Evropské unie pro zavádění interoperability z mnoha důvodů, který mi jsou zejména nedokončená finální technická specifikace nástrojů interoperability ze strany eu-LISA, absence finální legislativy a příruček pro uživatele. Analýza dále poukazuje na nedostatečné personální kapacity, včetně nedostatečné kvalifikace. Bude nutné přemýšlet o navýšení kapacit a rozsáhlého vzdělávání. Dále se ukazuje, že chybí jedno autoritativní místo, které by koordinovalo veškeré aktivity i dokumenty spojené s těmito projekty. Nyní jsou informace často roztříštěné nebo chybí jejich dostupnost. S tím souvisí i nejednotný postup členských států, kdy každý prosazuje především své zájmy. Problémem je i velké množství subjektů (např. Frontex, Evropská komise, eu-LISA aj.), které vidí interoperabilitu pouze ze svého úhlu pohledu a přehlíží se praktičnost projektu.

Za největší příležitosti autor práce považuje zavádění nových moderních technologií a propojení policejních databází evropských států, která interoperabilita přinese. Kromě zmíněného interoperabilita přinese propojení šesti agend napříč šesti evropskými systémy v oblasti, hranic, víz, imigrace, policejní a justiční spolupráce. Příležitost k rozvoji vidí autor práce zejména v oblasti zrychlení hraniční kontroly.

5 Závěr

Cílem předkládané práce bylo provést analýzu evropských policejních systémů určených k ochraně hranic a detailněji zkoumat jejich implementaci a využití při ochraně vnějších hranic, zejména na českých mezinárodních letištích. Jako dílčí cíl bylo stanoveno zhodnocení jejich efektivity při provádění hraniční kontroly s použitím počítačových aplikací v boji proti nelegální migraci osob.

Teoretická část práce se věnovala výčtu a popisu evropských bezpečnostních systémů a aplikací, které jsou využívány k ochraně vnějších hranic České republiky a k monitorování osob vstupujících a opouštějících naše území, a dále území Evropské unie. Dále je provedena analýza významu propojenosti těchto systémů, známé jako interoperabilita. Bylo důležité v této části zmínit i sice ryze český systém KODOX, který je momentálně stěžejní pro práci Cizinecké policie na mezinárodních letištích, protože v budoucnu bude nadále využíván, a ještě se stane „vstupní branou" České republiky do interoperability.

Praktickou část autor práce věnoval několika dílčím cílům. Prvním dílčím cílem byla analýza projektu systému Entry/Exit. Bylo zjištěno, že se jedná o nejvýznamnější projekt inteligentních hranic, protože systém začne evidovat vstupy a výstupy do Schengenského prostoru všech občanů třetích zemí a nahradí tím udělování přechodových razítek do cestovního dokladu. Tím velmi pomůže k odhalování nelegální migrace osob (str. 52-53 a příloha č.1). Druhým dílčím cílem bylo ověření důležitosti interoperability policejních informačních systémů a jejího přínosu při odhalování nelegální migrace osob. Ověření probíhalo prostřednictvím řízených rozhovorů s předem vybranými IT pracovníky zemí EU a samotnou analýzou Interoperability z teoretické části této práce. Výsledkem bylo, že interoperabilita je důležitý nástroj k propojení jak stávajících, tak nově budovaných systému, kterým se propojí šest různých agend a uživatelům zejména nové procesy v odhalování vícenásobných totožností, což přinese významnou změnu v současném způsobu práce (str. 39-43 a provedené rozhovory). Dalším cílem bylo zhodnocení efektivity evropských policejních informačních systémů při hraniční kontrole. Analýzou statistických dat bylo zjištěno, že tyto systémy významně zvyšují počty odhalených osob a doplňují tím národní systémy, které jsou v mezinárodním kontextu značně omezené a reflektují jen národní potřeby a poznatky a lze tak konstatovat, že samotnou hraniční kontrolu zefektivňují (str.

55). Je však nutné přihlédnout, že účinnost a efektivita těchto systémů jsou závislé na spolupráci a ochotě členských států sdílet informace a spolupracovat v rámci evropských struktur. Na závěr byla provedena SWOT analýza (str. 58), která shrnula veškeré zjištěné poznatky, které jsou blíže specifikovány v kapitole Výsledky a diskuse.

Výsledkem a samotným přínosem této předkládané práce je, že evropské bezpečnostní systémy mají své místo v procesu hraniční kontroly a jsou důležité nejen pro zvládání boje proti nelegální migraci osob, které momentálně evropská společenství čelí, ale i pro celkové zajištění bezpečnosti v Evropě.

Navrhovaným řešením pro odstranění zjištěných nedostatků je vytvoření mnohonárodnostní skupiny např. pod agenturou eu-LISA, která by shromažďovala požadavky a potřeby členských států, které by mohla v zastoupení prezentovat při různých legislativních projednávání. Zároveň by byla k dispozici projektovým pracovníkům členských zemí při samotné implementaci a zároveň by jako nejkompetentnější orgán mohla pomoc při řešení vzniklých problémů a případně je prezentovat dále. Dalším návrhem je zvážení centrálních nákupů potřebného hardware pro připojení a obsluhu systému vycházejících z ICD dokumentu. Tyto řešení by mohli vést k časové a finanční úspoře při realizaci evropských projektů.

6 Seznam použitých zdrojů

Literární zdroje

1. ČIŽINSKÝ, Pavel. *Cizinecké právo*. Praha: Linde, 2012. 373 s. ISBN: 978-80-7201-887-1.
2. GÁLA Libor, POUR Jan, TOMAN Prokop. *Podniková informatika. Druhé, přepracované a aktualizované vydání.* Praha: Grada Publishing, a. s., 2009. 493 s. ISBN 978-80-247-2615-1.
3. GÁLA Libor, POUR Jan, TOMAN Prokop. *Podniková informatika. Třetí aktualizované vydání.* Praha: Grada Publishing, a. s., 2015. 238 s. ISBN 978-80-247-5457-4.
4. HRABÁLEK, M. *Ochrana hranic EU a role agentury FRONTEX v ní.* Praha: Masarykova universita, 2012. 155 s. ISBN 978-80-210-5988-7.
5. KRAJČÍK, Vladimír. *Informační systémy I.* Ostrava: Vysoká škola podnikání, 2005. 73 s. ISBN 80-86764-24-9.
6. KURŽEJA, Jan. *Cizinecká policie a evropské právo.* Praha: Vydavatelství PA ČR, 2007. 346 s. ISBN 978-80-7251-272-0.
7. PIKNA, Bohumil. *Evropský prostor svobody, bezpečnosti a práva – Prizmatem Lisabonské smlouvy.* Praha: Linde, 2012. 435 s. ISBN 978-80-7201-889-5.
8. POŘÍZEK, Pavel, JÍLEK, Dalibor, ed. *Společný evropský azylový systém: transpozice směrnic.* Brno: Kancelář veřejného ochránce práv, 2008. ISBN 978-80-254-3615-8.
9. SODOMKA Petr, KLČOVÁ Hana. *Informační systémy v podnikové praxi. Druhé aktualizované a rozšířené vydání.* Brno: Computer Press, a. s., 2010. 491 s. ISBN 978-80-251-2878-7.
10. TOMEK, Petr. *Zákon o služebním poměru příslušníků bezpečnostních sborů: s komentářem, poznámkami a judikaturou*. Olomouc: ANAG, 20. října 2019. 854 s. Právo (ANAG). ISBN 978-80-7554-234-2.
11. VLÁČIL, Jiří. *Právo na vstup a pobyt na území členských států Evropské unie.* Praha: Univerzita Karlova, Právnická fakulta, 2016. 154 s. ISBN 978-80-87975-52-7.

Elektronické zdroje

1. MINISTERSTVO VNITRA. *Často kladené otázky* [online] 2021 Ministerstvo vnitra České republiky [cit. 2023-08-25]. Dostupné z WWW: https://www.mvcr.cz/migrace/clanek/migrace-casto-kladene-dotazy-casto-kladene-dotazy.aspx.
2. Cs.theastrologypage.com. *Co je to biometrické zařízení? - definice z techopedie* [online]. [cit. 2023-09-03]. Dostupné z WWW: https://cs.theastrologypage.com/biometric-device.
3. POLITICKÝ SLOVNÍK. *Mezinárodní ochrana: Azyl a doplňková ochrana* [online] 2021 Politický slovník [cit. 2023-08-25]. Dostupné z WWW: http://www.politicky-slovnik.cz/mezinarodni-vztahy/azyl-a-mezinarodni-ochrana/.
4. Commission Nationale de l'Informatique et des Libertés. *SIS II: Schengen Information System II* [online]. červen 2021 [cit. 2023-11-30]. Dostupné z WWW: https://www.cnil.fr/en/sis-ii-schengen-information-system-ii.
5. RADA EVROPSKÉ UNIE. *Interoperabilita mezi informačními systémy EU* [online] Evropská unie, 2019 [cit. 2023-11-22]. Dostupné z WWW: https://www.consilium.europa.eu/cs/press/press-releases/2019/02/05/interoperability-between-eu-information-systems-council-presidency-and-european-parliament-reach-provisional-agreement.
6. EUROPAN COMMISSION. *VIS – Visa Information System* [online] European Commission [cit. 2023-12-01]. Dostupné z WWW: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en.
7. Commission Nationale de l'Informatique et des Libertés. *Visa Information Systém (VIS)* [online]. červen 2021 [cit. 2023-11-30]. Dostupné z WWW: https://www.cnil.fr/en/visa-information-system-vis.
8. THALES. Thales. *Eurodac: the European Union's first multinational biometric system* [online]. 2023, 24.5. 2023 [cit. 2023-12-02]. Dostupné z WWW: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/eurodac.
9. Rada evropské unie. *Evropský systém pro cestovní informace a povolení (ETIAS): Rada přijala nařízení* [online]. 2018 [cit. 2023-12-02]. Dostupné z WWW: https://www.consilium.europa.eu/cs/press/press-releases/2018/09/05/european-travel-information-and-authorisation-system-etias-council-adopts-regulation/.

10. THALES. *The Schengen Entry/Exit System: biometrics to facilitate smart borders* [online]. [cit. 2023-12-02]. Dostupné z: WWW https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/eborder/entry-exit-systém.
11. EU-LISA. *European Criminal Records Information System – Third Country Nationals* [online]. 2019 [cit. 2023-12-02]. Dostupné z: https://www.eulisa.europa.eu/Publications/Information%20Material/Leaflet%20ECRIS-TCN.pdf.
12. PICUM. *Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status*. PDF. [online]. 2019 [cit. 2023-11-29]. Dostupné z WWW: https://picum.org/wp-content/uploads/2019/11/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf.
13. Policie ČR. *Národní programy Fondů EU v oblasti vnitřních věcí (ISF a AMIF)* [online]. [cit. 2024-01-18]. Dostupné z WWW: https://www.policie.cz/clanek/narodni-programy-fondu-eu-v-oblasti-vnitrnich-veci-isf-a-amif.aspx?q=Y2hudW09MTk%3d.
14. Ali, A., Baghel, V.S. & Prakash, S. *A novel technique for fingerprint template security in biometric authentication systems*. Vis Comput 39, 6249–6263 (2023). [cit. 2023-12-18]. Dostupné z WWW: https://doi-org.infozdroje.czu.cz/10.1007/s00371-022-02726-5.
15. A. K. Jain, A. Ross and S. Prabhakar, *"An introduction to biometric recognition,"* in IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, Jan. 2004, doi: 10.1109/TCSVT.2003.818349. [cit. 2023-12-21]. Dostupné z WWW: https://ieeexplore-ieee-org.infozdroje.czu.cz/stamp/stamp.jsp?tp=&arnumber=1262027&isnumber=28212.
16. Lott G. *The Dublin Convention and the Introduction of the 'First Entry Rule' in the Allocation of Asylum Seekers in Europe*. Contemporary European History. 2023;32(3):459-474.doi:10.1017/S0960777321000746. [cit. 2023-12-21].
17. van der Ploeg, I. The illegal body: `Eurodac' and the politics of biometric identification. Ethics and Information Technology 1, 295–302 (1999). [cit. 2023-12-18]. Dostupné z WWW:https://doi-org.infozdroje.czu.cz/10.1023/A:1010064613240.

18. Jurnal Kajian Ilmu Hukum dan Syariah. Volume 8, Number 2, 2023. P-ISSN: 2502-8006 E-ISSN: 2549-8274. [cit. 2023-12-21]. DOI: https://doi.org/10.22373/petita.v8i2.214.
19. MINISTERSTVO VNITRA. *Základní charakteristika cílového stavu infrastruktury IT PČR.* PDF. [online]. [cit. 2024-01-18]. Dostupné z WWW: https://www.zakazky.mvcr.cz/document_78965/99b65d7a7d74d2fd3bad33f188c75473-priloha-c-2-zakladni-charakteristika-cilove-infrastruktury-it-pcr-pdf.
20. MLADÝ PODNIKATEL. *Co to je SWOT analýza? A k čemu slouží?* [online]. [cit. 2024-01-08]. Dostupné z WWW: https://mladypodnikatel.cz/co-to-je-swot-analyza-t2797.
21. EVROPSKÝ PARLAMENT. *Řádný legislativní postup* [online]. [cit. 2024-02-28]. Dostupné z WWW: https://www.europarl.europa.eu/infographic/legislative-procedure/index_cs.html.

Legislativní dokumenty

1. ČESKO. Zákon č. 191/2016 Sb., o ochraně státních hranic České republiky a o změně některých zákonů, ve znění pozdějších předpisů.
2. Nařízení Evropského parlamentu a Rady (EU) 2016/399 ze dne 9. března 2016, kterým se stanoví kodex Unie o pravidlech upravujících přeshraniční pohyb osob (Schengenský hraniční kodex).
3. Nařízení Evropského parlamentu a Rady (EU) 2018/1860 ze dne 28. listopadu 2018 o využívání Schengenského informačního systému při navracení neoprávněně pobývajících státních příslušníků třetích zemí.
4. Nařízení Evropského parlamentu a Rady (EU) 2018/1861 ze dne 28. listopadu 2018 o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti hraničních kontrol, o změně Úmluvy k provedení Schengenské dohody a o změně a zrušení nařízení (ES) č. 1987/2006.
5. Nařízení Evropského parlamentu a Rady (EU) 2018/1862 ze dne 28. listopadu 2018 o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti policejní spolupráce a justiční spolupráce v trestních věcech, o změně a o zrušení rozhodnutí Rady 2007/533/SVV a o zrušení nařízení Evropského parlamentu a Rady (ES) č. 1986/2006 a rozhodnutí Komise 2010/261/EU.

6. Nařízení Evropského parlamentu a Rady (ES) č. 767/2008 ze dne 9. července 2008 o Vízovém informačním systému (VIS) a o výměně údajů o krátkodobých vízech mezi členskými státy (nařízení o VIS).
7. Nařízení Evropského parlamentu a Rady č. 603/2013 ze dne 26. 6. 2013 o zřízení systému EURODAC pro porovnávání otisků prstů za účelem účinného uplatňování nařízení EU č. 604/2013.
8. Nařízení Evropského parlamentu a Rady (EU) 2018/1240 ze dne 12. září 2018, kterým se zřizuje Evropský systém pro cestovní informace a povolení (ETIAS) a kterým se mění nařízení (EU) č. 1077/2011, (EU) č. 515/2014, (EU) 2016/399, (EU) 2016/1624 a (EU) 2017/2226.
9. Nařízení Evropského parlamentu a Rady (EU) 2017/2226 ze dne 30. listopadu 2017, kterým se zřizuje Systém vstupu/výstupu (EES) pro registraci údajů o vstupu a výstupu a údajů o odepření vstupu, pokud jde o státní příslušníky třetích zemí překračující vnější hranice členských států, kterým se stanoví podmínky přístupu do systému EES pro účely vymáhání práva a kterým se mění Úmluva k provedení Schengenské dohody a nařízení (ES) č. 767/2008 a (EU) č. 1077/2011.
10. Nařízení Evropského parlamentu a Rady (EU) 2019/817 ze dne 20. května 2019, kterým se zřizuje rámec pro interoperabilitu mezi informačními systémy EU v oblasti hranic a víz a mění nařízení Evropského parlamentu a Rady (ES) č. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 a (EU) 2018/1861 a rozhodnutí Rady 2004/512/ES a 2008/633/SVV.
11. Nařízení Evropského parlamentu a Rady (EU) 2019/818 ze dne 20. května 2019, kterým se zřizuje rámec pro interoperabilitu mezi informačními systémy EU v oblasti policejní a justiční spolupráce, azylu a migrace a kterým se mění nařízení (EU) 2018/1726, (EU) 2018/1862 a (EU) 2019/816.
12. Nařízení Evropského parlamentu a Rady (EU) 2019/816 ze dne 17. dubna 2019, kterým se zřizuje centralizovaný systém pro identifikaci členských států, jež mají informace o odsouzeních státních příslušníků třetích zemí a osob bez státní příslušnosti (ECRIS-TCN), na doplnění Evropského informačního systému rejstříků trestů, a kterým se mění nařízení (EU) 2018/1726.

Kvalifikační práce

1. DOSTÁL, Petr. *Policejní informační systémy a jejich využití v trestním řízení.* Brno, 2008. Bakalářská práce. Masarykova univerzita. Vedoucí práce prof. JUDr. Vladimír Kratochvíl, CSc.
2. PŠENICA, Tomáš. *Informační systémy ochrany vnějších hranic české republiky.* Příbram, 2021. Bakalářská práce. VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE. Vedoucí práce Mgr. Petr Malovec, Ph.D.

Ostatní zdroje

1. DOMANJA, Jindřich. Úvod do interoperability. PDF. Policie ČR, 2021.

7 Seznam obrázků, tabulek, grafů a zkratek

7.1 Seznam obrázků

7.2 Seznam grafů

7.3 Seznam použitých zkratek

API – Aplikační programové rozhraní

CAP – Centrální přístupový bod

CIR – The Common Identity Repository

EES – systém Entry/exit

ES – Evropské společenství

ESP – European Search Portal

EU – Evropská unie

ICD – Interface Control Document

IO – Interoperabilita

IS – Informační systém

ISF – Internal Security Fund

IT – Informační technologie

MID – The Multiple-Identity Detector

MVČR – Ministerstvo vnitra České republiky

NCIKT – Národní centrum informačních a komunikačních technologií

NS EES – Národní systém Entry/Exit

NUI – Národní jednotné rozhraní

PČR – Policie České republiky

ŘLZ – Ředitelství logistického zabezpečení

ŘMPS – Ředitelství pro mezinárodní policejní spolupráci

ŘSCP – Ředitelství služby cizinecké policie

SCIFA – Strategický výbor pro přistěhovalectví, hranice a azyl

sBMS – The shared Biometric Matching Service

Přílohy

Příloha 1 - Scénář strukturovaného rozhovoru se slovenským IT pracovníkem policie

Úvod

Tyto rozhovory jsou součástí praktické části diplomové práce, která si vede za cíl získat informace o zaváděných nových evropských systémech a jejich důležitosti v praxi z pohledu IT pracovníků policie. Pro získání relevantních dat a jejich posouzení byli osloveni pracovníci z České republiky, Slovenska a Belgie. Neméně důležitým cílem rozhovorů je analyzovat stavy zaváděných systémů ve zmíněných členských státech EU a z toho plynoucí příležitosti a rizika.

Otázky pro rozhovor byly sestaveny tak, aby naplnily stanovené cíle.

Vlastní otázky rozhovoru:

Otázka 1: **Myslíte si, že máte dostatečné informace, jak bude fungovat a co je interoperabilita ve smyslu EU nařízení č. 817/2019 a 818/2019?**

Odpověď: *Som presvedčený, že hlavný zmysel, resp. princíp fungovania IO mi je zrejmý. Vzhľadom však na rozsah právneho základu je veľmi pravdepodobné, že pri priamej technickej implementácii sa vyskytnú oblasti, ktoré bude nutné konzultovať s budúcimi biznis používateľmi na národnej úrovni a bude potrebné zohľadniť aj ich predpokladaný spôsob použitia. Rovnako dôležitá bude aj spolupráca s centrálnymi subjektmi (EK, eu-LISA), nakoľko skúsenosti z implementácie veľkých centrálnych EU systémov potvrdzujú, že priama implementácia otvorí otázky a bude požadovať riešenia, ktoré pri definovaní projektu, resp. jeho koncepcii nemuseli byť dostatočne známe. Veľkú rolu v tomto zohrávajú odlišnosti bežnej policajnej praxe v jednotlivých členských krajinách a od toho sa odvíjajú aj názory a spôsoby na implementáciu na EU úrovni spoločných IT riešení.*

Otázka 2: **Jakou vidíte praktickou využitelnost zaváděných systémů v rámci interoperability v praxi?**

Odpověď*: Vzhľadom na skúsenosti s implementáciou veľkých IT systémov EU (SIS, VIS) zastávam názor, že centralizácia policajne relevantných údajov za dodržania ich jednotnej štruktúry a vysokej technickej dostupnosti je veľmi efektívny spôsob podpory bežného výkonu policajnej praxe. Potvrdzujú to aj permanentne dosahované výsledky v oblasti medzinárodného pátrania po osobách a veciach, ktoré za dlhodobé obdobie používania*

majú neodiskutovateľný význam potvrdzovaný takmer z každej úrovne policajne relevantných subjektov v jednotlivých členských krajinách. Dostupnosť spoločne zdieľaných policajne relevantných údajov je bežným štandardom, ktorý je z úrovne aktívnych koncových používateľov vnímaný už ako samozrejmosť. Do tohto nastavenia IO vnáša nové prvky, ktoré s veľkým predpokladom pozitívne naviažu už získané skúsenosti z prevádzkovaných systémov. Zastávam názor, že každý jeden z pripravovaných systémov, ako aj ich vzájomná integrácia, významne ovplyvnia údajovú základňu nevyhnutnú pre správne posúdenie jednotlivých prípadov v rámci bežnej policajnej praxe nielen na vonkajších schengenských hraniciach, ale v podstatnej miere aj vo vnútrozemí členských krajín. Jednoznačným dopadom však bude požiadavka na zvýšenú erudíciu koncových používateľov týchto systémov a ich pochopenie vzájomnej integrácie týchto systémov. Každý zo systémov totiž podporuje špecifický výkon policajných činností, vyžadujúci si aj špeciálnu prípravu personálu. Integrácia IT systémov, najmä v závislosti na spôsobe ich technickej implementácie na národnej úrovni, môže spôsobiť prekrytie jednotlivých policajných úkonov. Tým sa môže otvoriť nie vždy transparentnú otázka prioritizácie policajných úkonov po línii jednotlivých policajných subjektov a ich kompetencií.

Otázka 3: **Jaké jsou náklady na zřízení a provoz takových systémů v porovnání s národními informačními systémy a jaké výhody/nevýhody spatřujete při implementaci evropských systémů?**

Odpověď: *Veľké EU IT systémy, vzhľadom na ich rozsah a dopady, sú na národnej úrovni dodávané externými IT subjektmi. Nakoľko implementácia zahŕňa nielen dodanie samotného technického SW riešenia a súvisiacej dokumentácie, ale častokrát aj HW podporu a podporu bežnej (a aj kritickej) prevádzky samotného systému, je ich finančná náročnosť vysoká. Je však porovnateľná s inými národnými IT systémami dodávanými externými subjektmi. Rozdiel je v tom, že národné aplikácie sú vytvárané výhradne na základe národného rozhodnutia a dispozícii potrebného finančného zabezpečenia. V prípade centrálnych systémov je rozhodnutie o ich implementácii nadnárodné a nie vždy korešponduje s reálnymi možnosťami ich časového, fyzického a finančného zabezpečenia. Veľmi negatívnu úlohu v tom zohráva posúvanie termínov implementácie jednotlivých IT systémov z úrovne EU, nakoľko alokácia dostupných zdrojov na národnej úrovni nie je nekonečná, resp. sa týmto výrazne predražuje. Negatívne môžu pôsobiť aj priebežné zmeny v už schválenej a na implementáciu publikovanej technickej dokumentácii.*

Otázka 4: **Co obnáší provoz těchto systémů z vašeho pohledu? Můžete vyjmenovat konkrétní příklady?**

Odpověď: *Požiadavky na prevádzku veľkých IT systémov predstavujú na národnej úrovni zvýšenú zodpovednosť za zabezpečenie ich vysokej dostupnosti a prevádzkyschopnosti pre koncových používateľov. Túto povinnosť je nutné integrovať aj do zmluvného zabezpečenia podpory týchto systémov s ich externými dodávateľmi, čo v konečnom dôsledku prináša zvýšenú mieru finančnej náročnosti na prevádzku systémov. Nakoľko sa jedná takmer výhradne o systémy kritickej infraštruktúry, ich prevádzka kladie zvýšené nároky aj na ich HW zázemie, fyzickú a objektovú bezpečnosť. V neposlednom rade zvýšený počet a dôležitosť prevádzkovaných systémov je potrebné pokryť aj dostatočnou kapacitou erudovaného personálneho zabezpečenia, ktoré musí byť dostupné v režime 24/7. Oblasť štátnej správy, ktorá tieto systémy prevádzkuje a používa, štandardne neposkytuje pre vysoko erudovaných IT pracovníkov adekvátne finančné zázemie, a preto je veľa prevádzkovo podporných činností pokrytých zmluvne s externými subjektmi.*

Otázka 5: **Popište, jak je řešeno technické zabezpečení v obecné rovině systémů v rámci interoperability (logování, síťové zabezpečení, přístupy uživatelů apod.).**

Odpověď*: Technické zabezpečenie systémov implementovaných a pripravovaných v rámci IO sa v princípe neodlišuje od štandardov aplikovaných na národnej úrovni. Okrem interného zabezpečenia na SW úrovni každého zo systémov, sú tieto integrované do národnej IT architektúry, ktorá, samozrejme pokrýva všetky oblasti technického zabezpečenia - logovanie, prístup používateľov, sieťovú konektivitu, HW cloud orientované riešenie, fyzickú a objektovú bezpečnosť, backup systémov v geograficky odlišných oblastiach. Určitým špecifikom je konektivita na EU sieťovú infraštruktúru, ktorá je čiastočne zabezpečovaná z EU úrovne v definovaných prístupových bodoch a technických komponentoch.*

Otázka 6: **Domníváte se, že nasazení těchto systémů v praxi bude odrážet v souladu s původním záměrem projektu (i myšlenkou) Smart Borders?**

Odpověď: *Domnievam sa, že každý zo systémov prinesie zvýšenú kvalitu pre potreby dennodennej policajnej praxe. Poskytne širšie údajové zdroje a možnosť ich posúdenia a akceptovania pre koncových používateľov. Zároveň však prinesie aj nutnosť ich ďalšieho vzdelávania sa a asi aj zvýšené pracovné zaťaženie, čo najmä u starších a konzervatívnejších pracovníkov môže vyvolať nevôľu a čiastočné odmietanie. Toto je ale*

pri novo implementovaných veciach bežný jav. Som presvedčený, že po určitej nábehovej dobe, klady prevýšia počiatočnú skepsu a dostupnosť významovo zaujímavých informácií bude vnímaná veľmi pozitívne.

Otázka 7: **Zhodnoťte přínosy, negativa tohoto řešení z pohledu pracovníků policie.**
Odpověď: *S odkazom na moju predchádzajúcu odpoveď bude akceptácia zo strany pracovníkov polície rôzna. Vo všeobecnosti by mala byť pozitívna, pre mnohých dokonca nové systémy poskytnú úplne nové pracovné zameranie a zaradenie. Na druhej strane to môže (takmer s určitosťou) priniesť zvýšenú pracovné zaťaženie na pracoviská, ktoré už dnes sú na hranici svojich aktuálnych personálnych kapacít – SIRENE pre SIS a CVO (centrálny vízový orgán) pre VIS. Oba subjekty budú konzumovať dopady implementácie IT systémov v rámci IO, čo sa prejaví na zvýšení ich zaťaženosti. Veľa bude záležať na miere automatizácie v rámci vzájomnej integrácie, resp. celkovej IT podpory pre ich úlohy v rámci IO.*

Otázka 8: **Je z Vašeho pohledu již celá Evropa připravená na zavedení interoperability systémů? V případě, že ano, uveďte, jaké kroky byly už uskutečněny.**
Odpověď: *Nie je, resp. iba čiastočne. Implementácia veľkých EU systémov je z úrovne EK (eu-LISA) sprevádzaná permanentnými zmenami časového harmonogramu, od toho sa odvíjajúcej zmeny legislatívneho rámca (alebo naopak), čo vytvára veľký tlak na členské krajiny a ich národné riešenia. V rámci harmonogramu IO sa vo veľmi krátkej časovej nadväznosti majú implementovať viaceré veľké EU systémy s rovnakou alebo približne rovnakou náročnosťou. Každý systém potrebuje určitý časový úsek na odladenie prípadných chýb a detailov a najmä na zapracovanie obslužného personálu a koncových používateľov – najpodstatnejších konzumentov týchto systémov. Súčasné alebo takmer súčasné nasadzovanie takýchto systémov bude sprevádzané štandardnými sprievodnými problémami a bude vnímane negatívne. Členské krajiny sú po policajnej línii a v zmysle harmonogramu viac-menej pripravené na implementáciu EES a ETIAS. Implementácia ďalších systémov je, aj vzhľadom na posúvanie časového harmonogramu zo strany EK, odsúvaná na neskoršie. Nie je v silách členských krajín (najmä z finančných dôvodov) mať sústavne k dispozícii dostatok alokovaných IT externých zdrojov, okrem interného a dostupného IT personálneho zabezpečenia. Rovnako, z dôvodu vysokého tempa vývoja technológií, nie je zmysluplné predčasné obstarávanie HW a infraštruktúrnych zdrojov.*

Otázka 9: **Kdy se očekává reálné spuštění všech komponent a systémů interoperability?**
Odpověď: *Tak ako som už uviedol, prvé bude EES a ETIAS. Ich reálne nasadenie je predpokladané v roku 2025. Osud ďalších systémov je, podľa mojich informácií z dôvodu stáleho vývoja právneho rámca a technických riešení predmetom ďalšieho obdobia. Doteraz nebol ešte publikovaný detailný integrovaný harmonogram, permanentne sa upravujú verzie ESP, CMD, ... Na Vami položenú otázku neviem odpovedať, akékoľvek tvrdenie bude iba v úrovni predpokladu, či odhadu.*

Otázka 10: **Jaké předpokládáte, že budou nutné organizační změny v rámci Policie ve vašem státě?**
Odpověď: *Nie som si celkom istý, či implementácia IO vyvolá aj organizačné zmeny v štruktúre Polície. To bude záležať na dostupných personálnych, priestorových a technických kapacitách už existujúcich pracovísk. Viaceré členské krajiny z dôvodu príbuznosti vykonávaných policajných činnosti pristupuje k ich kumulácii a uvažuje „iba" o personálnom posilnení už existujúcich pracovísk. Po IT línii nepredpokladám zmeny v organizačnej štruktúre.*

Otázka 11: **Obnáší z Vašeho pohledu zavádění evropských systémů pro členské státy nějaké problémy?**
Odpověď: *Zavedenie každého nového systému so sebou prináša prvotné problémy na každej úrovni technickej implementácie, podmienené overením ich správnej konfigurácie, výkonnosti, dostupnosti až po overenie korektnosti ich používateľskej funkcionality. V prípade zavedenia EU systémov ide navyše o aplikácie, resp. technológie, ktoré neboli iniciované z národnej úrovne, resp. určite nie zo všetkých národných úrovní. Preto nemusia a aj nie sú vnímané ako národná priorita. Skôr naopak, na úkor implementácie EU systémov sa odďaľuje nasadzovanie, resp. vývoj národných systémov. Dôvodom sú časové, finančné a personálne kapacity. Aj napriek finančnej podpore z prostriedkov EU fondov je implementácia veľkých EU systémov pre členské krajiny vynútenou záťažou, a teda aj problémom, riešenie ktorého treba prioritizovať.*

Otázka 12: **Přinese podle Vás řešení interoperability větší bezpečnost vnějších hranic EU?**
Odpověď: *Už som to spomínal, IO určite prinesie rozšírenie údajovej základne, komplexnejší pohľad na jednotlivé prípady a technicky modernejšie prostriedky. Toto všetko*

vytvára dosť veľký predpoklad a očakávania pre zvýšenie kvality činnosti policajných a spolupracujúcich bezpečnostných zložiek, čo by sa, v konečnom dôsledku, malo prejaviť na vyššej miere bezpečnosti vonkajších hraníc EU. Ako každé technické riešenie, tak aj veľké EU systémy majú však najslabší prvok vo svojom používateľovi – človeku, lebo finálne rozhodnutia budú vždy výsledkom humánnej činnosti. Technické riešenia, akokoľvek sofistikované, sú iba nástrojom. Veľmi dôležitým je preto vzdelávanie koncových používateľov, dôslednosť nimi vykonávaných činností a ich následnej kontrole pri dodržiavaní platného právneho rámca a nastavených pravidiel.

Otázka 13: **Myslíte si, že například systém Entry/Exit bude mít nějaký přínos při odhalování nelegální migrace? Konkretizujte ho, prosím.**

Odpověď: *V súvislosti s kontrolou pohybu osôb v teritóriu EU považujem zavedenie EES za jeden z najvýznamnejších krokov. Možnosť evidovania vstupu a opustenia tohto teritória osobami (aj nelegálnymi migrantmi) prejde z národných úrovní na centrálnu a umožní oveľa väčšiu mieru kontroly nad ich pohybom. Som presvedčený, že pri jeho dôslednom používaní môže veľmi výrazne pomôcť pri riešení otázky nelegálnej migrácie, minimálne poskytne údajovú základňu pre posudzovaní jednotlivých prípadov a korektnosť rozhodnutí o pobyte v EU.*

Otázka 14: **Chtěl byste ještě něco uvést případně doplnit?**

Odpověď: *V oblasti informatizácie policajných činností preferujem pre členské krajiny spoločné a vzájomné vyhovujúce riešenia, založené na jasne definovanej štruktúre údajov. Systémy by však zároveň mali reflektovať na reálne požiadavky a potreby členských krajín vyplývajúce z ich praktických skúseností. Pri tvorbe nových systémov je súčasne potrebné seriózne odborné posúdenie ich uvažovaného zamerania a aj reálna možnosť ich technickej implementácie a najmä zmysluplnej udržateľnosti..*

Děkuji Vám za poskytnutý rozhovor. Samozřejmě Vás rád s výsledky výzkumu a návrhem řešení mohu seznámit.

Poděkování.

Rozloučení.

Příloha 2 - Informovaný souhlas účastníka výzkumu

Informovaný souhlas týkající se poskytnutí informací pro zpracování praktické části diplomové práce na téma: „Evropské informační systémy a jejich využití v ČR při ochraně vnějších hranic".

Žádám Vás o souhlas s poskytováním rozhovoru ve formě audio nahrávky rozhovoru, který si vede za cíl získat informace o zaváděných evropských systémech a jejich důležitosti v praxi z pohledu IT pracovníků policie. Neméně důležitým cílem rozhovorů je analyzovat stavy zaváděných systémů a z toho plynoucí příležitosti a rizika.

Podpisem vyjadřuji souhlas s následujícími body:

- Byl/a jsem informován/a o účelu rozhovoru pro potřeby diplomové práce.
- Byla mi sdělena délka a průběh rozhovoru. Jsem seznámen/a s právem odmítnou odpovědět na jakoukoli otázku, případně do 3 dnů odmítnout účast na výzkumu.
- Souhlasím s nahráváním rozhovoru a jeho následným zpracováním. Zvukový záznam rozhovoru nebude poskytnut třetím stranám a po přepsání bude vymazán.
- Byl/a jsem obeznámen/a s tím, že bude zajištěna anonymita. Nikde nebude uvedeno mé jméno či jiné osobní údaje, díky kterým bych mohl/a být identifikován/a.

Já (dotazovaný), svobodně prohlašuji, že ve smyslu zákona č. 110/2019 Sb., o zpracování osobních údajů souhlasím se zpracováním osobních údajů a s účastí ve výše uvedeném výzkumném šetření a s poskytnutím dat.

Vlastnoruční podpis dotazovaného:.....

Bc. Tomáš PŠENICA (tazatel) se zavazuje nakládat se získanými daty ve smyslu výše zmíněného zákona č. 110/2019 Sb., o zpracování osobních údajů.

V Praze dne 8. 1. 2024 Podpis.....

Příloha 3 - Scénář strukturovaného rozhovoru s českým IT pracovníkem policie

Úvod

Tyto rozhovory jsou součástí praktické části diplomové práce, která si vede za cíl získat informace o zaváděných nových evropských systémech a jejich důležitosti v praxi z pohledu IT pracovníků policie. Pro získání relevantních dat a jejich posouzení byli osloveni pracovníci z České republiky, Slovenska a Belgie. Neméně důležitým cílem rozhovorů je analyzovat stavy zaváděných systémů ve zmíněných členských státech EU a z toho plynoucí příležitosti a rizika.

Otázky pro rozhovor byly sestaveny tak, aby naplnily stanovené cíle.

Vlastní otázky rozhovoru:

Otázka 1: **Myslíte si, že máte dostatečné informace, jak bude fungovat a co je interoperabilita ve smyslu EU nařízení č. 817/2019 a 818/2019?**

Odpověď: *Vzhledem k tomu, že jsem projektovým manažerem projektu interoperabilita v České republice (resp. v policii, na kterou padá 90 % všech povinností plynoucích z tohoto projektu), mám maximum možných informací, které jsou v různých dokumentech a na různých jednáních EU dostupné. A přesto tyto informace nejsou dostatečné pro plnohodnotnou realizaci tohoto projektu v ČR. Problém je, že neexistuje jedno autoritativní místo, kde by se sbíhaly veškeré informace. Jsou roztříštěny napříč různými nařízeními EU, napříč různými dokumenty různých agentur EU (eu-LISA, Frontex, Evropská komise, Europol, CEPOL), napříč technickou specifikací apod. Problém také je, že každý subjekt popisuje interoperabilitu pouze ze svého úzkého pohledu, tj. agentury EU zejména ze svého centrálního pohledu a příliš se nezabývají reálným fungováním interoperability v praxi z pohledu koncových uživatelů. To si musí odpracovat členské státy samy a nekoordinovaně, takže hrozí různá praxe v různých členských státech u procesů, které by ale měly být napříč EU jednotné.*

Otázka 2: **Jakou vidíte praktickou využitelnost zaváděných systémů v rámci interoperability v praxi?**

Odpověď*: V jádru interoperability sice stojí nové informační systémy, které mají lépe propojit současné i nově budované systémy, ale rozhodně se nejedná pouze o IT či technický projekt. interoperabilita pro koncové uživatele přináší zejména nové procesy odhalování vícenásobných totožností napříč šesti evropskými systémy podporujícími šest různých agend. Aby bylo možné tyto identitní vztahy řešit, musí spolu začít tyto dosud oddělené agendy začít komunikovat. V první řadě je tedy zapotřebí nastavit nové procesy tak, aby spolu koncoví uživatelé z oblasti hranic, víz, imigrace, policejní a justiční spolupráce mohli komunikovat a spolupracovat a identity společně řešit. Jde tedy o nový průřezový styl práce, který vyžaduje nejen nové komunikační nástroje, ale i nový mindset. Jedná se o značnou změnu v dosavadním způsobu práce, což s sebou přinese jak tradiční rezistenci uživatelů dělat věci jinak než dosud, tak ale i příležitosti k inovacím – nejen technickým, ale i organizačním a procesním.*

Otázka 3: **Jaké jsou náklady na zřízení a provoz takových systémů v porovnání s národními informačními systémy a jaké výhody/nevýhody spatřujete při implementaci evropských systémů?**

Odpověď: *Náklady na projekt interoperability jsou odhadovány cca na 200 milionů Kč, což řádově odpovídá obdobným rozsáhlým celoevropským projektům. Výhodou při implementaci je, že se jedná o povinný projekt plynoucí z legislativy EU, díky čemuž má „automatickou" prioritu oproti jiným čistě národním požadavkům. Pokud by totiž ČR nebyla v daný čas připravena, hrozilo by mezinárodní fiasko, za které by se musel zodpovídat ministr vnitra. Výhodou také je, že Evropská komise poskytuje fondy EU k financování těchto činností, byť ne v dostatečném objemu. Nevýhodou implementace evropských projektů je jejich složitost a přílišné množství subjektů, které se obtížně napříč EU koordinují a synchronizují.*

Otázka 4: **Co obnáší provoz těchto systémů z vašeho pohledu? Můžete vyjmenovat konkrétní příklady?**

Odpověď: *Nástroje interoperability (CIR, MID, ESP, sBMS) bude provozovat centrální evropská agentura eu-LISA, členské státy se k těmto komponentám mají pouze připojit a konzumovat jejich služby skrze národní (již existující) uživatelské systémy. Řada členských států vůbec žádný nový národní systém nebuduje a funkcionality interoperability pouze*

doimplementuje do již existujících systémů uživatelů. Tj. provoz těchto národních uživatelských systémů zůstane stejný jako dosud, jen budou obohaceny o nové funkčnosti. Naopak řada států, včetně ČR, buduje zcela nový národní back-endový systém interoperability, který bude jediným přípojným bodem k centrálním službám eu-LISA a který bude tyto služby konzumovat, obohacovat, harmonizovat a distribuovat dotčeným uživatelským národním systémům. Jde vlastně o middleware, resp. o integrační vrstvu mezi ČR a EU, která zajistí jednotnou orchestraci služeb. Tento systém bude provozovaný formou mikroslužeb s využitím technologií kontejnerizace (Kubernetes).

Otázka 5: **Popište, jak je řešeno technické zabezpečení v obecné rovině systémů v rámci interoperability (logování, síťové zabezpečení, přístupy uživatelů apod.).**

Odpověď*: Národní systém interoperability bude součástí významné či kritické infrastruktury dle zákona o kybernetické bezpečnosti č. 181/2014 a bude tedy muset být náležitě zabezpečen jak technickými, tak organizačními opatřeními. Základem bude bezpečnostní dokumentace, která bude pokrývat veškeré aspekty bezpečnosti, tj. fyzickou, řízení přístupu, reakce na incidenty apod. Systém bude logovat na třech úrovních – auditní logy, které uchovávají přístup uživatelů k osobním údajům (z důvodů GDPR a souvisejících kontrol), systémové logy (aplikační, technické události systému) a bezpečnostní logy, které budou monitorovat různá přednastavená pravidla, např. zadání špatného hesla třikrát po sobě v krátkém časovém úseku apod. Síťové zabezpečení do EU je řešeno evropskou zabezpečenou sítí TESTA-ng, která je skrze firewally propojena s interní sítí PČR. Systém interoperability je pouze back-endový, nemá přímé koncové uživatele – ti pracují se svými současnými uživatelskými systémy, které musí zajistit identifikaci, autentizaci a autorizaci uživatelů.*

Otázka 6: **Domníváte se, že nasazení těchto systémů v praxi bude odrážet v souladu s původním záměrem projektu (i myšlenkou) Smart Borders?**

Odpověď: *Otázkou je, který cíl máte na mysli – zda lepší zabezpečení hranic, nebo zefektivnění provádění hraniční kontroly ve smyslu jejího zrychlení. Formálně má totiž interoperabilita oba cíle, avšak v praxi jdou proti sobě. Vyšší zabezpečení znamená potřebu důkladnějšího prověřování osob a to znamená více potřebného času na každou osobu, případně její řešení na druhé kontrolní linii, kde se obecně z důvodu interoperability*

očekává vyšší nápor. Z dosavadních informací vyplývá, že interoperabilita povede k vyšší bezpečnosti, avšak na úkor delšího času.

Otázka 7: **Zhodnoťte přínosy, negativa tohoto řešení z pohledu pracovníků policie.**
Odpověď: *Odhalování vícenásobných totožností, což je hlavní proces, který interoperabilita přináší, doplní informace poskytované pracovníkům policie o to, zda daná osoba má nějakou potenciálně zneužitou či nejasnou identitu v jiných evropských systémech. To je určitě přínosem, protože se tak uživatel může lépe rozhodnout o tom, zda dotyčnému např. udělí vízum, cestovní povolení, vstup na území apod. Na druhou stranu je tato správa totožností velice komplikovaná, je založena na mnoha vazbách na úrovni identit, skupin souvisejících identit v rámci jednoho systému i skupin identit napříč systémy. Není vůbec jednoduché celou problematiku pochopit a je obtížně představitelné, že ji budou moci v rámci běžné agendy vykonávat všichni pracovníci policie. Zřejmě půjde o specializované činnosti směřované na hranicích na druhou kontrolní linii, což povede k jejímu zatížení.*

Otázka 8: **Je z Vašeho pohledu již celá Evropa připravená na zavedení interoperability systémů? V případě, že ano, uveďte, jaké kroky byly už uskutečněny.**
Odpověď: *Určitě ne. Evropská komise stále nedokončila finální sekundární legislativu (prováděcí předpisy – ty jsou hotovy cca z 90 %) ani příručku pro koncové uživatele (ta je hotova cca z 75 %). Agentura eu-LISA stále nevydala finální technickou specifikaci nástrojů interoperability, tudíž členské státy nemohou mít splněnou implementaci.*

Otázka 9: **Kdy se očekává reálné spuštění všech komponent a systémů interoperability?**
Odpověď: *Celý projekt měl původně být hotový do konce roku 2023. Postupně byl ne EU úrovni zpožďován a nyní by měl být hotov do konce roku 2027, avšak i nad tím visí mnoho otazníků.*

Otázka 10: **Jaké předpokládáte, že budou nutné organizační změny v rámci Policie ČR?**
Odpověď: *Dlouhodobě probíhá diskuse uvnitř PČR, zda bude kvůli interoperabilitě nutné zřídit novou organizační jednotku pro centralizované řešení vícenásobných totožností, anebo zda budou totožnosti řešeny jednotlivými pracovníky na hranicích, vízových orgánech, imigračních apod. Zatím se kloníme k druhé variantě, tj. k řešení totožností co*

nejblíže místu, kde jsou odhaleny, neboť tito pracovníci mají nejvíce informací k tomu, aby tyto totožnosti mohli zdárně vyřešit. Zřejmě tak bude mít každý útvar určeného aspoň jednoho specialistu na interoperabilitu, resp. odhalování totožností. V každém případě budou muset být pracovníci připraveni na to, že na rozdíl od současnosti budou muset komunikovat s pracovníky ostatních agend, aby společně vyřešili nejasné identity napříč různými agendami, tj. např. mezi agendami policie, justice, hranice, víza, imigrace apod. Také bude muset dojít k posílení daktyloskopických a antropologických expertů na Kriminalistickém ústavu, neboť součástí vícenásobných totožností jsou také nejasnosti v biometrii (otisky prstů, portrétní fotografie).

Otázka 11: **Obnáší z Vašeho pohledu zavádění evropských systémů pro členské státy nějaké problémy?**

Odpověď: *Interoperabilita je o významné změně práce uživatelů, což s sebou vždy nese riziko přijetí této změny ze strany uživatelů. Zároveň jde o projekt velmi náročný časově, finančně i personálně. Skutečnost, že se projekt dosud posunul z roku 2023 až na rok 2027, s sebou přináší značné vícenáklady, nutnost prodlužování smluv s dodavateli či uzavírání nových smluv apod. Z povahy věci je také projekt náročný na řízení/koordinaci, neboť zahrnuje řadu zainteresovaných subjektů nejen z různých útvarů policie, ale i z MV a dalších ministerstev, např. ministerstva spravedlnosti.*

Otázka 12: **Přinese podle Vás řešení interoperability větší bezpečnost vnějších hranic EU?**

Odpověď: *Pokud bude řešení interoperability implementováno chytře a jednoduše, aby jej přijali koncoví uživatelé, pak ano. Pokud však dojde k nesmyslnému a příliš složitému zatížení uživatelů novými a těžko srozumitelnými informacemi, pak budou uživatelé novinky interoperability ignorovat a žádný reálný benefit nepřinese.*

Otázka 13: **Myslíte si, že například systém Entry/Exit bude mít nějaký přínos při odhalování nelegální migrace? Konkretizujte ho, prosím.**

Odpověď: *Ano, zejména povede u třetizemců k systematickému využívání biometrie (otisky, fotky) na hranicích a pomůže odhalit osoby, které překročily povolenou délku pobytu v EU.*

Otázka 14: **Chtěl byste ještě něco uvést případně doplnit?**

Odpověď: *Vše již bylo řečeno ☺ Hodně štěstí celé EU s tímto projektem! Kéž je spuštěný včas, kvalitně a kéž jej uživatelé přijmou za své, aby přinesl reálné benefity ČR!*

Děkuji Vám za poskytnutý rozhovor. Samozřejmě Vás rád s výsledky výzkumu a návrhem řešení mohu seznámit.

Poděkování.

Rozloučení.

Příloha 4 - Informovaný souhlas účastníka výzkumu

Informovaný souhlas týkající se poskytnutí informací pro zpracování praktické části diplomové práce na téma: „Evropské informační systémy a jejich využití v ČR při ochraně vnějších hranic".

Žádám Vás o souhlas s poskytováním rozhovoru ve formě audio nahrávky rozhovoru, který si vede za cíl získat informace o zaváděných evropských systémech a jejich důležitosti v praxi z pohledu IT pracovníků policie. Neméně důležitým cílem rozhovorů je analyzovat stavy zaváděných systémů a z toho plynoucí příležitosti a rizika.

Podpisem vyjadřuji souhlas s následujícími body:

- Byl/a jsem informován/a o účelu rozhovoru pro potřeby diplomové práce.
- Byla mi sdělena délka a průběh rozhovoru. Jsem seznámen/a s právem odmítnou odpovědět na jakoukoli otázku, případně do 3 dnů odmítnout účast na výzkumu.
- Souhlasím s nahráváním rozhovoru a jeho následným zpracováním. Zvukový záznam rozhovoru nebude poskytnut třetím stranám a po přepsání bude vymazán.
- Byl/a jsem obeznámen/a s tím, že bude zajištěna anonymita. Nikde nebude uvedeno mé jméno či jiné osobní údaje, díky kterým bych mohl/a být identifikován/a.

Já (dotazovaný), svobodně prohlašuji, že ve smyslu zákona č. 110/2019 Sb., o zpracování osobních údajů souhlasím se zpracováním osobních údajů a s účastí ve výše uvedeném výzkumném šetření a s poskytnutím dat.

Vlastnoruční podpis dotazovaného:.....

Bc. Tomáš PŠENICA (tazatel) se zavazuje nakládat se získanými daty ve smyslu výše zmíněného zákona č. 110/2019 Sb., o zpracování osobních údajů.

V PRAZE dne 9. 1. 2024 Podpis.....

Příloha 5 - Scénář strukturovaného rozhovoru s belgickým IT pracovníkem policie

Introduction

These interviews are part of the practical part of the diploma thesis, which aims to obtain information about the new European systems being implemented and their importance in practice from the point of view of police IT workers. Workers from the Czech Republic, Slovakia and Belgium were approached to obtain relevant data and assess them. An equally important goal of the interviews is to analyze the status of the implemented system in the mentioned EU member states and the resulting opportunities and risks.

The interview questions were designed to meet the stated objectives.

Custom interview questions:

Question 1: **Do you think you have enough information about how interoperability will work and what it is (as per the EU regulation No. 817/2019 and 818/2019)?**

Answer: *I have enough information about what IO is, but no one actually knows yet how IO will work in real life. We are working on it in COM's working and expert groups together with other Member States (MS).*

Question 2: **How do you see the practical usability of the implemented systems within the scope of interoperability in practice?**

Answer: *IO must be used practically, in fact this is the main requirement. The project should be approached from end-users' perspective, not from the central technical side, which is currently the case. Otherwise the user acceptance is endangered.*

Question 3: **What are the costs of setting up and running such systems compared to national information systems and what advantages/disadvantages do you see when implementing European systems?**

Answer: *IO is another EU system besides EES, ETIAS, VIS, ECRIS, Eurodac and SIS. The costs of all of them are comparable. However, compared to national (not european) systems, the costs of EU systems in general are much higher, because the timeline is still moving and so it the target (what to do). That's the biggest disadvantage of the project.*

Question 4: **What does the operation of these systems involve from your point of view? Can you name specific examples?**

Answer: *BE is of the opinion that MS should bear no costs of the operations. Instead, eu-LISA should build the application for multiple identity detection (MID) and should provide it to MS cost-free. The disadvantage is that it would be another user application for end-user.*

Question 5: **Describe how technical security is handled at the general level of systems within the framework of interoperability (logging, network security, user access, etc.).**

Answer: *Should be secured by eu-LISA, MS should only be responsible for IAM (identity and access management). Logging and network shall be secured centrally.*

Question 6: **Do you think that the deployment of these systems in practice will reflect the original intention of the project (and the idea) of Smart Borders?**

Answer: I don't know exactly, Smart Borders are done by a different team and organ, but it should be alligned.

Question 7: **Evaluate the benefits, negatives of this solution from the perspective of police personnel.**

Answer: *As is mentioned above – BE thinks that eu-LISA should provide MS with a solution for MID, so that all MS would use the same tool for the same processes. This is good from costs perspective, but not so good from end-users' perspective, since they will have to have a separate app for this task.*

Question 8: **From your point of view, is the whole of Europe ready for the introduction of interoperability of systems? If yes, indicate what steps have already been taken.**

Answer: *No.*

Question 9: **When is the actual launch of all interoperability components and systems expected?**

Answer: *From 2024 till 2027.*

Question 10: **What organizational changes do you assume will be necessary within the Police in your state?**

Answer: *New MID unit will be established to deal with the identities.*

Question 11: **From your point of view, does the introduction of European systems entail any problems for the member states?**
Answer: *If each Ms develops their own application for MID, it will be a chaos and a mess, because everyone will do it differently and we will not understand each other.*

Question 12: **Do you think the interoperability solution will bring greater security to the EU's external borders?**
Answer: *It should, that's the whole purpose.*

Question 13: **Do you think that, for example, the Entry/Exit system will have any benefit in detecting illegal migration? Please specify it.**
Answer: *I don't know, EES is done by a different team, but MID will support them with new information for better decision-making, so I guess yes.*

Question 14: **Would you like to state/add anything else?**
Answer: *No. Thank you.*

Thank you for the interview. Of course, I would be happy to introduce you to the results of the research and the proposed solution.

Thanks.
Farewell.

Appendix 6 - Informed consent of the research participant

Informed consent regarding the provision of information for processing the practical part of the diploma thesis on the topic: "European information systems and their use in the Czech Republic in the protection of external borders".

I am asking for your consent to provide an interview in the form of an audio recording of the interview, which aims to obtain information about the introduced European systems and their importance in practice from the point of view of the IT staff of the police. An equally important goal of the interviews is to analyze the status of the implemented systems and the resulting opportunities and risks.

By signing, I agree to the following points:

- I was informed about the purpose of the interview for the needs of the diploma thesis.
- I was told the length and course of the interview. I am aware of the right to refuse to answer any question or to refuse to participate in the research within 3 days.
- I agree to the recording of the interview and its subsequent processing. The audio recording of the interview will not be provided to third parties and will be deleted after being transcribed.
- I am aware that anonymity will be ensured. Nowhere will my name or other personal information by which I could be identified be mentioned.

I (the respondent), freely declare that, in accordance with Act No. 110/2019 Coll., on the processing of personal data, I agree to the processing of personal data and to participation in the above-mentioned research investigation and to the provision of data.

Handwritten signature of the interviewee:.....

Bc. Tomáš PŠENICA (interviewer) undertakes to handle the obtained data in accordance with the aforementioned Act No. 110/2019 Coll., on the processing of personal data.

In PRAHA on 18.1.2024 Signature.....

Příloha 7 - Překlad přílohy 5 - Scénář strukturovaného rozhovoru s belgickým IT pracovníkem policie

Úvod

Tyto rozhovory jsou součástí praktické části diplomové práce, která si vede za cíl získat informace o zaváděných nových evropských systémech a jejich důležitosti v praxi z pohledu IT pracovníků policie. Pro získání relevantních dat a jejich posouzení byli osloveni pracovníci z České republiky, Slovenska a Belgie. Neméně důležitým cílem rozhovorů je analyzovat stavy zaváděných systémů ve zmíněných členských státech EU a z toho plynoucí příležitosti a rizika.

Otázky pro rozhovor byly sestaveny tak, aby naplnily stanovené cíle.

Vlastní otázky rozhovoru:

Otázka 1: **Myslíte si, že máte dostatečné informace, jak bude fungovat a co je interoperabilita ve smyslu EU nařízení č. 817/2019 a 818/2019?**

Odpověď: *Mám dostatek informací o tom, co je IO, ale nikdo zatím vlastně neví, jak bude IO fungovat v reálném životě. Pracujeme na tom v pracovních a expertních skupinách COM společně s dalšími členskými státy (ČS).*

Otázka 2: **Jakou vidíte praktickou využitelnost zaváděných systémů v rámci interoperability v praxi?**

Odpověď*: IO musí být prakticky využitelné, to je vlastně hlavní požadavek. K projektu je třeba přistupovat z pohledu koncových uživatelů, nikoliv z centrální technické stránky, jak je tomu v současnosti. V opačném případě je ohroženo přijetí uživateli.*

Otázka 3: **Jaké jsou náklady na zřízení a provoz takových systémů v porovnání s národními informačními systémy a jaké výhody/nevýhody spatřujete při implementaci evropských systémů?**

Odpověď: *IO je vedle systémů EES, ETIAS, VIS, ECRIS, Eurodac a SIS dalším systémem EU. Náklady na všechny jsou srovnatelné. V porovnání s národními (ne evropskými) systémy jsou však náklady na systémy EU obecně mnohem vyšší, protože se stále posouvá časová osa a s ní i cíl (co dělat). To je největší nevýhoda projektu.*

Otázka 4: **Co obnáší provoz těchto systémů z vašeho pohledu? Můžete vyjmenovat konkrétní příklady?**
Odpověď: *BE je toho názoru, že členské státy by neměly nést žádné náklady na provoz. Místo toho by agentura eu-LISA měla vytvořit aplikaci pro zjišťování vícenásobné totožnosti (MID) a měla by ji členským státům poskytnout bez nákladů. Nevýhodou je, že by se jednalo o další uživatelskou aplikaci pro koncového uživatele.*

Otázka 5: **Popište, jak je řešeno technické zabezpečení v obecné rovině systémů v rámci interoperability (logování, síťové zabezpečení, přístupy uživatelů apod.).**
Odpověď: *V tomto případě se jedná o zabezpečení, které je v rozporu se zásadami bezpečnosti: Mělo by být zajištěno agenturou eu-LISA, MS by měl být odpovědný pouze za IAM (správu identit a přístupu). Logování a síť by měly být zabezpečeny centrálně.*

Otázka 6: **Domníváte se, že nasazení těchto systémů v praxi bude odrážet v souladu s původním záměrem projektu (i myšlenkou) Smart Borders?**
Odpověď: *Nevím přesně, Chytré hranice dělá jiný tým a jiný orgán, ale mělo by to být sladěno.*

Otázka 7: **Zhodnoťte přínosy, negativa tohoto řešení z pohledu pracovníků policie.**
Odpověď: *ak je uvedeno výše – BE se domnívá, že by agentura eu-LISA měla poskytnout členským státům řešení pro MID, aby všechny členské státy používaly stejný nástroj pro stejné procesy. To je dobré z hlediska nákladů, ale ne tak dobré z hlediska koncových uživatelů, protože ti budou muset mít pro tento úkol samostatnou aplikaci.*

Otázka 8: **Je z Vašeho pohledu již celá Evropa připravená na zavedení interoperability systémů? V případě, že ano, uveďte, jaké kroky byly už uskutečněny.**
Odpověď: *Ne.*

Otázka 9: **Kdy se očekává reálné spuštění všech komponent a systémů interoperability?**
Odpověď: *V nejbližší době se počítá s interoperabilitou: Od roku 2024 do roku 2027.*

Otázka 10: **Jaké předpokládáte, že budou nutné organizační změny v rámci Policie ČR?**
Odpověď: *Bude zřízena nová jednotka MID, která se bude zabývat identitami.*

Otázka 11: **Obnáší z Vašeho pohledu zavádění evropských systémů pro členské státy nějaké problémy?**
Odpověď: *Pokud si každá paní vytvoří vlastní aplikaci pro MID, bude to chaos a zmatek, protože to každý bude dělat jinak a nebudeme si rozumět.*

Otázka 12: **Přinese podle Vás řešení interoperability větší bezpečnost vnějších hranic EU?**
Odpověď: *To by mělo, to je celý účel.*

Otázka 13: **Myslíte si, že například systém Entry/Exit bude mít nějaký přínos při odhalování nelegální migrace? Konkretizujte ho, prosím.**
Odpověď: *Jaký je váš názor na tuto otázku? Nevím, EES dělá jiný tým, ale MID je podpoří novými informacemi pro lepší rozhodování, takže asi ano.*

Otázka 14: **Chtěl byste ještě něco uvést případně doplnit?**
Odpověď: *Ne. Děkuji.*

Děkuji Vám za poskytnutý rozhovor. Samozřejmě Vás rád s výsledky výzkumu a návrhem řešení mohu seznámit.

Poděkování.
Rozloučení.

Příloha 8 - Překlad přílohy 6 - Informovaný souhlas účastníka výzkumu

Informovaný souhlas týkající se poskytnutí informací pro zpracování praktické části diplomové práce na téma: „Evropské informační systémy a jejich využití v ČR při ochraně vnějších hranic“.

Žádám Vás o souhlas s poskytováním rozhovoru ve formě audio nahrávky rozhovoru, který si vede za cíl získat informace o zaváděných evropských systémech a jejich důležitosti v praxi z pohledu IT pracovníků policie. Neméně důležitým cílem rozhovorů je analyzovat stavy zaváděných systémů a z toho plynoucí příležitosti a rizika.

Podpisem vyjadřuji souhlas s následujícími body:

- Byl/a jsem informován/a o účelu rozhovoru pro potřeby diplomové práce.
- Byla mi sdělena délka a průběh rozhovoru. Jsem seznámen/a s právem odmítnou odpovědět na jakoukoli otázku, případně do 3 dnů odmítnout účast na výzkumu.
- Souhlasím s nahráváním rozhovoru a jeho následným zpracováním. Zvukový záznam rozhovoru nebude poskytnut třetím stranám a po přepsání bude vymazán.
- Byl/a jsem obeznámen/a s tím, že bude zajištěna anonymita. Nikde nebude uvedeno mé jméno či jiné osobní údaje, díky kterým bych mohl/a být identifikován/a.

Já (dotazovaný), svobodně prohlašuji, že ve smyslu zákona č. 110/2019 Sb., o zpracování osobních údajů souhlasím se zpracováním osobních údajů a s účastí ve výše uvedeném výzkumném šetření a s poskytnutím dat.

Vlastnoruční podpis dotazovaného:……

Bc. Tomáš PŠENICA (tazatel) se zavazuje nakládat se získanými daty ve smyslu výše zmíněného zákona č. 110/2019 Sb., o zpracování osobních údajů.

V……dne……..Podpis……