

Příjemci podpory:
Poskytovatel:

AISEE - AI Softwarový expertní vyhledávač pro videa a fotografie
VJ02010029

Výzkumná zpráva

Typ výsledku dle Definice druhů výsledků	Evidenční číslo (příjemce)	Rok vzniku
Ostatní výsledky	AISEE výzkumná zpráva	2025
ISBN/ISSN (pokud je k dispozici)	Webový odkaz na výsledek (pokud je k dispozici)	Kde a kdy publikováno (v případě publikačních výsledků)
	aisee.utia.cas.cz	

Stručná anotace k výsledku v českém jazyce:

Výzkumná zpráva shrnuje a evaluuje vyvinuté softwarové řešení a jeho chování v okrajových a limitních podmínkách a robustnost při různé kvalitě vstupních videozáznamů. V navazující části obsahuje analýzu použitelnosti a efektivity vybraných AI přístupů využitých v platformě, a to s ohledem na reálné scénáře forenzní praxe. Druhá část se věnuje etickým, právním a lidsko-právním aspektům využití AI při vytěžování dat ve forenzní oblasti a doplňuje doporučení pro zodpovědné používání systému v kontextu aktuální regulace.

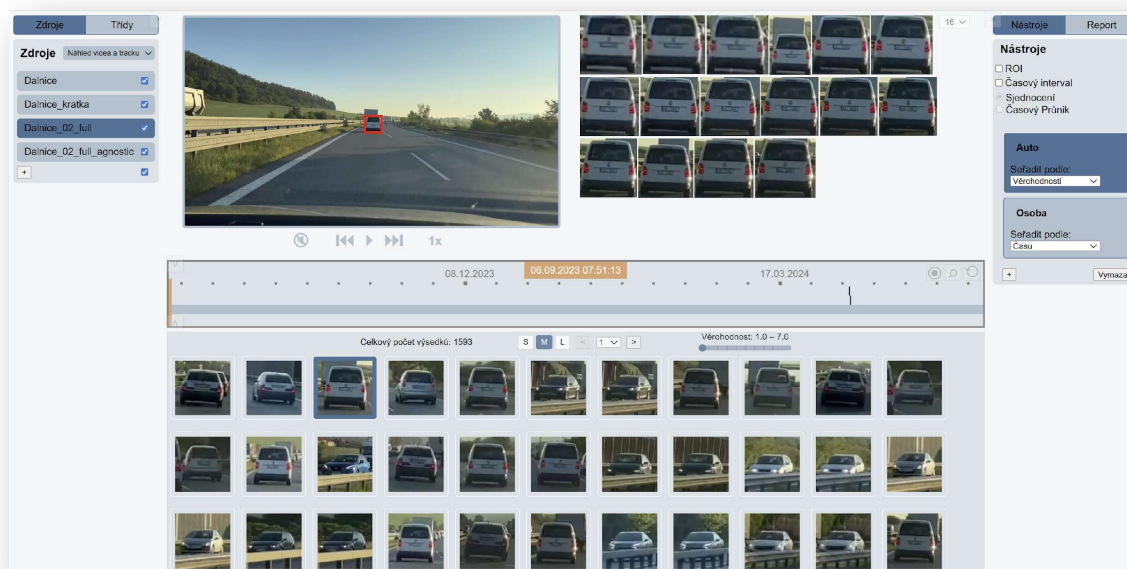
Řešitelský tým:

Jaroslava Marešová ÚTIA, Barbara Zitová ÚTIA, Ondřej Chum ČVUT, Alžběta Solarczyk Krausová ÚSP, Pavel Smrž VUT, Jan Fusser ÚTIA, Michal Bartoš ÚTIA, Jan Kamenický ÚTIA, Babak Mahdian ÚTIA, Filip Šroubek ÚTIA, Michal Neoral ČVUT, Ruslan Rozumnyj ČVUT, Michal Hradiš VUT, Roman Juránek VUT, Pavel Zemčík VUT, Marek Šolony VUT, Markéta Juránková VUT, Zdeněk Materna VUT

OBSAH

Evaluace AISEE.....	3
Kontext policejní operativy: typické scénáře	5
Parametry nahrávání a jejich operační význam	6
Úvod do metod a filtrů	6
Doporučené operační workflow (SOP pro analytika)	9
Reporty v operativě: Dokumentace nálezů	10
Technické limity a interpretace výsledků	11
Architektura detekce a klasifikace objektů	12
Detekce objektů	13
Tracking - trasování objektů	14
Popis a klasifikace.....	15
Doučování objektů z příkladů	15
Testování	16
Adaptace a optimalizace modelu SigLIP2 pro vyhledávání a re-identifikaci osob	16
Nastavení parametrů.....	17
Evaluace robustnosti detekční pipeline vůči degradaci vstupu	20
Evaluace robustnosti detekčně-klasifikační pipeline vůči degradaci vstupu.....	21
Evaluace detekčně-klasifikační pipeline	24
Doučování.....	25
Klasifikátor, trénování a doučování nových tříd.....	26
Závěry	28
Doporučení pro praxi.....	29
Právní, etické a procesní aspekty nasazení AISEE	29
1. Normativní rámec pro inteligentní systémy se zvláštním ohledem na oblast policejní práce..	29
2. Právní posouzení systému AISEE	37
3. Etické aspekty nasazení systému AISEE.....	45
Manuál pro používání systému AISEE	46
Příloha č. 1: Výsledek posouzení systému AISEE přes EU AI Act Compliance Checker	47
Příloha č. 2: Manuál pro používání systému AISEE	54
Appendix: Metriky AISEE	58

AISEE je softwarová platforma určená pro AI vytěžování a vyhledávání informací ve videozáznamech v kontextu forenzní praxe, tj. pro rychlé zúžení a prioritizaci částí záznamu relevantních pro vyšetřování. AISEE zrychluje práci analytika pomocí efektivní detekce objektů, jejich trasování (tracky) a následného vyhledávání a filtraci v čase. Výsledky slouží jako vodítko pro lidské ověření, nikoli jako samostatný důkaz bez kontroly člověkem.



EVALUACE AISEE

AISEE je navržen jako praktický nástroj pro rychlé zúžení a následnou prioritizaci prohlížení videozáznamů v operativní činnosti. Jeho hlavní přínos spočívá v tom, že místo čistě ručního „projíždění“ hodin záznamu umožňuje analytikovi během krátké doby vymezit relevantní úseky a objekty zájmu a soustředit pozornost na momenty, které s nejvyšší pravděpodobností souvisí se sledovanou událostí. V operativním pojetí se tedy AISEE používá primárně jako akcelérátor orientace v datech – pro rychlé vytipování stop, nikoli jako náhrada odborného posouzení.

Základní princip práce AISEE je dvoufázový. V první fázi systém po nahrání videozáznamu provede automatické předzpracování a analýzu. Nejprve proběhne extrakce snímků z videa podle parametru *Frame Step*, kdy systém neanalyzuje každý jednotlivý snímek, ale pouze každý *n*-tý (zvolený krok). Tím je možné řídit kompromis mezi rychlostí zpracování a jemností zachycení krátkých dějů. Na takto připravených snímcích se následně spustí detekce a tracking objektů jehož výsledkem nejsou izolované jednorázové detekce, ale tzv. tracky – tedy časové „stopy“ objektů, které propojují výskyty téhož objektu napříč snímky. Tracky jsou pro operativu klíčové: umožňují rychleji pochopit pohyb objektu v čase, omezují chaos způsobený jednotlivými náhodnými detekcemi a poskytují přirozený základ pro filtrování a procházení výsledků.

Na tento výstup navazuje pokročilá analýza, při níž se pro objekty/obrazové výřezy vytvářejí tzv. embeddingy (vektorové reprezentace). Tyto embeddingy jsou zásadní, protože umožňují nad stejnými daty provádět nejen „tvrdé“ filtrování podle předem definovaných tříd, ale také vyhledávání textem, vyhledávání obrázkem a funkci „najít podobné“ (vyhledání vizuálně podobných výskytů).

Ve druhé fázi už pracuje analytik přímo s výsledky systému. Z operativního hlediska AISEE poskytuje tři hlavní pracovní roviny. První rovinu tvoří filtry, které umožňují rychle zúžit prostor hledání – typicky na konkrétní oblast obrazu (*ROI*), na konkrétní časový úsek, na určitou třídu/typ tracku nebo jen na vybrané sekvence (kamery) v projektu. Druhou rovinu tvoří vyhledávání, které umožňuje formulovat dotaz buď textově (popisem hledaného jevu), obrázkem (referenčním snímkem či fotografií) nebo cestou podobnosti (rozšíření hledání od jednoho nalezeného „seedu“ k dalším podobným výskytům). Třetí rovinu představuje report, který slouží k rychlé a průběžné dokumentaci relevantních nálezů a k jejich předání v podobě srozumitelného výstupu (tj. zaznamenání „kde, kdy a co“ bylo nalezeno, včetně náhledu a komentáře).

Pro správné operativní použití je podstatné zdůraznit, že AISEE nenahrazuje lidské ověření. Výsledky je vhodné chápat jako indikace a vodítka, která mají analytikovi usnadnit rychlé nalezení relevantních momentů, nikoli jako definitivní závěry. Každý nález je proto nutné ověřit v kontextu původního záznamu (přehráním příslušného úseku, kontrolou návazností a případně porovnáním napříč kamerami). Tato zásada je důležitá zejména proto, že praktická použitelnost systému se vždy odvíjí od limitních vlastností vstupních dat i zvolených nastavení.

Klíčové limity, se kterými se v praxi typicky setkáváme, téměř vždy souvisí s několika opakujícími se faktory.

1. Kvalita videozáznamu – rozlišení, míra komprese, světelné podmínky (noc, protisvětlo), rychlý pohyb a rozmazání, případně zakrývání objektů.
2. Velikost objektu v obraze, prakticky vyjádřená v pixelech: pokud je objekt příliš malý, ztrácí se jeho rozlišitelné znaky a detekce i následné vyhledávání se stává nespolehlivé.
3. Nastavení *Frame Step*, které přímo určuje kompromis mezi rychlostí a rizikem, že systém „přeskočí“ krátkou událost (např. rychlé předání předmětu nebo krátké objevení objektu v záběru).

4. Způsob, jakým je položen dotaz: u textového vyhledávání záleží na přesnosti formulace (míra konkrétnosti, jazyk, popis atributů), zatímco u vyhledávání obrázkem a podobností je rozhodující kvalita referenčního obrázku (ostrost, velikost, míra ořezu na skutečný objekt, rozdíl mezi referencí a reálnými podmínkami CCTV).

Z uvedených důvodů každá metoda vyhledávání a filtrace určuje praktické hranice použitelnosti (např. minimální velikost objektu v pixelech, minimální velikost a typ referenčního obrázku, citlivost na kompresi a světlo, dopad Frame Step na zachycení krátkých dějů). Stanovené limity umožní nastavit realistická očekávání a vytváří doporučené pracovní postupy pro operativu. Ty pak zajistí, aby AISEE v praxi poskytoval stabilní přínos a minimalizoval riziko přehlédnutí relevantního jevu nebo naopak zahlcení falešnými nálezy.

KONTEXT POLICEJNÍ OPERATIVY: TYPICKÉ SCÉNÁŘE

Pro kavlitu vyhledávání je dobré si připomenout co a jak je vlastně potřeba hledat. V policejní operativě je AISEE použití myšleno jako rychlé vyfiltrování relevantních dat z (potenciálně velkého) množství dat. Typicky je znám přibližný čas události a je potřeba během několika minut vytáhnout relevantní osoby/vozidla/předměty v konkrétním incidentním okně, nebo se ví místo v záběru (např. vchod, pokladna, kufr auta) a pracuje se se zónou ROI, která výrazně zredukuje šum mimo zájmovou oblast. V řadě případů máme jen slovní popis („muž s batohem“, „červené auto“, „nůž v ruce“) a využije se textový dotaz jako rychlé předtřídění; pokud máte k dispozici přímo screenshot nebo fotografii hledané věci, je vhodné použít vyhledávání obrázkem. Jakmile se podaří najít jeden kvalitní výskyt, v operativě se často vyplatí postup „seed and expand“, tj. použít funkci Najít podobné pro dohledání dalších výskytů téhož nebo vizuálně velmi podobného objektu v záznamech. A konečně, pokud jde o specifický „netypický“ objekt, který základní třídy nepokrývají, AISEE umožňuje využít doučování (vlastní třídu), aby systém odpovídal konkrétním potřebám případu nebo lokálního prostředí. Tedy:

1. **Incidentní okno**

„V čase 21:10–21:25“ – rychle najít osoby/vozidla/objekty v daném intervalu.

2. **Zónový scénář**

„U vchodu“ / „u pokladny“ / „u kufru auta“ – ROI výrazně zredukuje šum.

3. **Popisový scénář**

„Muž s batohem“, „červené auto“, „nůž v ruce“ – textový dotaz jako rychlý filtr.

4. **Referenční scénář**

Máme screenshot / foto věci → hledání obrázkem.

5. **Seed-and-expand**

Najdeme jeden dobrý výskyt → „Najít podobné“ pro další výskyty.

6. **Specifický objekt**

Něco „netypického“, co základní třídy nepokrývají → doučování (vlastní třída).

PARAMETRY NAHRÁVÁNÍ A JEJICH OPERAČNÍ VÝZNAM

Při nahrávání videa je nutné definovat několik klíčových parametrů. Název sekvence slouží primárně k identifikaci konkrétní kamery, zatímco offset určuje její časové posunutí oproti ostatním. V případě pevně umístěných kamer, typicky u CCTV systémů, se doporučuje aktivovat funkci „Statická kamera“. Standardně jsou při nahrávání zapnuty oba hlavní procesy zpracování – detekce i pokročilá klasifikace.

Kritickým parametrem pro kvalitu analýzy je Frame Step (FS), který určuje, že systém zpracuje pouze každý n -tý snímek (např. při FS=2 se analyzuje každý druhý snímek, při FS=5 každý pátý). Tím se fakticky snižuje efektivní snímkovací frekvence (FPS) pro potřeby analýzy, což má přímé důsledky pro operativu.

Při volbě Frame Stepu je nutné zohlednit povahu hledané události i původní FPS videa. Pokud existuje riziko výskytu velmi krátkých dějů, jako je vytažení zbraně, rychlá výměna předmětu nebo přeběhnutí osoby, je nezbytné nastavit Frame Step na hodnotu 1 až 2, aby nedošlo k jejich ztrátě. Naopak vyšší hodnoty (např. FS=5) jsou vhodné pro rychlé předtřídění dlouhých záznamů nebo obecný monitoring, ovšem vždy s vědomím rizika, že krátké události nemusí být zachyceny. V případě, že je zdrojové video rozděleno na více částí (segmentů), je vhodné využít funkce pro seřazení souborů podle názvu a jejich následné sloučení do jedné sekvence.

ÚVOD DO METOD A FILTRŮ

Tato kapitola sjednocuje dostupné metody a filtry do jednotného metodického rámce, který uživateli usnadní rozhodování, kdy a jak konkrétní nástroj použít. U každé metody jsou definovány čtyři klíčové aspekty: situace vhodné pro její nasazení, postup aktivace v rozhraní AISEE, faktory ovlivňující kvalitu výsledku a přehled typických selhání, kterým je třeba předcházet.

5.1 ROI (REGION OF INTEREST)

Filtr Region of Interest (ROI) je určen primárně pro situace, kdy je nutné zaměřit analýzu na konkrétní zónu v obraze, jako je například vchod do budovy, okno automobilu, prostor před bankomatem nebo vymezený úsek chodníku. Tento nástroj je velmi efektivní v případech, kdy je scéna vizuálně „rušná“, a umožňuje výrazně snížit šum tím, že ignoruje dění mimo vyznačenou oblast. Pro aktivaci funkce stačí v panelu Nástroje zvolit položku ROI a následně myší přímo v obraze vyznačit požadovanou oblast zájmu.

Výslednou kvalitu detekce ovlivňuje několik faktorů, především správně zvolená velikost oblasti. Příliš velká ROI nemusí dostatečně odfiltrovat rušivé elementy, zatímco příliš malá oblast může vést ke ztrátě části děje. Roli hraje také perspektiva scény – objekt se sice může nacházet uvnitř vyznačené zóny, ale pokud je v daném místě příliš malý, detektor jej nemusí zaznamenat.

Při použití je nutné brát v úvahu typ kamery, protože ROI je fixována na souřadnice obrazu, nikoliv na fyzickou scénu. K typickému selhání v operativní praxi dochází v momentě, kdy je ROI nastavena na zdánlivě statickou scénu, ale kamera je ve skutečnosti lehce pohyblivá (například vlivem vibrací nebo posunu PTZ). V takovém případě se fyzický prostor „posouvá“ mimo vyznačený rámeček, což vede k nekonzistentním a nespolehlivým výsledkům.

5.2 ČASOVÝ INTERVAL

Filtr Časový interval je nezbytným nástrojem v situacích, kdy je vyšetřování ohraničeno konkrétním časovým oknem. Typicky se využívá v případech podložených přesným časem z tísňové linky, výpovědi svědka nebo systémových logů a výpisů událostí. Aktivace a nastavení tohoto filtru probíhá interaktivně přímo na časové ose (timeline) v panelu Nástroje.

Pro správnou funkčnost je kritickým faktorem přesné nastavení offsetu (časového posunu), a to zejména u projektů využívajících více kamer. Výsledek je rovněž ovlivněn zvoleným snímkovacím krokem (Frame Step) – při nevhodném nastavení hrozí riziko, že velmi krátký děj proběhne mezi zpracovávanými snímky a nebude zachycen. K typickému selhání dochází při práci s nesprávně posunutými sekvencemi, kdy analytik v důsledku chybného offsetu hledá událost v nesprávném reálném čase.

5.3 VÝBĚR SEKVENCÍ (ZDROJŮ)

Tento nástroj slouží k cílené práci s konkrétní kamerou či lokací, případně k porovnání záznamů ze dvou až čtyř kamer v režimu Multi-video. Výběr se provádí v levém panelu Zdroje, kde zaškrťovací pole určují, které sekvence se budou zobrazovat a analyzovat na časové ose.

Zásadním faktorem ovlivňujícím výsledek je viditelnost dat. Pokud je sekvence v panelu odškrtnutá, její data nejsou na časové ose zobrazena, což vytváří riziko mylného úsudku („nic tam není“). Nejčastějším selháním je lidská chyba, kdy má analytik omylem odškrtnutou důležitou sekvenci a následně chybně vyhodnotí situaci jako bezpředmětnou.

5.4 TŘÍDA

Filtr Třída umožňuje selekci objektů na základě jejich kategorie (např. osoba, auto, kamion) a zahrnuje i případné uživatelsky naučené třídy. Tento filtr je vhodné použít v momentě, kdy pátráte po obecném typu objektu bez bližšího popisu, a slouží jako efektivní první krok pro rychlé zúžení velkého množství výsledků. V praxi se nejčastěji kombinuje s filtry ROI a Časový interval.

Spolehlivost tohoto filtru je kriticky závislá na technické kvalitě videa a velikosti objektu v pixelech. Detekci negativně ovlivňují zákryty, rozmazání pohybem, protisvětlo či zhoršené podmínky jako déšť nebo noc. Nevhodný Frame Step může navíc způsobit fragmentaci tracků, kdy sledovaný objekt z detekce vypadává. K typickým selháním patří záměna vizuálně podobných tříd (tvarová podobnost, nízká kvalita záznamu) a chybějící detekce u příliš malých objektů. Pro operační nasazení je proto klíčové znát limity minimální velikosti objektu a rozlišovat práh pro spolehlivou detekci od hranice, kde již dochází k častému vynechání.

5.5 KOMBINACE FILTRŮ: SJEDNOCENÍ VS. PRŮNIK

Volba logiky, jakou se kombinují jednotlivé filtry, zásadně ovlivňuje množství a relevanci zobrazených výsledků. V nástrojích aplikace lze nastavit dva základní režimy:

Průnik (Intersection) představuje přísnou logiku „A ZÁROVEŇ“ (AND). Tento režim použijte, pokud chcete být maximálně specifictí – například hledáte objekt, který je „v konkrétní ROI a v daném čase a je to osoba“. Výhodou je dramatické snížení počtu výsledků, nevýhodou však riziko ztráty relevantního nálezu, pokud jeden z filtrů selže (např. systém chybně detekuje třídu). Příliš úzce nastavený průnik může vést k tomu, že operativa incident přehlédne.

Sjednocení (Union) naopak funguje na principu „NEBO“ (OR). Je vhodné pro zachycení variant, například když hledáte „osobu nebo auto“, případně pohyb v „ROI A nebo v ROI B“. Sjednocení zvyšuje návratnost (recall) a minimalizuje riziko přehlednutí, daní je však vyšší míra šumu, ve kterém se analytik může ztratit.

Optimalizovaná operační strategie doporučuje začít Průnikem pro získání rychlého, vysoce relevantního výsledku (top-hit). Pokud tento postup nevede k nálezu, je vhodné uvolnit kritéria na Sjednocení a případně snížit práh confidence.

5.6 CONFIDENCE A ŘÁZENÍ VÝSLEDKŮ

Hodnota confidence (věrohodnost) se nastavuje ve spodním panelu a slouží k filtraci výsledků podle skóre relevance modelu. Je důležité si uvědomit, že confidence není „pravděpodobnost pravdy“, ale technické skóre shody se vzorem. Typickým selháním je chybná interpretace tohoto čísla jako absolutní jistoty.

V operativní praxi se doporučuje postupovat ve dvou krocích: nejprve nastavit vyšší confidence pro rychlou kontrolu „nejlepších kusů“, a v případě neúspěchu hranici snižovat pro zvýšení záchytu (recall). Výsledky je možné řadit buď chronologicky, nebo právě podle confidence. Při vyhodnocování je nutné brát v úvahu, že různé scény (např. den vs. noc) mohou mít odlišné škálování hodnot a vyšší Frame Step může snižovat stabilitu tracků, což činí confidence hůře srovnatelnou.

Pro efektivní práci je vhodné definovat a empiricky zkalibrovat operativní režimy: „HIGH-precision“ (vysoká přesnost), „BALANCED“ (vyvážený) a „HIGH-recall“ (maximální záchyt), které budou mít přednastavené prahy pro různé typy úloh.

5.7 VYHLEDÁVÁNÍ TEXTEM

Textové vyhledávání je ideálním nástrojem v situacích, kdy hledáte specifické atributy, kompozice nebo objekty, pro které neexistuje předdefinovaná třída. Aktivuje se v pravém panelu volbou „Zadání textem“, kam uživatel запиše popis hledaného objektu. Platí pravidlo, že čím je popis podrobnější, tím přesnější jsou výsledky.

Výsledek je ovlivněn několika faktory. Ačkoliv je možné zadávat dotazy v češtině (včetně diakritiky), anglické popisy bývají obvykle stabilnější. Důležitá je také struktura dotazu – model rozlišuje mezi jednoduchým objektem („backpack“) a složeným popisem („person wearing black hoodie and backpack“), přičemž může preferovat typické kontextové asociace.

Mezi typická selhání v operativě patří používání příliš vágních dotazů (např. „podezřelá věc“), které vrací náhodné výsledky, nebo naopak nerealistická očekávání při hledání detailů v nízké kvalitě (např. čtení nápisů či log). Z testování vyplývá, že barvy jsou citlivé na vyvážení bílé a kompresi, proto je vhodné testovat dotazy na barvy (red/blue/black) s ohledem na specifika konkrétní kamery.

Zde je přepis dalších dvou sekcí do souvislého textu, včetně metodiky testování:

5.8 VYHLEDÁVÁNÍ OBRÁZKEM (REFERENČNÍ OBRÁZEK)

Tato metoda je určena pro situace, kdy máte k dispozici vizuální referenci hledaného objektu. Může se jednat o screenshot pořízený přímo ze záznamu, fotografii specifického předmětu (např. batoh, kus oblečení) nebo referenční obrázek vozidla. Pro spuštění vyhledávání stačí v pravém panelu kliknout na tlačítko +, zvolit možnost „Zadání obrázkem“, vybrat příslušný soubor a potvrdit tlačítkem „Hotovo“.

Klíčovým faktorem ovlivňujícím přesnost výsledků je kvalita a velikost referenčního obrázku (rozlišení, komprese, ostrost). Zásadní roli hraje také ořez (crop) – pokud referenční snímek obsahuje příliš velkou plochu pozadí, model může chybně hledat shodu s tímto pozadím namísto samotného objektu. Častým problémem je tzv. doménový posun, který nastává při použití dokonalých produktových fotografií s čistým pozadím pro vyhledávání v zašuměných záběrech z CCTV kamer. Paradoxně tak může být nekvalitní screenshot přímo z videa přesnější než profesionální fotka z webu. Typická selhání nastávají v případech, kdy reference nereprezentuje reálné světelné a úhlové podmínky kamery, nebo je hledaný objekt ve videu příliš malý.

5.9 NAJÍT PODOBNÉ (SEED Z VÝSLEDKŮ)

Funkce „Najít podobné“ slouží k rozšíření pátrání v okamžiku, kdy již máte jeden relevantní nález (tzv. seed) a hledáte další výskyty téhož nebo velmi podobného objektu – například stejný batoh, identický typ vozidla nebo konkrétní oděv. Použití je intuitivní: v mřížce náhledů ve spodním panelu klikněte pravým tlačítkem na nalezený objekt, zvolte „Najít podobné výsledky“ a následně potvrďte volbu v pravém panelu.

Kvalita výsledku je v tomto případě přímo závislá na kvalitě zvoleného „seedu“ (vzoru). Pokud je vybraný náhled rozmazaný, objekt je částečně zakrytý nebo snímek obsahuje výrazné rušivé pozadí, přesnost vyhledávání klesá. Systém v takovém případě může najít objekty, které jsou vizuálně podobné (např. shodná barva či tvar), ale sémanticky odlišné. Pokud je seed nekvalitní, podobnost se rozpadá.

5.10 DOUČOVÁNÍ (VYTVOŘENÍ VLASTNÍ TŘÍDY)

Funkce doučování je určena pro situace, kdy standardní modely systému stabilně nenacházejí objekt, který je pro policejní vyšetřování klíčový. Může se jednat o specifický typ zbraně, konkrétní předmět doličný, unifikovaný znak na oblečení nebo zvláštní výbavu. Tato funkce také umožňuje vytvořit dočasnou „projektovou“ třídu určenou výhradně pro potřeby konkrétního případu.

Proces vytvoření nové třídy probíhá v záložce „Třídy“. Uživatel nejprve novou kategorii pojmenuje (např. „Invalidní vozík“) a následně do systému nahraje sadu minimálně deseti referenčních obrázků, které lze získat z internetu (např. Google Images) nebo z kamerových záznamů. Klíčovým krokem je anotace – na každém obrázku je nutné pomocí nástroje „BBox“ nakreslit obdélník přesně kolem daného objektu. Jakmile mají všechny snímky zelený indikátor (hotové označení), stačí sadu uložit a spustit proces učení tlačítkem „Učit“. Trénování modelu obvykle trvá 3 až 10 minut v závislosti na počtu vložených příkladů.

Výsledná kvalita detekce je přímo závislá na kvalitě vstupních dat. Ačkoliv je technické minimum 10 obrázků, pro spolehlivé operativní nasazení je často nutné tento počet navýšit. Zásadní je variabilita trénovací sady – ta by měla obsahovat objekt z různých úhlů, v odlišných světelných podmínkách a na různém pozadí. Kritickým faktorem je preciznost a konzistence anotací (bounding boxů). Pokud jsou rámečky jednou nakresleny těsně a podruhé zahrnují i velkou část okolí či ruče, model se učí šum a jeho přesnost klesá.

Typickým selháním je tzv. doménový posun, kdy se model „přeučí“ na čisté produktové fotografie z webu, ale následně selhává na nekvalitních záběrech z CCTV kamer. Pozornost je třeba věnovat i vizuálně podobným objektům (tzv. confusables), jako je záměna nože za šroubovák nebo dlouhé zbraně za tyč, kde může docházet k falešným detekcím.

Také není dobré doučovat třídu, která je podtřída nějaké již existující.

DOPORUČENÉ OPERAČNÍ WORKFLOW (SOP PRO ANALYTIKA)

Tato kapitola definuje standardizované postupy pro práci se systémem AISEE v různých vyšetřovacích situacích. Cílem je zefektivnit práci analytika a minimalizovat riziko přehlédnutí důležitých stop.

6.1 RYCHLÝ INCIDENTNÍ POSTUP (DOPORUČENÝ STANDARD)

Pro většinu běžných úloh se doporučuje dodržovat následující sekvenci kroků. Práci začněte výběrem relevantních sekvencí (kamer) v levém panelu a vizuální kontrolou, zda jsou příslušná políčka skutečně

zaškrtnuta. Následně omezte pátrání nastavením časového intervalu a definujte oblast zájmu (ROI), pokud je zóna incidentu jasně daná.

Samotné vyhledávání zahajte buď filtrem Třída (např. osoba/auto), nebo textovým dotazem, pokud máte k dispozici popis pachatele či předmětu. Získané výsledky seřaďte podle confidence (věrohodnosti) a rychle zkontrolujte nálezy s nejvyšším skóre. Jakmile identifikujete relevantní stopu (tzv. "dobrý hit"), využijte funkci „Najít podobné“ pro dohledání dalších výskytů téhož objektu v záznamu. Všechny klíčové momenty průběžně přidávejte do Reportu, abyste neztratili kontext.

6.2 POSTUP PŘI NEGATIVNÍM VÝSLEDKU („NIC SE NENAŠLO“)

Pokud prvotní vyhledávání nepřinese žádné relevantní výsledky, je nutné systematicky uvolňovat vyhledávací kritéria. Začněte změnou logiky filtrů z přísného Průniku na volnější Sjednocení. Zvažte zvětšení oblasti ROI, případně tento filtr zcela vypněte, a rozšiřte časové okno pro případ nepřesného zadání času.

Dalším krokem je snížení prahu confidence, čímž systém přejde do režimu „high-recall“ (vysoká návratnost) a zobrazí i méně pravděpodobné nálezy. Pokud ani to nepomůže, změňte strategii dotazování. U textového vyhledávání zkuste formulovat obecnější popis, použít jiný jazyk nebo rozdělit komplexní dotaz na jednodušší části. Při hledání obrázkem vyzkoušejte jiný ořez (crop) nebo místo externí fotografie použijte screenshot přímo z videa, který lépe odpovídá světelným podmínkám.

6.3 OPTIMALIZACE PRO DLOUHÁ VIDEO

V případech, kdy analyzujete velmi dlouhé záznamy a časová tíseň neumožňuje čekat na detailní zpracování, se doporučuje dvoufázový postup. První průchod proveďte s vyšším snímkovacím krokem (např. Frame Step 5). Toto nastavení slouží jako rychlý hrubý screening, který vám pomůže lokalizovat relevantní časové úseky. Jakmile takový úsek najdete, vysekněte tento segment (mimo AISEE) nebo jej nahrajte znovu jako kratší část a zpracujte jej detailně s nastavením Frame Step 1–2 pro maximální přesnost.

REPORTY V OPERATIVĚ: DOKUMENTACE NÁLEZŮ

Efektivní dokumentace je pro vyšetřování klíčová, nesmí však analytika zdržovat od samotného pátrání. Systém AISEE je navržen tak, aby tvorba reportu probíhala plynule a bez nutnosti opouštět hlavní pracovní plochu.

7.1 ZPŮSOBY PŘIDÁNÍ NÁLEZU DO REPORTU

Aby nedocházelo k narušení plynulosti vyšetřování, nabízí aplikace tři intuitivní způsoby, jak zaznamenat důležitý moment. První možností je kliknutí na tlačítko „+“ přímo v panelu Report, což okamžitě uloží aktuálně zobrazený snímek videa. Druhou cestou je využití časové osy (timeline), kde po kliknutí pravým tlačítkem myši zvolíte možnost „Přidat do reportu“. Třetí způsob je určen pro práci s výsledky vyhledávání – v mřížce detekcí stačí vyvolat kontextové menu u konkrétního nálezu a odeslat jej do reportu.

7.2 OBSAH REPORTU A OPERATIVNÍ VYUŽITÍ

Každá položka v reportu je automaticky doplněna o kompletní sadu metadat, která jsou nezbytná pro důkazní řízení nebo zpětnou kontrolu. Záznam obsahuje název sekvence (identifikaci kamery), přesný globální čas události, název zdrojového souboru a lokální čas v rámci videa. Vizuální stránku tvoří náhled snímku, u kterého lze volitelně zapnout či vypnout zobrazení ohraničujícího rámečku (bounding box) pro zvýraznění objektu zájmu.

Nedílnou součástí je prostor pro textový komentář analytika. Finální výstup je generován jako interaktivní HTML stránka, která umožňuje snadné prohlížení nálezů v prohlížeči. Pro potřeby spisové dokumentace obsahuje hlavička exportu funkci „Vytisknout PDF“, která převede report do standardního tisknutelného formátu.

Operativní tip:

Komentáře k nálezům doporučujeme formulovat tak, aby byly bez dalších úprav použitelné pro okamžitý briefing nebo předání informace v terénu. Držte se struktury: KDO (popis osoby/objektu), CO (činnost), KDE (přesná lokace v záběru) a KDY (čas).

TECHNICKÉ LIMITY A INTERPRETACE VÝSLEDKŮ

Pro efektivní nasazení systému AISEE je nezbytné, aby analytik rozuměl nejen tomu, co systém umí, ale především tomu, kde leží jeho hranice. Následující body detailně rozebírají nejčastější příčiny chyb a metodiku jejich eliminace.

8.1 MALÉ OBJEKTY A ZTRÁTA DETAILŮ

Jedním z nejčastějších zdrojů chyb (zejména falešné negativy, tedy že systém objekt nenajde) je nedostatečné rozlišení cílového objektu.

- **Technické pozadí:** Detekční modely pracují na principu konvoluce, která postupně zmenšuje obraz pro získání sémantické informace. Pokud je vstupní objekt příliš malý (např. menší než 20 x 20 pixelů), v hlubších vrstvách sítě se jeho vizuální informace „rozpuští“ a stane se nerozlišitelnou od šumu pozadí.
- **Praktický dopad:** Systém spolehlivě detekuje osobu nebo auto, ale může selhat při detekci drobných předmětů, které tyto osoby nesou (mobilní telefon, nůž, specifické logo na tričku), pokud je kamera příliš daleko.
- **Doporučení:** Pokud hledáte drobné detaily, spoléhejte se primárně na kamery s detailním záběrem (např. u vchodu, bankomatu). U přehledových kamer nečekejte detekci malých předmětů.

8.2 VLIV KOMPRESÍ A SVĚTELNÝCH PODMÍNEK

Stabilita detekce a následné klasifikace (např. vyhledávání textem) je kriticky závislá na kvalitě vstupního signálu.

- **Kompresní artefakty:** Vysoce komprimovaná videa (nízký bitrate, starší kodeky) obsahují tzv. blokové artefakty a rozmazané hrany. AI model potřebuje ostré hrany (gradienty) k tomu, aby oddělil objekt od pozadí. V silně komprimovaném videu se objekt může slít s pozadím, což vede k výpadkům trackingu.

- **Noční vidění (IR):**

- **Ztráta barvy:** V nočním režimu s IR přísvitem je obraz monochromatický. Vyhledávání dotazů jako „červená bunda“ nebo „modré auto“ nebude fungovat, protože pro model jsou tyto objekty šedé.
- **Šum:** Zvýšený digitální šum v noci vytváří falešné textury, které může model mylně považovat za objekty (falešná pozitiva).

DILEMA FRAME STEP: VÝKON VS. SLEPÁ MÍSTO

Parametr *Frame Step* (FS) je klíčovým nástrojem pro řízení rychlosti analýzy, ale jeho nesprávné nastavení může vést ke ztrátě důkazů. Pro vyhledávání osob a vozidel používejte vyšší FS (rychlost). Pro analýzu specifických incidentů (rvačka, krádež) vždy zpracovávejte podezřelý úsek s FS = 1 nebo 2.

8.4 PRÁVNÍ ROVINA: VÝSTUPY JAKO VODÍTKA, NIKOLIV DŮKAZ

AISEE je navržen jako podpůrný analytický nástroj (Decision Support System), nikoliv jako automatický soudce.

- Probabilistická povaha: Každý výsledek AI je založen na pravděpodobnosti (Confidence Score). I při vysoké jistotě (např. 90 %) existuje šance, že se model mylí (tzv. halucinace nebo záměna vizuálně podobných objektů).
- Human-in-the-loop: Výstupem ze softwaru je „tip“ pro analytika. Právním důkazem není záznam v databázi AISEE, ale samotný videozáznam.
- Povinnost ověření: Operativní závěr nesmí být nikdy učiněn pouze na základě náhledu v reportu. Analytik má povinnost si vždy přehrát příslušný úsek videa a vizuálně potvrdit, že to, co AI označila, odpovídá realitě. Tím přebírá odpovědnost za interpretaci dat člověk, což je v souladu s požadavky AI Act na dohled nad vysoce rizikovými systémy.

ARCHITEKTURA DETEKCE A KLASIFIKACE OBJEKTŮ

Jádrem systému AISEE je dvoufázová architektura zpracování obrazu, která odděluje proces lokalizace objektu od jeho detailního popisu. Tento přístup zajišťuje vysokou citlivost systému i vůči předmětům, které nebyly součástí původní trénovací sady.

1. DETEKCE OBJEKTŮ (LOKALIZACE)

V první fázi systém v obrazu vyhledává oblasti zájmu. Detektor operuje ve dvou režimech:

- Detekce známých tříd: Model je natrénován na rozpoznávání 69 specifických tříd běžných objektů, jako jsou osoby, vozidla, batohy či elektronika. U těchto objektů systém s vysokou jistotou určuje jejich polohu a základní kategorii.
- Detekce generických objektů: Unikátní vlastností systému je schopnost vytvářet tzv. hypotézy neznámých objektů. Jde o jednu speciální třídu („Generický objekt“), která pokrývá předměty, jež model v době trénování neznal, ale na základě vizuálních příznaků je vyhodnotil jako potenciálně relevantní (oddělitelné od pozadí). Tato funkce je klíčová pro forenzní praxi, kde se často hledají atypické doličné předměty.

2. POPIS A HIERARCHICKÁ KLASIFIKACE

Ve druhé fázi jsou všechny detekované objekty (známé i generické) podrobeny hloubkové analýze pro získání detailního sémantického popisu. Systém využívá tři úrovně klasifikace:

- Hierarchická taxonomie: Znamé objekty jsou zařazeny do jemné struktury čítající celkem 377 tříd. Systém tak neidentifikuje pouze „auto“, ale v rámci hierarchie určí konkrétní typ karoserie (sedan, hatchback, SUV, minivan, sportovní vůz, formule atd.).
- Doučené objekty: Pokud uživatel definoval vlastní třídy (např. specifický typ loupežného náčiní), systém v této fázi porovnává nalezené objekty s těmito uživatelskými vzory.
- Filtrace pozadí: V případě, že generická hypotéza z první fáze neodpovídá žádné známé ani doučené kategorii a neobsahuje dostatečné vizuální rysy objektu, je klasifikována jako pozadí (falešná detekce) a z výsledného reportu je vyřazena. Tím se minimalizuje množství šumu v prezentovaných výsledcích.

DETEKCE OBJEKTŮ

Pro detekci objektů je v systému použit modifikovaný algoritmus YOLO, který oproti standardnímu přístupu umožňuje detekovat nejen známé objekty, ale také hypotézy generických objektů. Tyto hypotézy hrají klíčovou roli při dodatečném doučování nových objektů, které nebyly součástí původní trénovací množiny systému.

Detekční model byl natrénován na 56 veřejných datasetech, které se liší jak typem obsažených objektů, tak i způsobem jejich anotace. Například dataset COCO obsahuje anotace osob, avšak nezahrnuje zbraně, zatímco dataset Roboflow Weapon Detection Capstone obsahuje anotované zbraně, ale osoby v něm anotovány nejsou. Tento heterogenní charakter dat klade zvýšené nároky na způsob trénování a sjednocení tříd. Standardní YOLO model je obvykle trénován výhradně na datasetu COCO, který obsahuje přibližně 850 tisíc anotací na zhruba 117 tisících obrázků a zahrnuje 80 tříd. Naproti tomu detekční model AISEE YOLO byl trénován na výrazně rozsáhlejší datové sadě zahrnující celkem 5 758 tisíc anotací na 530 tisících obrázků a 70 třídách.

I přes rozšíření o nové, pro projekt klíčové třídy (např. pistole, drogy, peníze, pas aj.) je celkový počet tříd nižší než u COCO. Důvodem je slučování tříd, které nejsou pro projekt prioritní – například jednotlivé druhy zvířat (slon, zebra apod.) byly sjednoceny do obecnější třídy divocí savci.

Výstupní třídy detekčního modelu YOLO nejsou přímo zpřístupněny uživateli, jelikož jsou v dalších krocích zpracovatelské pipeline nahrazeny výstupy klasifikátoru založeného na architektuře SigLIP2, který pracuje s výrazně vyšším počtem tříd. Učení YOLO modelu se třídami je nicméně zachováno, protože přispívá k bohatšímu popisu vizuálního obsahu, a tím i ke zlepšení kvality následného trackovacího algoritmu.

Vybrané kvantitativní rozdíly mezi standardním detekčním datasetem COCO a trénovacím datasetem AISEE jsou shrnuty v následující tabulce.

	COCO	AISEE detekční dataset
celkový počet detekcí	849942	5758300
celkový počet obrázků	117266	530049
počet instancí “auto”	43531	439757
počet instancí “osoba”	257252	564844
počet instancí “pistole”	0	38334
počet instancí “generický objekt”	0	3650564

Ze všech anotovaných tříd byly vybrány typy objektů vhodné pro projekt a ty byly použity ke trénování známých objektů. Všechny třídy, vyjma lidí, byly následně použity k trénování jedné třídy generický objekt.

Vyhodnocení leave-one-out. Nad COCO datasetem byl natrénován detektor známých objektů a generického objektu, přičemž jedna z tříd byla vyňata z trénování. Následně bylo měřeno, jaké procento výskytů této třídy bylo detekováno v testovací sadě, ať už jako generický objekt, nebo jiný známý objekt podobného vzhledu.

Vzhledem k modifikaci detektoru bylo při inferenci v aplikaci potřeba modifikovat algoritmus “Non-Max Suppression”, který z mnoha překrývajících se detekcí vybere jen ty nejdůležitější. Jelikož třída generický objekt může dát vysokou odezvu i přes to, že se jedná o objekt ze známé třídy (např. auto), jsou známé třídy prioritizovány. Pouze pokud objekt nevykazuje dostatečnou odezvu jakožto známá třída, je označen za generický objekt.

TRACKING - TRASOVÁNÍ OBJEKTŮ

Trasováním objektů se rozumí vytvoření vazby mezi objekty v čase. V naší aplikaci využíváme přístup trasování detekcí, kde vstupem jsou detekce objektů v jednotlivých snímcích a výstupem je přiřazení jedinečného identifikátoru (čísla) konkrétnímu objektu a všem jeho následujícím výskytům. Tímto je vytvořena trasa konkrétního objektu (Auto 1, Osoba 3, ...) ve sledované videosekvenci. Z uživatelského hlediska toto umožňuje sledovat tento konkrétní objekt v čase, neboť všechny jeho detekce v jednotlivých snímcích jsou brány jako jeden objekt. Při absenci tohoto bloku „trasování objektů“ by detekce fyzicky stejných objektů v po sobě jdoucích snímcích byly brány jako různé objekty. Z hlediska implementačního má tento přístup výhodu v tom, že stačí teoreticky vytvořit pro vyhledávání pouze jeden embedding pro všechny detekce jednoho objektu. Prakticky je ovšem potřeba vytvořit embeddingů více, neboť je potřeba zachytit významné události ve stavu objektu (např. nástup člověka do vozu). Pro realizaci trasování byla vybrána metoda BoT-SORT [bφ ! K I-N;2yZ wφ hNUT I-λEΣ I-yR̄ . φπz/φ . 2ōN;2ōā}ēΣ ō . 2φπ{hwφY w2ōdzāŮ ! āā2ōλ I-ūū2yā a dzēŮπ t ŠŘŠāŮNŮ I-y' φN I-Ō} λyEΣē I-ŮŮ - λŌ LjN;ŠLjNŮŮ I-ŮŮ - λŌYŮNŮLcφmπcρmΣ nŮnŮ].

Algoritmus zjednodušeně probíhá následovně: 1) Vstupem do detektoru BoTSort jsou detekce na snímku definované pozicí objektu, spolehlivostí detekce – konfidencí a vektorem kódujícím další charakteristiky objektu. Ten je v našem případě vzat přímo z YOLO detektoru, tzn. nemusí se počítat zvlášť, jak by tomu bylo v případě originální implementace detektoru BoT-SORT. 2) Tyto detekce jsou zpracovány v bloku Asociace, kde jsou porovnány s existujícími objekty v databázi (detekce z předchozích snímků). Podobnost je definována pomocí překryvu objektů (Intersection Over Union) a vzdáleností jejich charakteristických vektorů (kosinová vzdálenost). Aby byla podobnost pomocí překryvu objektů spolehlivější, je na objekty z databáze použita predikce jejich výskytu v následujících snímcích pomocí Kalmanova filtru (KF). Stavové parametry KF jsou aktualizovány po každé úspěšné

asociaci. Výchozí stavové parametry KF jsou nastaveny podle snímkovací frekvence videa (FPS) a nastaveného FS. 3) Pokud nebyl v databázi nalezen podobný objekt, je detekce uložena do databáze jako nový objekt a je inicializován jeho KF. Pokud byl objekt asociován, získává identické číslo z databáze. Naopak pokud objektu v databázi nebyla po definovanou dobu přiřazena žádná detekce, je z databáze odstraněn.

POPIS A KLASIFIKACE

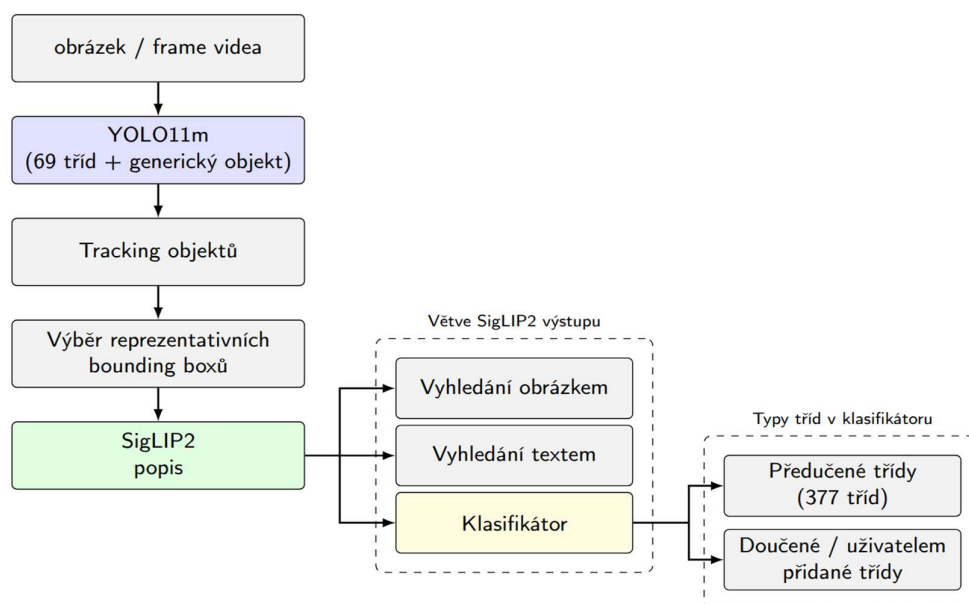
Každá detekce je v následujícím kroku pipeline popsána vizuálním deskriptorem SigLIP2, který zachycuje sémantický obsah detekovaného výřezu. Tyto deskriptory jsou následně vstupem do klasifikačního modelu, jenž provádí rozdělení do celkem 377 tříd.

Trénovací dataset klasifikátoru vychází ze stejné skupiny datasetů jako detekční část, avšak je dále rozšířen o dalších 8 datasetů, které umožňují jemnější a přesnější rozdělení objektů na podtřídy. Celková velikost trénovací datové sady dosahuje 11 055 tisíc obrázků (tj. více než 11 milionů trénovacích vzorků).

Použitý datový model i natrénovaný klasifikátor pracují s hierarchickou strukturou tříd, která zahrnuje 30 nadtříd (např. osobní automobil, zbraň apod.). Pro většinu nadtříd jsou dále definovány odpovídající podtřídy – například nadtřída osobní automobil zahrnuje podtřídy sedan, hatchback, formule, sportovní automobil, SUV a minivan.

V případech, kdy model není schopen spolehlivě rozhodnout o příslušnosti k určité podtřídě, případně pokud dotazovaný obrazový výřez neodpovídá žádné z definovaných podtříd, je jako výstup poskytnuta alespoň informace o příslušné nadtřídě. Tento mechanismus zajišťuje robustní a informativní klasifikační výstup i v případě nejednoznačných nebo hraničních vstupů.

DOUČOVÁNÍ OBJEKTŮ Z PŘÍKLADŮ



TESTOVÁNÍ

ADAPTACE A OPTIMALIZACE MODELU SIGLIP2 PRO VYHLEDÁVÁNÍ A RE-IDENTIFIKACI OSOB

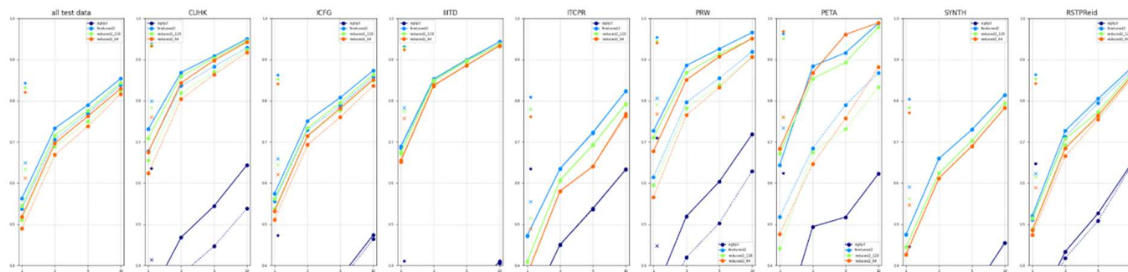
V rámci projektu byl adaptován multimodální model SigLIP2 (*SigLIP 2: Multilingual Vision-Language Encoders with Improved Semantic Understanding, Localization, and Dense Features*). Ačkoliv je tento model primárně určen pro obecné porovnávání obrazových a textových reprezentací, pro účely projektu byl specificky dotrénován na úlohy textového vyhledávání osob dle vizuálního popisu a na re-identifikaci osob napříč různými obrazovými daty. Hlavním cílem tréninku bylo zkvalitnit párování textových a obrazových reprezentací osob a současně redukovat dimenzi příznaků, což je nezbytný předpoklad pro nasazení v retrieval systémech s omezenými výpočetními a paměťovými prostředky.

Experimenty prokázaly, že přímá aplikace původního modelu SigLIP2 není pro specifické úlohy vyhledávání a re-identifikace osob vhodná. Model vykazoval tendenci zaměřovat vizuální atributy (zejména barvy a objekty) a priorizoval globální podobnost scény před identitou konkrétní osoby. To v praxi vedlo k vyhledávání vizuálně podobných snímků namísto identifikace téže osoby zachycené v odlišných pozicích či prostředích.

Výsledné řešení proto implementuje model, který transformuje textové popisy obsahující relevantní vizuální charakteristiky do prostoru příznaků, kde jsou porovnávány s příznaky extrahovanými z obrazových dat. Na základě podobnosti těchto reprezentací systém umožňuje efektivní vyhledávání osob pomocí textových dotazů a jejich re-identifikaci.

METODIKA A DATA

Pro trénink modelu byla využita veřejně dostupná data zaměřená na popisy osob, konkrétně datasey CUHK-PEDES, ICFG-PEDES, IIITD, ITCPR a PRW. Textové anotace byly předzpracovány pomocí velkého jazykového modelu (LLM) tak, aby obsahovaly výhradně relevantní vizuální atributy, jako je barva a typ oblečení, obuv nebo doplňky. Jako základní architektura byl zvolen model google/siglip2-base-patch16-224. Ten byl modifikován přidáním projekčních vrstev do textové i obrazové větve, což umožnilo redukci dimenze příznakového vektoru z původních 768 na menší cílovou velikost (např. 128).



VÝSLEDKY EVALUACE

Dotrénovaný model prokazatelně lépe zachycuje vizuální charakteristiky osob. Úspěšnost textového vyhledávání (text-to-image retrieval) je prezentována grafy prostřednictvím metriky Top-k recall (definice metrik viz. Appendix). Na ose x je zobrazena hodnota k (1, 3, 5, 10) a na ose y podíl identit, pro které se správná osoba nachází mezi k nejpodobnějšími výsledky. Pro každý textový dotaz je vyhledávání prováděno z celého poolu testovacích identit daného datasetu (přibližně 1000 identit), u

spojeného datasetu (vlevo) se vybírá z poolu o velikosti ~9000 identit. Čárkovaná čára zobrazuje výsledky pro všechny obrázky, plná po obrázky s výškou větší než 200px.

Výsledky re-identifikace osob jsou vyhodnoceny pomocí metrik mAP a top-k na široce používaných datasetech Market 1501, MSMT17, DukeMTMC a EntireID. Hodnoty jsou prezentovány v Tabulce A (mAP) a B (top-k) (definice metrik viz. Appendix). Metrika mAP hodnotí celkovou kvalitu pořadí výsledků, zatímco metrika top-k vyjadřuje, v kolika případech se správná identita nachází mezi k nejpodobnějšími výsledky.

Tabulka A

	Market 1501	MSMT17	DukeMTMC	EntireID
google/siglip2-base-patch16-224	7.5	12.0	17.0	17.2
finetuned2	81.0	65.1	66.6	60.6
reduced2_64	73.4	44.1	57.0	49.8

Tabulka B

	Market 1501	MSMT17	DukeMTMC	EntireID
google/siglip2-base-patch16-224	22.9 / 38.0 / 45.9	59.1 / 71.3 / 76.2	60.2 / 74.2 / 78.7	32.3 / 47.1 / 54.0
finetuned2	90.7 / 97.0 / 98.4	92.8 / 96.4 / 97.2	92.7 / 96.4 / 97.0	79.3 / 89.8 / 92.1
reduced2_64	87.1 / 95.1 / 96.5	84.4 / 90.9 / 92.9	89.0 / 94.4 / 95.6	68.0 / 83.0 / 86.9

NASTAVENÍ PARAMETRŮ

Experimentálně bylo ověřováno optimální nastavení jednotlivých parametrů AISEE.

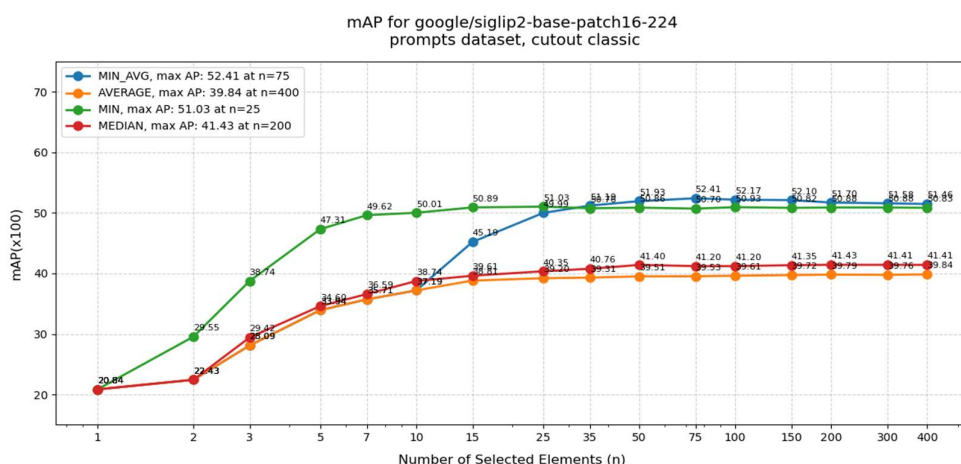
POČET KLÍČOVÝCH SNÍMKŮ REPREZENTUJÍCÍ TRACK A METRIKA PRO VYHLEDÁVÁNÍ:

Detekované objekty v jednotlivých snímcích videa jsou spojovány do tracků. Z důvodů velké paměťové a výpočetní náročnosti je nutné tracky reprezentovat pouze N vybranými snímky, kterým říkáme klíčové. Track je v příznakovém prostoru SigLIP reprezentován shlukem N vektorů (jeden vektor pro jeden klíčový snímek) a dotaz zadaný obrazem či textem je reprezentován jedním vektorem. Vyhledávání je převedeno na problém hledání vzdálenosti mezi vektorem (dotaz) a shlukem vektorů (track). V případě dotazu zadaného vícero obrázky se jedná o vzdálenost mezi dvěma shluky. Hledali jsme optimální počet N ekvidistantně vzdálených klíčových snímků na track a vhodnou metriku pro výpočet vzdálenosti mezi dvěma shluky. Na anotovaném datasetu vozidel jsme vyhledávali pomocí předem připravené množiny dotazů a vyhodnotili průměrné AP. Výsledky jsou shrnuty na následujícím grafu, který porovnává úspěšnost vyhledávání (vyšší AP) na počtu N klíčových snímků na track a zvolené metrice. Z grafu je zřejmé, že AP začíná saturovat pro $N > 15$. Metrika MIN (zelená křivka)

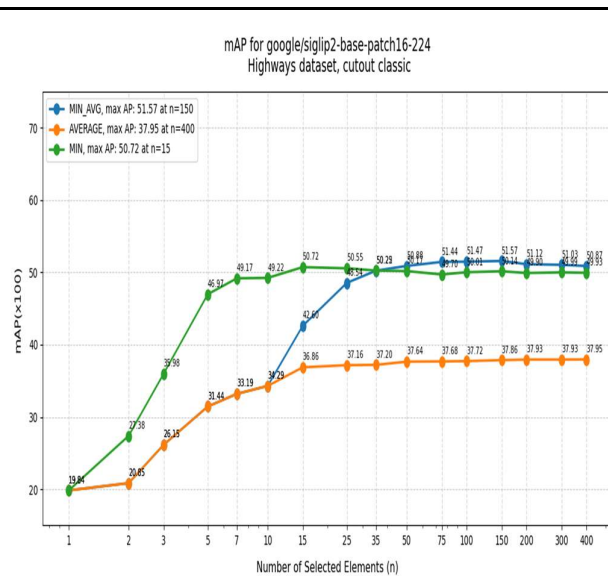
(definice metrik viz. Appendix), která definuje vzdálenost mezi dvěma shluky jako minimální kosinovu vzdálenost mezi všemi páry vektorů (dotaz, track), dosahuje daleko lepších výsledků než vzdálenost měřená jako průměr (oranžová) nebo medián (červená) těchto vzdáleností. Malého zlepšení, ale pouze pro vysoké N, lze dosáhnout počítáním průměrné kosinovy vzdálenosti z dolního kvartilu vzdáleností (modrá). Ve výsledné implementaci AISEE reprezentujeme tracky 16 klíčovými snímky a vzdálenost měříme pomocí MIN metriky, která je pro takto zvolené N lepší než průměr z dolního kvartilu.

TVAR VÝŘEZU (BOUNDING BOX)

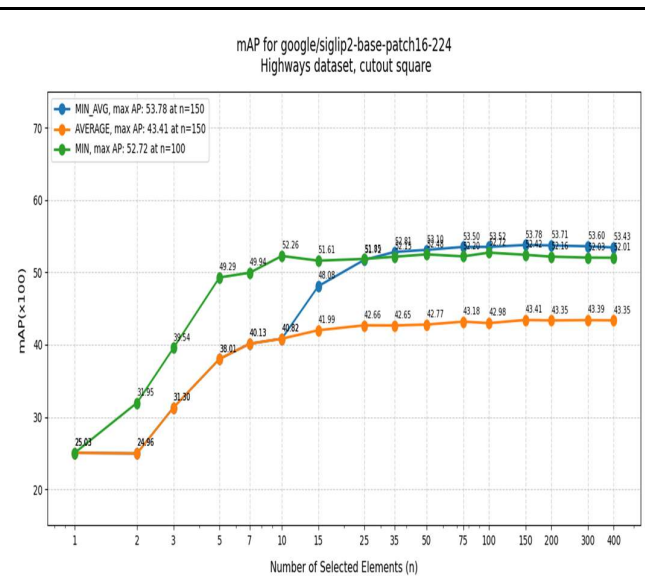
Další parametr, který ovlivňuje úspěšnost vyhledávání je tvar výřezu, který ohraničuje detekovaný objekt a na kterém se počítá SigLIP příznaky. Následující grafy ukazují závislost AP



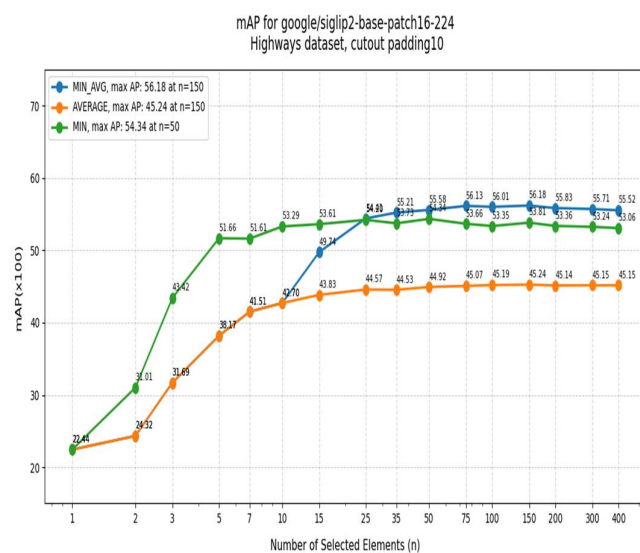
na počtu klíčových snímků pro 4 tvary výřezů: původní výřez daný detekcí YOLO (jedná se o obecný obdélník, který YOLO síť vrací při detekci objektů), čtvercový výřez ohraničující původní výřez, výřez zvětšený o 10% zachovávající původní poměr stran, výřez zvětšený o 20% zachovávající původní poměr stran. SigLIP předpokládá na svém vstupu čtvercový obrázek. Pokud je YOLO výřez obdélníkový, dojde automaticky k drobné deformaci při převádění na čtverec, což by mohlo zhoršovat výsledky vyhledávání. Čtvercové výřezy (horní pravý graf) sice nepatrně zvýšily AP, ale většího zlepšení bylo dosaženo při zvětšení výřezů a zachování původního poměru stran (spodní grafy). Zvětšení přidává pozadí do výřezu a pomáhá tak SigLIP příznakům zaznamenat větší kontext. Příliš velké zvětšení (20% - pravý spodní graf) ovšem způsobuje zmenšení vlastního objektu zájmu, což se začne projevovat opětovným snižováním AP. Ve všech případech zůstává MIN metrika a 16 klíčových snímků na track nejlepším kompromisem. Ve výsledné implementaci AISEE jsme zvolili zvětšené výřezy o 10%.



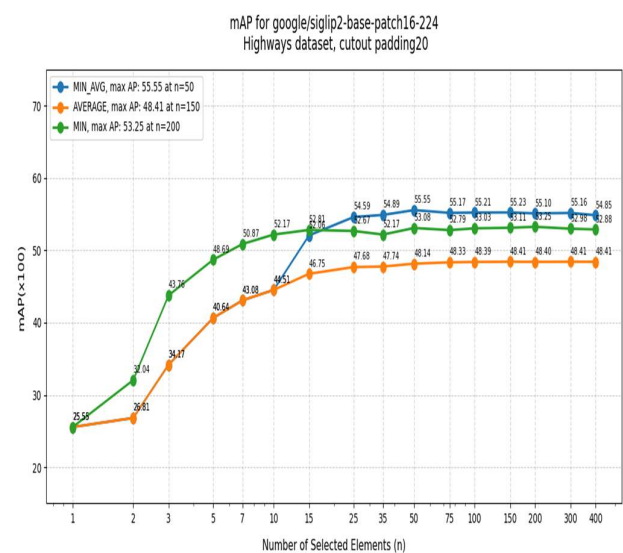
YOLO b.b. (obecný obdélník)



Čtvercový b.b.



YOLO b.b. zvětšený o 10%



YOLO b.b. zvětšený o 20%

POROVNÁNÍ DOTAZŮ ZADANÝCH OBRAZEM A TEXTEM

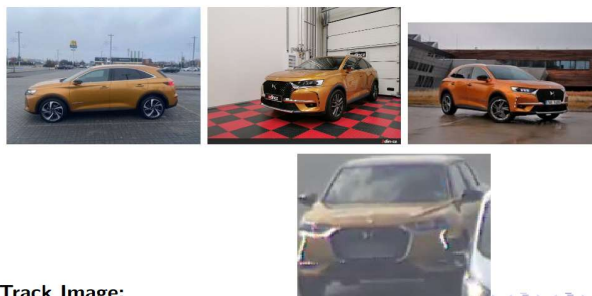
Na anotované datasetu vozidel jsme vyhodnotili Top-K Recall (K=1, 3, 5, 10) nad množinou dotazů zadaných buď obrazem anebo textem. Cílem každého dotazu bylo vyhledat jedno konkrétní vozidlo. Příklad ukázky jednoho vozidla (track image) a dotazu pomocí třech obrázků (queries):

Track: 176_19

Značka: Citroen Ds7

Track	frames	Centroid Rank	Single Linkage Rank
175_19	148	153	1

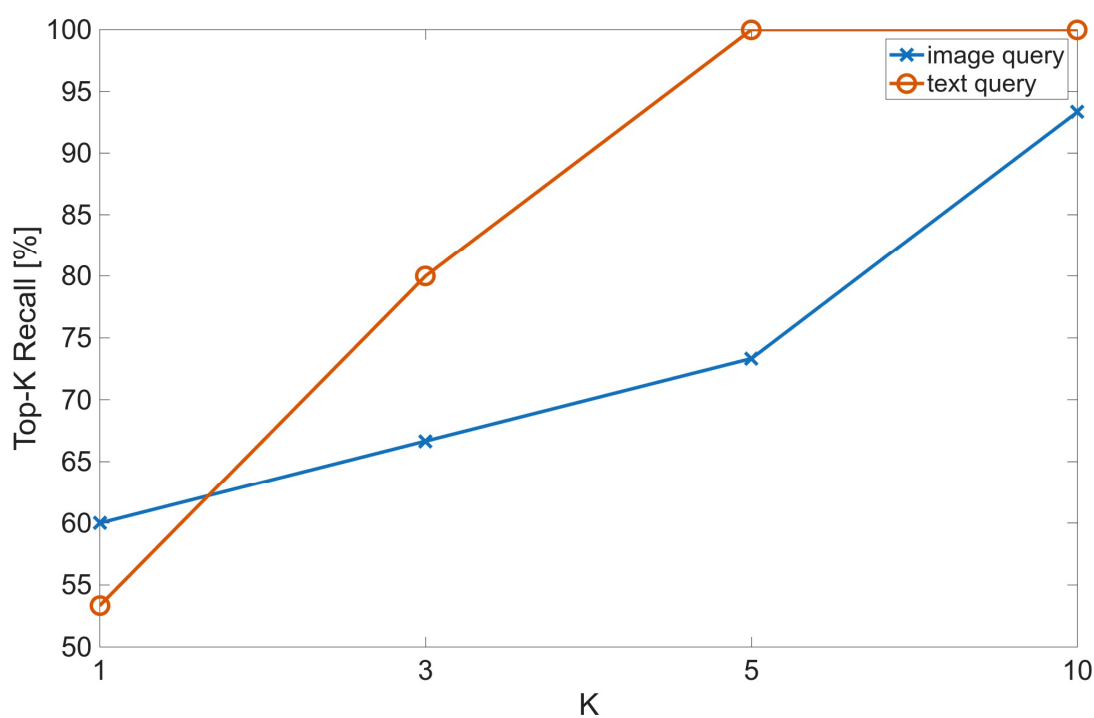
Queries:



Track Image:



Textové dotazy byly ve formátu <barva> <typ vozidla> , např. “A golden Citroen Ds7 car”. Obrázky použité k dotazování, byly vyhledány na internetu. Z graf dole je zřejmé, že dotazy zadané textem mají obecně vyšší úspěšnost než dotazy zadané obrazem.

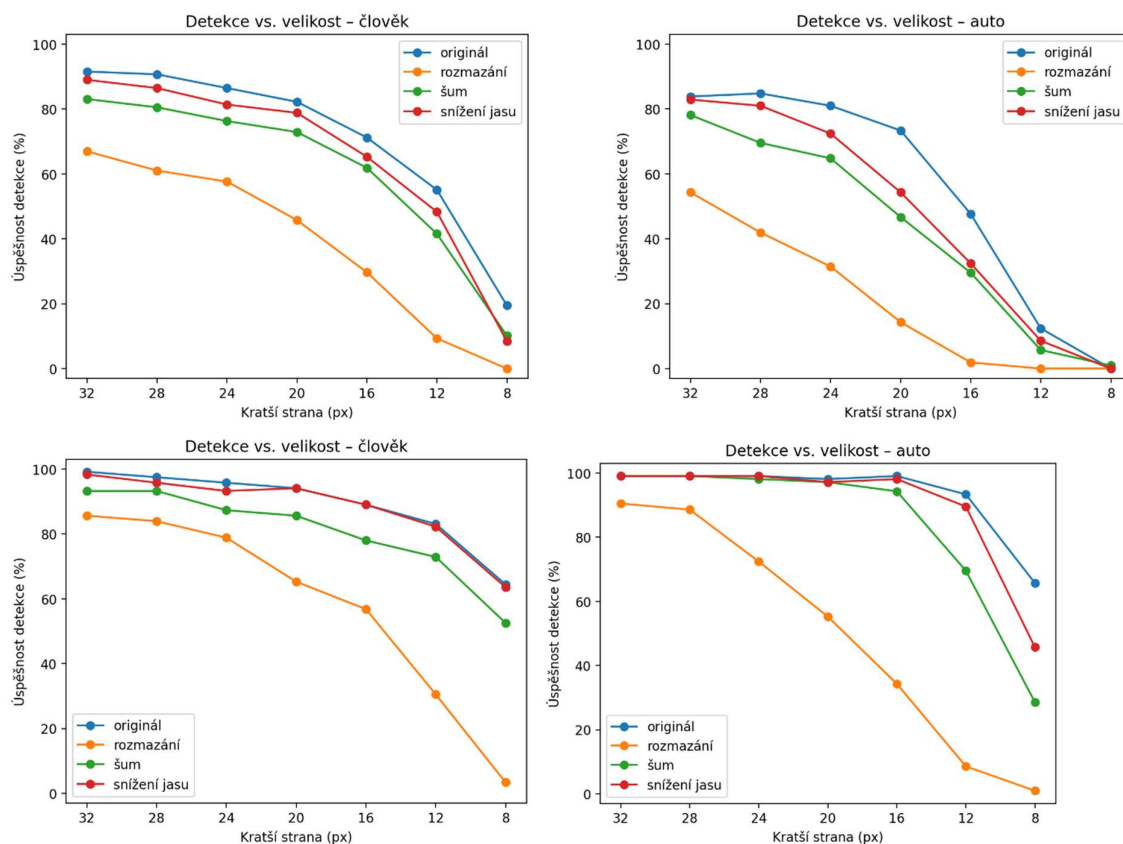


Porovnání top-K Recall na dotazy zadané textem a obrázkem.

EVALUACE ROBUSTNOSTI DETEKČNÍ PIPELINE VŮČI DEGRADACI VSTUPU

Aby mohl systém AISEE pracovat správně, musí být objekty našeho zájmu v obraze zachyceny s dostatečným množstvím obrazových informací. Pokud je objekt příliš malý nebo má nízkou obrazovou kvalitu, systém AISEE nedokáže z dostupných dat získat potřebné detaily, což vede ke snížení přesnosti

detekce, klasifikace i dalších navazujících funkcí. Detekční část pokud selže, tak už se v klasifikační části objekt nemá šanci najít. Následující grafy ukazují, jak se chová detekce, pokud se snímky zmenšují případně kazí jejich kvalita šumem, snížením jasu nebo rozmazáním. Jedná se o testování pouze detekční části.



Pro porovnání uvádíme grafy pro situaci použití standardní YOLO detekce (horní řádek) a upravené verze z AISEE (dolní řádek). Je patrné, že upravená verze má vyšší úspěšnost, takže se minimalizuje situace, že se objekt nedetekuje. Degradace má vliv na detekci až v poměrně vysoké úrovni.

EVALUACE ROBUSTNOSTI DETEKČNĚ-KLASIFIKAČNÍ PIPELINE VŮČI DEGRADACI VSTUPU

Cílem této experimentální části bylo analyzovat robustnost celé detekčně-klasifikační pipeline vůči změnám kvality vstupních obrazových dat. V reálných aplikačních scénářích se vstupní data často odchylojí od ideálních podmínek – objekty mohou být velmi malé, snímky mohou obsahovat obrazový šum nebo mohou být pořízeny za zhoršených světelných podmínek. Tyto faktory mají potenciál negativně ovlivnit jak fázi detekce objektů, tak následnou klasifikaci detekovaných výřezů.

Na rozdíl od izolované evaluace samotného detektoru nebo klasifikátoru je zde evaluována celá pipeline jako celek, tedy proces od vstupního obrázku až po finální přiřazení třídy detekovanému

objektu. Tento přístup lépe reflektuje skutečné nasazení systému, kde chyby nebo degradace v jedné části pipeline mohou ovlivnit celkový výsledek.

Výsledky experimentů jsou prezentovány pomocí standardních metrik, které jsou uvedené v Appendixu. Pro účely této analýzy jsou všechny metriky normalizovány vzhledem k referenčnímu nastavení bez degradace vstupních dat, které je definováno jako 100 % výkonu.

Normalizace je provedena samostatně pro každou metriku (precision, recall i F1) a odděleně pro každý experiment a vyhodnocovanou množinu tříd. Při evaluaci jednotlivých tříd (např. „osoba“, „auto“) jsou metriky normalizovány pouze vzhledem k výsledkům dané třídy, zatímco při evaluaci přes všechny třídy je použit vážený průměr přes všechny třídy, který je následně normalizován stejným způsobem. Prezentované grafy tedy zobrazují relativní změny výkonu.

VSTUPNÍ DATA A EXPERIMENTÁLNÍ NASTAVENÍ

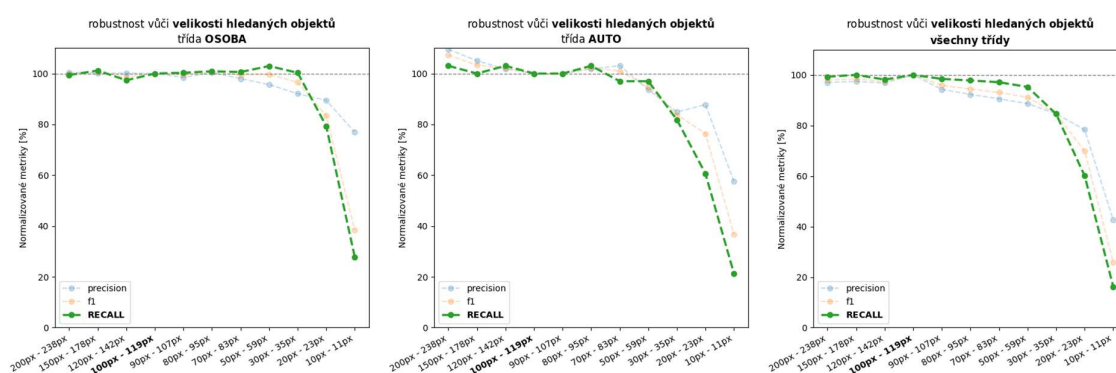
Všechny experimenty byly provedeny na SAMACOCO datasetu, který vychází z původního COCO datasetu, avšak obsahuje vyčištěné anotace a konzistentní množinu tříd. Dataset byl připraven s cílem minimalizovat chyby v anotacích a nejednoznačnosti tříd, což umožňuje spolehlivější vyhodnocení skutečného chování modelu. Evaluace byla provedena na reprezentativních třídách „osoba“ a „auto“, které jsou hlavními zájmovými třídami projektu, a dále na váženém průměru přes všechny třídy, který poskytuje agregovaný pohled na chování systému. Ve všech experimentech je vždy použit stejný poddataset, aby byla zajištěna plná porovnatelnost výsledků mezi jednotlivými nastaveními.

ROBUSTNOST VŮČI VELIKOSTI OBJEKTŮ (DETEKCE MALÝCH OBJEKTŮ)

Tento experiment se zaměřuje na schopnost pipeline detekovat a správně klasifikovat malé objekty. Pro tento účel byl vybrán poddataset obsahující pouze anotace objektů, jejichž kratší strana ohraničujícího obdélníku se v původních datech pohybuje v rozmezí 100–119 pixelů.

Vstupní obrázky jsou následně systematicky zmenšovány, čímž dochází ke snížení efektivní velikosti objektů i jejich anotací. Analogicky bylo testováno také zvětšování vstupních obrázků. Pro všechna nastavení je vždy použit identický poddataset.

Změna efektivní velikosti objektů je realizována globálním škálováním vstupních obrázků pomocí konstantního měřítka. Při zmenšování či zvětšování vstupních snímků dochází ke změně efektivní velikosti objektů i jejich anotací. Po provedení inference jsou výsledné detekované ohraničující obdélníky přepočteny zpět do souřadnic původního obrázku, aby byla zachována korektní geometrie vůči původním anotacím. Tento postup zajišťuje, že evaluace probíhá vždy v původním souřadném systému a není ovlivněna samotnou změnou rozlišení vstupu.



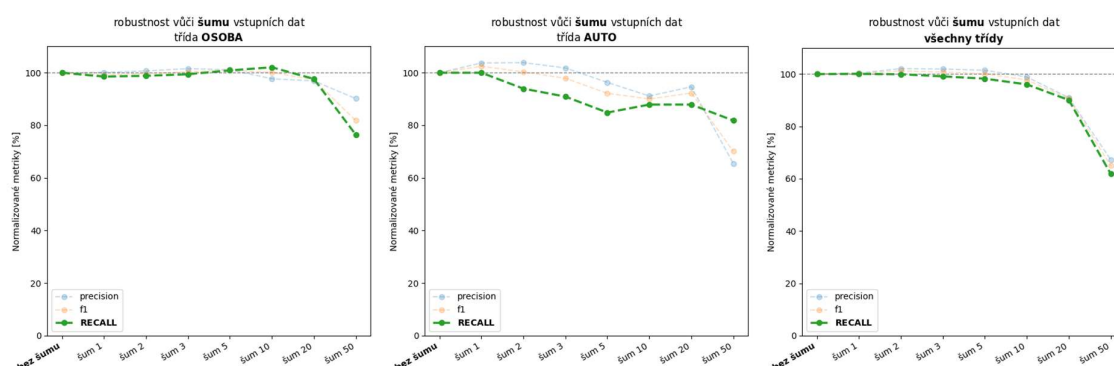
Výsledky jsou zobrazeny v grafu, kde osa x reprezentuje efektivní velikost objektů v daném experimentu. Výchozí stav (originální velikost) je v grafech zvýrazněn a všechny hodnoty jsou

normalizovány vzhledem k tomuto stavu (100 %). Výsledky ukazují, že pro třídu „osoba“ zůstává kvalita rozpoznání prakticky nezměněna až do velikostí přibližně 30–35 pixelů. I při velikostech objektů kolem 20–23 pixelů dosahuje recall přibližně 80 % hodnoty původního nastavení. Další snižování velikosti (cca 10–11 pixelů) však vede k výraznému poklesu počtu správně detekovaných a klasifikovaných osob. Analogický trend je pozorován i pro třídu „auto“ a pro vážený průměr přes všechny třídy.

Celá pipeline je schopna spolehlivě detekovat a klasifikovat objekty i při výrazném zmenšení jejich velikosti, a to až do určité rozumné hranice. Výrazný pokles výkonu nastává až u velmi malých objektů, které již neobsahují dostatek diskriminační informace pro spolehlivé rozpoznání. Toto chování je v souladu s obecně známými omezeními metod detekce a klasifikace objektů.

ROBUSTNOST VŮČI OBRAZOVÉMU ŠUMU

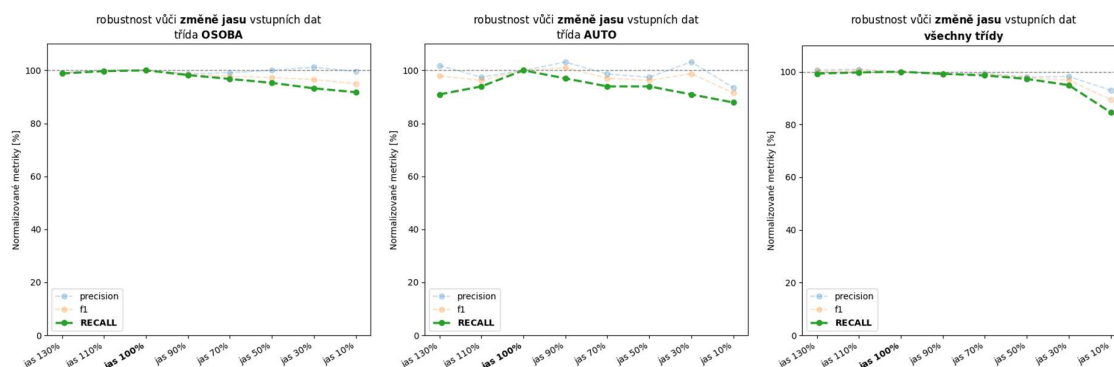
Robustnost pipeline vůči šumu je testována přidáním aditivního Gaussovského šumu přímo do pixelových hodnot vstupních obrázků. Šum je generován s nulovou střední hodnotou a se zadanou směrodatnou odchylkou σ , přičemž hodnota σ je vyjádřena ve stejných jednotkách jako intenzity pixelů (rozsah 0–255). Po přidání šumu jsou hodnoty pixelů oříznuty na platný rozsah a převedeny zpět na osmibitovou reprezentaci. Pro všechna měření je opět použit stejný poddataset. Tento postup simuluje degradaci kvality obrazu způsobenou senzorovým šumem a umožňuje analyzovat chování celé pipeline při postupně se zhoršující kvalitě vstupních dat.



Výsledky jsou zobrazeny v grafu, kde osa x reprezentuje hodnotu rozptylu Gaussovského šumu. Výsledky ukazují vysokou robustnost celé pipeline vůči šumu. I při relativně vysokých hodnotách rozptylu (cca 10–20) zůstávají hodnoty metrik nad 80 % výkonu bez šumu. Výraznější degradace výkonu je pozorována až při extrémních hodnotách rozptylu (cca 50), kdy již dochází k výraznému narušení struktury obrazu. Pipeline vykazuje vysokou odolnost vůči přítomnosti obrazového šumu. Podobné chování je pozorováno jak u jednotlivých tříd, tak i u váženého průměru přes všechny třídy, což naznačuje dobrou generalizační schopnost systému.

ROBUSTNOST VŮČI ZMĚNÁM JASU

Změna jasu vstupních obrázků je realizována multiplikativní transformací pixelových hodnot konstantním faktorem. Hodnota 1.0 odpovídá původnímu jasu obrázku, hodnoty menší než 1.0 simulují ztmavení a hodnoty větší než 1.0 zesvětlení obrazu. Po aplikaci této transformace jsou hodnoty pixelů opět oříznuty na platný rozsah 0–255. Tento přístup odpovídá globální změně expozičních podmínek a umožňuje analyzovat citlivost pipeline na výrazné změny jasových úrovní bez změny struktury obrazu. Pro všechna nastavení je opět použit stejný poddataset.

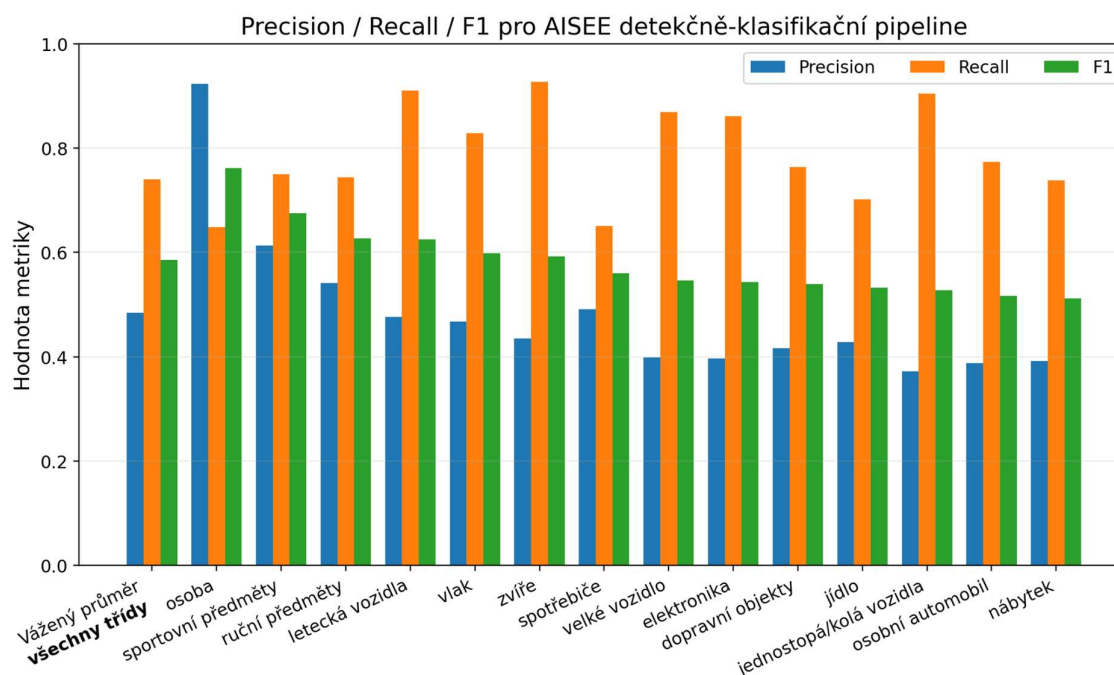


Výsledky jsou prezentovány v grafu, kde osa x reprezentuje změnu jasu v procentech, přičemž 100 % odpovídá původnímu jasu. Experimenty ukazují pouze zanedbatelný vliv změny jasu na výsledky pipeline. I při extrémním ztmavení na úroveň 10 % původního jasu dosahují výsledky více než 85 % výkonu referenčního nastavení. Podobné chování je pozorováno napříč sledovanými třídami i pro vážený průměr.

EVALUACE DETEKCČNĚ-KLASIFIKAČNÍ PIPELINE

VSTUPNÍ DATA A EXPERIMENTÁLNÍ NASTAVENÍ

Všechny experimenty byly provedeny na SAMACOCO datasetu, který vychází z původního COCO datasetu, avšak obsahuje vyčištěné anotace a konzistentní množinu tříd. Dataset byl připraven s cílem minimalizovat chyby v anotacích a nejednoznačnosti tříd, což umožňuje spolehlivější vyhodnocení skutečného chování modelu. Evaluace zobrazuje stejné metriky jako experiment s robustností pipeline, avšak absolutní hodnoty pro vybrané třídy + vážený průměr přes všechny třídy. Ačkoliv je dataset SAMACOCO konzistentní, neobsahuje podtřídy, které klasifikátor umí rozlišovat. Proto byly evaluovány pouze nadtřídy.



DOUČOVÁNÍ

Pro umožnění doučování na slabém hardware, trénovací data známých tříd jsou redukována do generativního modelu. Tento model je reprezentován nízkodimenzionálním Gausovým rozdělením v SigLIP2 prostoru. Při trénování jsou trénovací data známých tříd náhodně vzorkována z tohoto modelu. Data nových tříd jsou dodána formou obrazových příkladů uživatelem. Při trénování klasifikátoru je použita podmínka na podobnost modelu s prvotním modelem pro známé třídy, což zaručuje konzistenci a rychlou konvergenci trénování.

Vyhodnocení. Porovnali jsme kvalitu rozpoznávání nově naučených tříd vůči kvalitě rozpoznávání známých tříd prvotním klasifikátorem. Dále jsme studovali změnu kvality klasifikace známých tříd mezi prvotním klasifikátorem a klasifikátorem s dotrénovanými třídami.

PREREKVIZITA DOTRÉNOVÁVÁNÍ - NALEZENÍ BBOXU DETEKTOREM

V navržené architektuře není detektor během procesu přidávání (dotrénovávání) nových tříd dále upravován ani dotrénováván. Důvodem je extrémní výpočetní a časová náročnost plného dotrénování detektoru, která v referenční konfiguraci dosahuje přibližně 21 dnů trénování na čtyřech GPU NVIDIA A100 s pamětí 80 GB. Takový postup je zcela nevyhovující pro scénáře vyžadující rychlou adaptaci modelu na nová data nebo provoz na omezeném hardwaru.

Z těchto důvodů je dotrénováván výhradně klasifikátor, který je pro tento účel architektonicky i tréninkově uzpůsoben. Detektor slouží pouze k lokalizaci objektů v obraze, zatímco finální rozhodnutí o třídě objektu je delegováno na samostatný klasifikační modul.

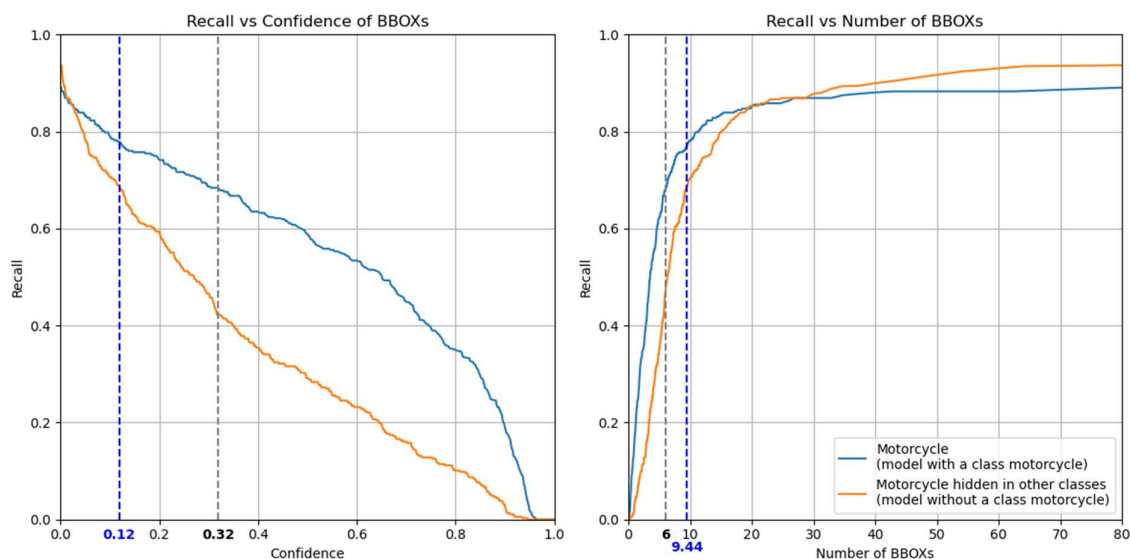
Základní prerekvizitou tohoto přístupu je schopnost detektoru lokalizovat objekty tříd, které nebyly zahrnuty v jeho trénovací sadě. Požadovaný objekt tedy musí být detektorem nalezen alespoň ve formě:

1. generické třídy objektu, nebo
2. záměny za jinou, vizuálně podobnou známou třídu.

Taková záměna není v rámci navrženého systému považována za chybu, jelikož detektor neposkytuje finální klasifikaci. Výsledná třída objektu je vždy určena až následným klasifikátorem, který pracuje nad výřezem definovaným detekčním bounding boxem.

EXPERIMENTÁLNÍ OVĚŘENÍ PREREKVIZITY (LEAVE-ONE-OUT)

Schopnost detektoru lokalizovat vyňaté třídy byla ověřena pomocí experimentu typu *leave-one-out*. Nad datasetem COCO byl natrénován YOLO detektor obsahující sadu známých objektových tříd doplněnou o generickou třídu objektu, přičemž jedna vybraná třída byla z trénování zcela vyňata. Následně bylo měřeno, jaké procento výskytů této vyňaté třídy bylo v testovací sadě detekováno, a to buď jako generický objekt, nebo jako jiná vizuálně podobná známá třída. Pozn.: dataset COCO byl použit pro tyto experimenty samostatně. Finální detektor byl natrénován na 56 datasetech, kde COCO dataset je pouze jedním z nich.



Konkrétní průběh experimentu je ilustrován v grafu XY pro třídu *motorka*. Modrá křivka odpovídá detektoru natrénovanému se všemi třídami COCO datasetu (80 tříd včetně motorky). Oranžová křivka reprezentuje detektor natrénovaný za stejných podmínek, avšak s vyňatou třídou motorka.

Výchozí minimální hodnota *confidence* detektoru je nastavena na 0,32, což znamená, že detekce s nižší hodnotou nejsou uvažovány. Pro detektor s kompletní sadou tříd dosahuje při této hodnotě *confidence* recall 0,74 a v průměru generuje 6 detekcí na jeden snímek ve validační sadě COCO.

Aby bylo dosaženo srovnatelného počtu detekovaných výskytů třídy motorka i u detektoru, který tuto třídu během trénování neviděl, je nutné snížit minimální hodnotu *confidence* na 0,12. Tím se průměrný počet detekcí zvýší na 9,44 detekce na snímek. Experiment byl opakován pro deset náhodně vybraných tříd s obdobnými výsledky; průměrná potřebná hodnota *confidence* byla 0,14 při průměrném počtu 10,2 detekce na snímek.

PREREKVIZA DOUČOVÁNÍ - ZÁVĚR

Provedené experimenty potvrzují, že lokalizace objektů tříd, které nebyly zahrnuty v trénování detektoru, je možná bez nutnosti jeho dotrénování. Detektor je schopen takové objekty zachytit buď jako generické objekty, nebo jako záměny za vizuálně podobné známé třídy. Tím je splněna klíčová prerekvizita navrženého přístupu, kdy nové třídy mohou být úspěšně rozpoznány výhradně pomocí dodatečně dotrénovaného klasifikátoru.

KLASIFIKÁTOR, TRÉNOVÁNÍ A DOUČOVÁNÍ NOVÝCH TŘÍD

Všechny detekované objekty (obrazové výřezy definované bounding boxem detektoru) jsou nejprve reprezentovány pomocí obrazového deskriptoru SigLIP2. Tyto deskriptory jsou následně zpracovány lehkou a výpočetně efektivní klasifikační hlavou, která zajišťuje finální přiřazení tříd.

Základní verze klasifikátoru byla natrénována na rozsáhlé datové sadě o velikosti 17,5 milionu obrázků a obsahuje celkem 377 tříd organizovaných hierarchicky do hlavních kategorií a jejich podkategorií. Příkladem je hlavní kategorie *zbraně*, která zahrnuje podkategorie jako sekera, granát, pistole, nůž, meč, samopal nebo raketomet. Klasifikátor je schopen vracet nejen konkrétní podkategorie, ale v

případě nejednoznačnosti i obecnější rozhodnutí na úrovni hlavní kategorie, pokud nelze spolehlivě určit jemnější rozlišení.

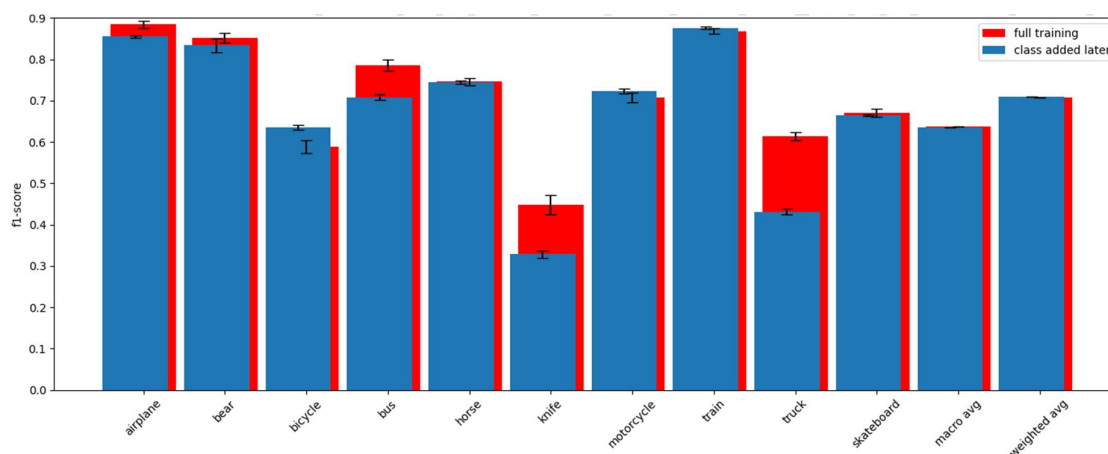
Architektura klasifikátoru i celý trénovací proces byly navrženy s důrazem na možnost velmi rychlého doučování nových tříd na omezeném hardwaru a s minimálním počtem trénovacích příkladů. Pro ilustraci rozdílu v měřítku: plné natrénování základního klasifikátoru probíhalo přibližně 188 hodin na GPU NVIDIA A100 s 80 GB VRAM a využívalo desítky tisíc trénovacích příkladů na jednu třídu. Naproti tomu proces doučování nových tříd je navržen tak, aby proběhl v řádu minut a vystačil si s jednotkami až nižšími desítkami trénovacích vzorků na třídu.

Při doučování nových tříd je nutné splnit dvě klíčové podmínky:

1. zhoršení klasifikační přesnosti na původních třídách musí být zanedbatelné,
2. nově doučené třídy musí mít k dispozici dostatečnou reprezentaci původních tříd, aby se vůči nim dokázaly jednoznačně vymezit.

Za účelem splnění těchto požadavků je původní trénovací sada pro účely doučování redukována a trénovací protokoly jsou rozšířeny o speciálně navržené regularizační mechanismy. Tyto mechanismy explicitně potlačují zapomínání již naučených tříd a stabilizují rozhodovací hranice klasifikátoru.

Redukce původní datové sady je realizována tak, že všechny trénovací obrázky jsou nejprve popsány SigLIP2 deskriptorem. Následně je pro každou třídu vytvořeno pevné množství reprezentantů (prototypů), konkrétně 1000 na třídu, pomocí clusterovacího algoritmu v prostoru deskriptorů. Během procesu doučování nejsou původní třídy zastoupeny jednotlivými obrázky, ale výhradně těmito prototypy, na které jsou aplikovány datové augmentace. Tím je výrazně snížena paměťová i výpočetní náročnost doučování při zachování reprezentativnosti původních tříd.



EXPERIMENTÁLNÍ OVĚŘENÍ DOUČOVÁNÍ (LEAVE-ONE-OUT)

Schopnost efektivního doučování nových tříd byla ověřena pomocí experimentu typu *leave-one-out*. Nad datasetem COCO byl nejprve natrénován referenční klasifikátor využívající kompletní množinu tříd. Následně bylo natrénováno deset dalších klasifikátorů, přičemž v každém případě byla z trénovací datové sady vyňata jedna třída. Tato vyňatá třída byla následně doučena postupem popsáným výše.

Doučování neprobíhalo nad celou trénovací sadou dané třídy, ale pouze nad 20 náhodně vybranými trénovacími obrázky, což simuluje realistický scénář omezené dostupnosti anotovaných dat. Výsledky experimentu jsou shrnuty v grafu. Červené sloupce v grafu reprezentují hodnoty F1-score pro plně natrénovaný referenční klasifikátor, zatímco modré sloupce odpovídají jednotlivým klasifikátorům s dodatečně doučenou třídou. Každý sloupec znázorňuje F1-score pro konkrétní doučenou třídu; poslední dva sloupce zobrazují průměrnou a váženou průměrnou hodnotu F1-score přes všechny ostatní (původní) třídy.

Z výsledků je patrné, že nově doučené třídy dosahují F1-score srovnatelného s hodnotami, kterých by bylo dosaženo při jejich plném trénování. Pouze malé množství tříd vykazuje mírné zhoršení výkonu, které je však i v těchto případech stále v prakticky použitelném rozsahu. Zároveň je patrné, že původní třídy nevykazují žádné systematické zhoršení přesnosti, což potvrzuje, že navržený redukovaný způsob doučování nevede k degradaci výkonu na již naučených třídách.

DOUČOVÁNÍ – ZÁVĚR

Navržený přístup k doučování nových tříd umožňuje rychlou a efektivní adaptaci klasifikátoru bez nutnosti jeho plného přetrénování a bez negativního dopadu na výkon na původních třídách. Kombinace SigLIP2 deskriptorů, redukované reprezentace původních tříd pomocí prototypů a cílených regularizačních mechanismů umožňuje dosahovat srovnatelné klasifikační přesnosti i při použití velmi omezeného množství trénovacích dat. Tím je splněn klíčový požadavek systému na rychlé, hardwarově nenáročné a stabilní doučování nových tříd v reálném provozu.

ZÁVĚRY

1. Limit malých objektů je kritický: pro spolehlivější detekci osoby se uvádí potřeba zhruba $\geq 30\text{--}35$ px (kratší strana bounding boxu), přičemž pro objekty $\sim 20\text{--}23$ px se stále uvádí alespoň $\sim 80\%$ úspěšnost detekce, ale s rizikem poklesu.
2. Robustnost vůči šumu je dobrá do určité úrovně: přidaný šum se směrodatnou odchylkou cca $10\text{--}20$ má podle experimentů jen malý dopad; výraznější pokles výkonu je pozorován až při úrovních okolo $\sigma \approx 50$.
3. Robustnost vůči změně jasu je relativně vysoká: i při snížení jasu na $\sim 10\%$ původní hodnoty je v experimentu uváděn výkon detekce objektů stále $> 85\%$.
4. Textové dotazy mohou být účinnější než obrazové (na anotovaném datasetu vozidel): v porovnání dotazů zadaných textem vs. obrázkem jsou textové dotazy podle výsledků obecně úspěšnější.
5. Funkce AISEE (detekce/tracky + sémantické vyhledávání + reporting) odpovídají typickému „human-in-the-loop“ modelu forenzního triage. AI urychlí vyhledání kandidátů, analytik je ověřuje a dokumentuje. Robustnostní limity (pixels, šum, světlo) ukazují, že kvalita vstupu a měřítko objektu budou v praxi hlavními prediktory spolehlivosti.

DOPORUČENÍ PRO PRAXI

1. Povinně dokumentovat nastavení zpracování (zejména Frame Step) a parametry dotazu do reportu / spisu, protože mohou měnit citlivost a časové značky výsledků.
2. Vynutit „human verification“, každý AI nález považovat za kandidáta, který musí být ověřen přehráním relevantní části videa; AISEE samo o sobě není důkazní prostředek bez kontextu a kontroly.
3. U textových dotazů preferovat popisné a konzistentní formulace, protože kvalita dotazu přímo ovlivňuje úspěšnost vyhledávání.
4. Pro vícekamerové případy používat synchronizaci/offset a multi-video zobrazení; zároveň zavést kontrolní krok ověření správného časového zarovnání.

PRÁVNÍ, ETICKÉ A PROCESNÍ ASPEKTY NASAZENÍ AISEE

1. NORMATIVNÍ RÁMEC PRO INTELIGENTNÍ SYSTÉMY SE ZVLÁŠTNÍM OHLEDEM NA OBLAST POLICEJNÍ PRÁCE

Systémy umělé inteligence (dále i jen AI z angl. Artificial Intelligence) jsou v posledních letech v popředí zájmu mezinárodní, evropské i české regulace. Přestože AI systémy nebyly v právním vakuu a vztahovaly se na ně vybrané evropské předpisy (např. Listina základních práv EU,¹ Obecné nařízení o ochraně osobních údajů,² Směrnice o rovném zacházení s osobami,³ apod.), přijala Evropská unie v souvislosti s inteligentními systémy zvláštní nařízení – Akt o umělé inteligenci (dále AIA, z angl. Artificial Intelligence Act).⁴ Důvodem přijetí této specifické regulace byl zejména fakt, že stávající předpisy nedokázaly eliminovat rizika spojená se stále autonomnějšími AI systémy a byly příliš vágní. EU chtěla dále předejít i situaci, kdy by členské státy vytvořily vlastní předpisy o AI a tím by narušily jednotný evropský trh.

Přijetí AIA předcházely roky studií, analýz a vyjednávání o tom, jak by tato regulace měla vypadat. Během této doby bylo třeba nejdříve vydefinovat hodnotový a politický rámec, který by sloužil jako základ pro uvedenou regulaci. Nutnost zaměřit se na tento rámec avizovala Evropská komise ve svém

¹ Listina základních práv Evropské unie. In: *EUR-Lex* [online]. 26.10.2012 [cit. 15.12.2025]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:12012P/TXT>

² Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Text s významem pro EHP). In: *EUR-Lex* [online]. 2016 [cit. 15.12.2025]. Dostupné z: <http://data.europa.eu/eli/reg/2016/679/oj>

³ Směrnice Rady 2000/43/ES ze dne 29. června 2000, kterou se zavádí zásada rovného zacházení s osobami bez ohledu na jejich rasu nebo etnický původ. In: *EUR-Lex* [online]. 2000 [cit. 15.12.2025]. Dostupné z: <http://data.europa.eu/eli/dir/2000/43/oj>

⁴ Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci) (Text s významem pro EHP). In: *EUR-Lex* [online]. 2024 [cit. 25.11.2025]. Dostupné z: <http://data.europa.eu/eli/reg/2024/1689/oj>

sdělení Umělé inteligence pro Evropu.⁵ Centrem pozornosti se následně stala v této souvislosti etika umělé inteligence. Evropská komise za tímto účelem ustavila Odbornou skupinu na vysoké úrovni pro umělou inteligenci (AI-HLEG z angl. High-Level Expert Group on Artificial Intelligence).⁶ Tato skupina v dubnu 2019 publikovala Etické pokyny pro zajištění důvěryhodnosti UI.⁷ Tyto pokyny nemají závaznou povahu, ale zároveň představují směr, který by měly následovat v EU vyvíjené systémy AI. Cílem by měl být vývoj tzv. důvěryhodné AI (angl. trustworthy AI). Důvěryhodná AI se vyznačuje tím, že má současně tři nezbytné složky: *legální* (AI systém je vyvinut a využíván v souladu s právem), *etickou* (AI systém je vyvinut a využíván v souladu s etickými zásadami a hodnotami) a *robustní* (AI systém by měl být odolný jak po technické, tak i po společenské stránce, aby nezpůsobil nesmyslnou újmu). Pokyny se nezaměřují na poskytování návodu k souladu s právními normami, ale mají sloužit především jako vodítko k posílení etické a robustní složky. Současně zdůrazňují, že samy o sobě nezakládají právní povinnosti. V praktické části stanoví sedm požadavků na důvěryhodnou AI. Tyto požadavky se následně promítly do struktury a obsahu AIA a ovlivnily i další politické dokumenty na AI.

Jedním z těchto dokumentů je Bílá kniha o umělé inteligenci – evropský přístup k excelenci a důvěře.⁸ Jde o koncepční dokument, který v oblasti AI vytyčuje dvojí cíl evropské politiky:

- podpořit rozvoj a zavádění AI vytvořením tzv. „*ekosystému excellence*“, který bude zahrnovat investice do výzkumu a inovací, rozvoj dovedností, podporu přijetí AI zejména u podniků a vytváření vhodných podmínek pro škálování AI v rámci vnitřního trhu, a zároveň
- řešit rizika spojená s některými způsoby použití AI prostřednictvím tzv. „*ekosystému důvěry*“ založeného na ochraně základních práv a evropských hodnot.

Dokument předkládá politické možnosti budoucího regulačního rámce zaměřeného především na „vysoce rizikové“ aplikace, kde navrhuje soubor požadavků (typicky kvalita dat a jejich správa, dokumentace, transparentnost a informování, lidský dohled, robustnost a bezpečnost) a uvažuje o nastavení dohledu a vymáhání práva, aby se předešlo roztržitosti pravidel mezi členskými státy. Je zde také navržen přístup k regulaci založený na riziku. Dokument současně zdůrazňuje, že jde o podklad pro širokou konzultaci a další rozhodování Komise.

V dubnu 2021 bylo představeno první znění návrhu Aktu o umělé inteligenci.⁹ To však v průběhu politického vyjednávání doznalo značných změn. Původní návrh byl pozměněn zejména v souvislosti

⁵ SDĚLENÍ KOMISE. Umělá inteligence pro Evropu (COM(2018) 237 final). In: *EUR-Lex* [online]. 25.4.2018 [cit. 25.11.2025]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52018DC0237>

⁶ Odborná skupina na vysoké úrovni pro umělou inteligenci | Utváření digitální budoucnosti Evropy. In: *Evropská komise* [online]. 6. 5. 2025 [cit. 12.12.2025]. Dostupné z: <https://digital-strategy.ec.europa.eu/cs/policies/expert-group-ai>

⁷ Nezávislá odborná skupina na vysoké úrovni pro umělou inteligenci. Etické pokyny pro zajištění důvěryhodnosti UI. In: *Evropský parlament* [online]. 2019 [cit. 12.12.2025]. Dostupné z: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_CS.pdf

⁸ BÍLÁ KNIHA o umělé inteligenci – evropský přístup k excelenci a důvěře (COM(2020) 65 final). In: *Evropská komise* [online]. 19. 2. 2020 [cit. 12.12.2025]. Dostupné z: https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_cs?filename=commission-white-paper-artificial-intelligence-feb2020_cs.pdf

⁹ Návrh Nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty unie (COM(2021) 206 final). In: *EUR-Lex* [online]. 21.4.2021 [cit. 25.11.2025]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52021PC0206>

se zpřístupněním modelů generativní AI veřejnosti.¹⁰ Velmi sporným bodem vyjednávání byla také samotná definice AI systému, rozsah zakázaných praktik a využívání biometriky v reálném čase. Právě tyto technologie jsou vysoce relevantní právě pro oblast policejní práce.

V souvislosti s přípravou regulace umělé inteligence a AIA byl přijat i klíčový dokument, který přímo na potenciál a rizika využívání AI v policejní práci směřuje. Konkrétně se jedná o Usnesení Evropského parlamentu o umělé inteligenci v trestním právu a jejímu využívání policií a soudními orgány v trestních věcech.¹¹ Toto usnesení stanoví, že AI může v prostředí prosazování práva a trestního soudnictví přinášet výhody ve smyslu účinnosti, přesnosti a pohodlnosti (bod A), ve smyslu zlepšování pracovních postupů (bod H) a ve smyslu poskytování vyšetřovací analýzy a pomoci (bod L). Zmiňuje výslovně případ posílené správy judikatury „prostřednictvím nástrojů umožňujících dodatečné možnosti vyhledávání“ (bod 5). Zároveň ale dokument stanoví, že využívání AI v této oblasti vytváří mimořádně vysoká rizika pro základní práva, protože zde rozhodnutí státu typicky zasahují do osobní svobody, soukromí, rovnosti a práva na spravedlivý proces. Proto Evropský parlament trvá na tom, aby se UI v této oblasti nepoužívala „automaticky“ ani nekontrolovaně, ale pouze v jasně vymezeném právním rámci, s přísnými zárukami a účinnou demokratickou kontrolou. V této souvislosti mimo jiné poukazuje na problematiku přesnosti AI systémů a na problémy spojené se zpracováním dat. Z hlediska konkrétních technologií je usnesení obzvláště přísné k využití biometriky a masového sledování. Rovněž kritizuje systémy pro prediktivní policejní práci.

Paralelně s přípravou AIA na půdě EU byla na půdě Rady Evropy připravována Rámcová úmluva o umělé inteligenci a lidských právech, demokracii a panství práva.¹² Tato úmluva má širší mezinárodní a hodnotový rozměr než AIA a klade si za cíl zajistit, aby činnosti v rámci životního cyklu systémů AI byly v souladu s ochranou lidských práv, demokracie a právního státu. Adresáty Úmluvy jsou primárně státy, kterým dokument slouží jako hodnotově-právní základna pro formování národní a mezinárodní politiky v oblasti AI. Vyjednávání Úmluvy a AIA bylo koordinováno a přijetím AIA naplnily členské státy EU své povinnosti plynoucí jim právě z Úmluvy Rady Evropy.

Následující text se detailně zaměří na aplikovatelný právní rámec, který se vztahuje na vývoj a využívání AI systémů v kontextu policejní práce. Tento přehled by měl sloužit jako základní vodítko pro posouzení právní povahy a dalších právních aspektů spojených se systémem AISEE.

Listina základních práv Evropské unie

Listina základních práv Evropské unie („Listina“) představuje soubor základních práv a svobod, které byly vyhlášeny v rámci práva Evropské unie. Sama o sobě neobsahuje konkrétní ustanovení věnovaná přímo technologiím nebo umělé inteligenci. Má ale ve svém jádru soubor obecně formulovaných základních práv, která jsou relevantní i pro používání AI systémů v trestním řízení. Jde především o

¹⁰ Pozměňovací návrhy přijaté Evropským parlamentem dne 14. června 2023 k návrhu nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)). In: *Evropský parlament* [online]. 14.6.2023 [cit. 12.12.2025]. Dostupné z:

https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_CS.html

¹¹ Usnesení Evropského parlamentu ze dne 6. října 2021 o umělé inteligenci v trestním právu a jejímu využívání policií a soudními orgány v trestních věcech (2020/2016(INI)). In: *Evropský parlament* [online]. 6.10.2021 [cit. 12.12.2025]. Dostupné z: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_CS.html

¹² Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. In: *Council of Europe* [online]. 5.9.2024 [cit. 12.12.2025]. Dostupné z: <https://rm.coe.int/1680afae3c>

právo na respektování soukromého a rodinného života (čl. 7), právo na ochranu osobních údajů (čl. 8), zákaz diskriminace (čl. 21), právo na účinnou právní ochranu a na spravedlivý proces (čl. 47), presumpce nevinu a právo na obhajobu (čl. 48) a zásadu proporcionality (čl. 52).

V souvislosti s vývojem a využíváním AI systémů v policejní práci a potažmo v trestním řízení je nutno vyzdvihnout zejména právo na ochranu soukromí a osobních údajů. Čl. 7 a čl. 8 Listiny poskytují obecnou normativní ochranu soukromého života a zpracování osobních údajů a výslovně zahrnují požadavek na to, aby osobní údaje byly „zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.“ V kontextu AI to znamená, že jakýkoli systém využívaný v trestním vyšetřování, který zpracovává osobní údaje (například analýza dat z mobilních zařízení, biometrická identifikace, prediktivní analýzy chování) musí být v souladu s těmito základními právy. Listina zde tedy vytváří normativní rámec, který omezuje použití AI systémů, pokud by vedlo k nepřiměřenému zasahování do soukromí nebo neoprávněnému zpracování dat. Konkrétní podmínky pak určují další právní předpisy. Na úrovni evropského práva jde o již zmíněné Obecné nařízení o ochraně osobních údajů (GDPR) a v kontextu policejní práce o směrnici 2016/680, která se zkráceně označuje jako Policejní směrnice.¹³

I když samotná Listina neobsahuje technologicky specifickou úpravu AI, její principy byly přeneseny do rámce specifické regulace AI, konkrétně do Aktu o umělé inteligenci. Ten např. výslovně zmiňuje princip presumpce nevinu a v recitálu 42 AIA říká, že v souladu s touto zásadou „by fyzické osoby v Unii měly být vždy posuzovány podle svého skutečného chování. Fyzické osoby by nikdy neměly být posuzovány na základě chování předvídaného AI pouze na základě jejich profilování, osobnostních rysů nebo charakteristik, jako je státní příslušnost, místo narození, místo bydliště, počet dětí, výše dluhu nebo typ vozidla, aniž by na základě objektivních ověřitelných skutečností existovalo důvodné podezření, že se dotčená osoba podílí na trestné činnosti, a aniž by bylo provedeno posouzení člověkem. Proto by mělo být zakázáno provádět posouzení rizik ve vztahu k fyzickým osobám za účelem posouzení pravděpodobnosti spáchání trestného činu těmito osobami nebo předvídání skutečného nebo potenciálního trestného činu pouze na základě profilování těchto osob nebo posouzení jejich osobnostních rysů a charakteristik“.

Míra rizikovosti AI systémů, která je v AIA klíčová pro určení povinností souvisejících s konkrétním AI systémem, je rovněž přímo navázána na Listinu. Podle recitálu 48 AIA je pro „klasifikaci určitého systému AI jako vysoce rizikového je zvláště relevantní míra nepříznivého dopadu takového systému AI na základní práva chráněná Listinou. Tato práva zahrnují právo na lidskou důstojnost, respektování soukromého a rodinného života, ochranu osobních údajů, svobodu projevu a informací, svobodu shromažďování a sdružování, právo na nediskriminaci, právo na vzdělání, ochranu spotřebitele, práva pracovníků, práva osob se zdravotním postižením, genderovou rovnost, práva duševního vlastnictví, právo na účinnou právní ochranu a spravedlivý proces, právo na obhajobu a presumpci nevinu a právo na řádnou správu. [...] Při posuzování závažnosti újmy, kterou může systém AI způsobit, a to i ve vztahu ke zdraví a bezpečnosti osob, by mělo být zohledněno také základní právo na vysokou úroveň ochrany životního prostředí zakotvené v Listině a provedené do politik Unie.“

¹³ Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV In: *EUR-Lex* [online]. 4.5.2016 [cit. 25.11.2025]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016L0680&qid=1769739965311>

Evropský Akt o umělé inteligenci

AIA je přímo použitelné evropské nařízení, což znamená, že určuje práva a povinnosti přímo jednotlivým subjektům a nemusí být nutně implementováno ve formě národního zákona v příslušném členském státě.¹⁴ Účelem AIA „je zlepšit fungování vnitřního trhu, podporovat zavádění důvěryhodné umělé inteligence (AI) zaměřené na člověka a zároveň zajistit vysokou úroveň ochrany zdraví, bezpečnosti, základních práv zakotvených v Listině, včetně demokracie, právního státu a ochrany životního prostředí, před škodlivými účinky systémů AI v Unii, jakož i podporovat inovace“ (čl. 1 odst. 1 AIA). Nařízení v sobě kombinuje pravidla pro klasifikaci AI systémů, pravidla pro jejich vývoj a využívání a pravidla pro jejich zavádění na trh. Těžištěm regulace je pak **přístup založený na riziku** (angl. risk-based approach). Ten lze charakterizovat jednoduše jako pravidlo, že čím vyšší představuje AI systém riziko pro bezpečnost a základní práva, tím přísnější povinnosti jsou pro něj stanoveny.

Toto pravidlo se promítá právě do stanovení klasifikace AI systémů na následující kategorie, pro které jsou určeny odpovídající povinnosti:

- Zakázané postupy v oblasti umělé inteligence (kapitola II. AIA, tj. čl. 5 AIA)
- Vysoce rizikové systémy AI (kapitola III. AIA, tj. čl. 6 – 49 AIA)
- AI systémy s povinností transparentnosti (kapitola IV. AIA, tj. čl. 50 AIA)
- Obecné modely AI (kapitola V. AIA, tj. čl. 51 – 56 AIA)
- Ostatní AI systémy

V následujícím textu budou jednotlivé kategorie AI systémů podle AIA analyzovány z hlediska jejich aplikace v oblasti trestního řízení a policejního vyšetřování, a to s ohledem na účel a povahu systému AISEE se zvláštním důrazem na systémy automatizovaného rozpoznávání obrazu.

Zakázané postupy v oblasti umělé inteligence

AIA zcela zakazuje určité způsoby využití systémů umělé inteligence, která představují nepřijatelná rizika pro základní práva jednotlivců. V oblasti trestního práva a využití rozpoznávání obrazu to zahrnuje zejména:

- Provozování nebo používání systémů AI pro posuzování rizik fyzických osob s cílem posoudit nebo předvídat riziko, že fyzická osoba spáchá trestný čin, a to výhradně na základě profilování fyzické osoby nebo posouzení jejích osobnostních znaků a vlastností (čl. 5, odst. 1, písm. (d))
- Provozování nebo používání systémů AI, které vytvářejí nebo rozšiřují databáze rozpoznávání obličeje prostřednictvím necíleného získávání zobrazení obličeje z internetu nebo kamerových záznamů (čl. 5, odst. 1, písm. (e))
- Provozování nebo používání systémů biometrické kategorizace, které jednotlivě kategorizují fyzické osoby na základě jejich biometrických údajů za účelem dovození nebo odvození jejich rasy, politických názorů, členství v odborových organizacích, náboženského nebo filozofického přesvědčení, sexuálního života nebo sexuální orientace; tento zákaz se nevztahuje na označování nebo filtrování legálně získaných souborů biometrických údajů, jako jsou snímky, na základě biometrických údajů nebo kategorizace biometrických údajů v oblasti vymáhání práva (čl. 5, odst. 1, písm. (g))

¹⁴ Nařízení však může obsahovat pokyny pro přijetí specifické právní regulace na úrovni členských států EU a umožnit tak odchylky v předem specifikovaných oblastech. To je i případ AIA.

- Provozování nebo používání systémů biometrické identifikace na dálku v reálném čase ve veřejně přístupných prostorech pro účely vymáhání práva, pokud to není nezbytně nutné pro jeden ze specificky určených cílů, a jen v nezbytně nutné míře (např. pátrání po obětech závažné trestné činnosti, prevence hrozícího útoku a stíhání pachatelů zvláště závažných trestných činů). I v těchto výjimečných případech je použití podmíněno předchozím soudním schválením nebo schválením nezávislého správního orgánu, s výjimkou naléhavých situací.

Vysoce rizikové systémy AI

Jde o systémy, u kterých se předpokládá, že představují významnou hrozbu pro zdraví, bezpečnost nebo základní práva jednotlivců. Správné určení, zda AI systém spadá do kategorie vysoce rizikových AI systémů, má významný dopad na to, jak jaké povinnosti jsou s ním následně spojeny. V kontextu policejní práce (a zejména využití AI systémů rozpoznávání obrazu) je relevantní Příloha III. AIA. V této příloze jsou nejrelevantnější následující dvě kategorie případů užití:

- **Biometrika (bod 1):** Tato kategorie zahrnuje systémy biometrické identifikace na dálku (nikoliv v reálném čase a nejsou zahrnuty ani systémy AI určené k použití za účelem biometrického ověřování, jejichž jediným účelem je potvrdit, že konkrétní fyzická osoba je skutečně osobou, za niž se prohlašuje, systémy pro biometrickou kategorizaci a systémy pro rozpoznávání emocí.
- **Vymáhání práva (bod 6):** Tato kategorie zahrnuje AI systémy pro podporu donucovacích orgánů nebo jejich jménem při posuzování rizika, že se určitá fyzická osoba stane obětí trestných činů, systémy na podporu donucovacích orgánů jako polygrafy nebo obdobné nástroje, systémy na podporu donucovacích orgánů za účelem hodnocení spolehlivosti důkazů v průběhu vyšetřování nebo stíhání trestných činů, systémy na podporu donucovacích orgánů za účelem posuzování rizika, že se určitá fyzická osoba jednou nebo opakovaně dopustí protiprávního jednání, a to nikoli výlučně na základě profilování fyzických nebo za účelem posuzování povahových vlastností a osobnostních rysů nebo dřívější trestné činnosti fyzických osob nebo skupin, a systémy na podporu donucovacích orgánů za účelem profilování fyzických osob v průběhu odhalování, vyšetřování nebo stíhání trestných činů.

Regulace vysoce rizikových AI systémů v AIA vytváří specifický operační rámec pro to, jak může policie používat technologie automatizovaného rozpoznávání obrazu, které jsou povolené, ale zároveň citlivé. Zatímco biometrická identifikace v reálném čase je z velké části zakázána, použití AI k biometrické identifikaci jednotlivců v zaznamenaných záběrech (následná biometrická identifikace osob) je klasifikováno jako vysoce rizikové.

Policie musí zajistit, aby systémy rozpoznávání obrazu, které využívá, byly vyvinuty s vysoce kvalitní správou dat, aby se předešlo zkreslení a případné podjatosti. Protože jsou tyto systémy vysoce rizikové, algoritmy musí být trénovány na dostatečně reprezentativních datových souborech, aby se předešlo chybám, které neúměrně postihují specifické rasové nebo etnické skupiny. V kontextu trestního řízení je to kritické pro předcházení tzv. „false positives“. Policejní orgány nemohou nasadit systém, který funguje přesně u jedné demografické skupiny, ale často nesprávně identifikuje ostatní.

Ústředním požadavkem pro policejní používání vysoce rizikových systémů rozpoznávání obrazu je přísný lidský dohled. Regulace nařizuje, že AI systém nemůže být jediným nebo konečným rozhodujícím subjektem v trestním vyšetřování (čl. 14 AIA). Když nástroj rozpoznávání obrazu označí „shodu“ mezi podezřelým a tváří ve videu, člověk musí tento výsledek ověřit a potvrdit. U biometrické identifikace musí být identifikace navíc „samostatně ověřena a potvrzena alespoň dvěma fyzickými osobami, které disponují nezbytnou odbornou způsobilostí, odbornou přípravou a pravomocí.“ Policisté také musí

rozumět omezením systému a být kompetentní odmítnout výstupy AI, pokud jsou v rozporu s jinými důkazy nebo s jejich profesionálním úsudkem.

Policie je také povinna udržovat vysokou úroveň transparentnosti a odpovědnosti týkající se používání těchto AI systémů. Před nasazením vysoce rizikového AI systému pro rozpoznávání obrazy jsou orgány činné v trestním řízení obecně povinny provést Posouzení dopadu na základní práva (Fundamental Rights Impact Assessment, FRIA) k vyhodnocení toho, jak by nástroj mohl ovlivnit práva občanů v daném konkrétním kontextu (čl. 27 AIA).

AI systémy s povinnostmi transparentnosti

U systémů AI, které nespádají do zakázaných či vysoce rizikových kategorií, ale přesto mohou ovlivnit jednotlivce, platí specifické požadavky na transparentnost. V trestním řízení jsou však některé z těchto požadavků upraveny – například policie není povinna označovat AI-generované obrazy při utajovaných operacích (např. falešné profily na sociálních sítích) nebo informovat podezřelého o tom, že jeho biometrické rysy byly analyzovány. Povinnost transparentnosti však zůstává v případě komunikace s veřejností – např. když občané hlásí trestné činy prostřednictvím AI chatbotů. Při forenzním zpracování obrazu smí policie použít AI k úpravám (např. zaostření), pokud nedojde ke změně samotného obsahu, avšak je povinna transparentně doložit tento postup v rámci vyšetřovací dokumentace.

Tento přehled ukazuje, že AIA přináší komplexní, diferencovaný přístup k regulaci systémů umělé inteligence podle míry rizika, které tyto technologie představují, a že v oblasti trestního práva a činnosti policie stanoví jasné hranice mezi zakázaným, přípustným a regulovaným využitím těchto systémů.

Český adaptační zákon k AIA

V souvislosti s přijetím AIA byl v české republice připraven návrh adaptačního zákona o umělé inteligenci.¹⁵ Tento zákon má umožnit efektivní uplatňování AIA v českém právním prostředí. Nestanovuje nové hmotněprávní pravomoci pro orgány činné v trestním řízení (např. Policii ČR), ale vytváří dodatečný právní rámec pro oznamování, dohled, schvalování, testování a kontrolu vysoce rizikových systémů umělé inteligence, včetně těch využívaných pro policejní účely. Zákon vymezuje příslušné orgány dozoru. Pro oblast ochrany osobních údajů, zejména pokud jde o vysoce rizikové AI systémy, je klíčovým orgánem Úřad pro ochranu osobních údajů. Specifickými kompetencemi pak disponuje Český telekomunikační úřad, který je jednotným kontaktním místem a příslušným orgánem pro více řízení dle AIA.

Zákon v § 13 zřizuje národní sandbox pro umělou inteligenci podle čl. 57 AI Aktu. Zřizovatelem je Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, provozovatelem Česká agentura pro standardizaci. Sandbox má sloužit pro testování a validaci AI systémů ve spolupráci s veřejnými i soukromými subjekty, avšak nezbavuje účastníky povinností plynoucích např. z regulace týkající se zpracování osobních údajů.

Návrh zákona o umělé inteligenci přenáší pravidla AI Aktu do českého právního prostředí a nastavuje nové institucionální a procesní požadavky na používání AI systémů, včetně těch využívaných při

¹⁵ Návrh zákona o umělé inteligenci a o změně zákona č. 87/2023 Sb., o dozoru nad trhem s výrobky a o změně některých souvisejících zákonů, ve znění pozdějších předpisů. In: *Portál informačního systému ODok Úřadu vlády České republiky* [online]. 24.10.2025 [cit. 5.11.2025]. Dostupné z: <https://www.odok.gov.cz/portál/veklep/material/KORNDLSJSEUC/>

trestním vyšetřování. Nedává nové pravomoci orgánům činným v trestním řízení, ale vyžaduje, aby nasazování těchto technologií probíhalo v souladu s regulacemi pro vysoce rizikové systémy, při respektu k zásadám ochrany osobních údajů a za dohledu určených orgánů. Zákon je zatím ve stavu návrhu.

Evropská policejní směrnice

Policejní směrnice představuje hlavní právní rámec EU upravující zpracování osobních údajů ze strany policejních a justičních orgánů v oblasti trestního práva. Jde o *lex specialis* k Obecnému nařízení o ochraně osobních údajů (GDPR), neboť se vztahuje specificky na zpracování údajů pro účely prevence, vyšetřování, odhalování a stíhání trestných činů nebo výkonu trestů. Jejím hlavním cílem je umožnit efektivní činnost a spolupráci bezpečnostních složek při potírání trestné činnosti, aniž by byla narušena základní práva jednotlivců, zejména právo na soukromí a ochranu osobních údajů.

Dá se říci, že směrnice stanoví přísnější pravidla než GDPR. Zásadním principem je, že každé zpracování osobních údajů musí být nezbytné, přiměřené a podložené právním základem. Výrazné omezení se vztahuje na tzv. zvláštní kategorie osobních údajů (například biometrické údaje), jejichž zpracování je přípustné pouze v případech, kdy je to výslovně stanoveno zákonem, je to nezbytné, a současně jsou přijata odpovídající záruky ochrany práv subjektu údajů (čl. 10). Dále směrnice přísně reguluje automatizované rozhodování a profilování (čl. 11), které jsou relevantní zejména při použití AI systémů k analýze videozáznamů nebo identifikaci podezřelých osob. Směrnice zakazuje rozhodnutí založená výlučně na automatizovaném zpracování, pokud by měla právní účinky vůči osobě nebo ji obdobně závažně ovlivnila. V praxi to znamená, že AI systém nemůže samostatně iniciovat zásah, například zadržení osoby, bez lidského přezkumu. Automatizovaný výstup může sloužit jako podnět pro lidského operátora, nikoli jako základ pro přímé rozhodnutí.

Směrnice dále klade důraz na odpovědnost správce údajů (čl. 19), na povinnost zavedení vhodných technických a organizačních opatření na ochranu údajů (čl. 20), povinnost vést záznamy o činnostech zpracování (čl. 24), povinnost vést logy (čl. 25), a zajištění bezpečnosti údajů (čl. 29). V tomto kontextu jsou AI systémy považovány za potenciálně rizikové technologie, které mohou zvyšovat pravděpodobnost porušení práv jednotlivců, pokud nejsou dostatečně zabezpečeny či transparentní.

Klíčovým požadavkem je povinnost provést posouzení vlivu na ochranu osobních údajů (čl. 27), pokud existuje vysoké riziko pro práva a svobody jednotlivců. Lze dovodit, že tento proces je povinný například při nasazení AI pro rozpoznávání osob ve veřejném prostoru. Orgány musí předem analyzovat rizika, dokumentovat způsob fungování technologie, její možné omyly či zkreslení a nastavit opatření na ochranu údajů a prevenci zneužití.

Policejní směrnice představuje klíčový právní nástroj pro regulaci využívání umělé inteligence v trestním vyšetřování. Stanovuje limity zpracování údajů, zakazuje nebo silně omezuje automatizované rozhodování a vyžaduje odpovědné, transparentní a zabezpečené zacházení s daty. Tím vytváří ochranný rámec pro jednotlivce a zároveň podmínky pro legální a legitimní použití AI v oblasti trestního práva. Pro úplnost je ale třeba dodat, že pokud policie vyvíjí vlastní AI systémy a zpracovává za tímto účelem osobní údaje, pak tato aktivita nespadá pod režim policejní směrnice, ale pod režim GDPR. To znamená, že policie musí identifikovat jasný právní základ pro trénování AI systému (např. plnění úkolu ve veřejném zájmu), dodržet základní zásady zpracování zásady jako minimalizace a účelové omezení a dodržovat všechna ostatní ustanovení GDPR.

Do českého práva byla policejní směrnice transponována zejména prostřednictvím zákona č. 110/2019 Sb., o zpracování osobních údajů.¹⁶ Pravidla jsou obsažena v části první, hlavě III (Ochrana osobních údajů při jejich zpracování za účelem předcházení, vyhledávání nebo odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti). Zákon č. 110/2019 Sb. je tak primárním právním nástrojem pro provedení policejní směrnice do českého práva a tvoří základní právní rámec pro ochranu osobních údajů v oblasti trestního práva. Povinnosti spravujícího orgánu jsou vymezeny především v § 32. Automatizované pořizování záznamů reguluje § 36 a povinnost provést posouzení vlivu na ochranu osobních údajů je stanovena v § 37. Zákon v § 39 rovněž výslovně stanoví, že „spravující orgán může na základě výhradně automatizovaného zpracování osobních údajů zasáhnout do práv a právem chráněných zájmů subjektu údajů nebo způsobit jiný obdobně závažný následek pro subjekt údajů, jen pokud to výslovně stanoví jiný zákon“. Povinnost zabezpečit osobní údaje je zakotvena v § 40.

V souvislosti s přijetím AIA byl zákon o zpracování osobních údajů novelizován¹⁷ a do zákona byla vložena nová ustanovení §39a až § 39c. Tato ustanovení speciální právní rámec pro používání tzv. „izolovaného systému“, tedy systému umělé inteligence určeného k vzdálené biometrické identifikaci osob v reálném čase v prostorách mezinárodního letiště. Izolovaný systém může být provozován výhradně v prostorách mezinárodního letiště s jasně vymezeným územním rozsahem. Jeho účelem je výlučně identifikace osob v souvislosti se závažnými hrozbami, jako jsou únosy, obchodování s lidmi, terorismus nebo závažná trestná činnost (např. s trestní sazbu alespoň 4 roky). Zásadní je omezení referenční databáze – lze do ní zařadit biometrická data jen za účelem dosažení těchto legitimních cílů. Zpracování dat musí být přísně odděleno a přístup k údajům je možný pouze se soudním povolením a za účelem trestního řízení. Vzniká tak důležitý prvek právní kontroly a ochrany soukromí. Cílem je umožnit využití těchto nástrojů pouze ve zcela výjimečných případech, s důrazem na zásadu proporcionality, nezbytnosti a soudní kontroly. Jedná se o konkrétní příklad implementace evropského rámce AI regulace do národní legislativy s důrazem na ochranu základních práv jednotlivců.

2. PRÁVNÍ POSOUZENÍ SYSTÉMU AISEE

Právní posouzení systému je významné z hlediska požadavků na jeho design a z hlediska jeho následného nasazení a využívání v praxi. Vychází jak z definovaného účelu systému, tak i z jeho konkrétních technických funkcionalit a možností následných úprav a způsobů užití (use-cases).

Popis systému a jeho funkcionalit

Systém je ve své podstatě softwarový nástroj, který slouží policii jako podpůrný nástroj při zpětné analýze obrazových dat souvisejících s konkrétní trestní věcí. Pracuje jak s fotografiemi, tak s videozáznamy. Typicky se bude využívat pro případy, kde bude třeba zpracovat velké datové objemy fotek/videozáznamů (zejm. záznamy z dlouhodobého sledování, velké množství videí z jedné události nebo případu).

Účelem systému je zrychlit vyhledávání relevantních výskytů osob, vozidel a dalších objektů tak, aby uživatel (policista) získal vyšetřovací stopy pro následnou práci. Vyšetřovací stopy jsou systémem

¹⁶ Zákon č. 110/2019 Sb., ze dne 12. března 2019 o zpracování osobních údajů, ve znění pozdějších předpisů.

¹⁷ Zákon č. 230/2025 Sb., ze dne 11. června 2025, kterým se mění zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů, a některé další zákony.

poskytnuty ve formě časových úseků a odkazů na zdrojové soubory. Systém není zamýšlen jako nástroj pro automatizované rozhodování či hodnocení a jeho výstupy mají sloužit pouze jako podklad pro další policejní práci a úvahy, které provádí člověk.

Typický způsob práce uživatele se systémem nejlépe ilustruje to, jak je naplňován účel, ke kterému je systém určen. Typický postup práce je následující:

Uživatel nejprve do systému nahraje videa související s případem. *Vstupem do systému* jsou fotografie, videozáznamy, případně z nich odvozené snímky nebo segmenty, které do systému nahraje uživatel v rámci konkrétního případu. Systém je určen výhradně pro zpětnou či následnou analýzu již existujících záznamů – neumí se přímo napojit na kamery a nepracuje se živým (live) streamem. U videozáznamů zpracovává pouze obrazovou složku; vyhledávání zvuku ani jeho analýza není podporována. Systém následně vstupy (fotky, videozáznamy) automaticky předzpracuje, což může být časově náročný proces.

Po nahrání a automatickém předzpracování videí může uživatel ve zpracovaných datech vyhledávat relevantní výskyty dvěma hlavními způsoby. Prvním je vyhledávání pomocí textového dotazu (*query-by-text*), kdy uživatel popíše, co hledá (například osobu s určitým oblečením, konkrétní objekt, typ vozidla, atd.). Druhým je vyhledávání podle vzoru (*query-by-image*), kdy uživatel nahraje referenční obrázek a systém vyhledá vizuálně podobné výskyty. Uživatel může dotazy dále zpřesňovat, například omezením na konkrétní časový úsek nebo na určitou část obrazu (oblast zájmu/ROI). Systém zároveň umožňuje pracovat s časovými vazbami mezi videi (například nastavit návaznost záznamů z jedné kamery nebo časy začátku), a tím podporuje i synchronní přehrávání více záběrů. Systém je zamýšlen pro vyhledávání osob a objektů především na *základě obecných vizuálních znaků*, jako je oblečení, barva a typ vozidla nebo logo. Není určen pro jednoznačnou identifikaci fyzických osob na základě biometrických údajů, nepoužívá rozpoznávání tváří ani biometrickou identifikaci a v zamýšlených scénářích se „nehledá podle obličeje“. Součástí funkcionality není ani rozpoznávání registračních značek vozidel (SPZ). Systém pracuje s předdefinovanými třídami objektů a umožňuje doplňovat (doučit) další třídy. Není však navržen pro dotrénování podtříd již existujících tříd (například vytvoření samostatné naučené třídy typu „smutný běloch“). Textové dotazy mohou teoreticky obsahovat i citlivé charakteristiky (například etnicitu, náboženské znaky nebo emoce). Tyto scénáře ale nebyly cíleně testovány a systém je přímo nepodporuje jako explicitní a garantovanou funkcionalitu. Zejména rozpoznávání emocí nebylo zamýšleno a v praxi může být vzhledem ke kvalitě typických záznamů obtížně použitelné. Předpokládá se, že textové dotazy lze technicky filtrovat a omezit, například tak, aby nebylo možné zadávat určité nepovolené kombinace.

Hlavním výstupem systému při práci s videozáznamy je seznam nalezených výskytů, který uživateli ukazuje, kdy a v jakém zdrojovém videu se podle dotazu vyskytuje hledaný objekt nebo situace. Každý výsledek je tedy vyjádřen především jako časový údaj (případně časový úsek) ve zdrojovém videu a zároveň obsahuje identifikaci konkrétního souboru (název nebo odkaz na video), v němž byl výskyt nalezen. Vedle těchto základních údajů může systém vytvářet také náhledy (snímky z videa). Uživatel si může vybrané výsledky ukládat do interního reportu a tento report následně vyexportovat do formátu PDF. PDF report obvykle obsahuje náhledy vybraných míst, identifikaci zdrojových videí, příslušné časy a poznámky, které k výsledkům doplní uživatel. Tyto výstupy slouží pouze jako vyšetřovací stopy, nikoliv jako důkaz sám o sobě. Uživatel má možnost a zároveň odpovědnost ověřit jejich relevanci a správnost tím, že si příslušné části videa znovu přehraje v běžném přehrávači a vyhodnotí je v kontextu případu. Výsledky obsažené v PDF reportu následně ověřuje a dál s nimi pracuje mimo samotný systém.

Vzhledem k tomu, že systém pracuje při vyhledávání s pravděpodobnostmi, bylo třeba pro výstupy vytvořit pravidla pro jejich řazení. Za tímto účelem přiřazuje systém ke každému nalezenému výsledku interní „věrohodnost“ na škále od 1 do 7. Tato hodnota vychází z použitých modelů nebo z metrik nad interními příznaky a slouží zejména k tomu, aby systém mohl výsledky u jednoho konkrétního dotazu seřadit nebo omezit jejich počet. Skóre není zamýšleno jako garantovaná míra přesnosti ani jako obecně srovnatelná metrika mezi různými dotazy. Jeho význam se může lišit podle toho, co uživatel dotazem sleduje (například zda mu jde o barvu, značku, typ situace nebo jiné vizuální rysy). Systém proto neposkytuje formalizovanou metriku podobnosti jako „důkaz shody“ a konečné posouzení významu výsledku zůstává na uživateli.

Co se týče režimu nasazení a zpracování či sdílení dat, pak je třeba zdůraznit, že systém je navržen tak, aby běžel výhradně v prostředí Policie ČR. Počítá se s jeho provozem na interních serverech Policie ČR v oddělené síti (on-premises) a případně také s provozem lokálně na přenosných počítačích Policie ČR. Z hlediska konektivity je důležité, že systém nebude napojen na žádné externí cloudové služby ani se nebude připojovat mimo prostředí Policie ČR. Zpracování bude probíhat lokálně a veškeré vstupy i výstupy zůstanou v prostředí spravovaném Policií ČR.

Z technického hlediska se systém skládá ze tří hlavních částí. První je výkonná část („worker“), která provádí výpočetně náročné operace, zejména předzpracování a analýzu videozáznamů, a běží na pozadí. Druhou částí je backend server, který zajišťuje aplikační logiku, poskytuje rozhraní pro uživatelskou práci a koordinuje zpracovatelské úlohy; funguje jako prostředník mezi uživatelským rozhraním a workerem. Třetí částí je frontend dostupný ve webovém prohlížeči, prostřednictvím něhož uživatel systém ovládá. Jednotlivé komponenty spolu komunikují definovanými rozhraními. Worker a backend si předávají úlohy a informace o průběhu zpracování prostřednictvím databáze PostgreSQL (například zadání úloh a jejich stav). Frontend komunikuje s backendem prostřednictvím HTTP API, přes které uživatel zadává dotazy a získává výsledky. Systém je dodáván jako jeden Docker image. Správce systému nastavuje úložiště prostřednictvím Docker „volume“, do kterého se ukládají data potřebná pro provoz, včetně nahraných videí a výstupů ze zpracování. Tento způsob distribuce a provozu je právně relevantní zejména tím, že umožňuje provoz systému bez externího přenosu dat a s kontrolou nad tím, kde jsou data fyzicky a logicky uložena.

Pro zpracování obrazové složky používá systém několik modelů strojového učení: přetrénované modely YOLO11 pro detekci objektů, model SigLIP2 v nepřetrénované variantě, model SigLIP2 v přetrénované variantě (zejména pro oblast oblečení) a vlastní klasifikační model. Tyto modely se používají k detekci a vyhledávání relevantních objektů a k posuzování vizuální podobnosti. Systém interně pracuje s příznaky a podobnostmi, které využívá pro vyhledávání a řazení výsledků. Jak již bylo zmíněno výše, tyto interní vztahy nepředává uživateli jako formalizované rozhodnutí o shodě. Konečné posouzení významu výsledku zůstává na uživateli.

Posouzení systému z pohledu AI Aktu

A) AISEE a jeho podřazení do definice „systém AI“

AIA je základním regulačním rámcem pro systémy AI. Aby bylo toto nařízení aplikovatelné, je nejdříve nutné posoudit, zda systém AISEE vůbec spadá do definice AI systému. Podle čl. 3 odst. 1 AIA je AI systémem „strojový systém navržený tak, aby po zavedení fungoval s různými úrovněmi autonomie a který po zavedení může vykazovat adaptabilitu a který za explicitními nebo implicitními účely z obdržených vstupů odvozuje, jak generovat výstupy, jako jsou predikce, obsah, doporučení nebo rozhodnutí, které mohou ovlivnit fyzická nebo virtuální prostředí“.

V souvislosti s touto definicí AI systému vydala Evropská komise nezávazné Pokyny,¹⁸ které slouží k podrobnějšímu výkladu zmíněného ustanovení a snazšímu určení, zda se definice vztahuje na konkrétní posuzovanou technologii. Podle těchto Pokynů obsahuje definice AI systému *sedm prvků*. Jsou jimi: strojový systém, míra autonomie, možná adaptabilita, účel systému (explicitní či implicitní), schopnost odvozování, povaha výstupů a schopnost ovlivnit prostředí. Zároveň Pokyny zdůrazňují, že se posouzení nemá dělat mechanicky podle „checklistu“, ale vždy podle skutečných vlastností posuzovaného systému a jeho fungování v praxi. Za klíčové odlišovací znaky vůči běžnému (tradičnímu) softwaru je považována zejména autonomie a schopnost odvozování. Autonomie znamená, že systém vykonává alespoň část činnosti nezávisle na člověku. Odvozování pak znamená, že výstupy nevznikají jen podle rigidních pravidel předem přesně určených člověkem, ale na základě modelu, který z vstupů vyhodnocuje a generuje výsledky. S ohledem na kritérium odvozování označují Pokyny za typické případy mimo definici AI systémů ty systémy, které jsou založeny na pravidlech vymezených výhradně fyzickými osobami k automatickému provádění operací. Jako typické příklady se uvádějí systémy pro zlepšení matematické optimalizace, základní zpracování údajů, systémy založené na klasické heuristice, nebo jednoduché systémy predikce. Pokyny současně vysvětlují, že adaptabilita (např. samoučení po nasazení) není nutnou podmínkou. Systém může být AI i tehdy, pokud se po zavedení už nemění a pouze odvozuje výstupy z vstupů.

Následující tabulka ilustruje, jak systém AISEE naplňuje jednotlivé prvky definice AI systému dle AIA:

Prvek definice	Aplikace na AISEE	Splnění
Strojový systém	Pokyny vymezují „strojový“ široce jako systém fungující pomocí hardwaru i softwaru. Systém AISEE je nasazen jako softwarový produkt (Docker image) běžící na serverech/noteboocích PČR; zahrnuje worker, backend a frontend. Jednoznačně jde o „strojový systém“ ve smyslu pokynů.	ANO
Autonomie	Autonomie znamená, že činnost je alespoň do určité míry nezávislá na zapojení člověka. Podmínka je splněna, pokud výstup není ručně řízen nebo explicitně a přesně určen člověkem. V systému AISEE po zadání textu nebo nahrání vzorového obrázku systém sám předzpracuje video, detekuje objekty/vyhodnotí podobnost, vyhledá možné výskyty, vrátí časové body a výsledky interně seřadí/omezí dle skóre.	ANO

¹⁸ Evropská komise. Sdělení Komise. Pokyny Komise k definici systému umělé inteligence podle nařízení (EU) 2024/1689 (akt o AI). C(2025) 5053 final. In: *Evropská komise* [online]. 2025 [cit. 02.12.2025]. Dostupné z: <https://digital-strategy.ec.europa.eu/cs/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application>

Adaptabilita	Adaptabilita je schopnost samoučení, které mění chování systému během jeho používání. Zároveň <u>není nutnou podmínkou</u>. To je pro AISEE klíčové. Systém AISEE není navržen jako samoučící se za provozu. Je však možné následně doučit nové třídy objektů (tj. adaptace spíše v režimu řízené aktualizace, nikoli samoučení).	ANO
Účel systému	Pokyny uvádějí, že účely mohou být explicitní (přímo zakódované) nebo implicitní (odvoditelné z chování systému). U systému AISEE je explicitní účel jasný – umožnit policistovi rychleji nalézt relevantní výskyty ve videích (osoba podle oděvu/kontextu, auto podle vizuálních znaků, případně jiné třídy objektů), a to formou vyšetřovacích stop (čas + zdroj).	ANO
Odvozování	Podle Pokynů spadají do typických AI přístupů, které umožňují odvozování, techniky strojového učení (včetně hlubokého učení). Systém AISEE používá přetrénované/nepřetrénované modely (YOLO11, SigLIP2, vlastní klasifikátor). Jde o modely strojového učení/hlubokého učení, které z dotazů (text nebo referenční obrázek) odvozují relevantní výsledky (podobnost, výskyty). Nefungují na základě „pevně daných pravidel“ typu databázového filtru, ale provádí výpočty založené na naučené reprezentaci.	ANO
Výstupy	Definice AI systému obsahuje výslovně tyto příklady výstupů: <i>predikce, obsah, doporučení nebo rozhodnutí</i>. Systém AISEE generuje výstupy typu: • predikce/detekce (např. přítomnost objektu/osoby v určitých framech), • doporučení v širším smyslu (seznam kandidátních časů a scén, které „odpovídají“ dotazu; interní skóre 1–7 pro řazení/filtraci), • volitelně „obsah“ v podobě náhledů zahrnutých do reportu. I když systém neprezentuje „metriku podobnosti“ jako formální důkaz shody a důrazně ponechává interpretaci na uživateli, výstup má z technického hlediska povahu prediktivního/retrieval doporučení, tj. výstupu ve smyslu definice.	ANO
Schopnost ovlivnit prostředí	Pokyny v tomto smyslu uvádějí, že „systémy AI nejsou pasivní, nýbrž aktivně ovlivňují prostředí, v němž jsou zaváděny.“ Výstupy systému AISEE (čas + zdrojové video + náhledy v reportu) mění virtuální prostředí vyšetřování. Spoluurčují totiž, co bude uživatel dále kontrolovat, jaké části videí se budou synchronně	ANO

	přehrávat a co se uloží do reportu. Nepřímo mohou ovlivnit i fyzické prostředí (následné policejní úkony), byť rozhodnutí činí člověk. Definice nevyžaduje, aby systém sám prováděl fyzické akce. Stačí, že jeho výstupy mohou prostředí ovlivnit.	
--	---	--

Tabulka č. 1 – Posouzení AISEE z pohledu definice AI systému

Uvedená analýza ukazuje, že **systém AISEE ve všech bodech splňuje definici AI systému dle čl. 3 odst. 1 AIA a tudíž se na něj vztahují příslušná ustanovení tohoto nařízení.**

B) Zařazení systému AISEE do odpovídající kategorie AI systému dle AIA

Vzhledem k tomu, že systém AISEE je AI systémem z pohledu AIA, je nutné určit, do jaké kategorie AI systémů na základě svojí povahy, účelu a způsobu fungování spadá. Posuzování AI systému bude provedeno s ohledem na klasifikaci AI systémů uvedenou v kapitole 1.2. Systém AISEE je deklarován jako vyhledávací nástroj, který umožňuje rychlé prohledávání velkých objemů dat. Nespadá pod žádnou z kategorií zakázaných AI praktik.

Z pohledu AIA je tak především důležité určit, zda spadá do kategorie vysoce rizikových AI systémů nebo ne. Klíčovým ustanovením je zde Příloha III, bod 6, písm. c), podle níž do kategorie vysoce rizikových AI systémů spadají „*systémy AI určené pro použití donucovacími orgány nebo jejich jménem či pro použití orgány, institucemi nebo jinými subjekty Unie na podporu donucovacích orgánů za účelem hodnocení spolehlivosti důkazů v průběhu vyšetřování nebo stíhání trestných činů*“. V tomto smyslu je tedy nezbytné zjistit, zda systém pro vyhledávání obrazového materiálu splňuje kritérium, jímž je **hodnocení spolehlivosti důkazů**. V současné době nejsou k dispozici žádná oficiální vodítka Evropské komise tak, jako u zakázaných AI praktik. Dostupná odborná literatura k AIA rovněž neposkytuje bližší upřesnění tohoto pojmu.¹⁹ Je tedy nutné provést právní analýzu a výklad s ohledem na samotnou vnitřní logiku AIA.

Východiskem pro právní kvalifikaci podle je „zamýšlený účel“ systému, tj. použití, pro které je systém určen. Nutno je však brát i v úvahu „rozumně předvídatelné nesprávné použití“, tedy použití mimo zamýšlený účel, které však může plynout z předvídatelného lidského chování nebo interakce s jinými systémy (čl. 3, odst. 13 AIA).

Při posuzování systému AISEE je klíčové oddělit dva typy funkcí:

- *Hodnocení spolehlivosti důkazů* míří na systémy, které samy provádějí evaluaci důkazního materiálu jako takového (např. věrohodnost, pravdivost, autenticitu, či srovnatelný závěr o tom, nakolik se lze na důkaz spolehnout).
- Vyhledávací a analytické nástroje, které pouze zefektivňují procházení velkých objemů dat a generují „vyšetřovací stopy“, typicky plní přípravnou roli: pomáhají najít kandidátní relevantní segmenty, ale samy *netvrdí, že jsou „spolehlivým důkazem“, ani neposkytují závěr o důkazní kvalitě*.

¹⁹ COUNESON, G. Article 6. Classification Rules for High-Risk AI Systems. In: C. Necati Pehlivan – N. Forgó – P. Valcke (eds.). *The EU Artificial Intelligence (AI) Act. A Commentary*. Alpen aan den Rijn: Kluwer Law International B. V., 2025, s. 212.

AISEE je primárně nástrojem pro zpětnou analýzu existujících foto/video dat, který policistovi umožňuje vyhledat možné výskyty osob/vozidel/objektů a vrací je jako časové úseky a odkazy na zdrojové soubory, s možností vytvoření reportu. Přitom je výslovně uvedeno, že výstupy slouží jen jako vyšetřovací stopy a uživatel je má ověřit opakovaným přehráním a posoudit v kontextu případu. Tato architektura použití odpovídá tomu, že systém „nepřiděluje důkazní význam“ a „nehodnotí spolehlivost důkazu“, nýbrž pomáhá s vyhledáním a organizací informací, ze kterých teprve může (po lidské verifikaci) vzniknout důkazní materiál.

Z pohledu AIA je třeba ale ještě zhodnotit, zda využívání interního skóre věrohodnosti na škále 1-7 pro řazení výsledků nenaplní pojem „hodnocení spolehlivosti důkazů“. Pokud toto skóre v praxi vyjadřuje pouze „míru shody s dotazem“ nebo „relevanci nálezu“ (tj. jak moc daný výskyt odpovídá tomu, co uživatel hledal), pak jde stále o vyhledávací funkci a přípravné třídění kandidátních výsledků. Pokud by však skóre bylo uživatelsky prezentováno nebo fakticky používáno jako závěr o „spolehlivosti důkazu“ (např. že tento segment je „důvěryhodnější důkaz“ než jiný), mohla by být naplněna podmínka o hodnocení spolehlivosti a systém by tak mohl být považován za vysoce rizikový. Právní riziko zde zvyšuje i to, že AIA výslovně počítá s „automation bias“, tedy tendencí uživatelů automaticky nebo nadměrně spoléhat na výstup systému. Nicméně s ohledem na to, že v případě systému AISEE hodnota skóre vychází z použitých modelů nebo z metrik nad interními příznaky a slouží především k tomu, aby systém mohl výsledky u jednoho konkrétního dotazu seřadit nebo omezit jejich počet, nesplňuje podmínku hodnocení důkazů.

Systém AISEE proto nelze považovat za vysoce rizikový AI systém ve smyslu, v jakém jej definuje AIA.

Za účelem ověření toho závěru bylo rovněž provedeno posouzení systému AISEE přes oficiální platformu EU AI Act Compliance Checker. Průběh posouzení a jeho výsledek je zdokumentován v příloze č. 1.

Pro úplnost je třeba ještě uvést, že i kdyby někdo systém formálně spojoval s ustanovením Přílohy III, bod 6, písm. c), tak ani za těchto okolností by systém AISEE nesplňoval definici vysoce rizikového AI systému. Důvodem je fakt, že by tento systém byl v tomto krajním případě považován za systém, jež je určen k provedení přípravného úkolu k posouzení relevantnímu pro účely použití uvedené v příloze III. Tento mechanismus přesně odpovídá situaci, kdy systém jen připravuje podklady (např. vytipuje časové úseky k lidskému ověření), aniž by materiálně ovlivňoval výsledné rozhodování.

C) Vyplývající právní povinnosti

Přestože systém AISEE nespadá do kategorie vysoce rizikových AI systémů, neznamená to, že by se na jeho využívání nevztahovaly žádné povinnosti. Provozovateli systému AISEE (zavádějící osobě) plynou specifické povinnosti z ustanovení čl. 4 a čl. 50 AIA.

Čl. 4 ukládá povinnost přijmout opatření, aby zaměstnanci provozovatele AISEE a další osoby, které jménem provozovatele zajišťují provoz a užití systému měly dostatečnou úroveň AI gramotnosti. AI gramotností se přitom rozumí „dovednosti, znalosti a chápání, které poskytovatelům, zavádějícím subjektům a dotčeným osobám umožňují, aby s přihlédnutím k jejich příslušným právům a povinnostem v souvislosti s tímto nařízením zaváděli systémy AI informovaným způsobem a aby si byli vědomi možností a rizik spojených s AI i možných škod, které může způsobit“ (čl. 3, bod 56) AIA). Opatření na proškolení mají být přiměřená tomu, jaké mají lidé technické znalosti a jaký je kontext nasazení. U systému AISEE to prakticky znamená nastavit školení a interní metodiku tak, aby uživatelé chápali, že výstupy jsou pouze vyhledávací indicie, že interní skóre je pomůcka pro řazení výsledků a

nikoliv indikátor spolehlivosti a že před další procesní prací je nutné výstupy vždy lidsky ověřit (přehráním záznamu, kontextualizací, prověřením alternativ). AI gramotnost v tomto pojetí není jednorázové „klikací školení“, ale soubor praktických kompetencí a pravidel jak správně formulovat dotazy, jak pracovat s ROI a časovou synchronizací, jak zacházet s falešnými shodami, jak dokumentovat lidské ověření a jak nepřipustit, aby se z interního skóre stal de facto „automatizovaný závěr“.

Čl. 50 AIA se neuplatní plošně na všechny AI systémy, ale jen na určité typy AI systémů. V kontextu systému AISEE se toto ustanovení převážně neuplatní – systém negeneruje syntetický obsah (pracuje s existujícími záznamy a dělá výběry/odkazy) a není určen pro rozpoznávání emocí ani biometrickou kategorizaci či tvorbu deepfake obsahu. Uživatelé by měli být pouze informováni o tom, že AISEE je systém využívající AI systém.

D) Možné nadcházející právní změny v regulaci AI

V souvislosti s hutnou legislativou regulující digitální ekonomiku a obavami z nedostatečné konkurenceschopnosti EU na poli zpracování dat a vývoje umělé inteligence, představila Evropská komise v závěru roku návrhy dvou nařízení, která by měla zjednodušit stávající regulaci.

Návrh nařízení o souhrnném digitální nařízení²⁰ představuje iniciativu Evropské komise ke zjednodušení a modernizaci současného digitálního právního rámce v Unii tím, že provádí širokou novelizaci vybraných digitálních předpisů a ruší některá existující nařízení, které jsou podle Komise nadbytečná nebo obsahují vzájemně se překrývající pravidla. Návrh se především zaměřuje na harmonizaci stávajících pravidel v oblasti dat a kybernetické bezpečnosti. Z hlediska vývoje a využívání AI systémů v policejní práci spočívá jeho nejvýznamnější přínos ve zpřesnění výkladu GDPR, konkrétně pokud jde o zpracování osobních údajů za účelem trénování systémů umělé inteligence. Návrh usiluje o kodifikaci „oprávněného zájmu“ jako platného právního základu pro trénování modelů umělé inteligence, což by mohlo usnadnit orgánům činným v trestním řízení a jejich technologickým dodavatelům vývoj algoritmů na základě reálných dat bez rizika právní nejistoty. Konkrétně návrh nařízení navrhuje doplnění článku 88c do GDPR s názvem „Zpracování v souvislosti s vývojem a provozem umělé inteligence“.

Digitální souhrnný návrh nařízení o umělé inteligenci²¹ představuje technicky orientovanou novelu stávající unijní regulace AI, která reaguje na první zkušenosti s implementací AIA a usiluje o usnadnění fungování pravidel pro poskytovatele AI systémů i dozorové orgány. Komise ve svém návrhu navrhuje řadu cílených změn, které mají překonat zpoždění ve vyhlášení norem a budování systému posuzování shody, snížit administrativní a implementační zátěž pro podniky, usnadnit proveditelnost nastavených pravidel a posílit rámce pro testování a regulační sandboxy. V oblasti prosazování práva a policejní práce bude mít tento návrh zásadní dopad. Návrh zejména počítá s odkladem účinnosti

²⁰ Návrh Nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 a směrnice 2002/58/ES, (EU) 2022/2555 a (EU) 2022/2557, pokud jde o zjednodušení digitálního právního rámce, a kterým se zrušují nařízení (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 a směrnice (EU) 2019/1024 (souhrnný balíček pro digitální oblast) (COM(2025) 837 final). In: *EUR-Lex* [online]. 19.11.2025 [cit. 27.11.2025]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52025PC0837>

²¹ Návrh Nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) 2024/1689 a (EU) 2018/1139, pokud jde o zjednodušení provádění harmonizovaných pravidel pro umělou inteligenci (souhrnný balíček pro digitální oblast týkající se umělé inteligence) (COM(2025) 836 final). In: *EUR-Lex* [online]. 19.11.2025 [cit. 27.11.2025]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52025PC0836>

povinností vztahujících se na vysoce rizikové AI systémy (původně stanovených na srpen 2026), a to tak, aby byly příslušné technické standardy plně připraveny ještě před zahájením jejich vymáhání. Pro orgány činné v trestním řízení to v praxi znamená posunutí termínu, od kterého musí být povinně dodržována pravidla, jako jsou posouzení dopadů na základní práva nebo přísná pravidla správy dat, pravděpodobně až na konec roku 2027 či 2028. Tento odklad sice poskytuje policejním složkám více času na přípravu, zároveň však prodlužuje období právní nejistoty. Návrh také počítá s doplněním článku 4a do AIA s názvem „Zpracování zvláštních kategorií osobních údajů za účelem odhalování a nápravy zkresení“. Podle tohoto ustanovení lze za splnění několika podmínek využít údaje původně shromážděné za účelem prevence, vyšetřování, odhalování nebo stíhání trestných činů podle policejní směrnice i k účelům detekce a nápravy zkresení. Tím se otevírá možnost, aby policejní složky vyvíjely systémy umělé inteligence, které budou lépe odpovídat požadavkům na ochranu základních práv a svobod.

3. ETICKÉ ASPEKTY NASAZENÍ SYSTÉMU AISEE

Vývoj a využívání AI systémů je z etického hlediska analyzováno v celé řadě mezinárodních a evropských dokumentů. Na nejvyšší úrovni stojí Doporučení UNESCO na etiku umělé inteligence.²² Tento globální normativní rámec vyzývá státy a další aktéry, aby řídili celý životní cyklus AI tak, aby posiloval lidská práva, základní svobody a lidskou důstojnost a současně chránil společnost i životní prostředí. Opírá se o hodnoty jako ochrana důstojnosti a práv, rozkvět životního prostředí a ekosystémů, diverzita a inkluze a podpora mírových, spravedlivých a propojených společností, a rozpracovává je do principů proporcionality a zabránění škodám, bezpečnosti, spravedlnosti a nediskriminace, udržitelnosti, ochrany soukromí a dat, lidského dohledu, transparentnosti a vysvětlitelnosti, odpovědnosti a gramotnosti.

Na úrovni Evropské unie jsou z pohledu etiky nejdůležitějším dokumentem již výše uváděné Etické pokyny pro zajištění důvěryhodnosti UI.²³ Tyto pokyny jsou primárně založeny na respektu k základním lidským právům. Z nich dokument odvozuje čtyři etické zásady, jež mají být dodržovány při vývoji, zavádění a používání UI: respektování lidské autonomie, předcházení újmám, spravedlnost a vysvětlitelnost. Dokument zároveň upozorňuje, že mezi zásadami mohou vznikat konflikty a je třeba je odpovědně rozpoznávat, vyhodnocovat a řešit je s ohledem na příslušný kontext.

Na tyto zásady navazuje praktická část: Pokyny převádějí uvedené etické základy do sedmi požadavků na tzv. **důvěryhodnou UI**, které mají být naplňovány v celém životním cyklu systému, a to technickými i netechnickými prostředky. Jedná se o následující zásady:

²² UNESCO. Recommendation on the Ethics of Artificial Intelligence. In: *UNESCO* [online]. 2022 [cit. 27.11.2025]. Dostupné z: <https://unesdoc.unesco.org/ark:/48223/pf0000381137>

²³ Nezávislá odborná skupina na vysoké úrovni pro umělou inteligenci. Etické pokyny pro zajištění důvěryhodnosti UI. In: *Evropský parlament* [online]. 2019 [cit. 12.12.2025]. Dostupné z: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_CS.pdf. Kromě těchto pokynů vznikly ještě další etické dokumenty, např. Rámec pro etické aspekty umělé inteligence, robotiky a souvisejících technologií – viz Usnesení Evropského parlamentu ze dne 20. října 2020 obsahující doporučení Komise k rámci pro etické aspekty umělé inteligence, robotiky a souvisejících technologií (2020/2012(INL)). In: *Evropský parlament* [online]. 20.10.2020 [cit. 1.12.2025]. Dostupné z: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_CS.html; nebo Evropská etická charta o používání umělé inteligence v soudních systémech – viz European Commission for the Efficiency of Justice (CEPEJ). European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. In: *Council of Europe* [online]. 4.12.2018 [cit. 1.12.2025]. Dostupné z: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>

- (1) lidský faktor a dohled
- (2) technická robustnost a bezpečnost
- (3) ochrana soukromí a správa dat
- (4) transparentnost
- (5) rozmanitost, nediskriminace a spravedlnost
- (6) dobré environmentální a sociální podmínky a
- (7) odpovědnost.

Dokument dále připojuje hodnotící seznam (checklist) jako konkrétní, avšak výslovně „neúplný“ nástroj pro posuzování důvěryhodnosti v praxi, který se má vždy přizpůsobit konkrétnímu použití. Hodnotící seznam byl následně publikován i zvlášť.²⁴

Při aplikaci tohoto hodnotícího seznamu na systém AISEE lze dospět k několika etickým doporučením, která budou významná při následném používání systému v praxi. Z hlediska etického posouzení je klíčové, že jde o vysoce citlivý kontext vynucování práva. I když systém pouze „zrychluje hledání“, může při nesprávném použití ovlivnit směr vyšetřování a tím zasahovat do práv jednotlivců. Největší rizika se týkají ochrany osobních údajů (nutnost DPIA, řízení přístupů, retence, logování, bezpečný export), a dále nediskriminace – zejména proto, že textové dotazy mohou teoreticky obsahovat citlivé charakteristiky (např. etnicitu či náboženské znaky), což může vést k profilování nebo nerovnému zacházení. Důležitá je také prevence přílišného spoléhání se na výsledky ze systému. Interní skóre věrohodnosti 1–7 nesmí být chápáno jako důkaz shody a výstupy musí být systematicky ověřovány přehráním zdrojového záznamu.

Opatření by proto měla zajistit (1) silnou datovou správu a bezpečnost včetně jasných retenčních pravidel, šifrování, auditních logů a kontrol exportů, (2) omezení a audit textových dotazů tak, aby nebylo možné (ani obcházením) zadávat zakázané či diskriminační požadavky, (3) doménové testování přesnosti a chyb (zejména falešných pozitiv) na typických policejních záznamech a zavedení režimu práce s nejistotou, a (4) procesní pojistky odpovědnosti a transparentnosti – školení uživatelů, jasné disclaimery jak v samotném systému, tak i v reportech, jasné označování použité verze modelů a auditovatelnost použití systému v čase.

MANUÁL PRO POUŽÍVÁNÍ SYSTÉMU AISEE

Přestože systém AISEE není klasifikován jako vysoce rizikový AI systém, je při jeho používání nutné mít na zřeteli několik hledisek a splnit právní povinnosti vyplývající z jiných právních předpisů a etických posouzení. Uživatelé systému by měli být jasně seznámeni s účelem a povahou systému a jeho případnými riziky a mít návod pro bezpečné a zodpovědné používání systému.

Instrukce pro používání systému AISEE je v příloze 2.

²⁴ Independent High-Level Expert Group on Artificial Intelligence. The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self assessment. In: *Evropská komise* [online]. 2020 [cit. 1.12.2025]. Dostupné z: <https://digital-strategy.ec.europa.eu/cs/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>

PŘÍLOHA Č. 1: VÝSLEDEK POSOUZENÍ SYSTÉMU AISEE PŘES EU AI ACT COMPLIANCE CHECKER

Právní povaha systému AISEE byla ověřena prostřednictvím online dotazníkového nástroje *EU AI Act Compliance Checker*, který provozuje Evropská komise prostřednictvím AI Act Service Desk na adrese:

<https://ai-act-service-desk.ec.europa.eu/en/eu-ai-act-compliance-checker>

EU AI Act Compliance Checker



The European Commission is pleased to introduce the AI Act Compliance Checker, a tool crafted to clarify the obligations and requirements of the AI Act. Currently in its beta version, the Compliance Checker represents an ongoing project, and we welcome your participation in its development. Your feedback and insights are important to refining this tool. Please send your feedback to the [AI Office \(CNECT-AIOFFICE@ec.europa.eu\)](mailto:CNECT-AIOFFICE@ec.europa.eu).



Disclaimer

Please note that the results generated by this compliance checker are for informational purposes only. The outputs generated are not to be considered as legal advice and we encourage seeking the assistance of a legal professional for advice tailored to your specific situation. The results, output, and other content of the compliance checker do not represent the European Commission's assessment of your situation, or of your obligations under the AI Act.



Check an AI system or an AI model

Do you want to check an AI model or an AI system?

Question information

The AI Act refers to AI models as 'essential components of AI systems, [yet] they do not constitute AI systems on their own. AI models require the addition of further components, such as for example a user interface, to become AI systems. AI models are typically integrated into and form part of AI systems' ([Recital 97](#)). 'Large generative AI models are a typical example for a general-purpose AI model, given that they allow for flexible generation of content, such as in the form of text, audio, images or video, that can readily accommodate a wide range of distinctive tasks' ([Recital 99](#)). The AI Act defines AI systems as 'machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments' ([Article 3 \(1\)](#), [Recital 12](#)).

If you wish to classify an AI system into which you have integrated your own AI model, use the Compliance Checker twice—once for the AI system and once for the AI model. The obligations under the AI Act for the general purpose AI model apply in addition to those for the AI system ([Recital 97](#)). Conversely, if you wish to classify your AI model, be aware that it may be incorporated into an AI system if you use it yourself or offer it as a service, in which case you may use the Compliance Checker twice, too.



AI model



[More info](#)



AI system



[More info](#)

Your situation involves a machine-based system that is designed to operate with varying level of autonomy, and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.



AI system definition

AI system definition

Is your system an AI system within the meaning of the AI Act?

Question information

The AI Act defines AI systems as 'machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments' ([Article 3 \(1\)](#), [Recital 12](#)).

The AI system definition should distinguish AI systems from 'simpler traditional software systems or programming approaches and should not cover systems that are based on the rules defined solely by natural persons to automatically execute operations' ([Recital 12](#)).

Sources : [Article 3](#)

☒ Yes

☐ No

☐ Uncertain

Your role within the AI Act

Are you or your organisation responsible for any of the following roles within the EU? Note: If you have multiple roles, such as provider and deployer, please complete the assessment separately for each role to ensure a comprehensive evaluation

Sources : [Article 2 \(1\)](#); [Article 3](#); [Recital 87](#)

☒ Provider [More info](#)

☐ Deployer [More info](#)

☐ Importer [More info](#)

☐ Distributor [More info](#)

☐ Authorised representative [More info](#)

☐ Product manufacturer [More info](#)

☐ You are a natural person using an AI system for purely personal non-professional activity

Are you within the scope of the AI Act?

Do you meet any of the following statement?

Question information

'In light of their digital nature, certain AI systems should fall within the scope of the AI Act even when they are not placed on the market, put into service, or used in the Union' ([Recital 22](#))

Sources : [Article 2](#) ; [Recital 21](#) ; [Recital 22](#)

☒ Your AI system is placed or put in service within the EU

☒ You are established or located within the EU

☒ Your AI system's output is used in the EU

☐ An AI system is integrated with your product under your own name or trademark

☐ None of the above

Out of scope: excluded systems

Does your AI system meet any of the following descriptions?

Sources : [Article 2](#) ; [Recital 22](#) ; [Recital 23](#) ; [Recital 25](#)

☐ The AI system is exclusively developed and used for military, defence or national security purposes

☐ The AI system is used by public authorities in third countries or international organisations in the framework of international cooperation for law enforcement and judicial cooperation

☐ The AI system is specifically developed and put into service for the sole purpose of scientific research and development

[More info](#)

☐ The AI system is used in research, testing or development activity prior to being placed on the market or put into service

☒ None of the above

Prohibited AI systems under the AI Act

Does your AI system fall under one of these AI practices?

Sources : [Article 3](#) ; [Article 5](#) ; [Recital 15](#) ; [Recital 16](#) ; [Recital 18](#) ; [Recital 29](#) ; [Recital 31](#) ; [Recital 42](#) ; [Recital 43](#) ; [Recital 44](#) ; [Guidelines on prohibited AI practices](#)

- ☐ AI system deploys subliminal, manipulative or deceptive techniques to materially distort a person's behaviour, thereby likely causing significant harm [More info](#)
- ☐ AI system exploits of vulnerabilities due to age, disability or a specific socioeconomic situation to materially distort a person's behaviour, thereby likely causing significant harm [More info](#)
- ☐ AI system carries out social scoring leading to detrimental or unfavorable treatment of certain natural persons or groups of persons [More info](#)
- ☐ AI system does individual criminal offence risk assessment and prediction for natural persons solely on the profiling or assessment of personality traits or characteristics [More info](#)
- ☐ Untargeted AI-enabled scraping of facial images from the internet or CCTV to create or expand databases [More info](#)
- ☐ AI system deploys emotion recognition in the areas of workplace and education institutions (except when used for medical and safety reasons) [More info](#)
- ☐ Biometric categorisation to deduce sensitive attributes like political opinion, religious beliefs or sexual orientation [More info](#)
- ☐ Use of remote biometric identification in 'real-time' in publicly accessible space for the purpose of law enforcement, unless explicitly authorised by national law based on the AI Act [More info](#)

☒ None of the above

Classification rules for high-risk AI systems

Is your AI system, or the product in which it is intended to be used as a safety component, subject to sector-specific regulations?

Question information

The AI Act defines safety component as 'a component of a product or of an AI system which fulfils a safety function for that product or AI system, or the failure or malfunctioning of which endangers the health and safety of persons or property' ([Article 3 \(14\)](#)).

Sources : [Article 3 \(14\)](#); [Article 6](#)

☐ Yes

☒ No

☐ Uncertain

Classification rules for high-risk AI systems (Annex III - AI Act)

Does your AI system fall within any of the following areas?

Sources : [Article 6 \(2\)](#); [Annex III](#); [Recital 52](#); [Recital 48](#); [Recital 54](#); [Recital 55](#); [Recital 56](#); [Recital 57](#); [Recital 58](#); [Recital 59](#); [Recital 60](#); [Recital 61](#); [Recital 62](#); [Recital 63](#)

- ☐ Critical infrastructure: AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity [More info](#)
- ☐ Biometrics
- ☐ Education and vocational training
- ☐ Employment, workers' management and access to self-employment
- ☐ Access to and enjoyment of essential private services and essential public services and benefits
- ☒ Law enforcement
- ☐ Migration, asylum and border control management
- ☐ Administration of justice and democratic processes
- ☐ None of the above

Law enforcement

Is your AI system intended to be used for any of the following use-cases?

Question information



Sources : [Article 6](#); [Annex III \(6\)](#)

- ☐ AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies in support of law enforcement authorities or on their behalf to assess the risk of a natural person becoming the victim of criminal offences
- ☐ AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies in support of law enforcement authorities as polygraphs or similar tools
- ☐ AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies, in support of law enforcement authorities to evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences
- ☐ AI systems intended to be used by law enforcement authorities or on their behalf or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for assessing the risk of a natural person offending or re-offending not solely on the basis of the profiling of natural persons as referred to in Article 3-(4) of Directive (EU) 2016/680, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups
- ☐ AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for the profiling of natural persons as referred to in Article 3-(4) of Directive (EU) 2016/680 in the course of the detection, investigation or prosecution of criminal offences

☒ None of the above

Transparency obligations of certain AI systems under the AI Act

Does your AI system perform any of these functions?

Sources : [Article 50](#) ; [Recital 132](#) ; [Recital 133](#)

☒ The AI system interacts directly with natural persons [More info](#)

☐ The AI system generates synthetic audio, image, video or text content [More info](#)

☐ None of the above

[< Back](#)

Results

Your role

According to the AI Act, you are considered as a provider under [Article 3 \(3\)](#).

Risk level assessment

Your AI system is likely covered by the AI Act as it does fall within the scope of [Article 3 \(1\)](#).

Your AI system is likely not considered as high-risk. It is likely that your AI system poses no to minimal risks.

Your obligations

According to [Article 4](#), you must ensure a sufficient level of AI literacy of your staff and other persons dealing with the operation and use of AI systems on your behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

Following [Article 50](#) of the AI Act, you must follow certain transparency requirements as a provider.

- If your AI system interacts directly with natural persons (e.g. a chatbot), you must ensure that AI systems are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system.

Unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use.

This obligation does not apply to AI systems authorised by law to detect, prevent, investigate or prosecute criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties, unless those systems are available for the public to report a criminal offence.

- If your AI system generates synthetic audio, image, video or text content you must ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated. You must ensure that your technical solutions are effective, interoperable, robust and reliable as far as this is technically feasible, taking into account the specificities and limitations of various types of content, the costs of implementation and the generally acknowledged state of the art, as may be reflected in relevant technical standards.

Transparency obligations shall not apply to the extent the AI systems perform an assistive function for standard editing or do not substantially alter the input data provided by the deployer or the semantics thereof, or where authorised by law to detect, prevent, investigate or prosecute criminal offences.

The information shall be provided to the natural persons concerned in a clear and distinguishable manner at the latest at the time of the first interaction or exposure. The information shall conform to the applicable accessibility requirements.

Your AI system is likely not considered as high-risk. It is likely that your AI system does not have to comply with Chapter 3 of the AI Act, which relates to high-risk AI systems.

Reset

PŘÍLOHA Č. 2: MANUÁL PRO POUŽÍVÁNÍ SYSTÉMU AISEE

1. Účel a povaha systému

Tento systém je podpůrný softwarový nástroj pro Policii ČR určený ke zpětné analýze již existujících fotografií a videozáznamů v konkrétní trestní věci. Systém neslouží k „živému“ monitoringu, neumí se přímo napojit na kamery a u videa zpracovává pouze obrazovou složku. Jeho úkolem je urychlit vyhledávání relevantních výskytů osob, vozidel a dalších objektů v rozsáhlých datových objemech tak, aby uživatel získal vyšetřovací stopy (časové úseky a odkazy na zdrojové soubory), se kterými dále pracuje mimo systém.

Systém není určen k automatizovanému rozhodování, k hodnocení viny ani k nahrazení lidského úsudku. Výstupy mají povahu vyšetřovacích stop, které musí být vždy ověřeny člověkem přehráním originálního záznamu a posouzením v kontextu případu. Tato zásada je klíčová i z hlediska prevence přehnaného spoléhání se na AI a pro udržení důkazní hodnoty následně zajištěného materiálu.

2. Právní rámec a role odpovědných osob

Systém se používá v prostředí trestního řízení, tedy v kontextu, který je z hlediska základních práv vysoce citlivý. To znamená, že i když systém „jen“ vyhledává ve videích, může reálně ovlivnit směr vyšetřování a tím zasahovat do práv dotčených osob (např. presumpce nevin, riziko diskriminace, atd.).

Z pohledu AI Aktu je podstatná zejména: (i) povinnost zajištění AI gramotnosti osob, které systém provozují a používají (čl. 4 AI Aktu), tedy aby uživatelé rozuměli funkcím, limitům a rizikům; a (ii) dodržení povinnosti transparentnosti, tj. uživatelé by měli být seznámeni s tím, že jde o AI systém.

Z pohledu ochrany osobních údajů při činnostech orgánů činných v trestním řízení se uplatní směrnice (EU) 2016/680 (tzv. policejní směrnice). Ta stanoví zásady zpracování (zákonnost, účelové omezení, minimalizace, přesnost, omezení uložení, bezpečnost) a odpovědnost správce za dodržení těchto zásad.

3. Základní pojmy pro práci v systému

„*Vyšetřovací stopa*“ je informace, která napovídá, kde by se v datech mohlo nacházet něco relevantního (např. časový úsek ve videu), ale sama o sobě ještě není závěrem o tom, co video prokazuje. Systém poskytuje stopy typicky jako seznam časů/časových úseků a odkazy na zdrojová videa, případně náhledové snímky a interní report exportovatelný do PDF.

„*Skóre 1–7*“ je interní hodnota, kterou systém používá k řazení výsledků jednoho dotazu. Tato hodnota není kalibrovaná pravděpodobnost, není to „míra shody“ a nesmí být prezentována jako důkaz. Proto se k ní přistupuje pouze jako k pořadí relevance pro konkrétní dotaz, nikoliv jako k „věrohodnosti“ ve smyslu dokazování.

4. Povinnosti a minimální kompetence uživatele (AI gramotnost podle čl. 4 AI Aktu)

Poskytovatel i uživatelé musí zajistit, aby osoby, které systém obsluhují nebo interpretují jeho výstupy, měly dostatečnou úroveň AI gramotnosti odpovídající jejich roli, zkušenostem a kontextu použití. To zahrnuje zejména porozumění tomu, že systém pracuje pravděpodobnostně, že bude mít falešná pozitiva i falešná negativa, že výkon závisí na kvalitě záznamu (noc, déšť, komprese, rozmazání, překrytí) a že výsledky musí být vždy ověřeny člověkem.

V praxi to znamená, že uživatel nesmí systém chápat jako „automatického znalce“ a nesmí delegovat klíčové úsudky (např. „osoba na videu je pachatel“, „na videu není zbraň“) jen na to, že AI něco našla nebo nenašla. Uživatel má mít schopnost zvolit vhodnou vyhledávací strategii (více dotazů, časové omezení, práce s ROI), kriticky číst výsledky a dokumentovat vlastní ověřovací kroky.

5. Co je se systémem dovoleno dělat

Systém je dovoleno používat výhradně jako nástroj pro vyhledávání a třídění stop v obrazových datech vztahujících se ke konkrétní trestní věci, a to v souladu s právním titulem a účelovým omezením dané věci. Z hlediska ochrany osobních údajů musí být zpracování nezbytné pro úkoly orgánu činného v trestním řízení a opřené o právo Unie nebo členského státu.

Je přípustné používat vyhledávání „query-by-text“ a „query-by-image“ pro obecné vizuální znaky (oblečení, barva, typ vozidla, logo, předmět), přičemž je nutné nastavit dotazy tak, aby byly přiměřené cíli a nevytvářely nepřiměřený zásah do práv osob.

6. Co je se systémem zakázáno dělat (protiprávní nebo nepřijatelné použití)

Zakázáno je používat systém k takovým dotazům nebo postupům, které by vedly k diskriminaci, nepřipustnému profilování nebo k selekci osob na základě citlivých charakteristik (např. etnicita, náboženské znaky, sexuální orientace, zdravotní stav, emoce). Směrnice 2016/680 připouští zpracování zvláštních kategorií údajů jen striktně nezbytně, se zárukami a za splnění taxativních podmínek.

Zakázáno je rovněž používat výstupy systému k rozhodnutí „na základě samotné automatizace“ způsobem, který by měl nepříznivý právní účinek nebo významně zasahoval do osoby, pokud to není výslovně autorizováno právem a se zárukami včetně práva na lidský zásah. Systém tedy nesmí sloužit jako automatizovaný filtr, který sám rozhoduje, koho podezírat, koho vyčlenit a koho „vyloučit“, a ani jako náhrada vyšetřovacího úsudku.

Zakázáno je „rozšiřování účelu“ (tzv. function creep), tedy použití mimo konkrétní trestní věc nebo bez odpovídajícího zákonného rámce, a dále jakékoli obcházení interních pravidel (např. skrývání citlivých dotazů pomocí synonym či kódů). Z hlediska zásad zpracování musí být použití účelově omezené, přiměřené a prezkoumatelné.

7. Transparentnost podle čl. 50 AI Aktu a dopady na tento systém

Čl. 50 AI Aktu stanoví povinnosti transparentnosti pro vybrané typy AI systémů: zejména pro systémy určené k přímé interakci s osobami, pro systémy generující syntetický obsah, pro rozpoznávání emocí/biometrickou kategorizaci a pro „deep fake“ výstupy.

U popsaného systému se tyto povinnosti typicky neuplatní, protože systém negeneruje syntetický obsah a není určen pro rozpoznávání emocí ani biometrickou kategorizaci. Přesto je nutné v manuálu výslovně uvést „hranice funkcí“ a nastavit proces, že jakýkoli budoucí rozvoj (např. přidání generování syntetických rekonstrukcí, automatické popisy osob s citlivými atributy, nebo funkce rozpoznávání emocí) spustí nové posouzení a potenciálně i povinnosti podle čl. 50. Uživatelé by měli být ale jasně informováni, že základem systému je AI.

8. Doporučený pracovní postup tak, aby výstupy měly maximální hodnotu pro dokazování

Uživatel má vždy začít tím, že si ujasní vyšetřovací otázku a vymezí rozsah dat, která jsou pro konkrétní věc relevantní. Před nahráním dat do systému je vhodné zajistit, aby originální soubory byly uchovány v nezměněné podobě a aby byl evidován jejich původ, časové údaje a integrita.

Po zpracování dat je vhodné používat kombinaci strategií: dotazování více způsoby (text i obraz), více alternativních dotazů a citlivé zacházení s ROI (region of interest, tj. oblast zájmu). Výsledky ze systému je třeba chápat jako navigaci k místům ve videu; pro každé místo, které má význam, musí následovat krok ověření v originálu, tj. přehrání úseku v běžném přehrávači, záznam toho, co uživatel skutečně viděl, a uložení odkazu na originální soubor a časový údaj.

PDF report ze systému má být používán jako pracovní pomůcka a dokumentace postupu, nikoliv jako důkaz sám o sobě. V reportu má být vždy jasné uvedeno, že jde o výběr stop a že interpretace proběhla po lidském ověření.

9. Jak předcházet „tichému vynechání“ (falešným negativům)

Základní pravidlo je, že „AI nic nenašla“ nesmí být samo o sobě považováno za „na záznamu nic není“, zejména u klíčových tvrzení (alibi, přítomnost zbraně, přítomnost osoby). Tato procesní brzda je zásadní i pro soudní použitelnost, protože chrání před nekontrolovaným přenesením omylu modelu do dokazování.

Prakticky se doporučuje zavést dvojí strategii hledání: vedle přímého dotazu („najdi zbraň“) vždy používat i obcházející dotazy („najdi ruce v kapse“, „najdi lesklý předmět“, „najdi osoby ve shluku“, „najdi rychlý pohyb“, apod.), doplněné časovým procházením kritických úseků. V těžkých podmínkách (noc, déšť, nízké rozlišení, proti světlu) je nutné předpokládat vyšší míru vynechání a tomu přizpůsobit intenzitu lidské kontroly.

Současně se má zavést kontrolní vzorkování z „negativních“ úseků: např. náhodná kontrola 2–5 % segmentů, které systém neoznačil, a cílené (stratifikované) vzorkování z problematických podmínek. Pokud se v kontrolních vzorcích opakovaně najdou relevantní jevy, musí následovat eskalace: úprava vyhledávací strategie, citlivosti/prahů, případně interní incident a revize vhodnosti použití v daném typu záznamů.

10. Opatření proti diskriminaci a zneužití dotazů

Protože textové dotazy mohou teoreticky obsahovat citlivé charakteristiky, je třeba nastavit kombinaci politiky, technických omezení a dohledu. Minimem je zavést pravidla zakázaných dotazů a kombinací, technickou blokaci citlivých atributů a detekci obcházení (synonyma, překlady, kódová slova), a dále audit log dotazů a exportů (kdo, kdy, jaký dotaz, co exportoval). Tyto kroky přímo snižují riziko

diskriminační selekce stop a pomáhají prokazovat zákonnost a přiměřenost zpracování v citlivých věcech.

Z hlediska ochrany osobních údajů platí, že zpracování zvláštních kategorií údajů je povoleno jen výjimečně a za striktních podmínek; proto má být uživateli výslovně zakázáno cílit dotazy na etnicitu, náboženství či emoce jako vyhledávací kritérium, pokud pro to neexistuje jasný a dokumentovaný právní základ a nezbytnost.

11. Děti, veřejná shromáždění a další citlivé scénáře

Pokud záznamy obsahují děti, má se uplatnit přísnější režim „need-to-know“, omezený okruh oprávněných osob, přísnější retenční pravidla a zvýšená kontrola exportů. U záznamů z demonstrací či veřejných shromáždění je nutné počítat s vyšším rizikem zásahu do svobody projevu a shromažďování; použití musí být vždy striktně vázáno na konkrétní trestní věc a podléhat internímu schvalovacímu kroku proporcionality.

12. Záznamy, logování, retence a bezpečnost (data governance)

Pro účely prokazatelnosti zákonnosti i pro interní audit musí být vedeny záznamy o tom, jak se systém používal. Směrnice 2016/680 výslovně vyžaduje vedení logů pro operace v automatizovaných systémech (sběr, změna, konzultace, zpřístupnění, kombinování, výmaz) a stanoví, že logy slouží pro ověření zákonnosti, self-monitoring, bezpečnost a trestní řízení.

Dále musí být nastaveny retenční doby pro: originální nahraná videa, odvozené snímky/segmenty, interní příznaky/embeddingy (pokud se ukládají), PDF reporty a auditní logy. Retence má být přiměřená a vázaná na potřeby trestní věci; zásady zpracování vyžadují omezení uložení a bezpečnostní opatření.

13. Změnové řízení a reprodukovatelnost

Každá změna modelu, prahů, konfigurace nebo doučení tříd musí být označená a prověřitelná, aby bylo možné zpětně doložit, v jakém nastavení systém pracoval v době vytvoření stopy a reportu. To je prakticky nezbytné jak pro férovost vůči dotčeným osobám, tak pro schopnost obhájit postup u soudu (včetně vysvětlení, proč se něco našlo/ne-našlo).

14. Incidenty, hlášení rizik a nápravné kroky

Je nutné zavést jednoduchý a reálně používaný mechanismus, jak hlásit (i interně) situace typu: opakované falešné pozitivní výsledky, zjištěné „tiché vynechání“ v kontrolních vzorcích, podezření na diskriminační dopady, pokusy o zakázané dotazy, nebo bezpečnostní incident. Součástí má být i postup nápravy: dočasné omezení použití v daném scénáři, úprava metodiky dotazů, revize nastavení a (pokud je to relevantní) přehodnocení, zda je systém pro daný typ dat vůbec vhodné nasadit.

1 Appendix: Metriky a evaluační protokoly

V tomto textu jsou formalizovány metriky používané v evaluační smyčce pro *detekci*, *klasifikaci*, *vyhledávání* (retrieval) a *re-identifikaci* (Re-ID), včetně metrik pro robustnost vůči degradacím a ověření nových validačních postupů (generický objekt, few-shot doučování bez katastrofického zapomínání).

1.1 Základní značení

Uvažujme dataset $\mathcal{D} = \{(x_i, y_i)\}_{i=1}^n$, kde x_i je vstupní obraz a y_i je anotace. Pro detekci použijeme standardní reprezentaci pravdivosti ve tvaru množiny referenčních bounding boxů

$$\mathcal{B}_i^* = \{(b_{ij}^*, c_{ij}^*)\}_{j=1}^{m_i},$$

a množiny predikcí $\hat{\mathcal{B}}_i = \{(\hat{b}_{ik}, \hat{c}_{ik}, \hat{s}_{ik})\}_{k=1}^{\hat{m}_i}$, kde b značí polohu (box), c třídu a $s \in [0, 1]$ konfidenční skóre.

Shodu predikce $\hat{b}$ s referencí b^* definujeme přes průnik nad sjednocením (IoU)

$$\text{IoU}(\hat{b}, b^*) = \frac{|\hat{b} \cap b^*|}{|\hat{b} \cup b^*|}.$$

Při pevném prahu $\tau \in (0, 1)$ považujeme predikci za správnou, existuje-li přiřazení (např. bipartitní matching) tak, že $\text{IoU}(\hat{b}, b^*) \geq \tau$ a (dle režimu) buď $\hat{c} = c^*$ (třídivě specifická detekce/klasifikace), nebo $\hat{c} \in \{c^*, \text{generic}\}$ (detekce s generickou třídou).

1.2 Metriky detekce a klasifikace: Precision, Recall, F1

Po určení shod na úrovni instancí definujeme počty true positives (TP), false positives (FP) a false negatives (FN). Pro pevnou konfiguraci parametrů a pevnou prahovou hodnotu τ platí

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}, \quad \text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}},$$

$$\text{F1} = \frac{2 \text{ Precision Recall}}{\text{Precision} + \text{Recall}}.$$

Náhled: Precision, Recall, F1

Precision odpovídá na otázku: „Když něco označím jako objekt, jak často mám pravdu?“. **Recall** odpovídá: „Kolik skutečných objektů vůbec najdu?“. **F1** je kompromis, který je vysoký jen tehdy, když jsou vysoké obě složky.

Makro vs. mikro průměrování. Pro množinu tříd $\mathcal{C}$ lze použít *mikro* průměrování (součet TP/FP/FN přes třídy) nebo *makro* průměrování (aritmetický průměr metrik po třídě). Formálně, např. makro-recall:

$$\text{Recall}_{\text{macro}} = \frac{1}{|\mathcal{C}|} \sum_{c \in \mathcal{C}} \frac{\text{TP}_c}{\text{TP}_c + \text{FN}_c}.$$

Normalizace vůči referenčnímu nastavení. Necht' pro metriku $M \in \{\text{Precision}, \text{Recall}, \text{F1}\}$ označuje $M(\theta)$ hodnotu při konfiguraci parametrů θ a θ_0 referenční nastavení. Normalizovanou metriku definujeme jako relativní výkon

$$\widetilde{M}(\theta) = \frac{M(\theta)}{M(\theta_0)}.$$

Tato normalizace umožňuje přímé porovnání dopadů degradací nebo změn parametrů vůči stabilnímu referenčnímu bodu.

1.3 Retrieval a Re-ID: top- K recall a mAP

V úlohách vyhledávání uvažujme pro každý dotaz q množinu relevantních prvků $\mathcal{R}(q)$ a seřazený seznam kandidátů $\pi_q = (d_1, \dots, d_N)$ dle rostoucí vzdálenosti (resp. klesající similarity).

top- K recall. Indikátorem úspěchu je, zda se alespoň jeden relevantní prvek objevil mezi prvními K položkami:

$$\text{Rec@}K(q) = \mathbb{I}(\mathcal{R}(q) \cap \{d_1, \dots, d_K\} \neq \emptyset).$$

Metrika top- K recall (přes dotazy $\mathcal{Q}$) je

$$\text{Rec@}K = \frac{1}{|\mathcal{Q}|} \sum_{q \in \mathcal{Q}} \text{Rec@}K(q).$$

Náhled: top- K recall

„Je správný výsledek v prvních K návrzích?“ Pokud ano, dotaz se počítá jako „úspěšný“.

Average Precision a mean Average Precision (mAP). Pro dotaz q definujeme precision na prefixu délky k jako $P_q(k) = \frac{1}{k} \sum_{i=1}^k \mathbb{I}(d_i \in \mathcal{R}(q))$ a relevanci v pozici k jako $\text{rel}_q(k) = \mathbb{I}(d_k \in \mathcal{R}(q))$. Potom

$$\begin{aligned} \text{AP}(q) &= \frac{1}{|\mathcal{R}(q)|} \sum_{k=1}^N P_q(k) \text{rel}_q(k), \\ \text{mAP} &= \frac{1}{|\mathcal{Q}|} \sum_{q \in \mathcal{Q}} \text{AP}(q). \end{aligned}$$

Náhled: AP a mAP

AP hodnotí „jak kvalitně jsou seřazeny výsledky“: odměňuje, když relevantní položky přicházejí brzy. **mAP** je průměr AP přes všechny dotazy.

1.4 Reprezentace tracku klíčovými snímky a agregační metriky vzdálenosti

Nechť dotaz je reprezentován embeddingem $z \in \mathbb{R}^d$. Track T je reprezentován množinou embeddingů klíčových snímků $\{t_1, \dots, t_N\} \subset \mathbb{R}^d$. Základní vzdálenost mezi embeddingy značme $\delta(\cdot, \cdot)$ (např. kosinová vzdálenost nebo ℓ_2).

Agregovanou vzdálenost dotazu k tracku definujeme:

$$D_{\min}(z, T) = \min_{1 \leq i \leq N} \delta(z, t_i),$$

$$D_{\text{avg}}(z, T) = \frac{1}{N} \sum_{i=1}^N \delta(z, t_i),$$

$$D_{\text{med}}(z, T) = \text{median}\{\delta(z, t_i)\}_{i=1}^N.$$

Náhled: MIN/AVG/MEDIAN vzdálenost k tracku

Track je „shluk“ vektorů z několika klíčových snímků. Pak:

- $D_{\min}$: stačí, když je dotaz podobný alespoň jednomu snímku v tracku (nej„optimističtější“ variant).
- D_{avg} : vyžaduje, aby dotaz byl podobný „průměrně“ (citlivější na odlehlé snímky).
- D_{med} : kompromis; je stabilnější vůči odlehlým snímkům než průměr.

Tracky seřadíme vzestupně dle $D(z, T)$; volba N a agregační funkce se optimalizuje maximalizací metriku $\text{Rec}@K$ a/nebo mAP na validační množině.

1.5 Robustnost vůči degradacím: parametrizované testy

Degradaci modelujeme operátorem g_λ s parametrem intenzity λ (např. rozptyl Gaussovského šumu, faktor jasu, měřítko). Pro každý λ vyhodnotíme metriku M na transformovaném datasetu $\mathcal{D}_\lambda = \{(g_\lambda(x_i), y_i)\}$.

Křivky výkonu. Studujeme funkci $\lambda \mapsto M(\lambda)$, případně normalizovaně $\widetilde{M}(\lambda) = M(\lambda)/M(0)$.

Mezní bod robustnosti. Pro prah $\alpha \in (0, 1)$ definujeme maximální tolerovatelnou degradaci

$$\lambda^*(\alpha) = \sup\{\lambda : \widetilde{M}(\lambda) \geq \alpha\}.$$

Náhled: mez robustnosti

„Jak moc můžu obraz zhoršovat, než mi výkon spadne pod např. 80%?“ Hodnota $\lambda^*(0.8)$ je právě tato „mez“.

Tato definice formalizuje tvrzení typu „metriku udržíme nad 80% do určité intenzity šumu“.

1.6 Evaluace generického objektu: leave-one-out protokol

Nechť $\mathcal{C}$ je množina tříd dostupných při původním trénování. Pro každou třídu $c \in \mathcal{C}$ definujeme leave-one-out trénovací množinu (třída c odstraněna) a natrénovaný detektor f^{-c} .

Na testovací množině obsahující objekty třídy c měříme schopnost detekce buď jako „generic“ nebo jako vizuálně podobnou třídu. Formálně zavedeme množinu přijatelných predikovaných tříd

$$\mathcal{A}(c) = \{\text{generic}\} \cup \mathcal{S}(c),$$

kde $\mathcal{S}(c)$ je předem určená množina podobných tříd (např. dle embeddingů prototypů nebo ručně). Predikce je „správná“ pro instanci třídy c , pokud existuje match s $\text{IoU} \geq \tau$ a $\hat{c} \in \mathcal{A}(c)$. Výsledkem je $\text{Recall}_c^{\text{gen}}$ a (volitelně) $\text{Precision}_c^{\text{gen}}$, a agregace např. průměrem přes $c \in \mathcal{C}$.

Náhled: generický objekt (leave-one-out)

Jednu třídu z trénování záměrně „vynecháme“. Pak se ptáme: „Když teď uvidím tuto neznámou třídu, dokáže ji model aspoň označit jako **generic**?“

1.7 Few-shot doučování bez katastrofického zapomínání

Nechť $\mathcal{C}_{\text{old}}$ jsou původní třídy a $\mathcal{C}_{\text{new}}$ nově přidané třídy. Označme θ_{base} parametry modelu původně natrénovaného a θ_{ft} parametry po few-shot doučení.

Katastrofické zapomínání kvantifikujeme rozdílem výkonu na původních třídách:

$$\Delta \text{F1}_{\text{old}} = \text{F1}_{\text{old}}(\theta_{\text{ft}}) - \text{F1}_{\text{old}}(\theta_{\text{base}}),$$

Náhled: katastrofické zapomínání

Model se doučí něco nového, ale nesmí při tom „zapomenout“ staré věci. Hodnota $\Delta \text{F1}_{\text{old}} < 0$ znamená, že výkon na původních třídách klesl.

kde F1_{old} je mikro nebo makro F1 omezené na $\mathcal{C}_{\text{old}}$. Současně vyžadujeme, aby $\text{F1}_{\text{new}}(\theta_{\text{ft}})$ dosáhlo požadované hodnoty na $\mathcal{C}_{\text{new}}$.

Prototypová aproximace původních tříd. V praxi lze pro každou $c \in \mathcal{C}_{\text{old}}$ uchovat množinu prototypů $\{p_{c,1}, \dots, p_{c,M}\}$ (např. $M = 1000$) reprezentující původní rozložení embeddingů. Testovací sada pro ověření zapomínání pak může být definována jako klasifikace/projekce vůči těmto prototypům; konkrétní implementace je závislá na použitém modelu a dostupných anotacích.

1.8 Poznámky k implementaci v testovací smyčce

Metriky výše je vhodné počítat konzistentně pro všechny experimenty (změna λ , změna N , volba $D_{\text{min}}/D_{\text{avg}}/D_{\text{med}}$, leave-one-out, few-shot), aby bylo možné přičíst rozdíly ve výkonu pouze danému faktoru.