VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

BIOMETRICKÁ IDENTIFIKACE OSOB V ČESKÉ REPUBLICE: PRÁVNÍ REGULACE, ETICKÉ OTÁZKY A POSTOJE VEŘEJNOSTI

Autor práce: Josef Paleček

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: Mgr. Bc. Radovan Sládek

Katedra: Katedra právních oborů a bezpečnostních studií

2026

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Josef Paleček

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Biometrická identifikace osob v České republice: právní regulace, etické otázky a postoje veřejnosti

Název bakalářské práce v anglickém jazyce: Biometric Identification of Individuals in the Czech Republic: Legal Regulation, Ethical Issues and Public Attitudes

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, včetně titulů): Mgr. Bc. Radovan Sládek

Datum zadání bakalářské práce (měsíc, rok): Listopad 2025

Cíl bakalářské práce:
Hlavním cílem bakalářské práce je vyhodnotit postoje veřejnosti k využívání biometrických údajů k identifikaci osob a porovnat je s reálným fungováním biometrických systémů v praxi na příkladu Letiště Václava Havla v Praze.
Vedlejším cílem je posoudit, jak veřejnost vnímá bezpečnost, spolehlivost a přijatelnost těchto technologií ve vztahu k jejich skutečnému využití a legislativnímu rámci.

Student: Josef Paleček, DiS.	29. 11. 2025 *datum*	*podpis*
Vedoucí práce: Mgr. Bc. Radovan Sládek	14. 11. 2025 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	9. 12. 2025 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	11. 12. 2025 *datum*	*podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	20. 12. 2025 *datum*	*podpis*

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú. ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucímu bakalářské práce Mgr. Bc. Radovanu Sládkovi za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

PALEČEK, J. *Biometrická identifikace osob v České republice: právní regulace, etické otázky a postoje veřejnosti: bakalářská práce*. České Budějovice: Vysoká škola evropských a regionálních studií, 2026. 75 s. Vedoucí bakalářské práce: Mgr. Bc. Radovan Sládek.

Klíčová slova: biometrie, identifikace osob, ochrana soukromí, postoje veřejnosti, umělá inteligence

Bakalářská práce se zabývá problematikou využití biometrických údajů k identifikaci osob. Hlavním cílem práce je vyhodnotit postoje veřejnosti k využívání biometrických údajů k identifikaci osob a porovnat je s reálným fungováním biometrických systémů v praxi na příkladu Letiště Václava Havla v Praze. Vedlejším cílem je posoudit, jak veřejnost vnímá bezpečnost, spolehlivost a přijatelnost těchto technologií ve vztahu k jejich skutečnému využití a platnému legislativnímu rámci. Získaná data jsou hodnocena a analyzována především z hlediska věkových odlišností respondentů.

Práce je členěna na teoretickou a praktickou část. V teoretické části se autor zabývá analýzou odborné literatury se zaměřením na základy a historii biometrie, detailní popis jednotlivých biometrických metod, právní regulaci v kontextu evropského nařízení AI Act a etické otázky spojené s plošným sledováním. V praktické části práce je provedeno průzkumné šetření formou kvantitativního sběru dat u široké veřejnosti. Získané poznatky z dotazníkového šetření jsou následně komparovány s reálným provozem bezpečnostních systémů, jmenovitě automatizovaných bran e-Gate a kamerových systémů na rozpoznávání obličejů, na mezinárodním Letišti Václava Havla v Praze.

ABSTRACT

PALEČEK, J. *Biometric Identification of Persons in the Czech Republic: Legal Regulation, Ethical Issues and Public Attitudes: Bachelor Thesis*. České Budějovice: College of European and Regional Studies, 2026. 75 pp. Supervisor: Mgr. Bc. Radovan Sládek.

Key words: artificial intelligence, biometric identification, biometrics, privacy protection, public attitudes

The bachelor thesis deals with the issue of using biometric data for personal identification. The main goal of the thesis is to evaluate public attitudes towards the use of biometric data for the identification of persons and to compare them with the real functioning of biometric systems in practice, using the example of Václav Havel Airport in Prague. The secondary goal is to assess how the public perceives the security, reliability, and acceptability of these technologies in relation to their actual use and the valid legislative framework. The obtained data are evaluated and analyzed primarily from the perspective of age differences among the respondents.

The thesis is divided into a theoretical and a practical part. In the theoretical part, the author analyzes professional literature focusing on the basics and history of biometrics, a detailed description of individual biometric methods, legal regulation in the context of the European AI Act, and ethical issues associated with mass surveillance. In the practical part, an exploratory survey is conducted in the form of quantitative data collection among the general public. The findings from the questionnaire survey are subsequently compared with the real operation of security systems, namely automated e-Gates and facial recognition camera systems, at the international Václav Havel Airport in Prague.

Obsah

Úvod

Biometrická identifikace. Bezesporu vysoce aktuální a dynamicky se rozvíjející téma. Moderní technologie prostupují do našich životů takovou rychlostí, že je takřka nemožné představit si dnešní společnost bez jejich každodenního využívání. Biometrie již nezahrnuje pouze otisky prstů v kriminalistice, ale můžeme pod ni zařadit široké spektrum metod, jako je rozpoznávání obličeje, skenování oční duhovky nebo analýza lidského hlasu a dynamiky chůze.

V dnešní době se významně zvýšila potřeba efektivního a rychlého zabezpečení, ať už v digitálním nebo fyzickém světě. Tradiční metody, jako jsou hesla či přístupové karty, narážejí na své limity, protože je lze snadno ztratit, zapomenout nebo odcizit. Z důvodu rostoucích bezpečnostních hrozeb a potřeby automatizace lze tedy předpokládat i nadále zvýšený přesun k biometrickým systémům, a to nejen v komerční sféře, ale potažmo i ve státní správě a na úrovni kritické infrastruktury.

Bezpečnostní složky a státní instituce se však musí vyrovnat s faktem, že plošné nasazování těchto technologií vzbuzuje u obyvatelstva řadu otázek a obav. Pokud se zaměříme na fungování moderních kamerových systémů s umělou inteligencí, můžeme získat dojem, že společnost směřuje k neustálému monitorování a postupné ztrátě anonymity ve veřejném prostoru.

U biometrie jde primárně o využívání jedinečných a celoživotně neměnných fyziologických či behaviorálních znaků člověka, které mají sloužit jako spolehlivý prostředek k určení identity. Biometrický údaj pak můžeme charakterizovat jako vysoce citlivou informaci, jejíž únik nebo zneužití ohrožuje samotnou podstatu jednotlivce a má velký účinek na jeho soukromí. Moderní sledovací technologie totiž nerespektují fyzické hranice a sběr dat probíhá často neviditelně. Samotný efektivní rozvoj těchto systémů by měl být proto veden v přísném souladu s etickými a legislativními pravidly.

Autor práce považuje téma biometrické identifikace za velmi aktuální, jelikož rychlost zavádění těchto systémů ve světě i v České republice představuje zároveň obrovský technologický pokrok i potenciální zásah do základních lidských práv. V rámci dané problematiky je také potřeba analyzovat, zda je česká veřejnost na takto razantní změny dostatečně připravena a jak tyto systémy reálně vnímá. Ve své bakalářské práci se autor zaměřil právě na otázku využívání biometrie, která představuje jednu z největších technologických a právních výzev dnešní doby. Téma bylo vybráno také z důvodu osobního zájmu autora o bezpečnostní technologie, jejich neustálý vývoj a aktuálnost.

1 Cíl a metodika bakalářské práce

Hlavním cílem bakalářské práce je vyhodnotit postoje veřejnosti k využívání biometrických údajů k identifikaci osob a porovnat je s reálným fungováním biometrických systémů v praxi na příkladu Letiště Václava Havla v Praze. Vedlejším cílem je posoudit, jak veřejnost vnímá bezpečnost, spolehlivost a přijatelnost těchto technologií ve vztahu k jejich skutečnému využití a legislativnímu rámci. Získaná data jsou hodnocena a analyzována především z hlediska věkových odlišností respondentů.

Bakalářská práce se člení na teoretickou a praktickou část. Teoretická část analyzuje odbornou literaturu a platnou legislativu. Zaměřuje se na historii biometrie, detailní popis jejích metod a každodenní využití. Významný prostor je věnován právní regulaci v kontextu obecného nařízení GDPR a evropského Aktu o umělé inteligenci (AI Act). Následně jsou posouzeny etické otázky, rizika kybernetické bezpečnosti a hrozba masového sledování.

V praktické části proběhlo kvantitativní průzkumné šetření u široké veřejnosti. Získané poznatky jsou v závěru práce komparovány s reálnou praxí. Jako hlavní praktický příklad byl zvolen provoz bezpečnostních systémů – konkrétně automatizovaných bran e-Gate a kamer na rozpoznávání obličejů – na Letišti Václava Havla v Praze. Analýza tohoto příkladu vychází ze sekundárních veřejných zdrojů, oficiálních zpráv a aktuálních soudních usnesení.

Vzhledem k exploračnímu a deskriptivnímu charakteru šetření nebyly stanoveny striktní hypotézy k exaktnímu potvrzování. Průzkum se soustředí na zmapování povědomí občanů, jejich osobních zkušeností a identifikaci klíčových obav z odevzdávání citlivých dat. Dotazník byl navržen tak, aby postupně gradoval od obecného vnímání biometrie až k vyhraněným bezpečnostním scénářům (např. pátrání po zločincích).

Sběr dat proběhl prostřednictvím anonymního elektronického dotazníku (Google Forms), distribuovaného převážně na sociálních sítích a fórech v období od 10. února do 3. března 2026. Odpovědi od celkem 151 respondentů byly zpracovány metodami deskriptivní statistiky a popsány v grafech. Pro hlubší interpretaci autor primárně využíval metodu křížové analýzy, která umožnila přesně identifikovat mezigenerační rozdíly v postojích veřejnosti k biometrickým technologiím.

2 Základy a historie biometrie

2.1 Základy biometrie

Nejdříve je třeba si stanovit, co znamená pojem biometrie. V literatuře se můžeme setkat s pojmy biometrie a biometrika. Dříve byl každý z pojmů samostatným vědním oborem, ačkoliv se v obou případech jednalo o spojení matematiky a biologie. Postupem času ale docházelo k postupnému propojování těchto oborů až v podstatě došlo k jejich spojení. V současnosti jsou tyto termíny víceméně považovány za synonyma. Dále je v textu pro srozumitelnost používán hlavně pojem biometrie.

Biometrie je založena na principu, že na světě neexistují dva naprosto totožní jedinci. Tato skutečnost je vědecky prokázaná a díky tomu můžeme říct, že každý člověk je jedinečný svým vzhledem, ale i svým chováním a jednáním a že všichni neseme unikátní znaky, např. otisky prstů, tvar obličeje a další. Tyto znaky se navíc v průběhu celého lidského života prakticky nemění a lze je nazvat jako biometrické údaje. Díky moderním technologiím jsou tyto údaje měřitelné a lze tak jednotlivé osoby od sebe rozeznat.[1]

Biometrické údaje lze rozdělit na dvě skupiny, a to na vlastnosti fyziologické a vlastnosti behaviorální. Do fyziologických vlastností můžeme zařadit např. otisk prstu, tvar obličeje, geometrii ruky nebo oční sítnici. Behaviorální vlastnosti vychází z chování člověka, a proto biometrickým údajem může být třeba dynamika chůze, psaní nebo hlas.

S biometrií a biometrickými údaji dále pracují samotné biometrické systémy, které zpravidla slouží k automatickému rozeznání (identifikaci) nebo ověření (verifikaci) osoby, kdy jsou k tomuto procesu využity jedinečné měřitelné znaky a vlastnosti člověka. Z toho vyplývá, že biometrické systémy mohou fungovat ve dvou režimech – režim identifikace a režim verifikace.[2]

Při verifikaci systém porovnává biometrická data osoby s jejími uloženými vzory v databázi. Nejprve se člověk prokáže například PINem nebo kartou a systém následně ověří, zda mu biometrická data skutečně patří. Tento režim se využívá v systémech, jejichž cílem je zabránit tomu, aby více lidí mělo stejnou kartu nebo PIN.

[1] VANČO, Emil. Biometrie, biometrika - geneze, vývoj a současné pojetí. *Kriminalistika* [online]. 2005, roč. 38, č. 1. [cit. 2025-12-20]. Dostupné z WWW: http://www.mvcr.cz/soubor/kriminalistika-archiv-2005-01-zip.aspx.

[2] BITTO, Ondřej. *Šifrování a biometrika aneb tajemné bity a dotyky*. 1. vyd. Kralice na Hané: Computer Media, 2005. s. 118-119. ISBN 80-86686-48-5.

Při identifikaci systém vyhledává odpovídající biometrická data v celé databázi, aniž by osoba musela předem cokoli zadávat.[3]

Ať už biometrický systém pracuje v jakémkoliv režimu, princip fungování je stejný. Vždy je v daném systému biometrický senzor sloužící k získání biometrického vzorku, z něhož jsou extrahovány výrazné znaky, tzv. markanty, které jsou následně uloženy do databáze. Tímto se daná osoba stává registrovanou. Pokud následně bude osoba chtít např. vstoupit do budovy, je přes senzor opět odebrán vzorek. Systém poté porovná tento vzorek s údaji v databázi, najde, případně nenajde shodu a podle výsledku umožní, nebo neumožní přístup do budovy.[4] Obecně lze říci, že na tomto principu fungují všechny biometrické systémy.

2.2 Historie biometrie

Slovo biometrie či biometrika pochází z řeckých slov „bios“ a „metron“, tedy život a měřit. Používání biologických znaků k rozpoznávání lidí má velmi dlouhou historii. Už před tisíci lety se lidé poznávali a rozeznávali podle jedinečných rysů obličeje a místo podpisu používali mimo jiné otisky dlaní. Některé z těchto otisků jsou staré až 30 000 let.[5]

První záznamy o použití slova biometrie pochází z první poloviny 19. století. Definice slova jako taková vzniká až na konci 19. století díky rozvoji statistiky a biologie.

Spojení biologie a matematiky a vznik slova biometrie je spojován s anglickým matematikem a statistikem Karlem Pearsonem, který se zabýval kromě jiného matematickými metodami pro studium procesů dědičnosti a evoluce.

Další významnou osobností, která se podílela na vývoji základů biometrie, byl belgický vědec, matematik, astronom a sociolog Adolphe Lambert Quételet. Byl znám tím, že mnoho měření prováděl sám, a jedním z nejznámějších případů bylo měření obvodu prsou skotských vojáků. Také vytvořil tzv. Quételův index sloužící ke stanovení stupně obezity na základě výšky a váhy jedince. Tento index je dnes znám pod názvem body mass index neboli BMI.

---

[3]JAIN, Anil K., Patrick J. FLYNN a Arun A. ROSS (eds.). *Handbook of biometrics*. New York: Springer, 2008. s. 6. ISBN 978-0-387-71040-2.

[4] DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. [Brno: M. Drahanský], 2011. s. 15. ISBN 978-80-254-8979-6.

[5] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. Ostrava: VŠB-TU Ostrava, 2008. s. 4. [cit. 2025-12-21]. Dostupné z WWW: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/biometricke_metody.pdf.

V historii biometrie byl v 19. století důležitou osobností i Francis Galton, a to zejména díky svému přínosu k rozvoji daktyloskopie. Právě tato metoda se později stala jedním z hlavních nástrojů využívaných k identifikaci osob v kriminalistice.[6]

Historie biometrie je kromě matematiky a biologie úzce spojena právě s kriminalistikou. Alphonse Bertillon vytvořil první biometrickou metodu využívanou policií. Jednalo se o antropometrickou metodu, která vycházela z tvrzení, že délky kostí se u člověka po dovršení 20 let nemění a že nelze najít dva jedince se stejnými rozměry různých částí těla. Jednoduše řečeno šlo o to, že byly měřeny a zaznamenávány tělesné rozměry zločinců, čímž vznikala jakási databáze, kde byly osoby tříděné do různých kategorií např. podle barvy očí, vlasů apod. Tato metoda velice pomohla policii po celém světě při identifikaci osob. Nebyla však dlouho používaná a postupně ji nahradila jednodušší a rychlejší daktyloskopie.[7]

S rozvojem počítačů a celkově výpočetní techniky v druhé polovině 20. století se biometrie jakožto věda sloužící k identifikaci osob dostala i mimo kriminalistiku. Časem přibylo mnoho znaků člověka, které mohou sloužit jako biometrický údaj, např. geometrie obličeje, ruky, sítnice nebo DNA. Biometrie se stala součástí mnoha jiných oblastí, hlavně oblasti ochrany osob a majetku a dnes se setkáváme s jejím využitím každý den v rámci běžného života. S rozvojem biometrie je však spojen i rozvoj způsobů, jak biometrickou identifikaci obejít, což jí brání v ještě širším rozšíření.[8]

2.3 Výhody a nevýhody biometrie

Biometrické ověřování představuje významný pokrok v oblasti digitální bezpečnosti a autentizace uživatelů a díky tomu přináší několik zásadních výhod oproti tradičním metodám zabezpečení.

V první řadě poskytuje biometrie výrazně vyšší úroveň bezpečnosti než konvenční metody. Zatímco hesla, PIN kódy nebo přístupové karty mohou být ztraceny nebo odcizeny, u biometrických charakteristik jako otisk prstu nebo geometrie obličeje taková situace teoreticky nastat nemůže. Moderní systémy navíc obsahují pokročilé mechanismy

[6] VANČO, Emil. Biometrie, biometrika - geneze, vývoj a současné pojetí. *Kriminalistika* [online]. 2005, roč. 38, č. 1. [cit. 2025-12-21]. Dostupné z WWW: http://www.mvcr.cz/soubor/kriminalistika-archiv-2005-01-zip.aspx.

[7] RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. Profesionál. s. 146-152. ISBN 978-80-247-2365-5.

[8] VANČO, Emil. Biometrie, biometrika - geneze, vývoj a současné pojetí. *Kriminalistika* [online]. 2005, roč. 38, č. 1. [cit. 2025-12-21]. Dostupné z WWW: http://www.mvcr.cz/soubor/kriminalistika-archiv-2005-01-zip.aspx.

detekce živosti, které zabraňují obejít systém za pomoci fotografií či jiných umělých biometrických charakteristik.

Z hlediska uživatelského komfortu nabízí biometrie bezkonkurenční jednoduchost. Namísto procesu zadávání komplexních, často velmi dlouhých a složitých hesel stačí krátký pohled do kamery nebo přiložení prstu ke čtečce. Biometrické systémy navíc eliminují častý problém zapomínání přihlašovacích údajů, jelikož své biometrické charakteristiky člověk zapomenout nemůže.

Významnou vlastností biometrického ověřování je jeho nepřenositelnost. Na rozdíl od hesel nebo přístupových karet nelze biometrické údaje jednoduše předat jiné osobě. To zajišťuje, že přístup k zabezpečeným systémům má skutečně pouze oprávněný uživatel.

Také stojí za zmínku skutečnost, že moderní cloudová řešení biometrického ověřování nabízejí vynikající škálovatelnost. Na rozdíl od systémů vázaných na konkrétní zařízení mohou cloudové platformy pružně reagovat na měnící se požadavky a obsluhovat rostoucí počet uživatelů napříč různými aplikacemi a geografickými oblastmi.

Ačkoli biometrické technologie nabízejí řadu výhod, je důležité nezapomínat na jejich potenciální nevýhody.

Jak se biometrické technologie stávají běžnější součástí našeho života, organizace a firmy musí řešit zásadní otázku - jak ochránit tyto mimořádně citlivé osobní údaje. Na rozdíl od tradičních bezpečnostních prvků, jako jsou hesla nebo PIN kódy, mají biometrické údaje jednu klíčovou nevýhodu v tom, že jejich kompromitace představuje trvalý problém. Zatímco prolomené heslo můžeme jednoduše změnit, naše fyziologické charakteristiky jako otisk prstu či struktura duhovky zůstávají neměnné prakticky po celý život.

Tato skutečnost klade mimořádné nároky na organizace spravující biometrická data. Musí investovat značné prostředky do sofistikovaných bezpečnostních systémů, které dokáží odolat stále sofistikovanějším útokům hackerů. Nejde přitom pouze o samotné zabezpečení dat, ale i o to, že organizace musí implementovat komplexní ochranná opatření zahrnující šifrování, bezpečný přenos dat a jejich oddělené ukládání od ostatních osobních informací.

Dále je třeba zmínit legislativní rámec. Evropské nařízení GDPR a další předpisy stanovují přísné požadavky na zpracování biometrických údajů. Organizace musí zajistit nejen technickou bezpečnost, ale také transparentnost zpracování, získání informovaného souhlasu a respektování práv subjektů údajů. To vyžaduje úzkou spolupráci

s poskytovateli, kteří mají prokazatelné zkušenosti s implementací těchto požadavků a dodržováním osvědčených postupů v oblasti ochrany osobních údajů.[9]

Další nevýhodou systémů, které využívají biometrické údaje, je fakt, že nelze zajistit, aby tyto systémy mohlo používat 100 % lidí. Na světě je mnoho osob s různými omezeními, např. osoby bez horních končetin nebo prstů na ruce zákonitě nemohou využívat systémy, které potřebují k autentizaci otisk prstu. Pro osoby se zrakovým postižením nemusí být příjemné používat systémy, které jsou založeny na principu skenu oční duhovky nebo sítnice. Na těchto příkladech je zřejmé, že je nutné systém pak rozšířit tak, aby ho mohly používat i osoby, které daný biometrický údaj nemohou poskytnout, což ve výsledku může snížit celkovou úroveň zabezpečení.

Avšak i osoby bez jakýchkoliv omezení se mohou setkat s potížemi při autentizaci.

Je totiž mnoho faktorů, které mohou mít vliv na správné rozeznání uživatele. Může se jednat o situace, kdy je osoba nachlazená, stane se jí úraz, ale může jít i o drobnosti jako např. příliš mastné nebo suché prsty. V důsledku to znamená, že systém nerozená uživatele, který pak musí celý proces opakovat.

Důležité je zmínit i problém standardizace. Přestože již existuje několik mezinárodních standardů, je stále problematické použít v jednom systému produkty od různých výrobců. Každý výrobce totiž ve svých produktech používá vlastní řešení algoritmů, šifrování a přenosu dat, což pak ztěžuje, někdy i znemožňuje kombinovat produkty od různých firem do jednoho systému.

Pokud vezmeme v potaz zmíněné nevýhody, lze odvodit poslední nedostatek, jímž je cena. Systémy využívající biometrické údaje jsou zpravidla dražší než ostatní běžné alternativy.[10]

[9] KIICHLE-GROSS, Becky. Advantages and disadvantages of biometrics. In: *Mitek* [online]. 7. 1. 2025 [cit. 2025-12-21]. Dostupné z WWW: https://www.miteksystems.com/blog/advantages-and-disadvantages-of-biometrics.

[10] RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. Profesionál. s. 619-620. ISBN 978-80-247-2365-5.

3 Metody biometrické identifikace využívané v praxi

Tato kapitola obsahuje stručné shrnutí jednotlivých biometrických metod, které jsou v současnosti využívané při biometrické identifikaci nebo verifikaci člověka. Jak již bylo zmíněno výše, tyto údaje lze rozdělit na údaje fyziologické a behaviorální.

3.1 Daktyloskopie (analýza otisků prstů)

Identifikace podle otisku prstu je pravděpodobně nejstarší biometrickou metodou. Lze říci, že jde o symbol biometrické identifikace.[11] S otisky prstů je historicky spojená především daktyloskopie. Jde o jednu z nejstarších metod kriminalistiky, sloužící k identifikaci osob, která je založena na existenci papilárních linií.

Papilární linie lze najít na vnitřní straně prstů rukou i nohou, na dlaních a plochách chodidel. Nikde jinde na těle nejsou. Jde o vyvýšené části kůže, které dosahují výšky přibližně 0,1 až 0,4 mm a šířky 0,2 až 0,7 mm. Tyto reliéfy poté tvoří daktyloskopické obrazce, které jsou základem daktyloskopické identifikace osob.

Tento způsob identifikace vychází z několika základních pravidel. Prvním je, že na světě nelze nalézt dva jedince, kteří by měli naprosto shodné obrazce papilárních linií. Další pravidlo říká, že se papilární linie v průběhu života prakticky nemění. Posledním pravidlem je skutečnost, že papilární linie nelze odstranit, jenom pokud by byla odstraněna i zárodečná vrstva kůže.[12]

Samotná identifikace spočívá v nalezení a porovnání určitých znaků, které jsou vytvořeny papilárními liniemi. Takovým znakům pak říkáme markanty. Těch je několik druhů, například různé body, ostrůvky a můstky. Markantů je na otisku prstu něco mezi 75 až 175. Rozpoznání otisku může probíhat dvěma způsoby. Buď podle globálního vzoru, kdy se porovnává základní vzor, oblasti vzoru, případně počet papilárních linií, nebo podle podrobností, kde se porovnávají jednotlivé markanty, konkrétně jejich typ, orientace nebo pozice.

Metod pro nasnímání otisku prstu je hned několik. Převážně je použit snímač otisku prstu až na výjimku ve formě daktyloskopických karet, které se používají dodnes

[11] PORADA, Viktor. *Kriminalistické, forenzní a právní souvislosti identifikace osob podle funkčních a dynamických znaků*. Karlovy Vary: Vysoká škola Karlovy Vary, 2010. s. 85. ISBN 978-80-87236-02-4.
[12] RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. Profesionál. s. 169-170. ISBN 978-80-247-2365-5.

v kriminalistické praxi. Jde o jednoduchou metodu, kdy se do karty otlačí jednotlivé prsty pomocí inkoustu. Pak se karta pomocí skeneru naskenuje do počítače. [13]

Snímání pomocí snímačů lze rozdělit na snímání statické a snímání šablonováním.

Statické snímání je nejběžněji používaný způsob. Osoba pouze přiloží prst ke snímači, aniž by s ním musela dál nějak pohybovat. Z toho vychází hlavní výhoda tohoto řešení – jednoduchost ovládání. Nevýhodou však může být šance na poškození snímače při přílišném tlaku nebo možnost zanechání latentního (skrytého) otisku, který pak má vliv na schopnost osobu identifikovat.

Snímání šablonováním je odlišné tím, že se prst na senzor nepřikládá, ale přejíždí se přes něj. Systém snímá pouze část otisku během pohybu prstu a následně z jednotlivých částí složí kompletní otisk. Výhodou je, že senzor je mnohem menší (úzký pruh) než u statického snímání, z čehož plyne nižší cena. Každé přejetí navíc snímač očistí, takže na něm nezůstávají latentní otisky. Nevýhodou je ovládání, které není tak jednoduché, a uživatel si musí zvyknout na určitý postup.[14]

Praktické využití otisků prstů dnes dalece přesahuje hranice kriminalistiky. Asi nejvíce se tyto technologie začaly používat na denní bázi díky rychlému vývoji chytrých mobilních telefonů. Ty dnes neslouží pouze ke komunikaci, ale k uchovávání citlivých údajů či přístupu do bankovnictví, a proto do nich výrobci implementovali čtečky otisků prstů, které uživateli zajišťují pohodlný a bezpečný způsob odemykání.[15] Biometrie se dále běžně využívá k zabezpečení domácností pomocí chytrých zámků, což eliminuje riziko ztráty klíčů a umožňuje snadnou vzdálenou správu přístupů.[16] Své místo nachází daktyloskopie i v automobilovém průmyslu. Automobilka Hyundai například integruje čtečky přímo do klik a startovacích tlačítek, díky čemuž se vůz po přiložení prstu nejen odemkne a nastartuje, ale také automaticky přizpůsobí nastavení sedadel a zrcátek konkrétnímu řidiči.[17]

---

[13] DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. [Brno: M. Drahanský], 2011. s. 100-101. ISBN 978-80-254-8979-6.

[14] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. Ostrava: VŠB-TU Ostrava, 2008. s. 35. [cit. 2026-1-6]. Dostupné z WWW: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/biometricke_metody.pdf.

[15] DATAHELP. Čtečky otisků prstů u mobilů a jejich bezpečnost. In: *Datahelp* [online]. [cit. 2026-01-6]. Dostupné z WWW: https://www.datahelp.cz/clanky/ctecky-otisku-prstu-u-mobilu-a-jejich-bezpecnost/.

[16] INTERNORM. Zámek na otisk prstu – proč ho chtít? In: *Internorm* [online]. 28. 10. 2020 [cit. 2026-01-6]. Dostupné z WWW: https://blog.internorm.cz/zamek-na-otisk-prstu-proc-ho-chtit/.

[17] HYUNDAI. Hyundai Reveals World's First Smart Fingerprint Technology to Vehicle. In: *Hyundai Newsroom* [online]. 24. 12. 2018 [cit. 2026-01-6]. Dostupné z WWW: https://www.hyundai.news/uk/articles/press-releases/hyundai-reveals-worlds-first-smart-fingerprint-technology-to-vehicles.html.

3.2 Biometrie oční duhovky

Biometrické systémy využívající k identifikaci člověka oční duhovku jsou v současnosti již zaběhlou metodou, jelikož se používají od 90. let 20. století. Duhovka je sval v oku, který slouží ke změně velikosti čočky na základě množství světla dopadajícího na oko. Jde o barevnou část oka, jejíž zbarvení a struktura je sice dána genetikou, její vzorování je však věcí čistě náhodnou, a tedy unikátní pro každého člověka. Dokonce ani jeden člověk nemá naprosto identické oční duhovky.[18]

Podíváme-li se na lidské oko zblízka, lze zahlédnout několik jasných specifických znaků jako např. záhyby, skvrny, rýhy nebo krypty (tmavá místa, kde je duhovka poměrně tenká).

Tyto znaky jsou pak digitalizovány, je vytvořena šablona a ta je registrovaná do databáze. Následně je při identifikaci (nebo verifikaci) kamerou nacházející se ve snímači pořízen snímek, který je černobílý z důvodu vyššího rozlišení. Tento snímek je pak zpracován softwarem, jenž v něm vyhledá duhovku a údaje z ní porovná s těmi, které jsou v databázi.

Tato metoda se považuje za jeden z nejbezpečnějších a nejpřesnějších způsobů biometrické identifikace. Je používaná v místech, kde je kladen vysoký důraz na bezpečnost, např. některé věznice nebo letiště. Nevýhodou jsou však vyšší náklady na pořízení.[19]

3.3 Biometrie oční sítnice

Další část oka, kterou lze využít pro biometrickou identifikaci člověka, je oční sítnice. To je zadní část oka, jejíž funkcí je detekování světla, které na ni dopadá.[20] Sítnice je zásobena krví pomocí tzv. choroidu. Jde o vrstvu nacházející se mezi bělmem a sítnicí, obsahující cévy, které ji vyživují.[21] Běžně se ve spojení s touto metodou využívají pojmy jako „sken sítnice“ nebo „snímek sítnice“. To je ale relativně nepřesné pojmenování, jelikož se nevyužívá k identifikaci sítnice jako taková, ale snímek odrazu struktury cév v choroidu.

[18] Tamtéž s. 23.
[19] BITTO, Ondřej. *Šifrování a biometrika aneb tajemné bity a dotyky*. 1. vyd. Kralice na Hané: Computer Media, 2005. s. 136-137. ISBN 80-86686-48-5.
[20] DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. [Brno: M. Drahanský], 2011. s. 188. ISBN 978-80-254-8979-6.
[21] Tamtéž s. 190.

Pro vytvoření tohoto snímku je třeba použít speciální kamery. Při vytváření snímku je třeba nejdříve sítnici osvětlit. K tomu se využívá primárně infračervené světlo, jelikož jeho vlnová délka dělá sítnici prakticky průhlednou a díky tomu je síť cév v choroidu jasně viditelná. Vytvořený snímek je pak následně porovnán s registrovanými snímky v databázi a osoba je identifikovaná / verifikovaná.[22]

Tato metoda má mnoho nevýhod. První z nich je skutečnost, že se nejedná o příliš příjemný způsob ověření totožnosti. Osoba musí přiložit oko k malému snímači a nehnutě vydržet několik sekund, přičemž přímo do oka svítí zdroj světla. Navíc osoby, které nosí brýle, je musí před použitím sundat. Další nevýhodou je nemožnost použít snímač venku, jelikož okolní světlo ovlivňuje získaný snímek. Poslední nevýhodou je pak cena, která je zpravidla výrazně vyšší než u jiných biometrických metod.

Výhody této metody primárně spočívají v její vysoké bezpečnosti a přesnosti. Mnoho biometrických metod lze různými způsoby obelstít, ale obelstít tuto metodu by vyžadovalo vytvořit umělé oko, které by muselo napodobovat mnoho vlastností skutečného oka, což je považováno za velmi složitý úkol. Proto je identifikace pomocí oční sítnice používaná hlavně na místech s nejvyšším stupněm zabezpečení. Příkladem může být výzkum a ochrana jaderných zbraní. Pro zajímavost - tuto metodu vyžívají i organizace jako NASA, FBI nebo CIA.[23]

3.4 Analýza geometrie ruky

Ruka, respektive její tvar, je další část těla, která je pro každého jedince naprosto jedinečná. Každý z nás má prsty rukou jinak dlouhé, široké, tlusté a celkově mají různý tvar. Navíc se u člověka od dospělosti, pokud nedojde k nějakému úrazu nebo nemoci, rozměry ruky nemění. Díky těmto skutečnostem lze tvar (geometrii) ruky použít jako další biometrickou metodu.

I u této metody je využit speciální skener. Ruka se přikládá na předem stanovenou plochu (základovou desku), na které jsou distanční kolíčky zajišťující, že ruka bude pokaždé ve stejné poloze. Skenování jako takové provádí digitální černobílá kamera. Ta u starších provedení skenerů směřovala přímo na ruku a byla umístěna zhruba 28 cm od základové desky. Moderní skenery ale používají soustavu zrcadel, díky kterým je

[22] RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. Profesionál. s. 515-516. ISBN 978-80-247-2365-5.
[23] Tamtéž s. 520–521.

velikost skeneru zhruba o polovinu menší a navíc umožňují snímání dlaně z boku. Aby sken ruky byl kvalitní, využívají se LED diody pro nasvícení.

Při samotném procesu identifikace/verifikace skener porovnává přiloženou ruku s databází. V ní se nachází referenční šablony, které se vytváří při prvním snímání a každá šablona je vytvořena aritmetickým průměrem trojího snímání. U některých modelů skenerů může databáze obsahovat přes 30 000 šablon. Aby nebylo nutné pokaždé porovnávat takové množství šablon, je u každé z nich přidružen navíc druhý údaj, který se zadává před samotným skenem ruky. Zpravidla se jedná o číselný kód, tzv. PIN nebo lze využít jiný údaj uložený na fyzickém nosiči, např. identifikační karta nebo čárový kód. Tento údaj poté slouží pro rychlé nalezení referenční šablony v databázi. Následně je porovnána vzdálenost několika stanovených bodů, jejichž místo a počet se mění v závislosti na modelu skeneru.[24]

Výhodou této metody je bezesporu její jednoduchost, rychlost a hlavně uživatelská přívětivost. Nevýhody však převažují, hlavně jde o přesnost, která není příliš vysoká, a s tím je spojená i úroveň bezpečnosti, kterou může tato metoda poskytnout. Kvůli tomu se sken geometrie ruky používá primárně pro verifikaci osoby.[25]

Nejčastěji se lze setkat se skenem ruky v různých režimových pracovištích, výrobních závodech nebo skladech, kde slouží jako prvek systému kontroly vstupu nebo jako způsob kontroly docházky apod.[26]

3.5 Hlasová biometrie

Lidský hlas představuje další možnost, kterou lze využít pro identifikaci osob. Tato metoda, která se obecně nazývá „hlasová biometrie“, je založena na skutečnosti, že každá osoba má jedinečný tzv. „otisk hlasu“. To je způsobeno odlišným tvarem hlasivek, zubů nebo jazyka a následnou rezonancí vokálního traktu, která je pro každého jedince naprosto odlišná.[27] Rozpoznání řeči lze rozdělit z různých pohledů, primárně jde o rozpoznání řeči a rozpoznání mluvčího.

[24] Tamtéž s. 267–269.
[25] Tamtéž s. 276–278.
[26] Tamtéž s. 272.
[27] VANČO, Emil. Biometrie, biometrika - geneze, vývoj a současné pojetí. *Kriminalistika* [online]. 2005, roč. 38, č. 1. [cit. 2026-1-8]. Dostupné z WWW: http://www.mvcr.cz/soubor/kriminalistika-archiv-2005-01-zip.aspx.

Rozpoznáním řeči rozumíme snahu extrahovat z řeči její význam nebo obsah. Jde o vytvoření systému, který bude schopný řeč analyzovat a pochopit její obsah.[28] V praxi to znamená, že je řeč převedena na text, se kterým může systém dále pracovat. Tento princip je hojně implementován do mobilních telefonů (ale i do jiných zařízení), kdy je díky tomu možné např. vytvářet automatické přepisy hovorů nebo schůzek, anebo využívat osobní asistenty na bázi umělé inteligence jako Google Assistant nebo Siri.[29] Ve výsledku je tedy možné určit, co bylo řečeno, ale ne která osoba mluvila. Nelze tak tyto systémy využít pro identifikaci nebo verifikaci.

Tím se dostáváme k rozpoznání mluvčího. Princip je obdobný jako u ostatních způsobů identifikace nebo verifikace osoby, tedy spočívá v porovnání vstupního vzorku s dříve vytvořeným registračním vzorkem. Při registraci vytvoří osoba svůj vzorek hlasu, který je uložen do databáze. Míra bezpečnosti se odvíjí od délky věty, která je použita pro vzorek. Při následné identifikaci musí osoba vyslovit danou větu, kterou použila při registraci. Systém pak následně vyhodnotí míru shody. Některé systémy vyžadují při registraci více různých vět a při identifikaci náhodně vyberou některou z nich.

Výhodou této metody, respektive metody rozeznání mluvčího, je především její nenáročnost na hardware. Vstupním zařízením je zpravidla mikrofon, případně na větší vzdálenost lze využít telefon. Nevýhodou je, že tyto systémy příliš nepočítají s náhlou změnou v hlase uživatele, která může být způsobena například nemocí.[30]

Hlasová biometrie v současnosti nachází široké komerční uplatnění. Běžnou součástí každodenního života se stali hlasoví asistenti (např. Siri či Alexa), kteří díky analýze jedinečných charakteristik hlasu a umělé inteligenci umožňují bezdotykové ovládání chytrých domácností, rychlé vyhledávání informací nebo bezpečnější obsluhu zařízení během řízení automobilu.[31] Významný potenciál představuje rozpoznávání mluvčího také v bankovním sektoru. Například Česká spořitelna zavedla možnost telefonického ověření identity klienta na základě analýzy více než stovky fyzických a behaviorálních rysů hlasu, což umožňuje bezpečně provádět bankovní operace z domova bez nutnosti navštěvovat pobočku.[32]

---

[28] DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. [Brno: M. Drahanský], 2011. s. 203-204. ISBN 978-80-254-8979-6.

[29] MOBBEEL. What is voice biometrics? In: *Mobbeel* [online]. [cit. 2026-01-8]. Dostupné z WWW: https://www.mobbeel.com/en/what-is-voice-biometrics/.

[30] BITTO, Ondřej. *Šifrování a biometrika aneb tajemné bity a dotyky*. 1. vyd. Kralice na Hané: Computer Media, 2005. s. 140. ISBN 80-86686-48-5.

[31] JIŘÍK, Pavel. The Future of Voice Assistants. In: *Phonexia* [online]. 25. 4. 2022 [cit. cit. 2026-1-8]. Dostupné z WWW: https://www.phonexia.com/blog/the-future-of-voice-assistants/.

[32] ČESKÁ SPOŘITELNA. Spořitelna umožní zřízení hlasové biometrie jen po telefonu a bez nutnosti návštěvy pobočky. In: *Česká spořitelna* [online]. 6. 4. 2020 [cit. 2026-01-8]. Dostupné z

3.6 Biometrie obličeje

Nejběžnějším a nejstarším způsobem, jakým se lidé mezi sebou rozeznávají, je pomocí svých tváří. Lidský mozek si umí zapamatovat velké množství tváří a zcela automaticky porovnat tváře uložené v paměti s těmi, které vidí před sebou a na základě toho má schopnost osoby identifikovat. Celý tento proces mu navíc zabere pouze zlomek vteřiny. Od druhé poloviny 20. století je snaha přenést tuto jedinečnou lidskou vlastnost do oblasti forenzních a komerčních aplikací a využít ji jako další metodu biometrické identifikace osob.[33] V současné době se to daří díky rychlému vývoji umělé inteligence a počítačového vidění, kdy tyto technologie umožňují systémům rozpoznávání obličeje být mnohem efektivnější a přesnější.

Základní princip je shodný s ostatními biometrickými metodami. Jde tedy o porovnání uloženého vzorku, v tomto případě jsou to data obličeje, respektive obličejové rysy jako poměr výšky k šířce tváře, barva obličeje, rozměry a poloha očí, nosu, úst apod., nebo charakteristické rysy obličeje, s aktuálně posuzovaným vzorkem dané osoby.

Systémy na rozpoznání obličeje mohou pracovat různými způsoby. Princip je však obecně pro všechny stejný. Systém nejdříve musí obličej detekovat, zpravidla z obrazu kamery nebo fotoaparátu. Moderní systémy jsou schopné rozeznat lidskou tvář např. od tváře na soše nebo plakátu. Následně systém ze snímku analyzuje jedinečné obličejové rysy. Klíčové rysy tváře, nazývané uzlové body, pomáhají vytvořit mapu obličeje. Každý člověk má asi 80 těchto bodů, což umožňuje přesnou identifikaci pomocí databáze. Po zachycení obrazu se obličej převede na digitální data podle jeho rysů. Tato data, známá jako otisk obličeje, se porovnávají s databázemi, které jsou na systém napojeny.

Tento druh identifikace osob je již dnes běžně využívanou metodou. Do povědomí lidí ji pravděpodobně nejvíce rozšířila společnost Apple pomocí funkce Face ID, která slouží k rychlému odemykání telefonů nebo přihlašovaní se do aplikací.[34] Jde o velmi moderní a rychle se rozšiřující metodu, která kromě spotřební elektroniky nachází

WWW:https://www.csas.cz/cs/o-nas/pro-media/tiskove-zpravy/2020/04/06/ceska-sporitelna-pomuze-klientum-v-karantene-a-umozni-jim-zrizeni-hlasove-biometrie-jen-po-telefonu.

[33] RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. Profesionál. s. 287. ISBN 978-80-247-2365-5.

[34] SHAIP. Jak sběr dat hraje klíčovou roli při vývoji modelů rozpoznávání obličeje. In: *Shaip* [online]. 17. 12. 2024 [cit. 2026-1-12]. Dostupné z WWW: https://cs.shaip.com/blog/data-collection-for-facial-recognition-models/.

uplatnění na letištích, nádražích a obecně místech, kde by se mohly pohybovat osoby, které jsou např. hledané nebo pohřešované.[35]

3.7 Dynamická analýza podpisu

Podpis, respektive jeho dynamika, se oproti ostatním již popsaným metodám řadí do skupiny behaviorálních biometrických údajů. Písmo a podpis již stovky let slouží jako forma identifikace člověka. Lze ho považovat jak za statický, tak dynamický údaj. Záleží pouze na tom, zda ho využijeme pouze jako výsledek psaní, nebo jestli zaznamenáme i průběh jeho vzniku.[36] V současnosti je totiž možné pomocí speciálních per a tabletů z ručního podpisu elektronicky zjistit tah, tvar nebo tlak při psaní a tím stanovit i základní dynamické hodnoty podpisu jako rychlost, akcelerace nebo tlak při podepisování, kdy tyto hodnoty jsou pro každého člověka unikátní.[37]

Systémy pro verifikaci osob na základě podpisu lze podle způsobu fungování rozdělit na dva typy – off-line a on-line systémy.

Off-line systémy pracují s podpisem pouze jako s výsledkem psaní. Porovnávají tedy jeho tvar a vzhled. Osoba se podepíše na běžný papír a její podpis je následně digitalizován skenerem nebo kamerou. Systém následně porovná digitalizovaný podpis se vzory v databázi.

Naproti tomu on-line systémy navíc přidávají k podpisu jeho dynamické vlastnosti. Osoba se zde podepisuje pomocí speciálního pera a tabletu, kdy jsou v reálném čase zaznamenávány veškeré údaje právě psaného podpisu. Tyto údaje jsou poté porovnány s databází.

Oba typy systémů mají však shodné dvě základní etapy verifikace.

V první etapě se systém musí naučit charakteristiku podpisu dané osoby prostřednictvím jednoho, většinou ale několika vzorových podpisů. Následně je vytvořenému referenčnímu vzorku přiřazeno identifikační číslo, které pak slouží k jeho rychlému nalezení. Tuto etapu lze pojmenovat jako etapu učení nebo registrace.

---

[35] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. Ostrava: VŠB-TU Ostrava, 2008. s. 23. [cit. 2026-1-12]. Dostupné z WWW: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/biometricke_metody.pdf.

[36] DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. [Brno: M. Drahanský], 2011. s. 233. ISBN 978-80-254-8979-6.

[37] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. Ostrava: VŠB-TU Ostrava, 2008. s. 32. [cit. 2026-1-12]. Dostupné z WWW: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/biometricke_metody.pdf.

V druhé etapě, tedy etapě verifikace, osoba nejdříve předloží identifikační číslo vzorku a začne se podepisovat. Systém mezitím najde referenční vzorek a ten porovná s údaji získanými z aktuálně vytvořeného podpisu. Systém následně vyhodnotí, zda je osoba verifikovaná, nebo ne.[38]

Výhoda této metody spočívá především v tom, že se jedná o využití konvenčního způsobu identifikace osob, pouze je zde zvýšena úroveň zabezpečení pomocí moderních technologií. Další výhodou může být jednoduchost integrace do již používaných systémů. Nevýhodou těchto systémů naopak je, že je lze použít pouze na verifikaci osob a dále, že mohou být méně efektivní u osob, u nichž se při každém podpisu dynamika psaní značně liší.[39]

3.8 Analýza DNA

Identifikace pomocí kyseliny deoxyribonukleové neboli DNA je v oblasti biometrické identifikace osob naprosto odlišnou metodou. Oproti ostatním metodám totiž nevyužívá morfologické nebo fyziologické údaje člověka, ale zaměřuje se na genetickou informaci člověka, respektive její nosič, tedy na DNA. Jde rovněž o metodu relativně mladou, její historie začíná v 80. letech 20. století. [40]

Identifikace pomocí DNA je založena na zjištění, že určité části DNA jsou pro úplně jakoukoliv osobu naprosto rozdílné a unikátní. Jedinou výjimkou jsou jednovaječná dvojčata. Analýza DNA nachází stále širší uplatnění díky své vysoké přesnosti, i když proces získávání otisků DNA je poměrně komplikovaný a zdlouhavý. Typicky zahrnuje pět hlavních kroků. Na počátku se z tkáně izoluje spirála DNA, která se následně rozštěpí pomocí enzymu EcoRI na menší části. Tyto části jsou dále tříděny podle velikosti, aby bylo možné získat specifické fragmenty vhodné pro analýzu. Fragmenty DNA jsou poté přeneseny na speciální nylonovou membránu. Přidáním genových sond, které mohou být radioaktivně nebo barevně označeny, vzniká rentgenový obraz, jenž připomíná čárový

[38] RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. Profesionál. s. 439. ISBN 978-80-247-2365-5.
[39] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. Ostrava: VŠB-TU Ostrava, 2008. s. 32. [cit. 2026-1-12]. Dostupné z WWW: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/biometricke_metody.pdf
[40] RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. Profesionál. s. 535. ISBN 978-80-247-2365-5.

kód. Dále se převádí do digitální formy, což umožňuje jeho snadnější uchování a další zpracování.[41]

Výhod je u této metody hned několik. DNA je považovaná za tzv. „definitivní identifikátor“, jelikož je naprosto jedinečná pro každou osobu na světě a v průběhu života se nijak nemění. Analýzu DNA lze navíc provést skoro z jakékoliv lidské tkáně, tedy i z té, která je na DNA chudší, např. nehty, vlasy nebo šupinky kůže. DNA se totiž nachází v každé lidské buňce a lze z ní vyčíst mnoho informací o daném člověku. Poslední výhodou je stálost DNA, která vydrží velmi dlouho, pokud je ovšem správně uložena.

Přestože má identifikace pomocí DNA mnoho výhod a vysoký potenciál stát se nejefektivnější biometrickou metodou, kvůli zdlouhavému, složitému a finančně náročnému procesu ji nelze masově v praxi využít. Od vzniku této metody sice došlo k zásadnímu zrychlení z několika hodin na několik desítek minut, přesto je stále nevhodná pro komerční biometrické systémy.

V praxi je DNA využívaná převážně v oblasti forenzní medicíny a v kriminalistice. Je známo mnoho případů, kdy bylo možné pomocí DNA stanovit, kdo je skutečným pachatelem trestného činu, kdo je naopak nevinný.[42]

3.9 Některé další biometrické metody

Kromě již popsaných biometrických metod existuje ještě mnoho dalších, které nejsou běžně tolik využívané. Zpravidla jsou tyto metody známé úzkému kruhu zasvěcených osob a v běžné praxi se nepoužívají. Některé z nich jsou krátce popsány v této podkapitole.

Identifikace osob podle krevního řečiště ruky je moderní biometrická metoda s vysokou bezpečností a obtížností falšování. Využívá infračervené světlo, které snímá strukturu žil na hřbetu ruky. Jelikož cévy jsou uvnitř těla a krev musí obíhat, zaručuje metoda autentičnost a živost ruky. Cévní vzor je jedinečný, neměnný v dospělosti a odlišný i u jednovaječných dvojčat. Bezkontaktní princip zvyšuje hygienu a uživatelský komfort. Systém umožňuje jak identifikaci, tak verifikaci např. s identifikační kartou.

[41] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. Ostrava: VŠB-TU Ostrava, 2008. s. 44. [cit. 2026-1-12]. Dostupné z WWW: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/biometricke_metody.pdf.

[42] DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. [Brno: M. Drahanský], 2011. s. 267-268. ISBN 978-80-254-8979-6.

LED světlo prosvítí ruku, speciální kamera zachytí obraz a software analyzuje klíčové vlastnosti cév, jako jsou větvení nebo tloušťka.[43]

Další částí těla, kterou lze použít jako biometrický údaj, je ucho. Tvar ucha je jedinečný a neměnný po většinu života, což ho umožňuje využít jak pro identifikaci, tak i pro verifikaci osob. Růst ucha probíhá hlavně během prvních čtyř měsíců života, poté se mění jen jeho velikost, zatímco struktura zůstává stejná. Díky možnosti dálkového snímání je metoda neinvazivní a uživatelsky dobře přijatelná.[44]

Behaviorálním biometrickým údajem může být například i lidská chůze. Ta je ovlivněna anatomickými a psychofyziologickými faktory, které jsou pro každého člověka odlišné. Můžeme sem zařadit výšku, hmotnost, zdravotní stav nebo různé anatomické odchylky jako např. zakřivení páteře, ploché nohy či různou délku končetin. Rozpoznávání osoby podle jejího stylu chůze vyniká možností identifikace na velkou vzdálenost, kde jiné biometrické metody selhávají, například kvůli nízkému rozlišení obrazu. Chůze se analyzuje z obrazových sekvencí pomocí moderních technologií počítačového vidění, které jsou již srovnatelné s jinými biometrickými metodami.[45]

V neposlední řadě je biometrickým údajem také lidský pach. Pachové stopy již desítky let používá policie jako nepřímý důkaz, v civilní sféře však využití pachu stále zůstává okrajovou metodou. Lidský pach, který je složený z přibližně třiceti chemických sloučenin, vytváří jedinečný profil každého jednotlivce. V kriminalistice se místo senzorů používají speciálně vycvičení psi, ale v civilní praxi je potřeba porovnávat více vzorků současně, což zatím senzory nedokážou. Dalším problémem nasazení této metody do běžné praxe jsou změny v pachu způsobené emocionálními či hormonálními výkyvy člověka. Výzkum v této oblasti pokračuje, ale reálné nasazení je otázkou budoucnosti.[46]

[43] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. Ostrava: VŠB-TU Ostrava, 2008. s. 26. [cit. 2026-1-13]. Dostupné z WWW: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/biometricke_metody.pdf.

[44] DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. [Brno: M. Drahanský], 2011. s. 252. ISBN 978-80-254-8979-6.

[45] PORADA, Viktor, Dušan ŠIMŠÍK et al. *Identifikace osob podle dynamického stereotypu chůze*. Karlovy Vary: Vysoká škola Karlovy Vary, 2010. s. 307. ISBN 978-80-87236-01-7.

[46] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. Ostrava: VŠB-TU Ostrava, 2008. s. 44. [cit. 2026-1-13]. Dostupné z WWW: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/biometricke_metody.pdf.

4 Právní regulace biometrické identifikace osob

Tato kapitola se zaměřuje na legislativní rámec zpracování biometrických údajů na úrovni Evropské unie i České republiky. Autor analyzuje klíčové právní normy, zejména obecné nařízení GDPR a nový Akt o umělé inteligenci (AI Act), které stanovují hranice pro využívání těchto technologií. Text dále vymezuje specifické pravomoci bezpečnostních sborů a popisuje právní podmínky, za nichž mohou státní instituce zasahovat do soukromí osob v zájmu zajištění veřejné bezpečnosti.

4.1 Ochrana biometrických údajů na úrovni EU

Hlavním právním rámcem pro ochranu biometrických údajů v EU je tzv. obecné nařízení o ochraně osobních údajů, které je spíše známé pod zkratkou GDPR (z anglického General Data Protection Regulation). Jde o nařízení, které se zabývá ochranou a hájením práv občanů proti neoprávněnému nakládání s jejich osobními údaji a daty, které plošně platí na celém území Evropské unie.[47] V české legislativě je toto nařízení promítnuto v zákoně č. 110/2019 Sb., o zpracování osobních údajů, který byl vytvořen v souladu s nařízením GDPR.[48]

Obecné nařízení, konkrétně článek 9, řadí biometrické údaje do kategorie tzv. zvláštních osobních údajů. Lze je také nazvat jako „citlivé“ osobní údaje. Od „běžných“ osobních údajů je rozdíl v tom, že jde o takové údaje, které by mohly osobu např. v zaměstnání, ve škole nebo obecně ve společnosti poškodit a mohlo by dojít k její diskriminaci. Jde například o údaje, podle kterých lze zjistit rasový či etnický původ, politické názory, zdravotní stav apod. Spadají sem však genetické a biometrické údaje, které mohou být použity s cílem jedinečné identifikace osoby. Proto jsou tyto údaje ve zvláštní skupině, jelikož je na jejich ochranu kladen vyšší důraz než na ochranu „běžných“ osobních údajů.[49]

Je důležité zdůraznit, že samotný zákaz zpracování biometrických údajů (uvedený v prvním odstavci článku 9 GDPR) je koncipován jako základní pravidlo. Veškeré možnosti, které zpracování těchto citlivých údajů umožňují, jsou pouze

[47] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada, 2017. Právo pro praxi. s. 27. ISBN 978-80-271-0668-4.
[48] CHLEBUS, Tomáš a Jakub DOSTÁL. *Nový zákon o zpracování osobních údajů*. In: *Epravo.cz* [online]. 30. 5. 2019 [cit. 2026-02-10]. Dostupné z WWW: https://www.epravo.cz/top/clanky/novy-zakon-o-zpracovani-osobnich-udaju-109312.html.
[49] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada, 2017. Právo pro praxi. s. 35. ISBN 978-80-271-0668-4.

výjimkami. Odborná literatura k tomu dodává, že tyto výjimky musí být vykládány velmi restriktivně. V praxi to znamená, že pokud existují jakékoliv pochybnosti o tom, zda je využití biometrie pro daný účel skutečně nutné, neměl by správce k tomuto kroku přistoupit.

Klíčovým pojmem pro legalitu takového zpracování je slovo „nezbytné“. Podle komentáře k nařízení není faktický rozdíl mezi výrazy „nutné“ a „nezbytné“ – oba vyjadřují striktní požadavek, aby byl zásah do soukromí subjektu omezen na minimum potřebné k dosažení stanoveného cíle. Biometrické systémy by proto neměly být nasazovány plošně, pokud to není pro daný účel vyloženě nepostradatelné.[50]

V kontextu zajišťování veřejné bezpečnosti a ochrany státu se uplatňuje specifická výjimka podle písmene g), tedy zpracování z důvodu významného veřejného zájmu. Tento právní titul je určen primárně pro orgány veřejné moci, instituce plnící úkoly ve veřejném zájmu nebo pro zajištění bezpečnosti státu (což v praxi dopadá například na provozovatele kritické infrastruktury, jako jsou mezinárodní letiště). Naopak v běžném komerčním sektoru by se tento důvod obhajoval jen velmi obtížně a soukromé subjekty musí zpravidla spoléhat na jiný právní titul, nejčastěji na výslovný souhlas subjektu podle odstavce 2, písmene a) článku 9 GDPR.[51]

Je však nutné doplnit, že ani existence významného veřejného zájmu neopravňuje k neomezenému sběru dat. Evropská právní praxe v této souvislosti akcentuje princip proporcionality. I v případech, kdy vnitrostátní právo umožňuje zpracování biometrických údajů pro účely veřejného zájmu, musí být takové opatření vždy striktně přiměřené sledovanému cíli. Zásah do soukromí tedy nesmí překročit míru nezbytnou pro dosažení daného účelu a musí respektovat podstatu práva na ochranu osobních údajů, aby nedocházelo k nadměrné invazi do práv subjektů.[52]

4.1.1 Specifický režim pro bezpečnostní sbory a trestní řízení

Působnost obecného nařízení GDPR není absolutní. Dle článku 2 odst. 2 písm. d) se toto nařízení nevztahuje na zpracování osobních údajů prováděné příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů. Na tyto specifické

[50] PATTYNOVÁ, Jana. *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě : komentář*. Praha: Leges, 2018. s. 124. ISBN 978-80-7502-288-2.
[51] Tamtéž, s.128
[52] USTARAN, Eduardo. *European Data Protection Law and Practice*. Portsmouth: International Association of Privacy Professionals, 2018. s. 131. ISBN 978-0-9983223-5-3

bezpečnostní činnosti dopadají odlišná pravidla stanovená v samostatné Směrnici (EU) 2016/680.

Zatímco GDPR je přímo účinným předpisem, zmíněná směrnice byla do českého právního řádu implementována zákonem č. 110/2019 Sb., o zpracování osobních údajů. Specifická úprava pro bezpečnostní sbory je obsažena v Hlavě III tohoto zákona. Právě tato část legislativy vymezuje pravomoci Policie ČR, Generální inspekce bezpečnostních sborů a dalších orgánů činných v trestním řízení.

Rozhodujícím faktorem pro aplikaci správného právního režimu je tedy účel zpracování. Pokud bezpečnostní složky využívají biometrické systémy k odhalování trestné činnosti, postupují podle speciální úpravy v zákoně č. 110/2019 Sb., která umožňuje efektivnější zásahy do soukromí. V případech, kdy by policie zpracovávala data pro jiné (například administrativní či personální) účely, podléhala by standardnímu režimu GDPR.[53]

Tato legislativní konstrukce, kdy je policejní agenda vyňata z GDPR, má své opodstatnění. Podle zahraniční odborné literatury je cílem této úpravy zaplnit legislativní mezeru tak, aby byla zajištěna konzistentní ochrana osobních údajů i v oblasti trestního práva. Existence samostatné směrnice a na ni navazujících národních zákonů je klíčová pro mezinárodní policejní spolupráci. Umožňuje totiž efektivní výměnu informací a biometrických údajů mezi bezpečnostními sbory členských států, aniž by byla snížena úroveň ochrany práv dotčených osob.[54]

4.2 AI Act

Současný právní rámec, reprezentovaný především obecným nařízením o ochraně osobních údajů (GDPR) a navazující policejní směrnicí, tvoří nezbytný základ pro nakládání s biometrickými daty a ochranu soukromí. Rychlé tempo technologických inovací si ovšem vyžádalo novou úroveň regulace. Ačkoliv prvotní motivací evropských institucí bylo přijmout normu zaměřenou čistě na preventivní (*ex ante*) řízení rizik spjatých s umělou inteligencí, finální podoba Aktu o umělé inteligenci (AI Act) odráží spíše složité politické debaty, které se ve velké míře vrátily zpět k otázkám ochrany osobních dat.

[53] VÍTEK, Dominik. Kapitola I Obecná ustanovení. In: PATTYNOVÁ, Jana. Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě : komentář. Praha: Leges, 2018. s. 38. ISBN 978-80-7502-288-2.

[54] USTARAN, Eduardo. *European Data Protection Law and Practice*. Portsmouth: International Association of Privacy Professionals, 2018. s. 98. ISBN 978-0-9983223-5-3

V důsledku tohoto legislativního vývoje nová evropská úprava v mnoha ohledech překrývá, rozšiřuje, nebo dokonce pozměňuje zavedené principy GDPR. Jedním z nejkontroverznějších bodů celého schvalovacího procesu se stala právě problematika plošného zákazu biometrické identifikace v reálném čase využívané bezpečnostními sbory, jež podléhala silné politizaci. Přijatý text nařízení tak představuje obtížně dosažený kompromis. Nalezení přesné hranice a vyřešení případných kolizí mezi stávajícími pravidly ochrany osobních údajů a novou regulací umělé inteligence tak pravděpodobně zůstane úkolem pro budoucí judikaturu Soudního dvora EU.[55] Co se týče časového rámce, samotné nařízení vstoupilo v platnost v srpnu 2024, přičemž klíčová pasáž zakazující systémy s nepřijatelným rizikem – zahrnující i zmíněnou real-time biometrii – nabyla účinnosti 2. února 2025.[56]

Základním architektonickým prvkem Aktu o umělé inteligenci je uplatnění takzvaného přístupu založeného na riziku (risk-based approach). Namísto plošné regulace veškerých technologií zavádí nařízení princip proporcionality, kdy jsou normativní požadavky a povinnosti cíleně dimenzovány čistě podle reálné hrozby, kterou konkrétní aplikace představuje. V rámci této koncepce jsou systémy umělé inteligence systematicky rozřazovány do čtyř odstupňovaných kategorií: s nepřijatelným, vysokým, omezeným a minimálním rizikem.

Zatímco systémy představující minimální riziko nepodléhají žádným novým pravidlům, aplikace spadající do kategorie nepřijatelného rizika jsou zcela zakázány, neboť jsou v přímém rozporu se základními evropskými hodnotami. U vysoce rizikových systémů, kam spadají nástroje s potenciálním negativním dopadem na zdraví, bezpečnost či fundamentální práva jednotlivců, je vyžadován specifický dohled a splnění striktních podmínek. U systémů s omezeným rizikem, mezi které legislativa řadí i nástroje pro biometrickou kategorizaci či rozpoznávání emocí, je pak stěžejním požadavkem transparentnost. V praxi to znamená, že fyzické osoby musí být o vystavení těmto technologiím prokazatelně informovány.[57]

Kategorie systémů s nepřijatelným rizikem zahrnuje aplikace, které jsou v přímém rozporu s evropskými hodnotami a jsou tudíž na trhu Evropské unie zcela zapovězeny.

[55] POLČÁK, Radim et al. *Právo informačních technologií*. 2. vyd. Praha: Wolters Kluwer, 2024. Právní monografie. s. 777-778. ISBN 978-80-286-0059-4.
[56] EVROPSKÝ PARLAMENT. EU AI Act: first regulation on artificial intelligence. In: *European Parliament* [online]. 8. 6. 2023, poslední aktualizace 19. 2. 2025 [cit. 2026-02-12]. Dostupné z WWW: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.
[57] BULLOCK, Justin B. et al. The Oxford Handbook of AI Governance. New York: Oxford University Press, 2024. s. 265-267. ISBN 978-0-19-757932-9.

V oblasti zpracování biometrických údajů se tento absolutní zákaz vztahuje na několik specifických praktik, jako je plošné a necílené stahování podoby obličejů z internetového prostředí pro vytváření rozsáhlých databází. Nepřípustné jsou rovněž systémy biometrické kategorizace třídící jednotlivce na základě citlivých osobních charakteristik či nasazování technologií pro rozpoznávání emocí v pracovním prostředí a ve vzdělávacích institucích. Zásadním omezením z pohledu bezpečnostních složek je pak plošný zákaz využívání systémů pro biometrickou identifikaci ve veřejných prostorech ze strany policie, přičemž použití je přípustné pouze ve výjimečných situacích. Tyto principy jsou s konečnou platností a explicitně ukotveny v platném znění Nařízení (EU) 2024/1689.[58] Výjimky z tohoto plošného zákazu biometrie v reálném čase pro účely vymáhání práva jsou v aktuální legislativě striktně omezeny pouze na specifické situace, jakými jsou například pátrání po pohřešovaných osobách nebo prevence bezprostředních hrozeb a závažných trestných činů.[59]

Druhou stěžejní skupinu tvoří vysoce riziková umělá inteligence, u níž hrozí závažné dopady na základní lidská práva, což ve svých analýzách zdůrazňuje i Agentura Evropské unie pro základní lidská práva. Nasazení těchto technologií může ohrozit zejména právo na ochranu osobních údajů, právo na účinnou právní ochranu a v neposlední řadě právo nebýt diskriminován. Z toho důvodu je hlavním cílem regulace zajistit, aby tyto nástroje fungovaly transparentně a bezpečně. Z hlediska biometrie spadají do této přísně střežené kategorie samotné systémy biometrické identifikace, pokud nejsou nasazeny v již zmíněných zakázaných kontextech. Pro aplikovanou bezpečnostní praxi je klíčové, že mezi vysoce rizikové oblasti spadá vymáhání práva a prioritně také pohraniční kontrola, řízení migrace a azylová politika.[60] Oficiální text aktuálního nařízení tuto klasifikaci potvrzuje a systémy umělé inteligence využívané pro řízení migrace, azylu a ochrany hranic striktně definuje jako vysoce rizikové, na které se vztahují nejpřísnější pravidla a povinnosti. Právě do této přísně regulované sféry spadá i využívání biometrických identifikačních systémů v prostorech mezinárodních letišť, kde

[58] ŠTĚDROŇ, Bohumír, Roman JAŠEK, Miroslav SVÍTEK et al. *Umělá inteligence a právo*. Plzeň: Aleš Čeněk, 2024. s. 150-151. ISBN 978-80-7380-947-8.
[59] ÚŘAD PRO PUBLIKACE EVROPSKÉ UNIE. Rules for trustworthy artificial intelligence in the EU. In: *EUR-Lex* [online]. Poslední aktualizace 11. 3. 2025 [cit. 2026-02-12]. Dostupné z WWW: https://eur-lex.europa.eu/EN/legal-content/summary/rules-for-trustworthy-artificial-intelligence-in-the-eu.html.
[60] ŠTĚDROŇ, Bohumír, Roman JAŠEK, Miroslav SVÍTEK et al. *Umělá inteligence a právo*. Plzeň: Aleš Čeněk, 2024. s. 150-152. ISBN 978-80-7380-947-8.

dochází k nezbytnému zpracování citlivých údajů cestujících za účelem bezpečnostního screeningu.[61]

Zařazení biometrického identifikačního systému do kategorie vysokého rizika s sebou pro jeho poskytovatele a provozovatele nese nutnost splnění přísných regulatorních požadavků, a to jak před samotným uvedením do provozu, tak i v jeho průběhu. Klíčovým prvkem je princip proporcionality a s ním spojený požadavek na zajištění vysoké míry transparentnosti, včetně vedení detailní technické dokumentace a záznamů o fungování systému. Provozovatelé těchto technologií mají navíc povinnost zavést mechanismy pro aktivní a systematické monitorování rizik a shromažďování dat o výkonnosti systému na trhu (tzv. post-market monitoring). Záměrem těchto legislativních opatření není bránit technologickému pokroku, ale zajistit zachování lidské kontroly a odpovědnosti v celém dodavatelském a provozním řetězci umělé inteligence, čímž se minimalizuje riziko skrytých nebo klamavých praktik vůči koncovým uživatelům.[62]

4.3 Právní úprava v České republice

4.3.1 Adaptační zákon a vztah k evropskému nařízení

Základním vnitrostátním předpisem upravujícím ochranu osobních údajů v České republice je zákon č. 110/2019 Sb., o zpracování osobních údajů (dále jen ZZOÚ). Ačkoliv je tento předpis v běžné praxi označován jako zákon adaptační, jeho skutečný rozsah a účel je širší. Kromě nezbytné adaptace přímo použitelného evropského nařízení GDPR totiž obsahuje i transpozici dalších unijních směrnic. Vzhledem k přímé účinnosti GDPR nebylo možné do národní úpravy plošně převzít existující evropská pravidla a vytvořit tak jejich duplikát. Český zákonodárce proto vyhrazený legislativní prostor využil primárně ke konkretizaci vybraných ustanovení a ke stanovení specifických vnitrostátních výjimek, aniž by základní evropský standard jakkoliv zpřísňoval.[63] Národní úprava tak netvoří zcela nezávislý celek a v aplikační praxi musí být český zákon a evropské obecné nařízení vždy vykládány a aplikovány v nerozlučné vzájemné

[61] EVROPSKÁ KOMISE. AI Act. In: *Shaping Europe's digital future* [online]. Poslední aktualizace 27. 1. 2026 [cit. 2026-02-12]. Dostupné z WWW: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

[62] BULLOCK, Justin B. et al. The Oxford Handbook of AI Governance. New York: Oxford University Press, 2024. s. 266-267. ISBN 978-0-19-757932-9.

[63] BAČA, Ján et al. *Zákon o zpracování osobních údajů: praktický komentář*. Plzeň: Aleš Čeněk, 2020. s. 38. ISBN 978-80-7380-804-4.

souvislosti. Cílem tohoto komplexního právního rámce je zajištění efektivní ochrany práva na soukromí, které je pevnou součástí českého ústavního pořádku.[64]

Samotný obecný zákaz zpracování biometrických údajů za účelem jedinečné identifikace a taxativní výčet výjimek z tohoto zákazu jsou zakotveny přímo v článku 9 obecného nařízení GDPR. Český zákon o zpracování osobních údajů tento plošný zákaz záměrně znovu nedefinuje, čímž důsledně respektuje princip přímé použitelnosti evropského práva. V textu národního zákona je zpracování biometrických a zvláštních kategorií osobních údajů explicitně regulováno až ve specifických ustanoveních (zejména v § 39a a násl., § 63 a § 66 ZZOÚ). Tato ustanovení slouží k transpozici takzvané policejní směrnice a upravují přísné podmínky, za kterých mohou s těmito vysoce citlivými údaji nakládat příslušné orgány za účelem předcházení, vyhledávání, odhalování nebo stíhání trestné činnosti. Tímto je na národní úrovni ukotven zcela specifický právní režim pro získávání a vytěžování biometrických charakteristik ze strany bezpečnostních sborů.[65]

4.3.2 Zpracování biometrických údajů Policií ČR

Tento obecný ochranný rámec je v aplikační praxi naplňován prostřednictvím zvláštních zákonů upravujících činnost a kompetence jednotlivých orgánů. Stěžejním předpisem je v tomto kontextu zákon č. 273/2008 Sb., o Policii České republiky. Právě jeho § 65 explicitně zakotvuje oprávnění k proaktivnímu získávání osobních údajů pro účely budoucí identifikace. Na základě tohoto ustanovení disponují policejní orgány pravomocí snímat daktyloskopické otisky, provádět měření těla, pořizovat obrazové záznamy a odebírat biologické vzorky. Tento postup je aplikovatelný výhradně vůči taxativně vymezenému okruhu subjektů, mezi které patří primárně osoby obviněné ze spáchání úmyslného trestného činu, osoby podezřelé či osoby ve výkonu trestu. Získaný biologický materiál je posléze transformován do profilu DNA, což představuje alfanumerický kód odrážející pouze nekódující části genetické výbavy. Současná právní úprava rovněž umožňuje odebírat tyto vzorky osobám mladším 15 let, a to z důvodu nezbytné prevence u dětské a mladistvé delikvence, která se vyznačuje vysokým rizikem recidivy. V případě aktivního odporu dotčené osoby je zasahující policista oprávněn tento odpor překonat. Absolutní výjimku z tohoto pravidla představují úkony spojené s přímým

[64] Tamtéž, s. 21-22.
[65] ČESKO. Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: *Sbírka zákonů, Česká republika*. 2019, částka 47. Dostupné z WWW: https://www.e-sbirka.cz/sb/2019/110?zalozka=text

zásahem do tělesné integrity, jako je například odběr krve, k jejichž vynucení nelze přistoupit.[66]

Zcela specifický a vysoce pokročilý biometrický režim pak představuje plošné zpracování digitálních fotografií obličeje. Ustanovení § 66a opravňuje policii k provozování a vytěžování rozsáhlé databáze digitálních fotografií fyzických osob. Do tohoto centrálního systému jsou kontinuálně a dálkově stahovány fotografie a agendové identifikátory z primárních státních evidencí, typicky ze systémů evidence občanských průkazů, cestovních dokladů či registru cizinců. Takto shromážděná datová základna je následně využívána pro automatickou identifikaci neznámých osob prostřednictvím softwarového vyhledávání a technologií pro rozpoznávání obličeje. Za účelem minimalizace plošného zásahu do práva na soukromí občanů probíhá samotné algoritmické porovnávání obrazových záznamů primárně s anonymizovanou referenční databází. K prolomení anonymity a zjišťování konkrétních osobních údajů dochází až v momentě, kdy systém na základě vytipování detekuje relevantní shodu.[67]

4.3.3 Biometrické prvky v cestovních a osobních dokladech

Další stěžejní oblastí státem nařízeného plošného zpracování biometrických charakteristik je agenda vydávání cestovních dokladů. Právní rámec této agendy tvoří primárně zákon č. 329/1999 Sb., o cestovních dokladech. Dle této úpravy jsou standardní cestovní, diplomatické a služební pasy obligatorně koncipovány jako doklady obsahující strojově čitelné údaje a elektronický nosič dat, takzvaný čip. V tomto nosiči jsou bezpečně uloženy biometrické údaje, kterými jsou smyslu zákona digitální zobrazení obličeje a daktyloskopické otisky prstů. Z povinnosti plošného snímání otisků prstů zákon explicitně vyjímá občany mladší 12 let, u nichž se do biometrického nosiče ukládá pouze digitalizovaná podoba obličeje.[68]

Nakládání s těmito vysoce citlivými daty podléhá v prostředí cestovních dokladů striktnímu účelovému omezení. Biometrické údaje uložené v čipu pasu lze podle zákona využít výlučně k ověřování pravosti samotného dokladu a k verifikaci totožnosti jeho držitele. Tato identifikace probíhá prostřednictvím specializovaného technického

[66] ŠTEINBACH, Miroslav et al. *Zákon o Policii České republiky: komentář*. 2. vyd. Praha: Wolters Kluwer, 2024. s. 199-200. ISBN 978-80-7676-830-7
[67] Tamtéž, s. 206-207.
[68] HEJDUK, Marek. *Zákon o cestovních dokladech*. Praha: Wolters Kluwer, 2022. s. 27-29. ISBN 978-80-7598-467-8.

zařízení, které v reálném čase algoritmicky srovnává aktuálně sejmuté biometrické rysy přítomné osoby s referenčními daty bezpečně uloženými v nosiči.[69]

Vedle cestovních pasů se biometrické údaje začaly v nedávné době povinně vyskytovat rovněž v občanských průkazech. Od srpna 2021 vydává Česká republika modernizované průkazy vybavené bezkontaktním čipem, do nějž jsou bezpečně nahrány otisky prstů a digitální zobrazení obličeje držitele. Tato inovace, jež bezprostředně vychází z požadavků evropské legislativy, plní dvojí účel. Primárně významně zvyšuje ochranu dokladů proti padělání a zneužití, a zároveň občanům umožňuje využívat občanský průkaz jako plnohodnotný cestovní doklad při pohybu v rámci Evropské unie, což by bez implementace těchto bezpečnostních prvků nebylo možné. Nakládání s daty je i zde přísně regulováno – v národním systému jsou uchovávána maximálně po dobu 90 dnů od vydání průkazu a jejich následné čtení z čipu je omezeno výhradně na ověření pravosti dokladu a totožnosti konkrétní osoby.[70]

Lze tedy konstatovat, že výše popsaný legislativní mechanismus, jenž umožňuje exaktní strojové porovnávání biometrických dat z cestovních dokladů, představuje naprosto nezbytný právní i technologický fundament pro modernizaci plynulosti hraničních kontrol. Ukázkovou aplikací tohoto teoretického rámce v reálném prostředí – jíž se bude věnovat praktická část této práce – je nasazení samoobslužných biometrických bran (tzv. e-Gate), které v současnosti figurují jako standardní prvek bezpečnostního odbavení na mezinárodním Letišti Václava Havla v Praze.

[69] Tamtéž, s. 32.
[70] DLUBALOVÁ, Klára. Sněmovna schválila nový typ občanských průkazů s biometrickými údaji. In: *Ministerstvo vnitra ČR* [online]. [cit. 2026-02-13]. Dostupné z WWW: https://mv.gov.cz/clanek/snemovna-schvalila-novy-typ-obcanskych-prukazu-s-biometrickymi-udaji.aspx.

5 Etické a společenské aspekty biometrické identifikace

Se stále častější implementací biometrických systémů do každodenního života vyvstává nutnost kritické reflexe souvisejících etických rizik. Ačkoliv tyto technologie přinášejí nesporné výhody v oblasti bezpečnosti a efektivity, generují zároveň zcela bezprecedentní výzvy v rovině lidských práv, ochrany soukromí a společenské rovnosti.

5.1 Zásah do soukromí a nezměnitelnost biometrických dat

Primární oblastí etického zájmu je povaha samotných biometrických údajů. Při jejich zpracování dochází ke shromažďování vysoce citlivých osobních dat, která jsou intimně spjata s fyzickou podstatou člověka. Zásadní rozdíl oproti tradičním autentizačním prvkům spočívá v jejich nezměnitelnosti. Pokud dojde ke kompromitaci či krádeži běžného hesla nebo přístupové karty, lze tyto prvky okamžitě zneplatnit a nahradit. Jednou zcizený biometrický údaj (například otisk prstu či mapa obličeje) však změnit nelze. V případě úniku těchto dat z centrálních databází tak vzniká trvalé a nevratné bezpečnostní riziko, které otevírá prostor pro celoživotní krádež identity. Z etického i právního hlediska je proto vyžadováno, aby byl sběr těchto dat striktně minimalizován a chráněn nejvyššími možnými technickými zárukami.

5.2 Iluze informovaného souhlasu a asymetrie moci

Další významný etický problém představuje proces získávání souhlasu se zpracováním biometrických údajů v prostředích, kde panuje takzvaná asymetrie moci. Ukázkovým příkladem jsou pracovněprávní vztahy. Spoléhání se na informovaný souhlas zaměstnance, například při zavádění biometrických docházkových systémů, je z etického i praktického hlediska problematické. Aby byl souhlas skutečně platný, musí být poskytnut zcela svobodně. Zaměstnanec však často čelí tlaku autority a obavám z možných negativních důsledků, což svobodnou vůli narušuje. Podle výkladové praxe je takový souhlas fakticky neplatný, pokud subjekt údajů nemá možnost jej kdykoliv a bez jakýchkoliv sankcí odvolat. Pokud zaměstnanec souhlas odvolá, musí mu být okamžitě

poskytnut plnohodnotný alternativní systém (např. čipová karta), aniž by byl jakkoliv znevýhodněn. V opačném případě se ze souhlasu stává pouze vynucená iluze.[71]

5.3 Algoritmická předpojatost a systémová diskriminace

Kromě narušení soukromí čelí biometrické systémy, a to zejména technologie pro automatizované rozpoznávání obličejů, kritice pro svou technologickou nedokonalost. Zásadním etickým rizikem je takzvaná algoritmická předpojatost (bias). Jak upozorňují pokyny Evropského sboru pro ochranu osobních údajů, plošné nasazování těchto technologií s sebou nese vysoké riziko diskriminace a generování falešných výsledků. Umělá inteligence se učí na obrovských datových sadách, které často nejsou dostatečně reprezentativní. V důsledku toho vykazují systémy biometrické identifikace statisticky prokazatelně vyšší chybovost u určitých demografických skupin – typicky u žen, mladistvých či příslušníků etnických menšin. Pokud jsou tyto zatížené algoritmy využívány k rozhodování, například donucovacími orgány, může docházet k nespravedlivému zacházení, bezdůvodnému odepření práv či k falešným obviněním.[72]

5.4 Masové sledování a mrazivý účinek

Extrémní etické riziko představuje plošné nasazení biometrických technologií ve veřejném prostoru. Zatímco úřady obhajují chytré kamerové sítě prevencí kriminality, lidskoprávní organizace varují před infrastrukturou umožňující absolutní kontrolu obyvatelstva. Neustálé algoritmické sledování generuje sociologický fenomén tzv. mrazivého účinku (*chilling effect*). Vědomí všudypřítomného dohledu prokazatelně mění přirozené chování jednotlivců. Lidé se podvědomě uchylují k autocenzuře a omezují uplatňování svých základních svobod, jako je svoboda projevu či shromažďování. Tato plošná kontrola tak postupně narušuje základy demokratické společnosti a presumpci neviny, neboť ke každému občanovi a priori přistupuje jako k potenciální hrozbě.[73]

[71] HANZEL, Petr. Právní aspekty využívání biometrických dat v HR: GDPR, etika a balanční testy. In: *ARROWS advokátní kancelář* [online]. 14. 8. 2025 [cit. 2026-02-20]. Dostupné z WWW: https://arws.cz/novinky-v-arrows/pravni-aspekty-vyuzivani-biometrickych-dat-v-hr.

[72] EVROPSKÝ SBOR PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Pokyny 05/2022 k používání technologie rozpoznávání obličeje v oblasti prosazování práva* [online]. 2022. s. 5. [cit. 2026-02-20]. Dostupné z WWW: https://uoou.gov.cz/media/zahranici/dokumenty/schvalene-pokyny/pokyny-2022-05-k-pouzivani-technologie-rozpoznavani-obliceje-v-oblasti-prosazovani-prava.pdf.

[73] SOARES, Joana. Velký bratr se dívá. Země EU včetně Česka rozšiřují sledování občanů. In: *Ekonomický deník* [online]. 18. 8. 2025 [cit. 2026-02-20]. Dostupné z WWW: https://ekonomickydenik.cz/eu-rozsiruje-sledovani-obcanu/.

6 Dotazníkové šetření

Empirická část práce plynule navazuje na teoretická východiska a jejím hlavním cílem je poskytnout ucelený obraz o tom, jak problematiku biometrické identifikace vnímá široká veřejnost. Zjištěné postoje jsou následně komparovány s reálným fungováním těchto systémů v praxi. Vedlejším cílem je zhodnotit subjektivní vnímání bezpečnosti, technologické spolehlivosti a společenské přijatelnosti těchto technologií.

K dosažení těchto cílů se empirická část dělí na dva celky. Prvním je vlastní průzkumné šetření mapující aktuální názory občanů. Druhým krokem je analýza konkrétního příkladu z praxe, zaměřená na fungování biometrických a kamerových systémů na Letišti Václava Havla v Praze. Zjištění z tohoto reálného bezpečnostního prostředí pak slouží jako faktický základ pro závěrečnou komparaci a syntézu s daty získanými od respondentů.

6.1 Metodika a struktura dotazníkového šetření

Pro sběr primárních dat byla zvolena metoda kvantitativního průzkumu formou anonymního online dotazníku. Ten byl vytvořen v prostředí Google Forms a distribuován primárně prostřednictvím sociálních sítí a diskusních fór. Sběr odpovědí probíhal od 10. února do 3. března 2026. Do průzkumu se úspěšně zapojilo 151 respondentů, což tvoří plně dostačující vzorek pro formulaci relevantních analytických závěrů.

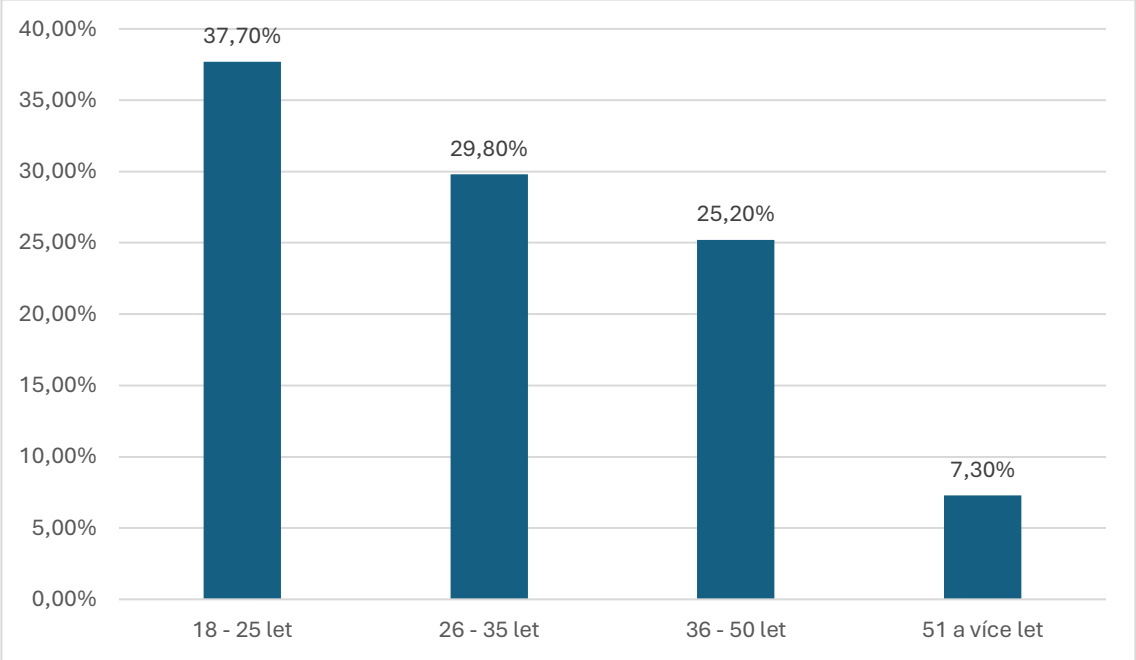
Šetření mělo primárně deskriptivní povahu a vzhledem k jeho exploračnímu charakteru nebyly stanoveny striktní hypotézy. Cílem bylo zmapovat současný stav a reálné zkušenosti respondentů.

Dotazník obsahoval celkem 13 uzavřených otázek s možností jedné či více odpovědí. Po úvodním zjištění věkové struktury se otázky systematicky zaměřily na obavy ze zneužití citlivých dat a důvěru ve státní i komerční instituce spravující biometrické databáze. Závěrečná část mapovala ochotu respondentů tyto moderní technologie aktivně využívat v běžném životě, při překračování státních hranic i v rámci zajištění bezpečnosti ve veřejném prostoru.

6.2 Analýza a interpretace dat

Otázka č. 1 – Váš věk

Graf č. 1 – Věk respondentů



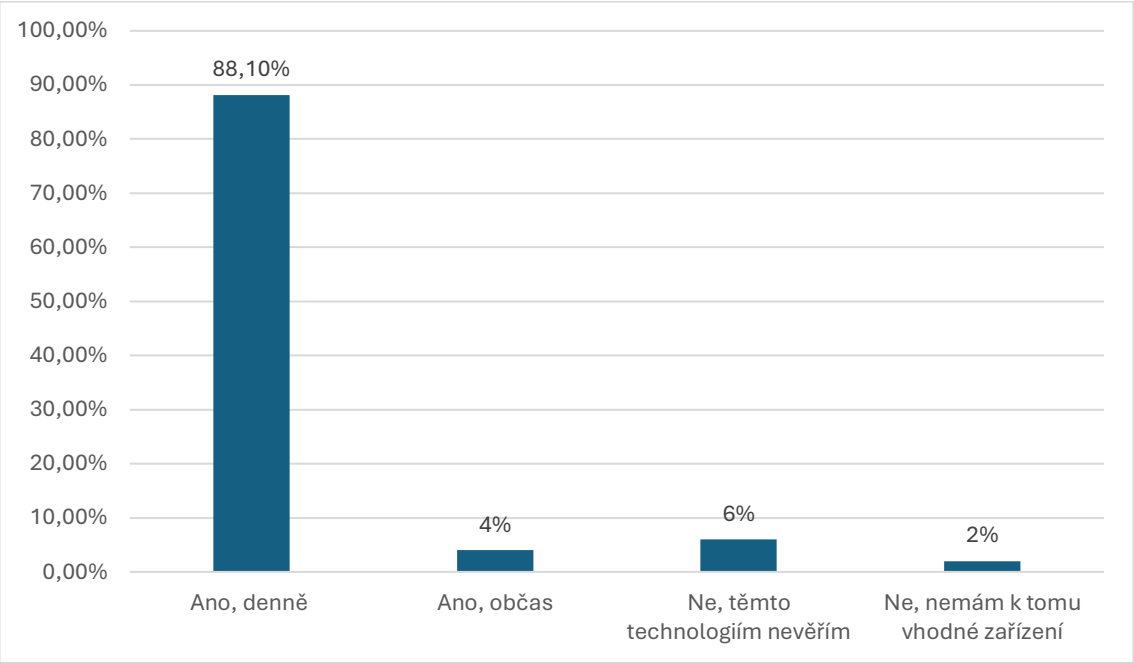
(Zdroj: Vlastní šetření)

Úvodní otázka průzkumného šetření zjišťovala věkovou strukturu zúčastněných respondentů, což je klíčový faktor pro následné posouzení generačních rozdílů v přístupu k biometrickým technologiím. Z celkového počtu 151 dotázaných tvořila nejpočetnější skupinu nejmladší generace ve věku 18–25 let (37,7 %, 57 osob). Druhou nejvíce zastoupenou kategorií byli respondenti ve věku 26–35 let, kteří představovali téměř třetinu celkového vzorku (29,8 %, 45 osob).

Lidé středního věku (36–50 let) tvořili čtvrtinu dotázaných (25,2 %, 38 osob) a nejmenší zastoupení měla podle předpokladů nejstarší věková skupina 51 a více let (7,3 %, 11 osob). Celkové rozložení vzorku tak velmi dobře reflektuje skutečnost, že mladší a střední generace jsou v digitálním prostoru aktivnější a častěji s biometrickými technologiemi (například v chytrých telefonech) v běžném životě přicházejí do styku. Získaná data poskytují dostatečně diverzifikovaný základ pro relevantní křížové porovnání názorů napříč všemi generacemi.

Otázka č. 2 – Využíváte v běžném životě biometrické funkce?

Graf č. 2 – Využívání biometrických funkcí v běžném životě



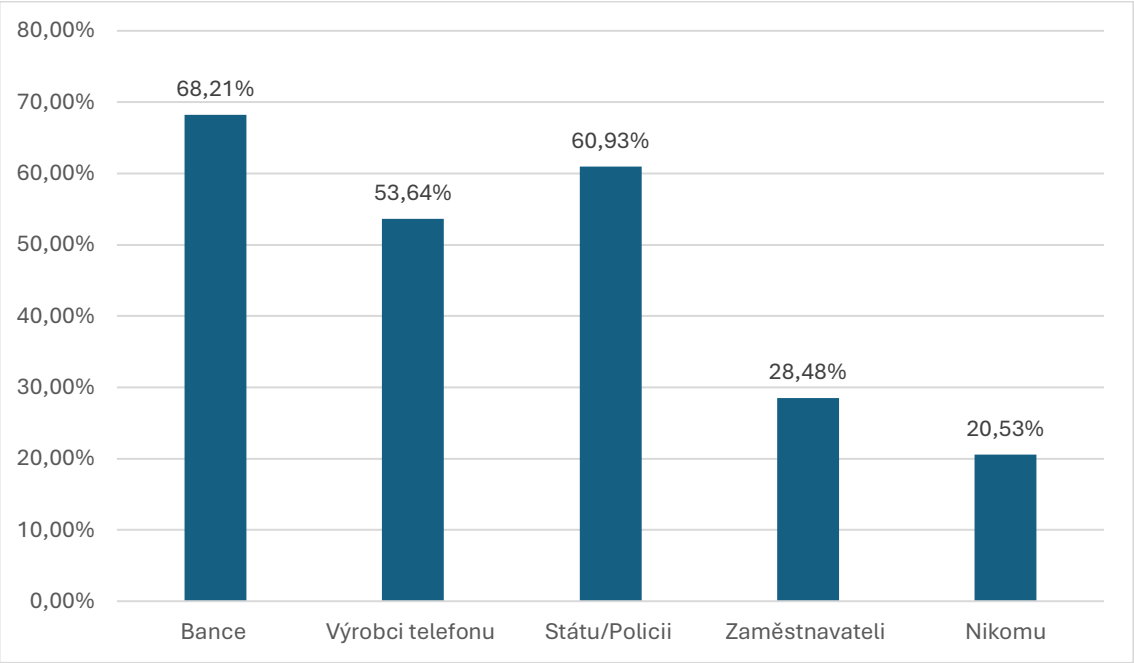
(Zdroj: Vlastní šetření)

Druhá otázka dotazníkového šetření zjišťovala, do jaké míry respondenti v každodenním životě využívali biometrické funkce, jako bylo odemykání telefonu otiskem prstu či skenem obličeje. Z analýzy dat vyplynulo, že tyto technologie se staly pevnou součástí běžné rutiny pro drtivou většinu dotázaných. Téměř devět z deseti respondentů (133 ze 151 osob) je využívalo na denní bázi, a při započtení občasných uživatelů tento podíl celkově přesáhl 92 %.

Křížová analýza podle věku však odhalila výrazné generační rozdíly, a to zejména v otázce celkové důvěry k těmto systémům. Zatímco pro mladší generace do 35 let představovala biometrická autentizace naprostý standard s více než 95% každodenním využitím a téměř nulovou nedůvěrou, u starších ročníků situace vypadala odlišně. Ve věkové skupině 36–50 let kleslo každodenní používání na 71 % a více než desetina osob v této kategorii technologiím výslovně nevěřila. Nejsilnější skepse se logicky projevila u respondentů nad 51 let, z nichž více než čtvrtina (27,3 %) biometrii z důvodu obav o zabezpečení zcela odmítala. Z dat tak zřetelně vyplynulo, že s rostoucím věkem plynule klesala míra využívání a naopak stoupala nedůvěra.

Otázka č. 3 – Komu byste byli ochotni svěřit své biometrické údaje?

Graf č. 3 – Ochota respondentů sdílet biometrické údaje s vybranými subjekty



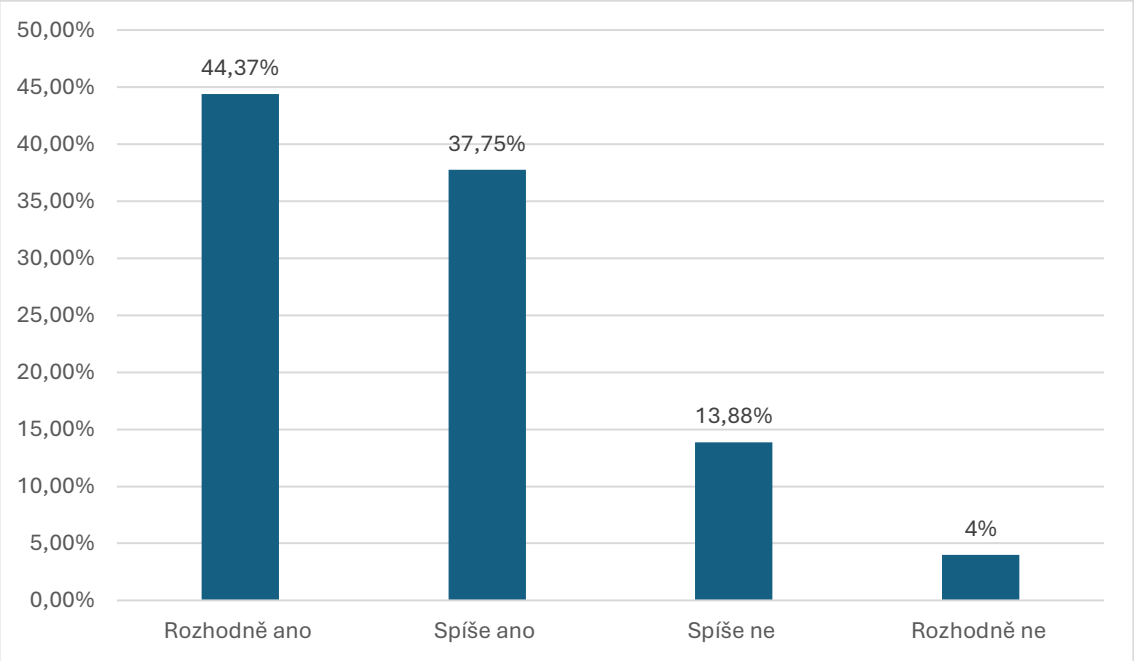
(Zdroj: Vlastní šetření)

Třetí otázka průzkumného šetření jako jediná umožňovala výběr více možností a mapovala ochotu respondentů sdílet svá citlivá data. Celkově si nejvyšší důvěru získaly banky (68,21 %) a státní aparát s policií (60,93 %). Výrobcům telefonů důvěřovala mírně nadpoloviční většina (53,64 %), zatímco zaměstnavatele zvolilo pouze 28,48 % osob. Celá pětina vzorku (20,53 %) by svá data nesvěřila vůbec nikomu.

Křížová analýza podle věku opět potvrdila, že ochota sdílet data s rostoucím věkem strmě klesala. Nejmladší respondenti (18–25 let) vykazovali vysokou důvěru v banky (82,46 %) i stát (75,44 %) a absolutní nedůvěru („nikomu“) u nich zvolilo pouhých 7,02 %. U skupiny 26–35 let podíl nedůvěřivých vzrostl na rovných 20 % a u osob středního věku (36–50 let) dosáhl již 31,58 %. Největší skepse panovala u nejstarší generace nad 51 let, kde by více než polovina (54,55 %) data nesvěřila nikomu a důvěra k bankám i státu klesla na shodných 27,27 %.

Otázka č. 4 – Pokud byste na letišti mohli projít automatickou biometrickou bránou (tzv. E-Gate) a ušetřit tak 30 minut čekání ve frontě, využili byste to?

Graf č. 4 – Ochota využít automatickou bránu E-Gate za účelem úspory času na letišti



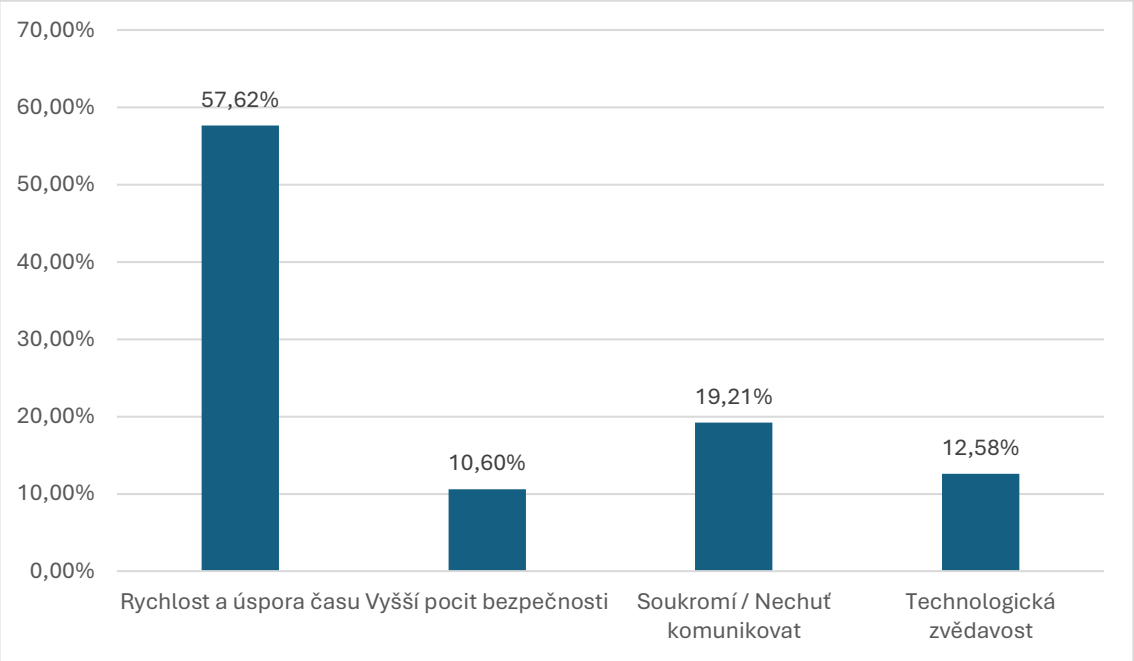
(Zdroj: Vlastní šetření)

Čtvrtá otázka průzkumného šetření přesunula pozornost k praktickému scénáři a zjišťovala, zda by respondenti využili automatickou biometrickou bránu (E-Gate) při pasové kontrole, pokud by tím ušetřili 30 minut čekání. Vidina významné časové úspory se ukázala jako silný motivační faktor. V celkovém součtu by tuto možnost zvolilo přes 82 % dotázaných (přičemž 44,37 % uvedlo odpověď „rozhodně ano“ a 37,75 % „spíše ano“). Možnost odmítnutí si vybralo necelých 18 % vzorku, přičemž absolutní zamítnutí („rozhodně ne“) tvořilo pouze okrajová 4 %.

Při srovnání napříč generacemi se potvrdil předpokládaný trend, avšak pragmatický benefit v podobě úspory času dokázal částečně prolomit i nedůvěru starších ročníků, která se objevila v předchozích odpovědích. U nejmladší generace (18–25 let) byla podpora biometrického odbavení drtivá, když jej pozitivně hodnotilo téměř 90 % z nich. Podobně vstřícný postoj (přes 84 % kladných odpovědí) zaujali i dospělí ve věku 26–35 let. U respondentů ve věku 36–50 let celková ochota klesla na 73,68 % a podíl odmítavých odpovědí překročil čtvrtinu. Největší míra odporu se opět soustředila do nejstarší kategorie (51 a více let), kde by E-Gate odmítlo využít přes 36 % osob. Přesto i v této nejvíce skeptické skupině téměř 64 % respondentů nakonec dalo přednost technologickému řešení a rychlému odbavení před osobním kontaktem s policistou.

Otázka č. 5 – Co by pro Vás bylo hlavním důvodem pro využití automatické brány (E-Gate) při pasové kontrole na letišti?

Graf č. 5 – Hlavní motivace pro využití automatické biometrické brány (E-Gate)



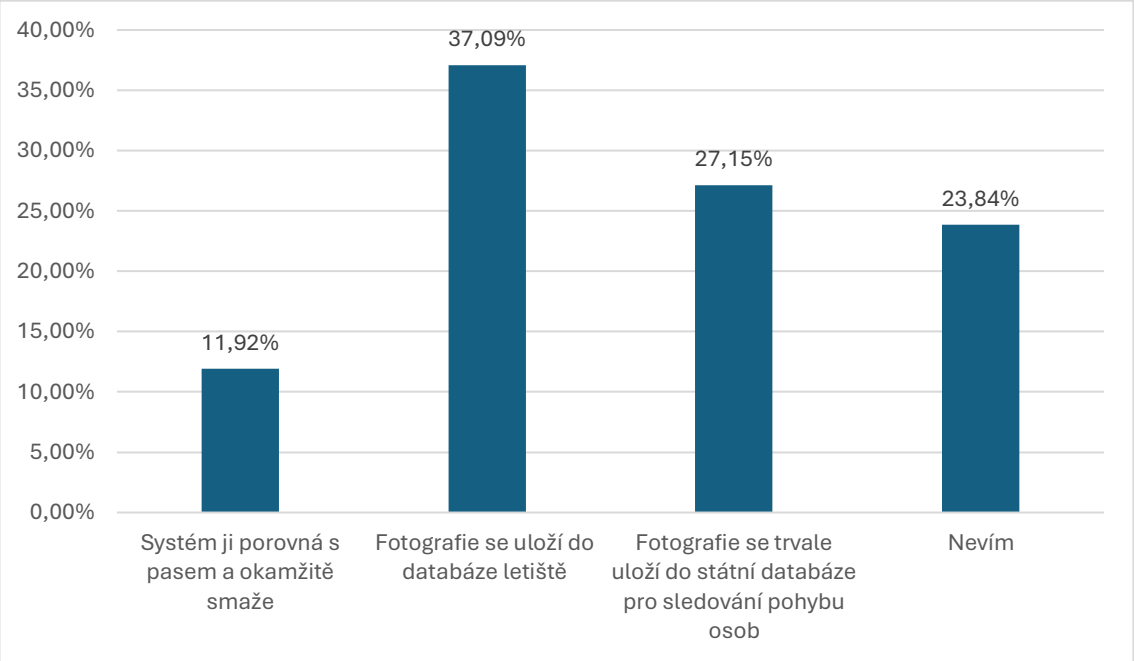
(Zdroj: Vlastní šetření)

Pátá otázka plynule navazovala na předchozí zjištění a zkoumala primární motivaci, která by respondenty přiměla k využití automatického odbavení. Z celkových výsledků vyplynulo, že s velkým náskokem zvítězil čistý pragmatismus – rychlost a úsporu času označila za hlavní důvod více než polovina celého vzorku (57,62 %). Druhým nejsilnějším motivem se stala ochrana soukromí spojená s nechutí komunikovat s policistou (19,21 %), těsně následovaná technologickou zvědavostí (12,58 %). Vyšší pocit bezpečnosti plynoucí z přesnosti biometrického stroje motivoval pouze desetinu dotázaných (10,60 %).

Mezigenerační srovnání v tomto případě odhalilo velmi zajímavý paradox. Časová úspora představovala absolutní prioritu pro mladé dospělé (26–35 let), kde přesáhla 71 %, a pro nejmladší generaci (18–25 let) s více než 63 %. U starších ročníků však tento utilitární přístup slábl a překvapivě jej nahrazovala touha po objevování. Zatímco pro respondenty do 35 let nebyla technologická zvědavost nijak zásadním motivem (okolo 5 %), u osob středního věku (36–50 let) již představovala silný sekundární faktor (23,68 %). Zcela nejvíce se pak touha „vyzkoušet, jak to funguje“ projevila u nejstarší generace nad 51 let, kde dosáhla více než 36 %. Z dat tak zřetelně vyplynulo, že zatímco mladší lidé brali E-Gate jako běžný nástroj ke zrychlení procesu, u starší generace zafungovala biometrie z velké části jako lákavá technologická novinka.

Otázka č. 6– Co se podle vás děje s vaší fotografií po průchodu automatickou bránou (pasová kontrola) na letišti?

Graf č. 6 – Povědomí respondentů o nakládání s biometrickými údaji po průchodu E-Gate



(Zdroj: Vlastní šetření)

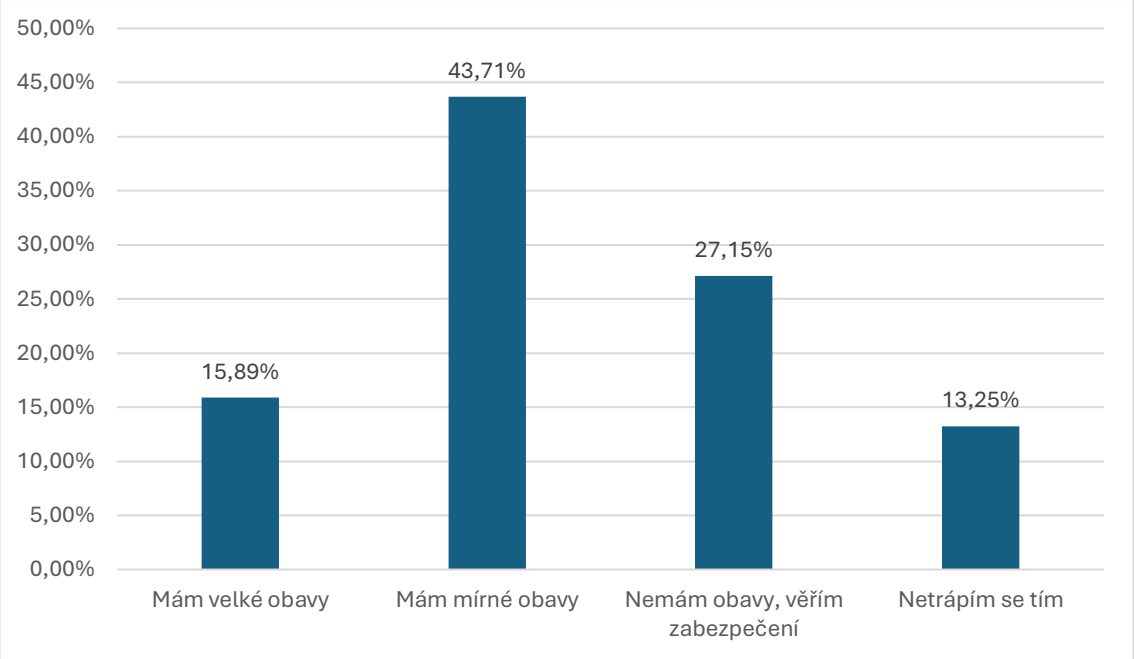
Šestá otázka průzkumného šetření se zaměřila na informovanost a zjišťovala povědomí respondentů o tom, co se reálně dělo s jejich fotografií po průchodu automatickou pasovou bránou. Analýza výsledků odhalila hlubokou neznalost skutečného stavu napříč celým vzorkem. Ačkoliv reálná praxe spočívala v tom, že systém snímek po porovnání s pasem okamžitě smazal, tento fakt znalo pouhých 11,92 % dotázaných. Největší část vzorku (37,09 %) se mylně domnívala, že se fotografie ukládala do databáze letiště na zhruba 30 dnů. Více než čtvrtina osob (27,15 %) dokonce podlehla obavám z plošného sledování a věřila v trvalé uložení do státní databáze. Zbylých téměř 24 % respondentů otevřeně přiznalo absolutní neznalost („nevím“).

Generační srovnání ukázalo, že informační deficit panoval ve všech věkových skupinách, avšak projevoval se odlišnými způsoby. U mladší generace do 35 let sice klesal podíl odpovědí „nevím“ (pohyboval se od 10 do 17 %), ale o to více tyto ročníky volily nesprávné varianty. Nejmladší respondenti (18–25 let) se téměř z poloviny (49,12 %) mylně klonili k dočasnému uložení na 30 dnů. U skupiny 26–35 let zase silně rezonovala obava z trvalého státního sledování (31,11 %). Zcela odlišný přístup pak zvolily starší ročníky. U respondentů ve věku 36–50 let i nad 51 let se dominantní volbou stalo otevřené přiznání nevědomosti („nevím“), které v obou skupinách přesáhlo hranici 44 %. Data tak přesvědčivě prokázala, že bez ohledu na věk drtivá většina

(více než 88 %) veřejnosti neznala skutečný postup ochrany osobních údajů u biometrických bran, což u mnohých generovalo falešné představy a zbytečné obavy.

Otázka č. 7 – Máte obavy, že by vaše biometrická data mohla být zneužita?

Graf č. 7 – Míra obav respondentů ze zneužití biometrických dat



(Zdroj: Vlastní šetření)

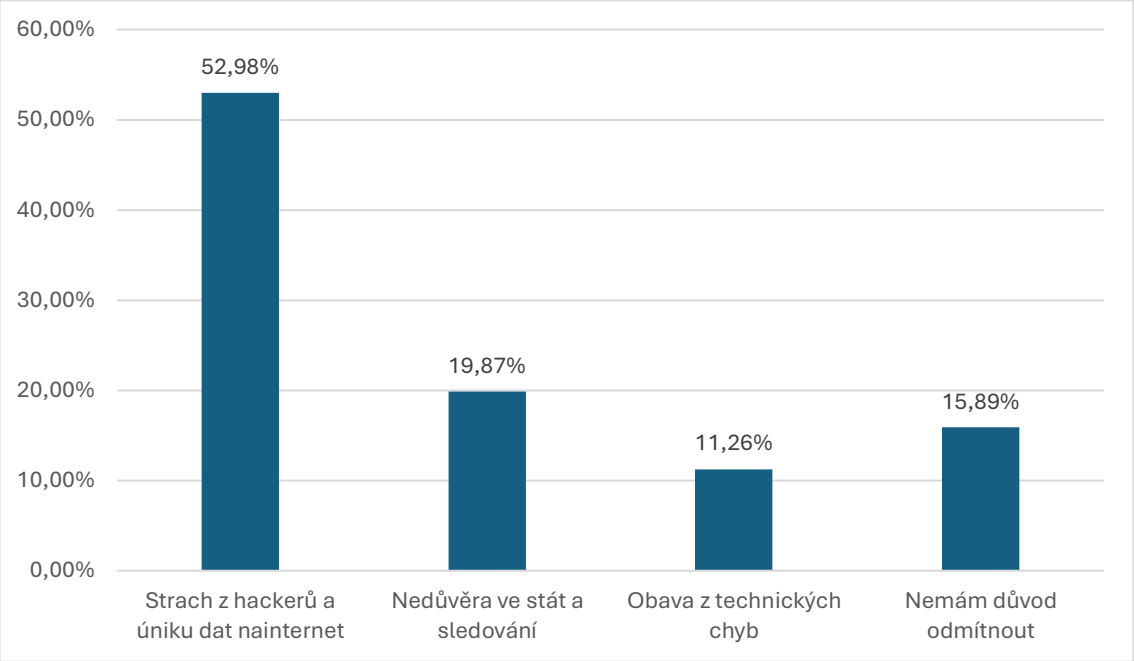
Sedmá otázka průzkumného šetření zkoumala, do jaké míry se respondenti obávali zneužití svých citlivých dat. Výsledky ukázaly, že určitá míra ostražitosti ve společnosti silně rezonovala. Nejpočetnější skupina dotázaných (43,71 %) přiznala mírné obavy a dalších 15,89 % osob dokonce obavy velké. V celkovém součtu tak téměř 60 % vzorku vnímalo riziko zneužití, což logicky navazovalo na předchozí zjištění o plošné neznalosti principů zpracování dat. Naopak plnou důvěru v zabezpečení projevilo 27,15 % respondentů a zbylých 13,25 % se možnými riziky vůbec nezabývalo.

Křížová analýza podle věku přinesla překvapivé zjištění – nejsilnější pocit ohrožení nepanoval u nejstarší generace, jak by se dalo očekávat, ale u osob středního věku (36–50 let). Právě v této skupině dosáhly velké obavy svého maxima (34,21 %) a v kombinaci s mírnými obavami se cítilo ohroženo téměř 80 % z nich. Nejmladší generace (18–25 let) sice rovněž často volila obezřetný postoj v podobě mírných obav (52,63 %), ovšem silný strach pro ni představoval marginální záležitost (8,77 %). Zcela největší důvěru v technické zabezpečení projevili mladí dospělí (26–35 let), u kterých varianta „nemám obavy“ s 37,78 % zvítězila. U nejstarší generace nad 51 let se naopak nejčastěji mísila mírná skepse s odevzdaností, jelikož se více než 27 % z nich touto

problematikou zkrátka odmítalo trápit. Zjištěná data tak potvrdila, že strach ze zneužití byl ve společnosti značný, avšak jeho intenzita se napříč generacemi nelineárně proměňovala.

Otázka č. 8 – Co by pro vás bylo hlavním důvodem, proč biometrii odmítnout?

Graf č. 8 – Hlavní důvody pro případné odmítnutí biometrické identifikace



(Zdroj: Vlastní šetření)

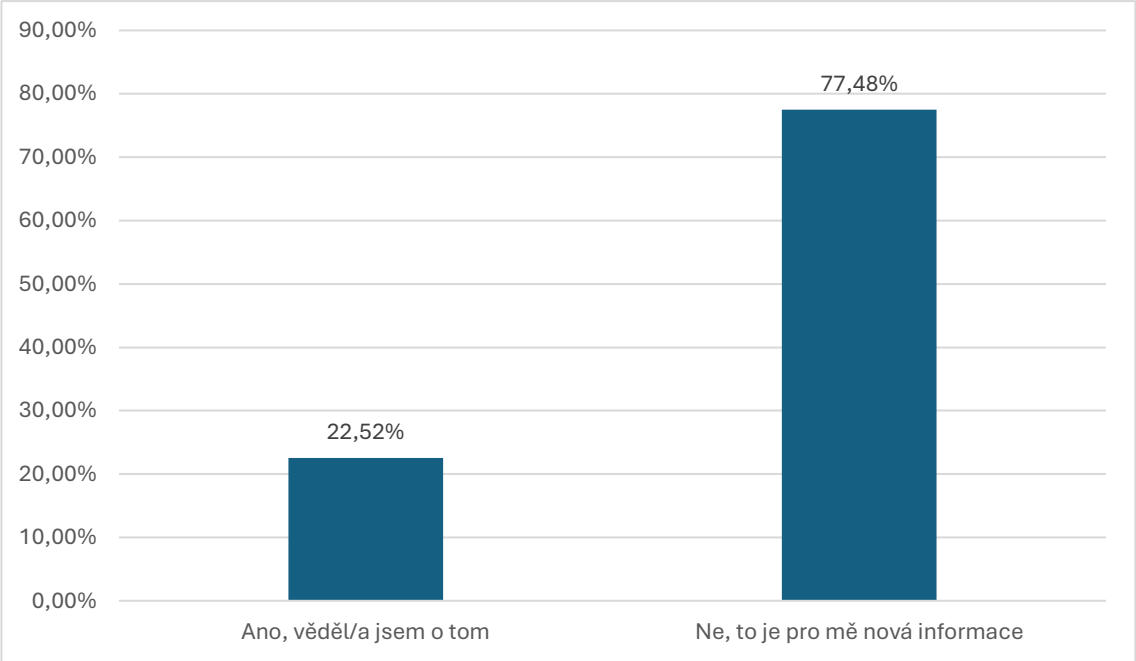
Osmá otázka průzkumného šetření blíže specifikovala povahu obav respondentů a zjišťovala, jaký argument by pro ně představoval hlavní překážku k využívání biometrie. Z celkových výsledků jednoznačně vyplynulo, že největší hrozbu pro veřejnost představovala rizika spojená s kybernetickou bezpečností. Strach z hackerů a úniku citlivých dat na internet označila za primární důvod k odmítnutí více než polovina celého vzorku (52,98 %). Na druhém místě se s téměř pětinovým podílem (19,87 %) umístila nedůvěra ve státní aparát a obava ze sledování (efekt „Velkého bratra“). Strach z technických selhání, například že systém uživatele nerozpozná, hrál s 11,26 % spíše okrajovou roli. Necelých 16 % osob pak neshledávalo pro odmítnutí biometrie žádný relevantní důvod.

Při detailní křížové analýze podle věku se ukázalo, že strach z úniku dat představoval univerzální hrozbu, jež dominovala napříč většinou ročníků. Tento motiv rezonoval nejsilněji u osob středního věku (36–50 let), kde dosáhl téměř 58 %. Výrazné odchylky však nastaly u strachu ze státního sledování. Zatímco u nejmladší generace (18–25 let) se obava z „Velkého bratra“ projevila jen u 15,79 % osob, s rostoucím věkem

postupně sílila. U nejstarší generace nad 51 let se strach z neoprávněného sledování státem stal dokonce stejně silným argumentem jako obava z hackerů (obě varianty zvolilo shodně 36,36 % respondentů z této skupiny). Naopak nejméně kritickou skupinou se ukázali být mladí dospělí (26–35 let), u kterých více než čtvrtina (26,67 %) nenacházela žádný pádný důvod, proč by se biometrickým technologiím měla vyhýbat.

Otázka č. 9 – Věděli jste, že Policie ČR na Letišti Václava Havla v minulosti testovala systém na rozpoznávání tváří v davu, který byl v roce 2025 kvůli ochraně soukromí vypnut?

Graf č. 9 – Povědomí respondentů o testování rozpoznávání tváří na Letišti Václava Havla



(Zdroj: Vlastní šetření)

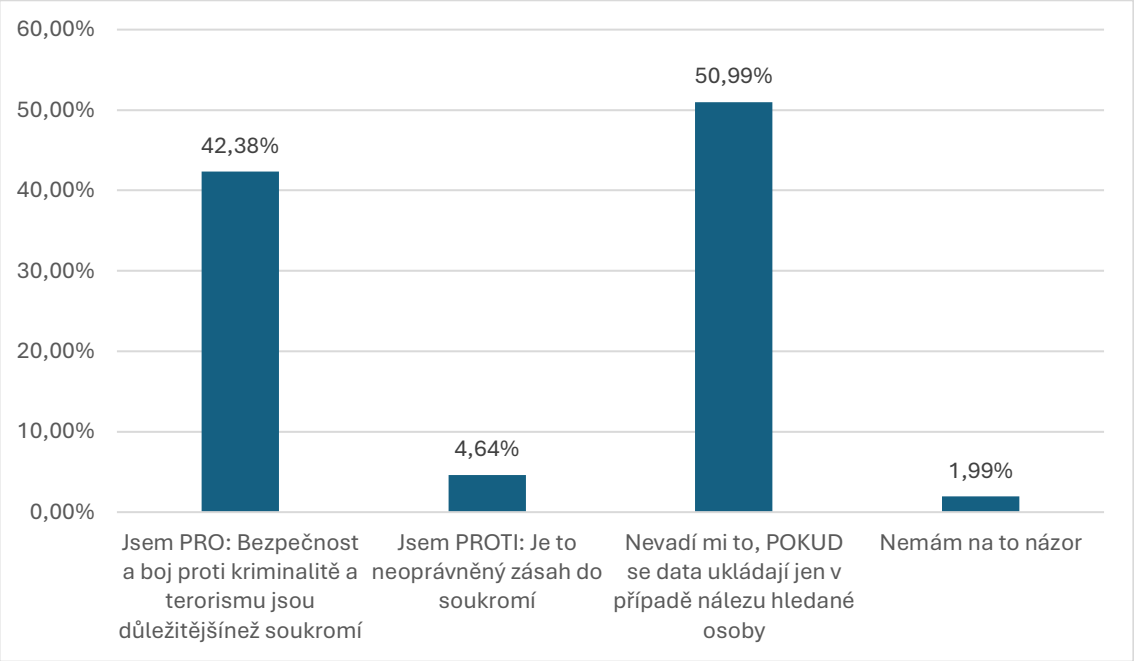
Devátá otázka průzkumného šetření otevírala sekci zaměřenou na kamerové systémy a tvořila přímý můstek k následné komparaci. Zjišťovala, zda respondenti zaznamenali, že Policie ČR na pražském letišti testovala systém pro plošné rozpoznávání tváří v davu, který byl posléze v roce 2025 z důvodu ochrany soukromí vypnut. Získaná data potvrdila, že veřejnost o reálném nasazování biometrických technologií státem měla jen minimální přehled. Pro více než tři čtvrtiny celkového vzorku (77,48 %) se jednalo o zcela novou informaci. Skutečnost, že k tomuto testování a následnému vypnutí došlo, zaregistrovalo pouze 22,52 % dotázaných.

Křížová analýza podle věku ukázala, že informační bublina byla nejsilnější na obou okrajích věkového spektra. Nejnižší povědomí o této události panovalo u nejmladší generace (18–25 let), pro kterou to byla novinka v téměř 86 % případů. Podobně odtržena

od tohoto společenského dění byla i nejstarší generace nad 51 let s téměř 82% neznalostí. Nejlepší (ačkoliv stále silně menšinový) přehled o situaci si udržovaly střední generace. U respondentů ve věku 26–35 let i 36–50 let se informovanost pohybovala těsně pod hranicí 29 %. Data tak naznačila, že lidé v produktivním věku sledovali zpravodajství a domácí bezpečnostní témata mírně aktivněji, nicméně v celospolečenském měřítku tato významná událost na poli ochrany soukromí proběhla z velké části bez povšimnutí veřejnosti.

Otázka č. 10 – Jaký je váš postoj k využívání kamer na automatické rozpoznávání obličejů policií na místech se zvýšeným rizikem (letiště, nádraží, metro)?

Graf č. 10 – Postoj respondentů k plošnému využívání kamer s rozpoznáváním obličejů



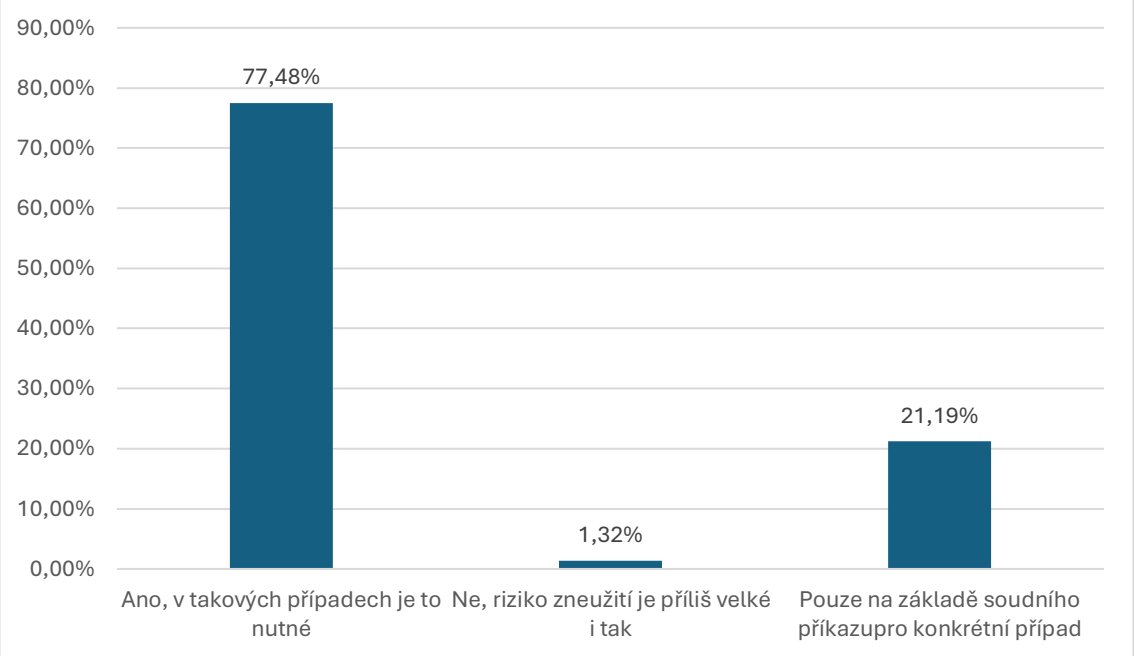
(Zdroj: Vlastní šetření)

Desátá otázka průzkumného šetření se zaměřila na toleranci respondentů vůči plošnému nasazení biometrických kamerových systémů bezpečnostními sbory na místech se zvýšeným rizikem. Získaná data odhalila významný posun v uvažování dotázaných. Ačkoliv předchozí výsledky naznačovaly značné obavy ze zneužití dat, v kontextu veřejné bezpečnosti převládla ochota ke kompromisu. Zcela dominantním postojem se stala podmíněná akceptace – mírně nadpoloviční většina (50,99 %) respondentů systém tolerovala pod podmínkou, že se data ukládala výhradně při nalezení hledané osoby. Dalších 42,38 % vzorku zaujalo radikálnější postoj a upřednostnilo veřejnou bezpečnost a boj proti kriminalitě před osobním soukromím. Striktní odmítnutí z důvodu neoprávněného zásahu do soukromí představovalo marginální záležitost (4,64 %).

Křížová analýza podle věku ukázala, že podmíněný souhlas se stal silným společným jmenovatelem pro většinu ročníků, přesto se objevily zajímavé odchylky. Největší ochotu obětovat své soukromí ve prospěch bezpečnosti vykazovala skupina mladých dospělých (26–35 let), kde varianta absolutní podpory („jsem PRO“) zvítězila s téměř 58 %. Naopak u nejmladší generace (18–25 let) a u osob středního věku (36–50 let) dominoval zmíněný kompromis vázaný na jasná pravidla uchovávání dat (pohyboval se kolem 60 %). Nejkritičtější postoj tradičně zaujala nejstarší generace (51 a více let). Ačkoliv i zde převládala ochota systém za určitých podmínek akceptovat, podíl striktně odmítavých odpovědí se v této věkové kategorii vyšplhal na více než 18 %, což představovalo suverénně nejvyšší míru odporu napříč celým vzorkem. Výsledky tak potvrdily, že česká veřejnost byla k nasazení biometrických kamer obecně velmi tolerantní, pokud vnímala jasný bezpečnostní přínos a transparentní pravidla.

Otázka č. 11 – Souhlasili byste s nasazením rozpoznávání tváří, pokud by to prokazatelně pomohlo při pátrání po unesených dětech nebo teroristech?

Graf č. 11 – Ochota respondentů podpořit rozpoznávání tváří v krizových bezpečnostních situacích



(Zdroj: Vlastní šetření)

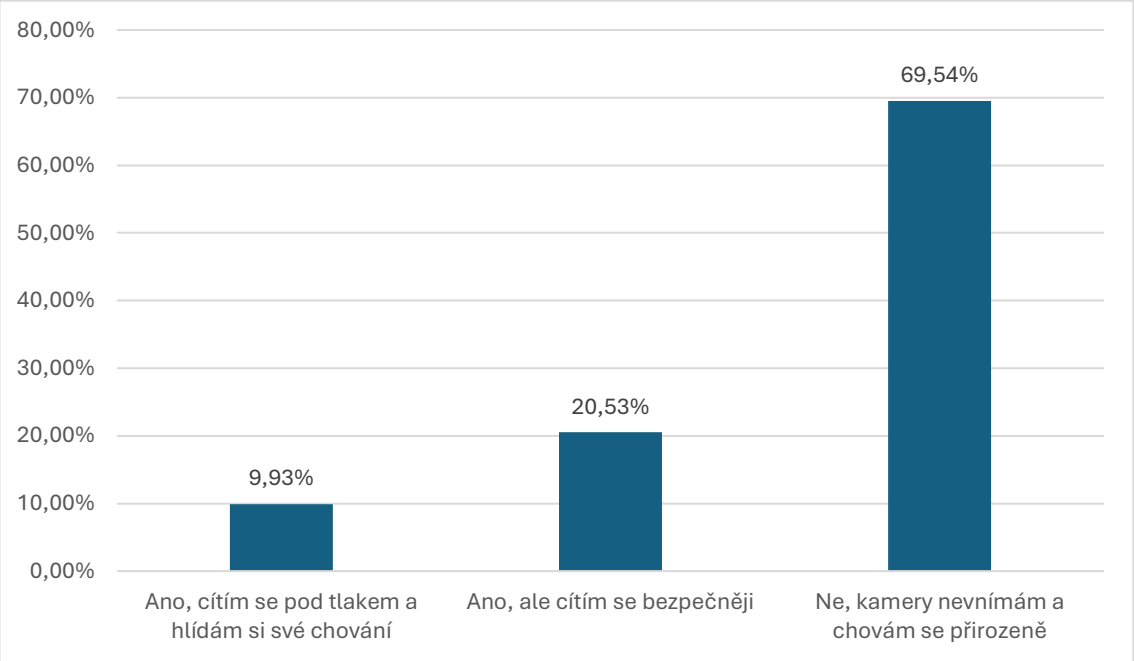
Jedenáctá otázka průzkumného šetření eskalovala zkoumanou problematiku do podoby extrémní bezpečnostní hrozby a zjišťovala, jak by respondenti reagovali na nasazení kamer s rozpoznáváním tváří v případě pátrání po unesených dětech či teroristech. Emocionálně vypjatý kontext způsobil naprosto radikální posun v postojích.

Dřívější silné obavy o soukromí šly stranou a více než tři čtvrtiny celkového vzorku (77,48 %) bez váhání zvolily možnost absolutní podpory („ano, v takových případech je to nutné“). Dalších 21,19 % dotázaných sice zachovalo jistou zdrženlivost, ale i ti nasazení biometrie podpořili, avšak s požadavkem předchozího soudního příkazu pro daný případ. Varianta striktního odmítnutí kvůli riziku zneužití spadla na naprosto marginální 1,32 % (pouhé 2 osoby ze 151).

Při bližším pohledu na jednotlivé generace se ukázalo, že tento fenomén masové akceptace zafungoval napříč celou společností, lišila se pouze míra benevolence k formálním pravidlům. Nejsilnější bezpodmínečnou podporu (86,67 %) projevili mladí dospělí ve věku 26–35 let, kde se logicky promítlo i to, že jde o věkovou kategorii, která nejčastěji zakládá rodiny. Velmi podobně a vstřícně reagovali i nejmladší respondenti (18–25 let) a osoby středního věku (36–50 let), kde plná podpora dosahovala hodnot od 73 do 77 %. Jedinou výraznější odchylku vykazovala jako obvykle nejstarší generace (51 a více let). I v této skupině sice ochota povolit kamerový dohled převládla, ale bezpodmínečný souhlas (54,55 %) se zde téměř vyrovnal s přísnějším požadavkem na soudní dohled, který vyžadovalo více než 45 % seniorů. Získaná data tak spolehlivě demonstrovala, že česká veřejnost byla ochotná obětovat své soukromí novým technologiím, avšak pouze v případech zjevných a nanejvýš závažných hrozeb.

Otázka č. 12 – Ovlivňuje přítomnost kamer na letišti nebo veřejných místech vaše chování?

Graf č. 12 – Vliv kamerových systémů na chování respondentů ve veřejném prostoru



(Zdroj: Vlastní šetření)

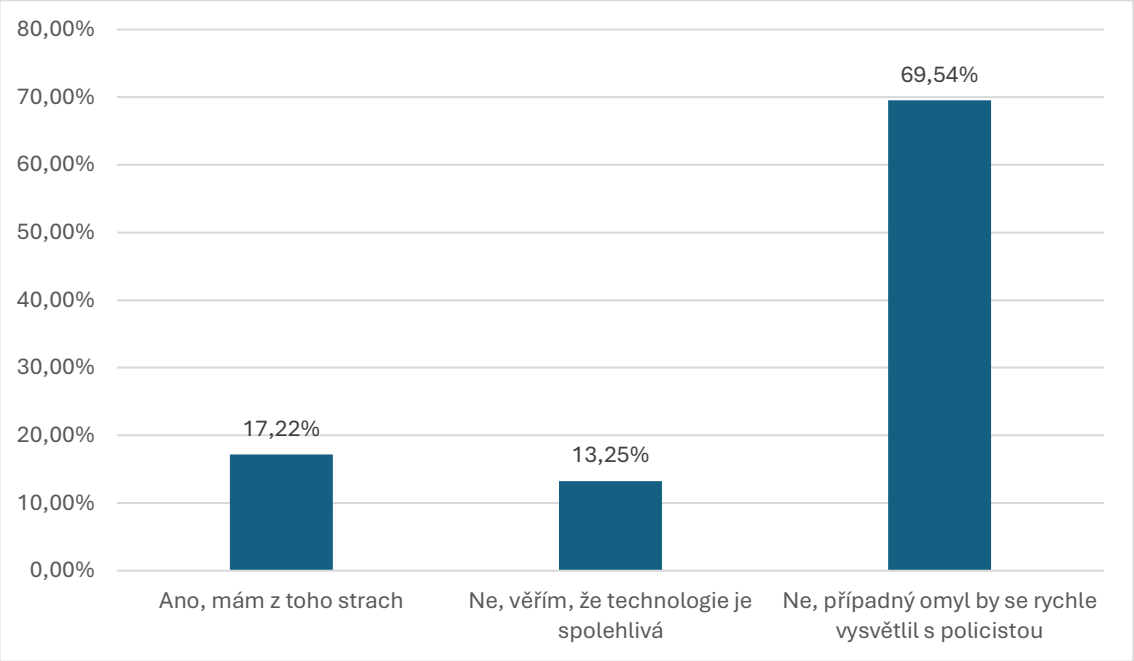
Dvanáctá otázka průzkumného šetření navazovala na teoretický koncept takzvaného mrazivého účinku (chilling effect) a zjišťovala, zda všudypřítomné kamery na rizikových místech, jakými jsou letiště, ovlivňovaly přirozené chování respondentů. Z výsledků jasně vyplynulo, že deklarované hrozby masového sledování se v reálném prožívání veřejnosti zatím příliš neodrážely. Drtivá většina (69,54 %) dotázaných uvedla, že kamery ve veřejném prostoru zcela ignorovala a chovala se přirozeně. Přibližně pětina vzorku (20,53 %) si sice sledování aktivně uvědomovala, avšak tento fakt u ní generoval pozitivní emoci v podobě vyššího pocitu bezpečí. Zásadní negativní dopad, tedy pocit tlaku a nutnost autocenzury vlastního chování, potvrdila pouze desetina osob (9,93 %).

Křížová analýza podle věku přinesla velmi překvapivé zjištění – odolnost vůči psychologickému tlaku kamer s rostoucím věkem lineárně stoupala. Zcela nejvyšší míru ignorance kamerových systémů vykazovala nejstarší generace nad 51 let (téměř 82 %), těsně následovaná osobami ve věku 36–50 let (více než 76 %). Naopak nejcitlivěji vnímaly vizuální dohled mladší ročníky. U nejmladší generace (18–25 let) vědomě registrovalo kamery bezmála 40 % osob, ačkoliv u nich tento dozor vedl primárně k pocitu bezpečí (29,82 %). Jedinou skupinou, u níž negativní mrazivý účinek dosáhl znatelnějších hodnot, se stali mladí dospělí (26–35 let), u kterých se pod tlakem kamerových systémů cítilo 15,56 % dotázaných. Výsledky tak jednoznačně potvrdily, že

pro převážnou část české společnosti představoval kamerový dohled natolik zavedený standard, že jeho omezující vliv na svobodné chování občanů byl minimální.

Otázka č. 13 – Měli byste strach, že vás takový systém omylem označí za hledanou osobu (tzv. falešný poplach)?

Graf č. 13 – Obavy respondentů z chybného označení systémem



(Zdroj: Vlastní šetření)

Závěrečná otázka průzkumného šetření zjišťovala, zda měli respondenti obavy z takzvaného falešného poplachu, tedy ze situace, kdy by je systém pro rozpoznávání tváří omylem označil za hledanou osobu. Zjištěná data poukázala na silný pragmatismus veřejnosti a důvěru v lidský faktor. Drtivá většina (69,54 %) dotázaných uvedla, že strach neměla, jelikož spoléhala na to, že by se případný omyl rychle vysvětlil s přítomným policistou. Možnost absolutní důvěry v samotnou technologii, u níž by respondenti spoléhali na její neomylnost, zvolilo pouze 17,22 % osob. Čistý strach z takové situace pak přiznalo zbylých 13,25 % z celkového vzorku.

Mezigenerační srovnání v tomto bodě přineslo jeden z nejzajímavějších paradoxů celého šetření. Zatímco v předchozích odpovědích projevovaly největší skepsi starší ročníky, strach z falešného poplachu a z něj plynoucí konfrontace s úřady rezonoval nejsilněji u nejmladší generace. Ve věkové skupině 18–25 let přiznala strach z chybného označení téměř čtvrtina osob (22,81 %), což představovalo suverénně nejvyšší hodnotu napříč vzorkem. Ve všech starších kategoriích nad 26 let se tato obava propadla pod hranici 10 %. Největší míru důvěry v neomylnost biometrických technologií

(„věřím, že technologie je spolehlivá“) naopak neprojevila nastupující generace, nýbrž osoby středního věku (36–50 let), kde si tuto možnost vybralo téměř 29 % respondentů. Data tak v samotném závěru potvrdila, že pro společenskou akceptaci biometrických systémů byla naprosto klíčová přítomnost lidského operátora (policisty), který pro občany představoval nezbytnou pojistku proti selhání stroje.

7 Praktický příklad - Letiště Václava Havla Praha

Tato kapitola představuje praktický příklad, který v rámci empirické části práce slouží pro komparaci s výsledky realizovaného průzkumného šetření. Jejím cílem je poskytnout reálný kontext fungování biometrické identifikace ve vysoce rizikovém bezpečnostním prostředí největšího mezinárodního letiště v České republice.

Z etického a metodologického hlediska je nutné transparentně uvést, že předkládaná analýza vychází primárně ze sekundárních veřejně dostupných zdrojů, jako jsou technické specifikace, oficiální zprávy Ministerstva vnitra ČR, mediální výstupy a soudní usnesení, případně z e-mailové konzultace s Policií ČR. Přímé terénní šetření v neveřejných a tranzitních prostorách letiště nebylo z logických bezpečnostních důvodů a z důvodu striktního režimu ochrany prvků kritické infrastruktury možné realizovat. Tato sekundární analýza však poskytuje plně dostačující a validní faktický základ pro následnou syntézu s postoji veřejnosti.

7.1 Automatizované brány e-Gate v praxi

Na mezinárodním Letišti Václava Havla v Praze je v rámci projektu automatizované kontroly ePasů nasazen systém Easy-GO, slangově označovaný jako e-Gate. Tyto samoobslužné brány jsou primárně určeny pro rychlé a spolehlivé strojové odbavení cestujících, přičemž na Terminálu 1 je jich umístěno devět v lokalitě příletů a osm v lokalitě odletů. Aby mohl cestující tento zrychlený proces využít, musí splnit několik přesně definovaných podmínek. Systém je zpřístupněn výhradně osobám starším 15 let, které jsou občany států Evropské unie, Norska nebo Švýcarska. Zcela nezbytným technickým předpokladem pro průchod je pak vlastnictví platného biometrického cestovního pasu, který obsahuje elektronický čip a je označen symbolem specifikace ICAO 9303.

Samotný systém e-Gate představuje komplexní technologickou sestavu koncových zařízení. Fyzicky se automatická brána skládá ze čtecího zařízení pasů, vstupních dvoukřídlých dveří z bezpečnostního skla, vnitřního uzavřeného prostoru a výstupních dveří s integrovanou biometrickou jednotkou. Zásadním bezpečnostním prvkem je 3D stereoskopická kamera umístěná v horním čelním panelu, jež spolehlivě detekuje přítomnost více osob ve vnitřním prostoru a brání tak neoprávněnému průchodu dalších jedinců. Celý proces je pro potřeby dohledu nepřetržitě monitorován přehledovou

kamerou, která přenáší obraz operujícímu policistovi, jenž má možnost v případě nestandardní situace do procesu zasáhnout.

Průběh samotného odbavení je plně automatizovaný a probíhá v několika na sebe navazujících úrovních. Poté, co cestující přiloží doklad na čtečku, systém nejprve provede optickou kontrolu bezpečnostních prvků pasu ve viditelném, ultrafialovém i infračerveném spektru a následně vyčte data z elektronického čipu. Poté se otevřou vstupní dveře a cestující přejde k výstupnímu terminálu, kde pohyblivá digitální kamera, jež se automaticky přizpůsobí výšce postavy, pořídí aktuální snímek obličeje. Tento takzvaný živý obraz je následně algoritmicky porovnán s referenční fotografií vyčtenou z čipu. Souběžně s touto biometrickou verifikací probíhá na pozadí lustrační kontrola osoby v policejním systému KODOX. Pokud jsou všechny tyto prověrky úspěšné, výstupní brána se otevře. Celý tento komplexní proces je přitom vysoce efektivní – průměrná doba hraniční kontroly je kratší než 18 sekund a typicky trvá pouhých 15 sekund.[74]

Z hlediska ochrany osobních údajů a obecných principů takzvaného Privacy by Design je u občanů Evropské unie zcela klíčovým prvkem celého procesu okamžité odstraňování zachycených biometrických stop. Vzhledem k přísným požadavkům evropského nařízení GDPR slouží živé snímky tváře, pořizované senzory uvnitř bezpečnostních bran, výhradně k jednorázové algoritmické verifikaci vůči čipu v pasu. Architektura samotného systému e-Gate je tedy z logiky věci a platné legislativy záměrně nastavena tak, že k žádnému trvalému či dlouhodobému ukládání těchto fotografií do policejních databází nedochází. Získaná data jsou bezprostředně po úspěšném průchodu cestujícího turniketem ihned a beze stopy smazána.

7.2 Kamerové systémy Policie ČR a vliv legislativy

Nasazení kamerových systémů s funkcí automatického rozpoznávání obličejů na Letišti Václava Havla v Praze představovalo průlomový bezpečnostní projekt. Jeho budování vycházelo z usnesení vlády č. 47/2015. Do zkušebního provozu byla technologie uvedena 15. června 2018, přičemž původní plán počítal s pokrytím tranzitního prostoru pomocí sta kamer. Následné testy prokázaly vysokou efektivitu, což vedlo Ministerstvo vnitra ČR v březnu 2019 k rozhodnutí o rozšíření infrastruktury o dalších 45 kamer. Tyto snímače byly umístěny do veřejně přístupných hal letiště

[74] HEJDUK, Marek. *Zákon o cestovních dokladech*. Praha: Wolters Kluwer, 2022. s. 14-21. ISBN 978-80-7598-467-8.

k informačním tabulím, kde se cestující přirozeně zastavují.[75] Z technického hlediska plnily kamery pouze funkci obrazových snímačů. Algoritmické rozpoznávání tváře probíhalo centralizovaně na vyhrazených policejních serverech. Pořízený biometrický obraz byl porovnáván s policejní databází zájmových a hledaných osob. Technologie umožňovala okamžitou identifikaci i zpětné dohledávání díky uchovávání biometrických otisků tváří po dobu třiceti dnů. Efektivitu řešení potvrdily policejní statistiky, podle kterých došlo mezi červnem 2018 a srpnem 2020 k 189 pozitivním identifikacím hledaných jedinců.[76]

Navzdory bezpečnostním přínosům čelil systém od počátku silné kritice ze strany lidskoprávních organizací. Technologie totiž plošně analyzovala tváře všech osob procházejících letištěm, což v roce 2019 představovalo přibližně 18 milionů cestujících. Kritici z organizace Iuridicum Remedium poukazovali na skutečnost, že český právní řád neobsahoval žádné explicitní povolení k plošnému biometrickému sledování v reálném čase. Policie navíc při spuštění systému nevypracovala posouzení vlivu na ochranu osobních údajů a zprovoznění obhájila pouhou ohlašovací povinností vůči Úřadu pro ochranu osobních údajů. Tento stav vytvářel výrazné legislativní a etické napětí.[77]

K zásadnímu zlomu došlo 1. srpna 2025, kdy Policie ČR musela systém automatické detekce obličejů dočasně zcela vypnout. Důvodem byla nová evropská legislativa – Nařízení o umělé inteligenci (AI Act) – a navazující novely českých zákonů. Nová právní úprava začala pro provoz biometrických systémů striktně vyžadovat takzvanou ex ante autorizaci, tedy výslovné předchozí povolení příslušného soudu.[78] Přerušení provozu představovalo pro policii citelnou ztrátu. Systém totiž od roku 2019 do června 2025 pomohl identifikovat a zadržet 155 hledaných osob. Společenskou nezbytnost technologie dokládala policie například případem ze září 2023, kdy biometrický systém umožnil včasné zadržení osoby podezřelé ze zvlášť závažné trestné činnosti proti lidské důstojnosti v sexuální oblasti zaměřené na děti. Přestože technologie

[75]PĚKNICOVÁ, Klára. Ministerstvo vnitra rozšíří zabezpečení Letiště Václava Havla o 145 kamer s automatickým rozpoznáváním obličejů. In: *Ministerstvo vnitra České republiky* [online]. 4. 3. 2019 [cit. 2026-03-2]. Dostupné z WWW: https://mv.gov.cz/clanek/ministerstvo-vnitra-rozsiri-zabezpeceni-letiste-vaclava-havla-o-145-kamer-s-automatickym-rozpoznavanim-obliceju.aspx.

[76] SCHIMMER, David. Systém detekce obličejů. In: *Policie České republiky* [online]. 23. 11. 2020 [cit. 2026-03-2]. Dostupné z WWW: https://policie.gov.cz/clanek/zverejnene-informace-2020-system-detekce-obliceju.aspx.

[77]TROJÁNEK, Hynek. TZ: Kamery rozpoznávající tváře na letišti v Praze. Jsou v souladu se zákonem? In: *Digitální svobody* [online]. 30. 11. 2021 [cit. 2026-03-2]. Dostupné z WWW: https://digitalnisvobody.cz/blog/2021/11/30/kamery-rozpoznavajici-tvare-na-letisti-v-praze-jsou-v-souladu-se-zakonem/.

[78]Policie: Rozpoznávání obličejů na letišti končí. Rozhodnout má soud. In: *Česká justice* [online]. 1. 8. 2025 [cit. 2026-03-2]. Dostupné z WWW: https://www.ceska-justice.cz/2025/08/policie-rozpoznavani-obliceju-na-letisti-konci/.

prokazatelně potírala kriminalitu, evropská regulace upřednostnila ochranu soukromí a provoz paralyzovala.[79]

Dne 30. prosince 2025 vydal Vrchní soud v Praze přelomové usnesení, kterým opětovné používání izolovaného systému biometrické identifikace povolil. Soud konstatoval, že ačkoliv jde o zásah do soukromí, je za striktních podmínek nezbytný a přiměřený riziku závažné trestné činnosti. Povolení bylo podmíněno robustními zárukami, konkrétně provozem ve zcela oddělené intranetové síti bez přístupu k internetu a s lidským dohledem, kdy každý pozitivní záchyt musí vizuálně ověřit dva pracovníci. Povolení soud vydal maximálně na dvanáct měsíců a biometrické záznamy umožnil uchovávat nejvýše 90 dnů.[80] Obnovení provozu koncem ledna 2026 nicméně vyvolalo kritiku právních expertů. Zástupci Iuridicum Remedium a akademické sféry upozornili, že plošné zařazování celých kategorií osob do referenční databáze může být v rozporu s AI Actem, jenž předpokládá individuální schvalování obdobně jako u odposlechů. Odborníci rovněž vyjádřili obavy z rozšiřování účelu (function creep), kdy by se stávající letištní povolení mohlo v budoucnu stát precedentem pro plíživé zavádění biometrického sledování do dalších veřejných prostor.[81]

7.3 Komparace reálné praxe s postoji veřejnosti

Závěrečná komparace syntetizuje reálné technologické a legislativní fungování biometrických systémů na Letišti Václava Havla s postoji a znalostmi české veřejnosti z realizovaného průzkumného šetření. Propojení těchto rovin odhalilo zásadní propast mezi chováním státu a informovaností občanů, ale zároveň i překvapivě silnou shodu mezi laickým morálním kompasem a rozhodovací praxí soudů.

Zásadním zjištěním je hluboký informační deficit ohledně nakládání s osobními údaji. Architektura bran e-Gate je striktně podřízena principu *Privacy by Design*, kdy systém živé snímky tváře po verifikaci s pasem okamžitě maže. Tento reálný stav však znalo necelých 12 % veřejnosti. Většina respondentů se mylně domnívala, že jsou fotografie dlouhodobě archivovány, což umocňovalo jejich celkovou ostražitost. Tato

[79] SCHÖN, David. Změny na pražském letišti. In: *Policie České republiky* [online]. 1. 8. 2025 [cit. 2026-03-2]. Dostupné z WWW: https://policie.gov.cz/clanek/zmeny-na-prazskem-letisti.aspx.
[80] Usnesení Vrchního soudu v Praze ze dne 30. 12. 2025, č. j. 0 Nc 1001/2025 - 25. In: *Veřejná databáze rozhodnutí* [online]. Ministerstvo spravedlnosti [cit. 2026-03-2]. Dostupné z WWW: https://rozhodnuti.justice.cz/rozhodnuti/?id=fdbfd3a4-e27d-4fe8-9562-48ac6a2e7aa8.
[81] KASÍK, Pavel. Soud povolil návrat AI detekce obličejů na pražské letiště. Detaily jsou tajné. In: *Seznam Zprávy* [online]. 25. 2. 2026 [cit. 2026-03-2]. Dostupné z WWW: https://www.seznamzpravy.cz/clanek/domaci-zivot-v-cesku-soud-povolil-navrat-kontroverzni-detekce-obliceju-na-prazske-letiste-299574.

neznalost skutečného postupu ochrany osobních údajů tak u mnohých generovala falešné představy a zbytečné obavy. Téměř 60 % dotázaných přiznalo obavy ze zneužití biometrických dat. Největší strach pramenil z hrozby kyberútoků a úniku dat (téměř 53 %), přičemž u generace nad 51 let se přidal i strach ze státního sledování.

Z komparace zřetelně vyplynulo, že tyto deklarované obavy nedokázaly převážit nad lidským pragmatismem. Jakmile byla do rovnice přidána úspora 30 minut čekání ve frontě, více než 82 % dotázaných by teoretickou hrozbu akceptovalo a automatickou bránu využilo. Zatímco pro mladé dospělé představovalo uživatelské pohodlí a rychlost odbavení absolutní prioritu (přes 71 %), u nejstarší generace tuto utilitární motivaci překvapivě nahrazovala pouhá technologická zvědavost a touha systém si vyzkoušet.

Obdobně propastný rozdíl se ukázal v otázce plošného kamerového sledování. Letiště muselo v srpnu 2025 kvůli nařízení AI Act dočasně vypnout systémy na detekci obličejů. Z dotazníku však vyplynulo, že pro více než tři čtvrtiny veřejnosti tato událost, představující milník v ochraně lidských práv, proběhla zcela bez povšimnutí. Zcela nejnižší povědomí o tomto kroku přitom panovalo na obou okrajích věkového spektra – u mládeže a u seniorů. Ochrana soukromí ve veřejném prostoru se navíc neukázala být absolutní prioritou. Mrazivý účinek (*chilling effect*), kdy by se lidé pod kamerami cítili omezováni, se u téměř 70 % osob nepotvrdil. Respondenti kamery zkrátka ignorovali, případně u nich vyvolávaly pocit bezpečí, zatímco zásadní negativní dopad v podobě nutnosti autocenzury vlastního chování potvrdila pouze necelá desetina dotázaných.

Nejvýznamnější průsečík představuje srovnání prosincového usnesení Vrchního soudu v Praze s postoji respondentů. Soud povolil návrat biometrických kamer pod dvěma podmínkami: využití výhradně pro pátrání po závažné trestné činnosti a nutnost striktního lidského dohledu. Tyto justiční požadavky naprosto přesně rezonovaly s vůlí veřejnosti. Nutnost lidského faktoru se ukázala jako primární pilíř důvěry. Téměř 70 % dotázaných nemělo strach z chybného označení systémem, protože spoléhali na rychlé vysvětlení omylu s přítomným policistou, a čistý strach z takové situace přiznalo jen zhruba 13 % osob. Zajímavým paradoxem přitom bylo, že největší obavy z falešného poplachu neměli senioři, nýbrž nejmladší respondenti do 25 let. V neomylnost samotné technologie věřilo pouze 17 % osob. Ostražitost soudů vůči plné automatizaci se tak exaktně protnula s lidskou intuicí.

Naprostá shoda nastala i u povoleného účelu sledování. K běžnému plošnému monitoringu se občané stavěli opatrně, avšak při modelové situaci pátrání po unesených dětech či teroristech dřívější obavy zcela padly. Přes 77 % respondentů vyjádřilo absolutní podporu kamerové detekce a dalších 21 % by systém podpořilo na základě

soudního příkazu. Soudní praxe tak přesně odráží vůli veřejnosti – ochotu obětovat část soukromí výměnou za ochranu před nejtěžšími hrozbami, ovšem výhradně pod neustálou lidskou a justiční kontrolou.

Závěr

Tato bakalářská práce poskytuje komplexní pohled na problematiku biometrické identifikace osob, a to od jejích technologických základů až po reálné vnímání těchto systémů českou společností. Autor konstatuje, že všechny cíle vytyčené v úvodu této práce, spočívající především v analýze postojů veřejnosti, posouzení bezpečnosti, spolehlivosti a přijatelnosti technologií a v jejich komparaci s praxí, byly na základě provedeného průzkumu úspěšně naplněny.

V teoretické části práce byly podrobně zmapovány samotné základy a historický vývoj biometrie. Text se věnoval analýze rozličných fyziologických i behaviorálních biometrických charakteristik, od tradiční daktyloskopie až po moderní systémy rozpoznávání tváře či analýzu DNA, a jejich uplatnění v každodenní praxi. Na tyto technologické základy následně navázalo zmapování složitého legislativního rámce, jemuž v současnosti dominuje nejen obecné nařízení GDPR, ale především evropský Akt o umělé inteligenci (AI Act), který plošné využití biometrických systémů bezpečnostními sbory na veřejných místech striktně reguluje. Závěr teoretické pasáže byl věnován palčivým etickým otázkám, rizikům spojeným s masovým sledováním a kybernetické bezpečnosti uchovávaných dat.

Vlastní průzkumné šetření ukázalo, že veřejnost posuzuje bezpečnost a přijatelnost těchto systémů spíše pragmaticky. Ačkoliv respondenti projevili obavy z kybernetických útoků a zneužití dat, dokážou tuto ostražitost potlačit, pokud jim technologie nabídne výrazný osobní benefit – typicky v podobě úspory času u automatizovaných kontrolních systémů. Přijatelnost kamerových systémů ve veřejném prostoru je pak u občanů vysoce závislá na účelu a na přítomnosti lidského faktoru. Veřejnost podporuje biometrické sledování při pátrání po závažných zločincích či unesených dětech, avšak spolehlivost samotné technologie zpochybňuje a jako pojistku proti algoritmickému omylu vyžaduje přítomnost člověka. Z pohledu autora je velmi zajímavým zjištěním, že tyto laické postoje do značné míry korespondují s nedávným usnesením Vrchního soudu v Praze, který návrat kamer na pražské letiště povolil za obdobně přísných podmínek. Teoretické obavy z takzvaného mrazivého účinku (*chilling effect*) se v průzkumu navíc výrazněji nepotvrdily.

Příklad z praxe v podobě Letiště Václava Havla posloužil jako zrcadlo pro reálnou informovanost obyvatelstva a odhalil značný informační deficit, který má celospolečenský přesah. Ačkoliv moderní systémy často respektují princip *Privacy by*

Design a data občanů po kontrole okamžitě mažou, podstatná část veřejnosti se domnívá, že jsou trvale archivována. Podle názoru autora je tento stav alarmující, neboť lidé se biometrických systémů státu obávají z nesprávných důvodů. Podobně nepozorovaně prošla u občanů i přelomová událost z roku 2025, kdy byly biometrické kamery kvůli nové legislativě plošně vypínány a omezovány.

Z těchto poznatků vyplývá i hlavní praktický přínos práce, který přesahuje zkoumaný praktický příklad a je aplikovatelný na jakékoliv budoucí rozšiřování biometrických technologií ve veřejném prostoru (např. na nádražích, v rámci konceptů Smart City či u jiných prvků kritické infrastruktury). Autor spatřuje hlavní problém v nedostatečné a netransparentní komunikaci státních institucí s občany. Pokud se mají tyto systémy v budoucnu úspěšně rozšiřovat, je nezbytné zavést srozumitelné vizuální informační kampaně přímo v místech jejich nasazení. Jasné upozornění, které občanům garantuje například okamžité smazání dat, by efektivně zmírnilo strach z plošného dohledu. Stejně tak je pro budoucí praxi kriticky důležité zachovat u bezpečnostních systémů princip lidského dohledu, bez něhož by plně automatizované sledování pravděpodobně narazilo na silný společenský odpor.

Závěrem lze shrnout, že česká veřejnost není vůči biometrické identifikaci a priori odmítavá a je ochotna přistoupit na kompromis mezi soukromím a ochranou před závažnými hrozbami. Vyžaduje však transparentnost a lidskou i justiční kontrolu. Přestože současná praxe a rozhodování soudů v České republice tyto požadavky v zásadě naplňují, bez adekvátní komunikace o tom veřejnost neví. I když tato práce nemohla postihnout veškeré aspekty rozsáhlého oboru biometrie, poskytuje ucelený pohled na to, jak se legislativní teorie a technologická praxe reálně potkávají s vnímáním občanů, a nabízí vodítko pro budoucí nasazování těchto systémů ve společnosti.

Seznam použitých zdrojů

Literární zdroje

1. BAČA, Ján et al. *Zákon o zpracování osobních údajů: praktický komentář*. Plzeň: Aleš Čeněk, 2020. 361 s. ISBN 978-80-7380-804-4.
2. BITTO, Ondřej. *Šifrování a biometrika aneb tajemné bity a dotyky*. 1. vyd. Kralice na Hané: Computer Media, 2005. 168 s. ISBN 80-86686-48-5.
3. BULLOCK, Justin B. et al. *The Oxford Handbook of AI Governance*. New York: Oxford University Press, 2024. 1096 s. ISBN 978-0-19-757932-9.
4. DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. [Brno: M. Drahanský], 2011. 294 s. ISBN 978-80-254-8979-6.
5. HEJDUK, Marek. *Zákon o cestovních dokladech*. Praha: Wolters Kluwer, 2022. 212 s. ISBN 978-80-7598-467-8.
6. JAIN, Anil K., Patrick J. FLYNN a Arun A. ROSS (eds.). *Handbook of biometrics*. New York: Springer, 2008. 556 s. ISBN 978-0-387-71040-2.
7. NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada, 2017. Právo pro praxi. 304 s. ISBN 978-80-271-0668-4.
8. PATTYNOVÁ, Jana. *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě : komentář*. Praha: Leges, 2018. Komentátor. 487 s. ISBN 978-80-7502-288-2.
9. POLČÁK, Radim et al. *Právo informačních technologií*. 2. vyd. Praha: Wolters Kluwer, 2024. Právní monografie. 988 s. ISBN 978-80-286-0059-4.
10. PORADA, Viktor, Dušan ŠIMŠÍK et al. *Identifikace osob podle dynamického stereotypu chůze*. Karlovy Vary: Vysoká škola Karlovy Vary, 2010. 311 s. ISBN 978-80-87236-01-7.
11. PORADA, Viktor. *Kriminalistické, forenzní a právní souvislosti identifikace osob podle funkčních a dynamických znaků*. Karlovy Vary: Vysoká škola Karlovy Vary, 2010. 174 s. ISBN 978-80-87236-02-4.
12. RAK, Roman, Václav MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. Profesionál. 664 s. ISBN 978-80-247-2365-5.
13. ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. Ostrava: VŠB-TU Ostrava, 2008. 58 s. [cit. 2025-12-21]. Dostupné z WWW: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/biometricke_metody.pdf.

14. ŠTĚDROŇ, Bohumír, Roman JAŠEK, Miroslav SVÍTEK et al. *Umělá inteligence a právo*. Plzeň: Aleš Čeněk, 2024. 233 s. ISBN 978-80-7380-947-8.
15. ŠTEINBACH, Miroslav et al. *Zákon o Policii České republiky: komentář*. 2. vyd. Praha: Wolters Kluwer, 2024. 340 s. ISBN 978-80-7676-830-7.
16. USTARAN, Eduardo. *European Data Protection Law and Practice*. Portsmouth: International Association of Privacy Professionals, 2018. 382 s. ISBN 978-0-9983223-5-3.
17. VANČO, Emil. Biometrie, biometrika - geneze, vývoj a současné pojetí. *Kriminalistika* [online]. 2005, roč. 38, č. 1, s. 5-20. [cit. 2025-12-20]. Dostupné z WWW: http://www.mvcr.cz/soubor/kriminalistika-archiv-2005-01-zip.aspx.
18. VÍTEK, Dominik. Kapitola I Obecná ustanovení. In: PATTYNOVÁ, Jana. *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě : komentář*. Praha: Leges, 2018. s. 23-46. ISBN 978-80-7502-288-2.

Právní předpisy a judikatura

1. ČESKO. Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: *Sbírka zákonů, Česká republika*. 2019, částka 47. Dostupné z WWW: https://www.e-sbirka.cz/sb/2019/110?zalozka=text.
2. Usnesení Vrchního soudu v Praze ze dne 30. 12. 2025, č. j. 0 Nc 1001/2025 - 25. In: *Veřejná databáze rozhodnutí* [online]. Ministerstvo spravedlnosti [cit. 2026-03-16]. Dostupné z WWW: https://rozhodnuti.justice.cz/rozhodnuti/?id=fdbfd3a4-e27d-4fe8-9562-48ac6a2e7aa8.

Elektronické zdroje

1. ČESKÁ SPOŘITELNA. Spořitelna umožní zřízení hlasové biometrie jen po telefonu a bez nutnosti návštěvy pobočky. In: *Česká spořitelna* [online]. 6. 4. 2020 [cit. 2026-01-8]. Dostupné z WWW: https://www.csas.cz/cs/o-nas/pro-media/tiskove-zpravy/2020/04/06/ceska-sporitelna-pomuze-klientum-v-karantene-a-umozni-jim-zrizeni-hlasove-biometrie-jen-po-telefonu.
2. DATAHELP. Čtečky otisků prstů u mobilů a jejich bezpečnost. In: *Datahelp* [online]. [cit. 2026-01-6]. Dostupné z WWW: https://www.datahelp.cz/clanky/ctecky-otisku-prstu-u-mobilu-a-jejich-bezpecnost/.

3. DLUBALOVÁ, Klára. Sněmovna schválila nový typ občanských průkazů s biometrickými údaji. In: *Ministerstvo vnitra ČR* [online]. [cit. 2026-02-13]. Dostupné z WWW: https://mv.gov.cz/clanek/snemovna-schvalila-novy-typ-obcanskych-prukazu-s-biometrickymi-udaji.aspx.
4. EVROPSKÁ KOMISE. AI Act. In: *Shaping Europe's digital future* [online]. Poslední aktualizace 27. 1. 2026 [cit. 2026-02-12]. Dostupné z WWW: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
5. EVROPSKÝ PARLAMENT. EU AI Act: first regulation on artificial intelligence. In: *European Parliament* [online]. 8. 6. 2023, poslední aktualizace 19. 2. 2025 [cit. 2026-02-12]. Dostupné z WWW: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.
6. EVROPSKÝ SBOR PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Pokyny 05/2022 k používání technologie rozpoznávání obličeje v oblasti prosazování práva* [online]. 2022. 54 s. [cit. 2026-02-20]. Dostupné z WWW: https://uoou.gov.cz/media/zahranici/dokumenty/schvalene-pokyny/pokyny-2022-05-k-pouzivani-technologie-rozpoznavani-obliceje-v-oblasti-prosazovani-prava.pdf.
7. HANZEL, Petr. Právní aspekty využívání biometrických dat v HR: GDPR, etika a balanční testy. In: *ARROWS advokátní kancelář* [online]. 14. 8. 2025 [cit. 2026-02-20]. Dostupné z WWW: https://arws.cz/novinky-v-arrows/pravni-aspekty-vyuzivani-biometrickych-dat-v-hr.
8. HYUNDAI. Hyundai Reveals World's First Smart Fingerprint Technology to Vehicle. In: *Hyundai Newsroom* [online]. 24. 12. 2018 [cit. 2026-01-6]. Dostupné z WWW: https://www.hyundai.news/uk/articles/press-releases/hyundai-reveals-worlds-first-smart-fingerprint-technology-to-vehicles.html.
9. CHLEBUS, Tomáš a Jakub DOSTÁL. *Nový zákon o zpracování osobních údajů*. In: *Epravo.cz* [online]. 30. 5. 2019 [cit. 2026-02-10]. Dostupné z WWW: https://www.epravo.cz/top/clanky/novy-zakon-o-zpracovani-osobnich-udaju-109312.html.
10. INTERNORM. Zámek na otisk prstu – proč ho chtít? In: *Internorm* [online]. 28. 10. 2020 [cit. 2026-01-6]. Dostupné z WWW: https://blog.internorm.cz/zamek-na-otisk-prstu-proc-ho-chtit/.

11. JIŘÍK, Pavel. The Future of Voice Assistants. In: *Phonexia* [online]. 25. 4. 2022 [cit. 2026-1-8]. Dostupné z WWW: https://www.phonexia.com/blog/the-future-of-voice-assistants/.

12. KASÍK, Pavel. Soud povolil návrat AI detekce obličejů na pražské letiště. Detaily jsou tajné. In: *Seznam Zprávy* [online]. 25. 2. 2026 [cit. 2026-03-2]. Dostupné z WWW: https://www.seznamzpravy.cz/clanek/domaci-zivot-v-cesku-soud-povolil-navrat-kontroverzni-detekce-obliceju-na-prazske-letiste-299574.

13. KIICHLE-GROSS, Becky. Advantages and disadvantages of biometrics. In: *Mitek* [online]. 7. 1. 2025 [cit. 2025-12-21]. Dostupné z WWW: https://www.miteksystems.com/blog/advantages-and-disadvantages-of-biometrics.

14. MOBBEEL. What is voice biometrics? In: *Mobbeel* [online]. [cit. 2026-01-8]. Dostupné z WWW: https://www.mobbeel.com/en/what-is-voice-biometrics/.

15. PĚKNICOVÁ, Klára. Ministerstvo vnitra rozšíří zabezpečení Letiště Václava Havla o 145 kamer s automatickým rozpoznáváním obličejů. In: *Ministerstvo vnitra České republiky* [online]. 4. 3. 2019 [cit. 2026-03-2]. Dostupné z WWW: https://mv.gov.cz/clanek/ministerstvo-vnitra-rozsiri-zabezpeceni-letiste-vaclava-havla-o-145-kamer-s-automatickym-rozpoznavanim-obliceju.aspx.

16. Policie: Rozpoznávání obličejů na letišti končí. Rozhodnout má soud. In: *Česká justice* [online]. 1. 8. 2025 [cit. 2026-03-2]. Dostupné z WWW: https://www.ceska-justice.cz/2025/08/policie-rozpoznavani-obliceju-na-letisti-konci/.

17. SHAIP. Jak sběr dat hraje klíčovou roli při vývoji modelů rozpoznávání obličeje. In: *Shaip* [online]. 17. 12. 2024 [cit. 2026-1-12]. Dostupné z WWW: https://cs.shaip.com/blog/data-collection-for-facial-recognition-models/.

18. SCHIMMER, David. Systém detekce obličejů. In: *Policie České republiky* [online]. 23. 11. 2020 [cit. 2026-03-2]. Dostupné z WWW: https://policie.gov.cz/clanek/zverejnene-informace-2020-system-detekce-obliceju.aspx.

19. SCHÖN, David. Změny na pražském letišti. In: *Policie České republiky* [online]. 1. 8. 2025 [cit. 2026-03-2]. Dostupné z WWW: https://policie.gov.cz/clanek/zmeny-na-prazskem-letisti.aspx.

20. SOARES, Joana. Velký bratr se dívá. Země EU včetně Česka rozšiřují sledování občanů. In: *Ekonomický deník* [online]. 18. 8. 2025 [cit. 2026-02-20]. Dostupné z WWW: https://ekonomickydenik.cz/eu-rozsiruje-sledovani-obcanu/.
21. TROJÁNEK, Hynek. TZ: Kamery rozpoznávající tváře na letišti v Praze. Jsou v souladu se zákonem? In: *Digitální svobody* [online]. 30. 11. 2021 [cit. 2026-03-2]. Dostupné z WWW: https://digitalnisvobody.cz/blog/2021/11/30/kamery-rozpoznavajici-tvare-na-letisti-v-praze-jsou-v-souladu-se-zakonem/.
22. ÚŘAD PRO PUBLIKACE EVROPSKÉ UNIE. Rules for trustworthy artificial intelligence in the EU. In: *EUR-Lex* [online]. Poslední aktualizace 11. 3. 2025 [cit. 2026-02-12]. Dostupné z WWW: https://eur-lex.europa.eu/EN/legal-content/summary/rules-for-trustworthy-artificial-intelligence-in-the-eu.html.

Seznam tabulek a grafů

Seznam příloh

Přílohy

Příloha I. – Dotazník[82]

Vnímání biometrické identifikace a její bezpečnosti

Dobrý den,

jmenuji se Josef Paleček a jsem studentem Vysoké školy evropských a regionálních studií (VŠERS). V rámci své bakalářské práce zpracovávám téma využití moderních technologií a biometrie (rozpoznávání tváře, otisky prstů) v bezpečnostní praxi, konkrétně na letištích.

Rád bych Vás požádal o vyplnění krátkého dotazníku, jehož cílem je zjistit, jak tyto technologie vnímáte Vy – zda dáváte přednost rychlému odbavení, nebo máte obavy o své soukromí.

Dotazník je zcela **anonymní** a jeho vyplnění Vám zabere maximálně **3–5 minut**. Získaná data poslouží výhradně pro účely mé bakalářské práce.

Předem Vám velice děkuji za Váš čas a ochotu.

* Označuje povinnou otázku

1. 1.Váš věk: *

Označte jen jednu elipsu.

- ◯ 18 - 25 let
- ◯ 26 - 35 let
- ◯ 36 - 50 let
- ◯ 51 a více let

[82] Vlastní zpracování

2. 2.Využíváte v běžném životě biometrické funkce (např. odemykání telefonu otiskem prstu nebo skenem obličeje)? *

Označte jen jednu elipsu.

- ◯ Ano, denně
- ◯ Ano, občas
- ◯ Ne, těmto technologiím nevěřím
- ◯ Ne, nemám k tomu vhodné zařízení

3. 3.Komu byste byli ochotni svěřit své biometrické údaje (sken tváře, otisk prstu)? * - Lze zvolit více možností.

Zaškrtněte všechny platné možnosti.

- ☐ Bance (např. pro vstup do aplikace)
- ☐ Výrobci telefonu (Apple, Samsung, Google)
- ☐ Státu/Policii (pro doklady a bezpečnost)
- ☐ Zaměstnavateli (pro vstup do práce)
- ☐ Nikomu

4. 4.Pokud byste na letišti mohli projít automatickou biometrickou bránou (tzv. E-Gate) a ušetřit tak 30 minut čekání ve frontě, využili byste to? *

Označte jen jednu elipsu.

- ◯ Rozhodně ano
- ◯ Spíše ano
- ◯ Spíše ne
- ◯ Rozhodně ne

5. 5.Co by pro Vás bylo hlavním důvodem pro využití automatické brány (E-Gate) při pasové kontrole na letišti? *

Označte jen jednu elipsu.

- Rychlost a úspora času (nechci čekat ve frontě)
- Vyšší pocit bezpečnosti (stroj je důkladnější než člověk)
- Soukromí / Nechuť komunikovat (je mi příjemnější jednat se strojem než s policistou)
- Technologická zvědavost (chci vyzkoušet, jak to funguje)

6. 6.Co se podle vás děje s vaší fotografií po průchodu automatickou bránou (pasová kontrola) na letišti? *

Označte jen jednu elipsu.

- Systém ji porovná s pasem a okamžitě smaže
- Fotografie se uloží do databáze letiště (např. na 30 dnů)
- Fotografie se trvale uloží do státní databáze pro sledování pohybu osob
- Nevím

7. 7.Máte obavy, že by vaše biometrická data mohla být zneužita? *

Označte jen jednu elipsu.

- Mám velké obavy
- Mám mírné obavy
- Nemám obavy, věřím zabezpečení
- Netrápím se tím

8. 8.Co by pro vás bylo hlavním důvodem, proč biometrii ODMÍTNOUT? *

Označte jen jednu elipsu.

- Strach z hackerů a úniku dat na internet
- Nedůvěra ve stát a sledování ("Velký bratr")
- Obava z technických chyb (že mě systém nepozná)
- Nemám důvod odmítnout.

9. 9.Věděli jste, že Policie ČR na Letišti Václava Havla v minulosti testovala systém na rozpoznávání tváří v davu, který byl v roce 2025 kvůli ochraně soukromí vypnut? *

Označte jen jednu elipsu.

- Ano, věděl/a jsem o tom
- Ne, to je pro mě nová informace.

10. 10.Jaký je váš postoj k využívání kamer na automatické rozpoznávání obličejů policií na místech se zvýšeným rizikem (letiště, nádraží, metro)? *

Označte jen jednu elipsu.

- Jsem PRO: Bezpečnost a boj proti kriminalitě a terorismu jsou důležitější než soukromí
- Jsem PROTI: Je to neoprávněný zásah do soukromí
- Nevadí mi to, POKUD se data ukládají jen v případě nálezu hledané osoby
- Nemám na to názor

11. 11.Souhlasili byste s nasazením rozpoznávání tváří, pokud by to prokazatelně pomohlo při pátrání po unesených dětech nebo teroristech? *

Označte jen jednu elipsu.

- Ano, v takových případech je to nutné
- Ne, riziko zneužití je příliš velké i tak
- Pouze na základě soudního příkazu pro konkrétní případ

12. 12.Ovlivňuje přítomnost kamer na letišti nebo veřejných místech vaše chování? *

Označte jen jednu elipsu.

- Ano, cítím se pod tlakem a hlídám si své chování
- Ano, ale cítím se bezpečněji.
- Ne, kamery nevnímám a chovám se přirozeně

13. 13.Měli byste strach, že vás takový systém omylem označí za hledanou osobu (tzv. falešný poplach)? *

Označte jen jednu elipsu.

- Ano, mám z toho strach
- Ne, věřím, že technologie je spolehlivá
- Ne, případný omyl by se rychle vysvětlil s policistou

Příloha II. – Online odkaz na dotazník

https://forms.gle/9KwU25qksatQNGJFA