Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

Návrh implementace přístupového systému na sportovní akce

Diplomová práce

2023 Bc. Šárka Razimová

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Šárka Razimová**
Osobní číslo:	**E21714**
Studijní program:	**N0688A140007 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Návrh implementace přístupového systému na sportovní akce**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je navrhnout implementaci vybraného přístupového systému v konkrétním sportovním prostředí.

Osnova:
- Rešerše stávajícího stavu přístupových systémů.
- Průzkum akceptace nového přístupového systému veřejností.
- Návrh implementace vybraného přístupového systému v konkrétním sportovním prostředí.

Rozsah pracovní zprávy: **Cca 50 stran.**
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

BURDA, K. *Základy elektronických zabezpečovacích systémů*. Brno: Akademické nakladatelství CERM, 2017. ISBN 978-80-7204-967-7.
DRAHANSKÝ, M., ORSÁG, F. *Biometrie*. [Brno: M. Drahanský], 2011. ISBN 978-80-254-8979-6.
Kyncl, J. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-80-260-7115-0.
MICHAEL, K., MICHAEL, M. G. *Innovative automatic identification and location-based services: from bar codes to chip implants*. Hershey, PA: Information Science Reference, c2009. ISBN 978-1-59904--795-9.
ŠTĚDROŇ, B. *Právo a umělá inteligence*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2020. ISBN 978-80-7380-803-7.

Vedoucí diplomové práce: **doc. Ing. Miloslav Hub, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání diplomové práce: **1. září 2022**
Termín odevzdání diplomové práce: **30. dubna 2023**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

RNDr. Ing. Oldřich Horák, Ph.D. v.r.
vedoucí ústavu

V Pardubicích dne 1. září 2022

Prohlašuji:

Práci s názvem Návrh implementace přístupového systému na sportovní akce jsem vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 28. 4. 2023

Šárka Razimová v. r.

PODĚKOVÁNÍ

Tímto bych ráda poděkovala svému vedoucímu práce doc. Ing. Miloslavu Hubovi, Ph.D., za jeho vstřícnost, pomoc a cenné rady, které mi pomohly při tvorbě této diplomové práce. Za skvělou spolupráci také děkuji Ing. Petru Mazánkovi ze společnosti Enigoo. Nakonec bych chtěla poděkovat své rodině, která mě po celou dobu studií podporovala.

ANOTACE

Tato diplomová práce popisuje přístupové systémy využívající biometrické metody. Teoretická část obsahuje rešerši přístupových systémů a jednotlivých biometrických metod. Dále práce analyzuje současné využití biometrie na veřejných místech v České republice i v zahraničí. Součástí práce je průzkum akceptace zavedení nového přístupového systému v konkrétním sportovním prostředí. Závěrečná část se zabývá návrhem implementace přístupového systému a analýzou aktuálního právního stavu s tímto systémem souvisejícím.

KLÍČOVÁ SLOVA

biometrie, biometrické systémy, přístupové systémy, rozpoznávání obličeje

TITLE

Proposal for the implementation of an access system for sports events

ANNOTATION

This thesis describes access systems using biometric methods. The theoretical part contains research of access systems and individual biometric methods. Furthermore, the work analyzes the current use of biometrics in public places in the Czech Republic and abroad. Part of the work is a survey of the introduction of a new access system in a specific sports environment. The final part deals with the proposal for the implementation of the access system and the analysis of the current legal status related to this system.

KEYWORDS

biometrics, biometric systems, access systems, facial recognition

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

ACS	Přístupové a docházkové systémy
CMOS	Kapacitní čtečka
ČR	Česká republika
DF	Dokazovací faktor
DPH	Daň z přidané hodnoty
EKV	Elektronická kontrola vstupu
EU	Evropská unie
FAR	False Accept Rate
FRR	False Reject Rate
FTA	Failure To Acquire
GDPR	Obecné nařízení o ochraně osobních údajů
HW	Hardware
ID	Identifikátor
OF	Ověřovací faktor
Sb.	Sbírka zákonů
ÚOOÚ	Úřad pro ochranu osobních údajů
2D	Dvourozměrný/dvoudimenzionální
3D	Trojrozměrný/trojdimenzionální

ÚVOD

Technologie využívající biometrické metody se stávají běžnou součástí našich životů. S ověřováním totožnosti na základě biometrických charakteristik se setkáváme na nejrůznějších místech u nás i v zahraničí, přičemž mnohdy si ani neuvědomujeme, kde všude je biometrie využívána. Biometrické metody jsou považovány za jedny z nejspolehlivějších metod ověření identity člověka, a proto jsou nasazovány i pro kontrolu vstupu do střežených oblastí. Ověření osoby na základě charakteristik obličeje využívají např. skiareály, letiště či stavební firmy. V rámci zvýšení bezpečnosti při pořádání hromadných sportovních akcí v zahraničí nachází biometrie své uplatnění i na fotbalových stadionech, v multifunkčních halách apod. V České republice se ve sportovním prostředí s technologiemi využívajícími biometrické metody v tuto chvíli nesetkáme.

Cílem této diplomové práce je provedení analýzy současného stavu přístupových systémů, realizace výzkumu zaměřeného na akceptaci nového přístupového systému ve vybraném sportovním prostředí a návrh implementace možné podoby tohoto systému.

První část práce popisuje druhy přístupových systémů a představuje jednotlivé biometrické metody, které se k ověřování identity osob využívají. Dále je provedena analýza veřejných míst v České republice i v zahraničí, na kterých se využívá metoda rozpoznávání obličeje. Ve druhé části práce je proveden výzkum zaměřený na zjištění akceptace nového přístupového systému veřejností, konkrétně hokejových fanoušků vybraného českého extraligového hokejového klubu. Stěžejní kapitola práce specifikuje požadavky na nový přístupový systém, analyzuje možnou podobu systému a na základě multikriteriálního rozhodování volí vhodné řešení. Závěrečná kapitola popisuje právní omezení týkající se využití biometrických metod.

1 PŘÍSTUPOVÉ SYSTÉMY

Přístupové a docházkové systémy (dříve známé pod zkratkou ACS) jsou dnes souhrnně označovány pojmem Elektronická kontrola vstupu (EKV). V zahraničí se můžeme setkat s pojmy Electronic Access Control System či Physical Access Control System. Elektronická kontrola vstupu je elektronický systém, který slouží k automatizovanému řízení vstupů v kontrolované oblasti. Vstupem rozumíme například turnikety, dveře či branky. K systémům EKV lze připojovat detektory a signalizační prvky poplachového zabezpečovacího systému, což může zvýšit bezpečnost kontrolované oblasti i komfort uživatelů. [2] Obvykle se přístupové systémy skládají ze senzorů, terminálů, rozhodovacích modulů, komunikační sítě a jedné či více databází. Součástí systému jsou i tzv. měkké prvky, tedy uživatelé, zásady a postupy či struktura řízení. [33]

1.1 Princip přístupových systémů

O tom, jak se bude systém chovat, rozhoduje tzv. autorita. Autorita určuje, kdo může dané vstupy používat a kdy je může používat, případně definuje i způsob použití. Prvotní fází celého procesu je autorizace. Při autorizaci je osobě přidělen unikátní identifikátor (identita) – ID, pod níž je osoba v systému vedena. Dále je stanovena dvojice ověřovací faktor OF a dokazovací faktor DF. Údaje ID a OF autorita uloží do systému, DF zůstává k dispozici dané osobě. V běžném životě je běžným identifikátorem např. rodné číslo, v EKV systémech se nejčastěji používají tzv. Wiegandova slova. Původně mělo Wiegandovo slovo délku 26 bitů (dnes už i např. 34 nebo 37 bitů) a skládá se ze sekvence bitů FC_1 až FC_8, která slouží jako identifikátor organizace, a posloupnosti bitů CN_1 až CN_{16}, která označuje číslo karty v dané organizaci. Wiegandovo slovo dále tvoří paritní bity SP (paritní bit první poloviny slova) a LP (paritní bit druhé poloviny slova). K výpočtu bitu SP využíváme techniku sudé parity, tedy jeho hodnota je nastavena tak, aby byl počet jedničkových bitů v první polovině slova sudý. Paritní bit LP využívá techniku liché parity, počet jedničkových bitů v druhé polovině slova je tedy lichý. [2], [28]

Aby mohla být spolehlivě určena identita osoby, je provedena identifikace, jejímž cílem je zjištění identifikátoru ID žadatele. Identitu můžeme zjistit bez důkazu či s důkazem. Při identifikaci bez důkazu žadatel svoje ID systému jednoduše sdělí a systém si dále jeho tvrzení nijak neověřuje. V EKV systémech se z bezpečnostních důvodů používá identifikace s důkazem (dokazováním identity), přičemž tento proces nazýváme autentizace. Autentizaci žadatelů provádí autentizátor, jehož funkci plní řídící jednotka EKV či terminál EKV. V praxi se poměrně často setkáváme s integrovaným řešením EKV, kdy řídící jednotka a terminál tvoří pouze jedno zařízení. Pokročilejším provedením jsou systémy, ve kterých jsou řídící jednotka i terminál integrální součástí vstupu. V průběhu procesu autentizace získá autentizátor potřebná data, ze kterých následně pomocí OF zjišťuje, zda žadatel vlastní příslušný DF. Jedná-li se například o autentizaci otiskem prstu, jsou autentizačními údaji data popisující sejmutý otisk prstu. Následně je porovnán tento DF s OF uživatele. Jestliže je autentizace úspěšná, řídící jednotka z přístupového seznamu zjistí, zda má žadatel udělena práva použít přístupový systém v daný čas. V případě kladné odpovědi řídící jednotka vyšle vstupu příkaz k otevření/odemčení. V opačném případě se stav v kontrolované oblasti nezmění. [2], [28]

1.2 Autentizační metody

Při procesu autentizace rozlišujeme, zda je dokazovacím faktorem rys či informace a zda je nosičem dokazovacího faktoru osoba či předmět. Dle toho klasifikujeme autentizační metody do 4 tříd, tyto třídy stručně představuje Tabulka 1. [2]

Tabulka 1: Autentizační metody

	Nosičem DF je osoba	Nosičem DF je předmět
DF je rys	Biometrie	Průkaz
DF je informace	Heslo	Hardware

Zdroj: vlastní zpracování dle [2]

Autentizace pomocí rysů je založena na faktu, že je osoba či předmět vlastníkem nepadělatelných a unikátních rysů. U osob je autentizace prováděna biometrií (otisk prstu, dlaně, rozpoznání obličeje, rozpoznání hlasu aj.). U předmětů prokazujeme identitu pomocí průkazu. Pokud je dokazovacím faktorem informace a nosičem je osoba, žadatel se prokazuje znalostí tajné informace (heslem). Jestliže je DF informace a nosičem předmět, žadatel se prokazuje vlastnictvím předmětu, který tajnou informaci obsahuje. Předmětem je běžně hardware ve formě smartphonu nebo mikroprocesorové karty. [2], [33]

Při autentizaci heslem osoba zadává heslo pomocí numerické klávesnice. Heslo má obvykle podobu PINu (čtyř- až osmimístná posloupnost číslic). PIN je osobě přidělen autoritou a musí být unikátní. Po zadání hesla prostřednictvím klávesnice terminálu je předána tato informace řídící jednotce, která ji vyhledá v přístupovém seznamu. V řádku, který odpovídá hodnotě PINu, nalezne příslušná práva žadatele. Výhodou této metody jsou nižší náklady na pořízení a provoz oproti ostatním metodám. Naopak nevýhodou je vysoká zranitelnost. Autorita musí zabránit použití odhadnutelných hesel a zajistit jejich dostatečnou délku. S rostoucí délkou hesla je ovšem spojena hrozba zapomenutí hesla oprávněnou osobou. Také zde vyvstává hrozba možného odpozorování hesla. [2]

U autentizace průkazem předpokládáme existenci unikátního, nepadělatelného předmětu. Takový předmět je vydávám autoritou v rámci procesu autorizace a je s danou osobou jednoznačně spjat. Při autentizaci žadatel předkládá průkaz autentizátorovi, který následně ověřuje pravost předmětu (za pomoci holografických prvků, reliéfu atd.). Tento způsob autentizace se používá na místech, kde je autentizátorem osoba, v praxi se většinou jedná o člena ostrahy objektu. Aby se zamezilo možnému zneužití průkazu, je možné zavést dvoufaktorovou autentizaci. Průkaz může být v takovém případě opatřen fotografií, přičemž autentizátor nejprve ověří pravost průkazu a následně ověří shodu obličeje žadatele s fotografií z průkazu. Tím je zamezeno zneužití průkazu neoprávněnou osobou. Nakonec jsou podle ID žadatele zjištěna jeho přístupová práva a žadateli je přístup povolen nebo odmítnut. [2]

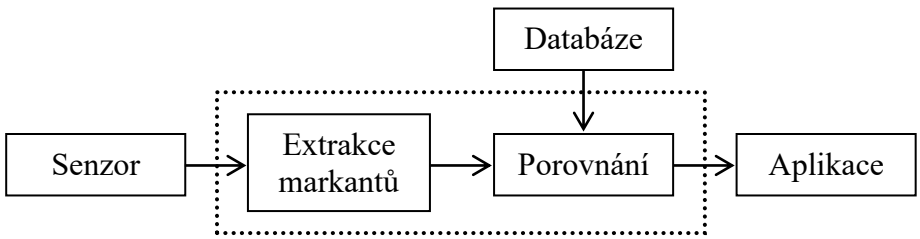
Autentizace hardwarem je založena na vlastnictví hardwarového zařízení, které obsahuje tajnou informaci. Na začátku procesu, při autorizaci, žadatel obdrží ID a stanovený typ autentizačního hardwaru. Tento hardware obsahuje kryptografický klíč, který slouží jako dokazovací faktor. Ověřovacím faktorem je stejný klíč nebo jiný klíč, díky kterému můžeme ověřit, že se v daném hardwaru nachází klíč náležící osobě s ID, které je shodné s Wiegandovým slovem. Nevýhodou této metody je možnost ztráty, zcizení či zapomenutí hardwaru. V případě zcizení má útočník umožněn vstup do kontrolované oblasti. Řešením může být využití vícefaktorové autentizace. [2], [38]

Posledním typem autentizace je autentizace pomocí biometrie. Biometrii lze zjednodušeně chápat jako čísly vyjádřitelnou charakteristiku člověka. Ověřovacím faktorem je datový obraz určité charakteristiky (např. obraz papilárních linií). Dokazovacím faktorem jsou pak unikátní charakteristiky dané osoby. Ověření probíhá tak, že si žadatel nechá při autorizaci sejmout obraz určitého rysu, a autorita ho následně uloží jako šablonu do terminálu. Při následném pokusu o vstup do kontrolované oblasti je snímačem sejmut otisk rysu a je porovnán s uloženou šablonou. [28]

2 BIOMETRICKÉ METODY

Biometrie označuje automatizované rozpoznávání osob na základě jejich unikátních charakteristických rysů. Biometrické metody jsou považovány za bezpečnější a pohodlnější způsob identifikace osob oproti ostatním starším metodám. [48]

Biometrický systém se skládá ze dvou částí. První částí je registrační modul, který zajišťuje autorizaci. Druhou částí je modul verifikační, který zajišťuje autentizaci. Součástí obou modulů je biometrický senzor, díky kterému je získán biometrický vzorek, který zajišťuje převod vzorku do digitální podoby. Dále oba moduly obsahují biometrický markant, tedy již získané charakteristiky ze vstupního vzorku. Charakteristiky vystupující z registračního modulu jsou uloženy do databáze. Oproti tomu charakteristiky vystupující z verifikačního modulu již nejsou ukládány do databáze, ale jsou porovnávány s údaji v databázi. V moderních přístupových systémech jsou zpravidla oba moduly součástí jednoho zařízení. [5], [24] Zjednodušené znázornění biometrického systému zobrazuje Obrázek 1.



Obrázek 1: Biometrický systém

Zdroj: vlastní zpracování dle [5]

2.1 Dělení biometrických systémů

Biometrické systémy můžeme dělit podle několika hledisek. První hledisko zohledňuje typ biometrických vlastností, se kterými systém pracuje. Vlastnosti dělíme na anatomické/fyziologické a behaviorální. Anatomické vlastnosti se týkají vnější podoby člověka. Do této kategorie řadíme obličej, sítnici oka, duhovku oka,

otisk prstu a dlaně, geometrii ruky, termogram obličeje a ruky, dentální obraz, snímek nehtu, tvar ucha či DNA. Anatomické vlastnosti nelze příliš snadno ovlivnit. [37], [48]

Druhou skupinou jsou vlastnosti behaviorální, týkající se chování osob, které jsou podmíněné nějakou akcí dané osoby. V rámci této skupiny zkoumáme chůzi, dynamiku podpisu, dynamiku stisku kláves, mimiku obličeje a hlas/řeč. Oproti vlastnostem anatomickým je poměrně snadné tyto vlastnosti ovlivnit (vzorky jednotlivých snímání se mohou lišit). [37], [48]

Další hledisko dělí biometrické systémy na unimodální a multimodální. Unimodální systém pracuje s právě jednou biometrickou vlastností. Jejich výhodou jsou nižší pořizovací náklady, nevýhodou pak nižší spolehlivost oproti systémům multimodálním. Tyto systémy se v praxi používají nejvíce. [5]

Multimodální biometrické systémy pracují s více biometrickými vlastnosti (např. rozpoznání otisku prstu a obličeje zároveň) nebo s více příznaky jedné vlastnosti (např. dynamické a statické vlastnosti podpisu). V tomto případě jsou pořizovací náklady vyšší, vyšší je i spolehlivost rozpoznání. [5]

2.2 Charakteristiky biometrických vlastností

Charakteristiky biometrických vlastností jsou důležitým aspektem při výběru konkrétního biometrického systému. Základních charakteristik je celkem sedm. Jsou to [5]:

1. univerzalita – všechny osoby by měly mít danou vlastnost,
2. jedinečnost – biometrická vlastnost musí být unikátní, stejnou vlastnost nemohou mít 2 lidé zároveň,
3. konstantnost – vlastnost se s časem nemění,
4. získatelnost – vlastnost musí být kvantitativně měřitelná,
5. akceptace – ochota lidí týkající se snímání dané vlastnosti,
6. odolnost proti falšování – snadnost vytvoření podvrhu biometrické vlastnosti,
7. finanční stránka – náklady na pořízení systému.

Tabulka 2 popisuje jednotlivé biometrické vlastnosti ve vztahu s uvedenými charakteristikami. Význam symbolů charakteristik biometrických vlastností v tabulce značí: ↑ vysoká, ↓ nízká, ○ střední.

Tabulka 2: Biometrické vlastnosti

	Univerzalita	Jedinečnost	Konstantnost	Získatelnost	Akceptace	Odolnost proti falšování	Finance
Obličej	↑	↓	○	↑	↑	↓	↓
Otisk prstu	○	↑	↑	○	○	↑	↓
Geometrie ruky	○	○	○	↑	○	○	○
Duhovka oka	↑	↑	↑	○	↓	↑	↑
Sítnice oka	↑	↑	○	↓	↓	↑	↑
Podpis	↓	↓	↓	↑	↑	↓	↓
Hlas	○	↓	↓	○	↑	↓	↓
Termogram	↑	↑	↓	↑	↑	↑	↑

Zdroj: vlastní zpracování dle [5]

K dalším důležitým aspektům můžeme dále řadit např. spolehlivost, tedy jak je řešena situace, pokud dojde k zestárnutí, osoba má zranění, použila brýle, výrazný make-up, došlo ke změně osvětlení atd. Při výběru systému bereme ohled i na údržbu systému, provedení, anonymitu, dostupnost aj.

Výhody nasazení biometrických metod:

- vyšší úroveň zabezpečení a bezpečí oproti ostatním metodám,
- charakteristika nemůže být zapomenuta či ztracena,
- její přenesení (zfalšování) je poměrně složité,
- působí preventivně proti útokům,
- zvyšuje pohodlí uživatele (není nutné si nic pamatovat nebo strážit přístupový průkaz či hardware).

Nevýhody nasazení biometrických metod můžeme spatřovat v:

- omezení soukromí,
- nepřesnosti některých biometrických systémů,
- vyšších pořizovacích nákladech v porovnání s ostatními metodami,
- právní problematice uchování biometrických údajů,
- v krajních případech je ověření uživatele pomocí biometrie znemožněno – poranění, některé typy nemocí aj.

2.3 Otisky prstů

Biometrické metody, při kterých je využíván otisk prstu, jsou postaveny na předpokladu, že na prstech mají lidé tzv. papilární linie, což jsou vystupující reliéfy kůže. Tyto linie jsou u každého člověka jiné. Jestliže papilární linie graficky znázorníme, mluvíme o otisku prstu. Otisky prstů se zabývá nauka zvaná daktyloskopie čili nauka o obrazcích papilárních linií na vnitřní straně článků, na dlaních a chodidlech. [37]

Na vznik a existenci papilárních obrazců se vztahuje několik zákonitostí. První zákonitost říká, že na světě nejsou dvě osoby, které by měly stejné obrazce papilárních linií. I proto se otisky prstů využívají v kriminalistice. Druhá zákonitost říká, že jsou obrazce papilárních linií po celý život prakticky neměnné. Výjimkou je vznik vráseček stárnoucí kůže ve vysokém věku a různá zranění či porušení spodní vrstvy kůže, kdy již nedochází k obnově papilárních linií. S tím souvisí poslední zákonitost o relativní neodstranitelnosti papilárních linií. Tato zákonitost říká, že pokud dojde k narušení pouze svrchní vrstvy kůže (sedřením, seříznutím i spálením), dojde k odstranění linií pouze krátce, do zahojení zranění. Obnova linií nenastane pouze v případě porušení zárodečné vrstvy kůže. [22], [37]

Aby bylo zabráněno pokusu o předložení falešného otisku prstu, kontroluje většina biometrických zařízení i některé fyzické vlastnosti. Mezi nejběžnější metody patří měření teploty, ačkoli se tato metoda ukazuje jako ne příliš vhodná. Teplota prstů se totiž může pohybovat v rozmezí 25 °C až 37 °C, mohou ji

ovlivnit podmínky okolního prostředí a v rámci snímání lze zaznamenat její kolísání. Obdobná negativa má i metoda měření odporu/vodivosti, protože i tato vlastnost je ovlivněna okolní teplotou, fyzickým i psychickým stavem dané osoby atd. Dalším způsobem ověření živosti je kontrola změn při přítlaku. Tato metoda vychází z předpokladu, že při přiložení prstu k ploše senzoru dochází ke změně tloušťky papilárních linií (tj. při zvýšení přítlaku prstu se papilární linie roztahují do stran). Také se kontroluje barva pozadí bříška, která se při větším tlaku mění. Poměrně účinnou metodou je měření pulsu. Pumpování srdce způsobuje objemové změny v žilách a tepnách, což způsobuje pulzování povrchu kůže. Toto pulzování není ovšem pro lidské oko postřehnutelné, na rozdíl od moderních technologií. Proto se v některých senzorech nachází i laser, který je schopný pulzování detekovat. Pro detekci falešného či amputovaného prstu je vhodná metoda založena na principu oxidaci krve. V těle vždy koluje krev okysličená i neokysličená, přičemž oba typy lze pomocí různých vlnových délek infračerveného záření u živého prstu detekovat. U falešného prstu nelze detekovat ani okysličenou, ani neokysličenou krev, u amputovaného prstu lze detekovat pouze neokysličenou krev. [5]

K ověření otisků prstů se využívají čtečky/snímače, které mohou být optické, kapacitní, tepelné a ultrazvukové. Nejvíce nasazované jsou čtečky optické, protože je lze pořídit i za poměrně nízké ceny. Snímač v těchto čtečkách má podobu digitálního fotoaparátu, který pořizuje vizuální obraz přiloženého prstu. Nevýhodou je, že jsou pořízené hodnoty ovlivněny např. znečištěnými prsty a navíc není příliš náročné tuto technologii oklamat. Kapacitní čtečky (tj. CMOS čtečky) nevyužívají k přečtení otisku prstu světlo, nýbrž kondenzátory, takže je obraz otisku vytvořen za pomocí elektrického proudu. Výhodou kapacitních čteček je, že je při ověřování vyžadován skutečný tvar otisku prstu, ne pouze vizuální obraz, jak je tomu u optických čteček. Díky tomu je oklamání čtečky těžší. Nevýhodou CMOS čteček je cena, která je oproti optickým čtečkám vyšší. Tepelné čtečky snímají rozdíly teplot mezi hřebeny a údolími prstů. Tepelné čtečky bývají nákladné, spotřebovávají více energie a výkonu. Posledním

a nejnovějším typem jsou ultrazvukové čtečky. Ultrazvukové snímače používají vysokofrekvenční zvukové vlny, které pronikají do kůže. Díky tomu jsou schopné přečíst i špinavý nebo poškozený otisk. Tento druh čteček je nákladný, ale je poměrně přesný a těžko oklamatelný. [12]

2.4 Geometrie ruky

Rozpoznávání ruky se od rozpoznávání otisků prstů poměrně liší. V případě rozpoznávání rukou je zachycován trojrozměrný obraz, který zachycuje například délky a šířky prstů, jejich tloušťku, zakřivení i jejich relativní umístění. Čtečka se tedy nezabývá otisky prstů či jinými povrchovými detaily ruky, nýbrž porovnává geometrické údaje o tvaru ruky jak z pohledu shora, tak i z pohledu bočního. [24]

Nejnovější 3D (trojrozměrné) skenery dokážou snímat desítky bodů geometrických charakteristik během pouhých pár vteřin. Pro osvícení se při skenování obvykle používají infračervené LED diody. Dále biometrické systémy obsahují soustavu zrcadel, která odráží obraz do snímací kamery. Díky tomu můžeme využít třírozměrného skenování, hmotnost a rozměry celého zařízení se mohou snížit až o polovinu. Některé čtečky mají na svých plochách umístěny fixační kolíčky, jimiž je pokaždé zajištěna stejná poloha ruky. [37]

Typicky můžeme na systémy ověřující geometrii ruky narazit ve zdravotnictví, věznicích, skladech, výrobních závodech, bezpečnostních a IT pracovištích, na hraničních kontrolách atd. Nejvíce se však nasazují v kombinaci s mechanickými a elektronickými prvky pro kontrolování přístupu do objektů. Čtečky mohou být nasazeny samostatně anebo mohou být síťově propojeny, takže jsou schopné ovládat velké množství vstupů najednou. [37], [48]

Výhodou pořizování geometrie ruky oproti otiskům prstů je především rychlejší ověření (ověření ruky zabere zpravidla méně času než ověření otisku). Uložený geometrický vzor také zabírá méně úložného prostoru v systému. [24]

Z pohledu psychologické akceptovatelnosti je tato metoda pro uživatele přívětivější než některé ostatní metody (ověření sítnice/duhovky, otisk prstu). [37]

Naopak nevýhodou je nutnost kvalitního zápisu geometrie do systému kvůli potenciálním chybám. Proto některé systémy vyžadují několikanásobné naskenování ruky, aby mohly být hodnoty skenování zprůměrovány a nedošlo k chybnému odmítnutí. [24]

2.5 Rysy oka

Identifikace osob podle charakteristik oka je velmi efektivní, ale poměrně nová metoda. První patent, který byl spojen s automatizovaným rozpoznáním na základě duhovky oka, byl registrován až roku 1994. [16] V případě lidského oka můžeme rozpoznávání zaměřit hned na několik jeho částí – nejvíce se metody zaměřují na sítnici a duhovku, dále pak například na rohovku či cévy na bělimě. Výhodou rysů oka je především jejich unikátnost, protože ani jednovaječná dvojčata nemají tyto rysy shodné. Prvky uvnitř oka jsou také dobře chráněny proti poškození a není lehké je nepovolaně získat a zneužít. [5]

2.5.1 Sítnice

Sítnice je světlocitlivá vrstva buněk, která snímá světelné paprsky, jež se k ní dostanou skrze panenku a oční čočku, která obraz odrazí a invertuje. Sítnice se nachází v zadní části oka a je považována za část centrálního nervového systému. Součástí sítnice jsou fotoreceptory, které dělíme na tyčinky a čípky. Tyčinky detekují světlo, čípky detekují barvy. [5] Technologie pracující se sítnicí zachycují a analyzují vzory krevních cév, nacházejících se na zadní straně oční bulvy, pomocí světla procházejícího zornicí. [48]

Biometrické systémy snímající sítnici jsou velice složité a pracují na principu lékařských přístrojů. Princip je stejný jako u retinoskopu (přístroj určený k vyšetření očí) – na sítnici je promítnut paprsek světla a CCD (z anglického Charge-Coupled Device) kamera snímá odražené světlo. Paprsek světla je zkalibrován tak, aby ho čočka zaostřovala jako bod na povrchu sítnice. Následně

sítnice odrazí část světla zpět k čočce, která ho znovu upraví. Paprsek odchází z oka pod stejným úhlem, pod kterým do oka vstoupil. Díky tomuto procesu můžeme získat snímek povrchu oka asi 10° kolem vizuální osy. Po získání vzorku dochází k porovnání se šablonou, čemuž předchází vzorkování, kdy se převede záznam oka do pole se shodným počtem prvků jako získané pole (tento proces zajistí překryv vzorků). Dále se normalizují intenzity vzorků a pole se korelují. Korelační hodnoty se pohybují od 1 (absolutní shoda) do -1 (absolutní neshoda), přičemž hodnoty pohybující se již okolo 0,7 mohou být považovány za shodu. [5]

Oproti ostatním biometrickým metodám má metoda rozpoznávání podle sítnice nejvíce omezení. Prvním omezením jsou vysoké pořizovací náklady, jelikož se cena optického aparátu odvíjí od jeho složitosti. Velkým problémem je otázka umístění aparátu (venkovní/vnitřní), protože pokud je panenka příliš malá, může se zvýšit míra falešného odmítnutí. Také je nutné oko přiblížit blízko k senzoru, což pro ověřované osoby nebývá příjemné. A omezení také spatřujeme v existenci poruch zraku, kdy je ověření ztíženo či znemožněno.

2.5.2 Duhovka

Duhovka je ta barevná část oka, kterou lze spatřit pouhým pohledem. Duhovku lze srovnat s clonou fotoaparátu, která reguluje světlo, které do objektivu (oka) vchází. Černému otvoru uprostřed duhovky říkáme pupila/panenka. Barva, vzor a textura se u každé osoby liší. Některé literární prameny udávají, že pravděpodobnost nalezení shody dvou stejných duhovek je menší než nalezení shody dvou stejných otisků prstů. [5], [48]

Prostup rozpoznávání duhovky je následovný. Prvním krokem je tzv. Gaborova demodulace, při níž je v pořízeném obraze duhovka lokalizována. K lokalizaci je použit operátor, který lze zjednodušeně popsat jako kruhový detektor hran. Po lokalizaci duhovky dochází obdobným způsobem i k lokalizaci víček (horního i dolního víčka). Následně je pomocí Daugmanova modelu hrubého zarovnání mapován každý bod duhovky do polárních souřadnic (model kompenzuje rozšíření panenky a nesoulad ve velikosti se šablonou). Z polárních souřadnic je

vytvořen kód o velikosti 256 bytů. Pro porovnání kódů dvou duhovek (duhovky a její šablony) je použit výpočet Hammingovy vzdálenosti, což je suma exkluzivních součtů mezi jednotlivými bity. Jestliže jsou porovnávané vzorky stejné, je Hammingova vzdálenost rovna či blízká nule. [5]

Výhody využití duhovky k identifikaci osoby:

- Duhovka je v průběhu života stabilní (s výjimkou úrazů a nemocí).
- Šablona má malou velikost.
- Vytvořit falzifikát je velice obtížné.
- Duhovka je relativně hodně odolná proti vnějším vlivům.

Nevýhody využití duhovky:

- Uživatelům nemusí být skenování očí příjemné.
- Některé systémy lze oklamat fotografií nebo kontaktními čočkami.
- Pořizovací náklady na tyto systémy jsou vysoké.
- U nevidomých lidí a při některých očních onemocněních může být duhovka zakalená a identifikace tak znemožněna.

2.6 Chůze

Chůze je v souvislosti s identifikací stále vyvíjenou a zkoumanou oblastí. Biometrické systémy rozpoznávající chůzi se zaměřují na její specifické vlastnosti tak, aby bylo možno ji rozpoznat v co možná nejširším spektru situací. Při rozpoznávání chůze je identifikace závislá na několika proměnných. Velkou roli v celém procesu hraje okolní prostředí, osvětlení i frekvence pohybu osob na daném místě. Dále jsou důležité změny obutí, zranění či úrazy i celkový fyzický stav uživatele. [18] Rozpoznávání chůze se aktuálně rozděluje do dvou směrů, přičemž každý směr vychází z jiných analytických metod. Jedná se o směr zaměřený na modelování pohybu a na směr zpracování siluety člověka.

Modelově orientované metody analyzují pohyb horní části těla nebo nohou. Tato metoda se zaměřuje na různé tělesné rozměry/délky a úhly při chůzi. Zaměřuje se tedy na dynamiku pohybu, ale ne na tvar postavy, jak je tomu u druhé

metody. V základu se v tomto přístupu využívají tři modely – drátěný, cylindrický, oválný. Nejjednodušší drátěný model lze využít i v 3D modelování, jednotlivé části modelu začínají a končí v kloubech, počet částí modelu se různí. Modelově orientovaný přístup vyžaduje kalibrovaný kamerový systém. [37]

Druhý přístup vyhodnocuje siluetu pohybující se osoby. Siluetu nejprve vyčlení z pozadí scény, poté ji sledují a vyhodnocují. Samotná analýza se pak může vztahovat k siluetě nebo jejímu pohybu. Aktuálně nejpoužívanější metodou je analýza délky kontury siluety, která se nejprve převádí do grafu a poté se normalizuje. [37]

Výhodou této metody je bezpochyby možnost identifikovat osoby na poměrně velké vzdálenosti, a to i za pomoci běžných typů kamer. Tato metoda je také uživatelsky přívětivá, protože nevyžaduje přímý kontakt se snímacím zařízením. Nevýhodou je, že lze tuto metodu poměrně snadno oklamat (běh, záměrná změna chůze).

2.7 Podpis

Ověřování osob na základě podpisu je specifickou skupinou biometrických metod, protože reprezentuje identitu osoby graficky. Podpis řadíme jak ke statickým, tak i z části k dynamickým biometrickým vlastnostem. Záleží, zda se zkoumá průběh psaní nebo pouze výsledek procesu psaní. [48] Ověřovaným prvkem je podmnožina písemného projevu osoby, jinými slovy rukopis. Na rukopis působí faktory vnitřní i vnější. Vnitřní faktory jsou dané stavem organismu a vlastnostmi dané osoby. Do vnitřních faktorů řadíme anatomicko – fyziologickou dispozici organismu, motivaci, cíl jednání či úroveň dovednosti (rychlost a kvalita psaní). Vnější faktory jsou vymezené prostředím, v němž se osoba při podepisování nachází, jeho polohou při psaní, druhem i stavem psacích prostředků a materiálů. [37]

Při autentizaci pomocí podpisu je nutné ruční zadání buď fráze, kdy uživatel musí zadat úryvek textu (proces zabere přibližně 5 sekund), nebo musí nakreslit jednoduchý náčrt (proces zabere přibližně 2 sekundy). [5]

Systémy pro autentizaci osob na základě podpisu můžeme rozdělit na [37]:

1. Off-line systémy – v případě těchto systémů se ověřovaná osoba podepisuje standardním způsobem na papír. Poté je podpis zdigitalizován pomocí optické kamery či skeneru. Nakonec je podpis a referenční vzor porovnán na základě celkového obrazu podpisu.
2. On-line systémy – využívají specializovaný hardware, nejčastěji tablet, k získávání charakteristik podpisu v reálném čase. Velkou výhodou těchto systému je schopnost zachytit statické i dynamické vlastnosti podpisu v průběhu jeho vzniku.

Zjednodušeně má verifikace podpisu tyto kroky. Nejprve jsou extrahovány charakteristiky z jednoho nebo více vzorků a je vytvořen referenční vzor, který je uložen do databáze. Zároveň je dané osobě přiděleno identifikační číslo. Toto ID je jednoznačně spojeno s příslušným referenčním vzorem. Při samotné autentizaci podpisu žadatel předloží své ID a podepíše se na vstupní zařízení. Nakonec systém vyhledá v databázi uložený vzor, který odpovídá předloženému ID, a porovná ho s podpisem. Po vyhodnocení je přístup povolen nebo zamítnut. [37]

Výhodou ověřování na základě podpisu je především jeho akceptace koncovými uživateli. Podepisování samotné je téměř rutinní činnost a s podepisováním skrz specializovaný hardware se setkáváme na úřadech, v bankách i při přebírání balíčků od kurýra. Oklamat systém falešným podpisem je poměrně těžké, ale především v off-line systémech to není nemožné, pokud je daný podpis zkoumám a trénován dostatečně dlouhou dobu.

2.8 Hlas

Metody rozpoznání hlasu jsou stále vyvíjeny a v praxi využívány jen málo. Důvodem je příliš velká různorodost lidské řeči, kterou nelze (zatím) spolehlivě rozpoznávat. Při analýze hlasu se systémy mohou zaměřit na jednu ze tří oblastí: rozpoznávání řeči (jejího obsahu), rozpoznávání mluvčího (identifikace osoby) a speciální rozpoznávání (např. analýza použitého jazyka). [5], [54] V rámci oblasti přístupových systémů bude dále popisována pouze oblast identifikace mluvčího.

Cílem verifikace mluvčího je ověření jeho totožnosti na základě vysloveného textu. Ověření může být textově závislé či nezávislé. Textově závislé systémy vyžadují vyřčení určitého předem stanoveného hesla. U textově nezávislých systému nehraje podoba vyřčeného slova nebo věty žádnou roli. [5]

Při této metodě je nejprve provedena segmentace signálu, protože hlasový signál různých mluvčí není shodný – liší se v délce vyslovených hlásek, intonací aj. Proto je stanovena maximální délka slova, se kterou je možné pracovat, a celý získaný signál se rozdělí na segmenty o délce N vzorků. Následuje extrakce charakteristik. Výsledkem celého procesu jsou příznaky (parametry), které popisují některé vlastnosti signálu. Díky těmto příznakům je možné analyzovaný signál dále klasifikovat. Mezi základní příznaky patří např. energie signálu, tedy kolik energie je v signálu soustředěno, nebo počet průchodů nulou čili hodnota, kolikrát je v daném vzorku protnutá časová osa průběhem signálu. Konečným procesem je prahování, kdy je rozhodnuto o přijetí/odmítnutí uživatele. [5], [37], [54]

Největším kladem této metody je bezesporu její akceptace uživateli. Hlas je běžný prostředek identifikace mezi lidmi a zařízeními, která rozpoznávají hlas, nejsou dotěrná a nevyžadují přímý kontakt. Naopak největší nevýhodou a důvodem poměrně malého využití v praxi je spolehlivost metody. Oproti ostatním biometrickým metodám se řadí tato mezi ty nejméně spolehlivé, protože lze hlas jednoduše cíleně pozměnit. Ke změně hlasu dochází i v případě nemoci nebo při změně psychického stavu. Zároveň je náročné získat „čistý“ hlasový záznam, protože je téměř vždy při pořizování záznamu přítomen šum a rušivé zvuky z okolí.

2.9 Rozpoznávání obličeje

Rozpoznávání druhých na základě jejich podoby je nejpřirozenější a nejpoužívanější způsob identifikace mezi lidmi. Každý den rozpoznáváme podle obličeje automaticky a s vysokou spolehlivostí i několik desítek lidí, což inspiruje vývojáře k vývoji a neustálému zlepšování biometrických metod, které lidskou

identifikaci ostatních jedinců napodobují. Zatímco většina biometrických metod vyžaduje přímý fyzický kontakt se čtecím zařízením, při procesu ověřování obličeje k fyzickému kontaktu se zařízením nedochází, což je i jedním z hlavních důvodů častého nasazování těchto systémů do běžného života za účelem ověřování a monitorování. [24]

Biometrický systém může pracovat s různými podobami pořizovaných snímků. Snímky mohou mít 2D podobu, 3D podobu nebo podobu termosnímku. Některé metody lze mezi sebou i kombinovat.

2.9.1 2D snímek

Pořizování 2D snímku při ověřování obličeje je stále nejrozšířenější metodou, i když ji pomalu nahrazuje pořizování 3D snímků. Obecný postup zpracování a vyhodnocení snímku je následovný – nejprve je detekován obličej na snímku, nalezený obličej je normalizován, dále dochází k extrakci příznaků a nakonec je vyhodnocena podobnost se šablonou. [5]

Při detekci obličeje dochází k lokalizaci obličeje na snímku. Především na frekventovaných místech se nezřídka stává, že je na jednom snímku zachyceno více obličejů či naopak není obličej zachycen celý. Zároveň může být snímek narušen nepříznivým osvětlením a barvou, pozice nebo orientace obličeje nemusí být pro rozpoznání vhodná. K detekci se využívají expertní znalosti nebo strojové učení. [5], [37]

1. Detekce obličeje pomocí expertních znalostí – metoda využívá známé informace, které jsou charakteristické pro lidskou tvář. Nejprve kompenzuje osvětlení, následně detekuje tón kůže, nakonec proběhne detekce rysů obličeje (ohraničení obličeje, úst a očí). [5]
2. Detekce obličeje pomocí strojového učení – využívá algoritmů strojového učení, které se trénují pomocí velkého množství snímků, ve kterých je manuálně vyznačena oblast tváře. Poté tyto snímky tvoří vstupní data pro některou učící se metodu (např. kaskáda klasifikátorů nebo neuronová síť), která následně obličeje automaticky detekuje. [5]

Po detekci obličeje je provedena normalizace, tedy předzpracování výřezu snímku, kde se obličej nachází. Díky normalizaci se zvyšuje spolehlivost porovnání. Do normalizace spadají úlohy typu: změna měřítka, nahrazení pozadí určitou barvou, úprava jasu či úprava klíčových obličejových bodů tak, aby seděly do šablonových pozic. [5], [37]

2.9.2 3D snímek

Při snímání obličeje do 2D roviny vždy dochází ke ztrátě určité části informace. Některé metody se tak snaží kompenzovat ztrátu informace určitou simulací předpokládaného tvaru obličeje. Aby byla ztráta informace co nejnižší a získaný obraz byl co nejvíce vypovídající, může být pořizován snímek ve 3D podobě.

3D snímek lze pořídit pomocí speciálního zařízení, které obvykle funguje na principu 2,5D skeneru. 2,5D sken lze zjednodušeně popsat jako 2D obraz, který má pro všechny uložené body i informaci o jejich hloubce. Takto vytvořený obraz je následně dokreslen pomocí viditelného nebo infračerveného světla. Případné nedostatky v modelu lze doplnit dalšími snímky, které jsou získány z různých úhlů či míst při skenování. [5]

V případě využití 3D snímání se nabízí několik možností využití podle toho, zda je pouze šablona v 3D podobě nebo je i pořizovaný snímek v 3D podobě [5]:

- 2D snímek a 3D šablona – 3D projekce šablony se upraví do 2D podoby tak, aby co nejvíce odpovídala pořízenému 2D snímku a následně se tyto snímky porovnají. Výhodou tohoto použití je, že stačí vlastnit pouze jedno 3D zařízení, které bude využíváno při registraci osoby do databáze. Ostatní skenovací zařízení mohou být obyčejná, čímž se celkové náklady sníží.
- 3D snímek a 2D šablona – v tomto případě je postup zpracování stejný jako v předchozím bodě. Rozdíl spočívá v nutnosti pořízení 3D zařízení na všechna přístupová místa. Nevýhodou jsou vyšší náklady na pořízení, výhodu je naopak vyšší bezpečnost, protože 3D snímač je těžší oklamat.

- 3D snímek a 3D šablona – při vzájemném porovnávání 3D modelů máme k dispozici nejvíce informací, díky čemuž jsou tomuto způsobu přisuzovány nejlepší výsledky.

Stejně jako u 2D snímků je i u 3D snímků důležitý proces normalizace, protože je pravděpodobné, že ani dva snímky stejné osoby nebudou naprosto stejné. Ve 3D prostoru probíhá normalizace na základě detekce klíčových bodů, kterými jsou hlavně koutky očí a špička nosu. Po detekci bodů je model transformován do určené polohy a je porovnán se šablonou. [5], [37]

2.9.3 Termosnímek

Při pořizování termosnímku se pracuje s infračerveným zářením dlouhých vlnových délek. Tento způsob snímání vyžaduje pořízení tzv. termokamery, tedy zařízení specializovaného na pořizování termosnímků. Výsledkem záznamu jsou termomapy obličeje. V termomapách je identifikována pozice očí, nosu, úst a hranic obličeje. [5]

Výhodou nasazení termokamer je především to, že lze snímek pořídit za jakýchkoliv světelných podmínek (za šera, v noci, při slunečním světle). Druhou velkou výhodou je obtížnost vytvoření falzifikátu, jelikož by falzifikát musel mít různou teplotu na různých místech v závislosti na daném obličeji. S tím se ale pojí i pravděpodobně největší nevýhoda tohoto způsobu snímání, a to změna teplotních charakteristik osob v souvislosti s teplotou okolí, předcházející aktivitě, zvýšené teplotě z důvodu nemoci či emocí atd. Z toho důvodu je z pohledu bezpečnosti nejlepším řešením spojení více metod dohromady – např. využití klasických 2D snímků v kombinaci s termosnímáním.

Při procesu rozpoznávání nemusí být nutně nakládáno s celou fotografií ověřované osoby, ale mohou být zpracovávány pouze vzdálenosti a deformace bodů (markantů), nebo lze k porovnání snímku a šablony využít například neuronových sítí.

2.9.4 Metoda identifikačních markantů

Tato metoda vychází z definování geometrických charakteristik, které jsou předem určené člověkem. Konkrétně se jedná o charakteristiky určené úhly a vzdálenostmi mezi jednotlivými identifikačními markanty, kterých pro popis individuality člověka stačí pouze dvanáct. Mezi tyto markanty patří: vnitřní a vnější koutky oka, bod přechodu nosu v čelo, bod špičky nosu, vnější body rtů, body chrupavky ucha a body přechodu tváře a ušních lalůčků. [37] Získané markanty se v průběhu ověřovacího procesu vzájemně propojí, díky čemuž je získáno 66 úseček (viz Obrázek 2). Takto vytvořená síť úseček je následně porovnána se sítí úseček šablony.

Obrázek 2: Identifikace markantů

Zdroj: [37]

2.9.5 Metoda mozaiky

Metoda mozaiky pracuje s rozložením odstínů šedi tváře ze snímku. Princip metody je poměrně jednoduchý – snímek ověřované osoby je rozložen do jednotlivých geometrických bloků, přičemž se stejný rozklad provede i se šablonami uloženými v databázi. Po rozkladu se postupně porovnávají jednotlivé bloky snímku s rozloženými šablonami z databáze tak dlouho, dokud není nalezena shoda s některou ze šablon. [37]

Nevýhodou této metody je výpočetní náročnost, protože se porovnává každý segment se segmentem a zároveň se vyhodnocuje i jejich okolí. Rychlost ověření uživatele je proto závislá i na množství uložených šablon v databázi. [37]

2.9.6 Metoda optických toků

Metoda optických toků se převážně používá při experimentech rozpoznávání emocí, jejichž automatické vyhodnocení se následně ověřuje. Kromě toho může být využita např. i při potřebě sledování pohybů rtů při vyslovování slov a vět. Jestliže bude při procesu ověřování uživatele pronášeno pokaždé stejné předem dohodnuté slovo, může tato metoda sloužit i k přímé autentizaci osoby, protože pohyb rtů při vyslovování bude pro každou osobu specifický. [37]

Metoda je založena na analýze sekvence snímků pohybu hlavy ověřované osoby. Při analýze dvou snímků, které jdou časově po sobě, registrujeme dynamické změny. Na snímcích se mění světelná intenzita mezi sledovanými body a mění se prostorový pohyb těchto bodů (tento pohyb je možné vyjádřit vektorově). Každý z bodů má nějaký směr pohybu, za určitý čas urazí určitou vzdálenost a zároveň mají odpovídající si body i svou rychlost. Obraz tak podléhá změnám strukturálním (prostorovým) a texturálním (změna intenzity). Rozdíly mezi dvěma snímky jsou vyjádřeny pomocí optických toků. Optické toky následně slouží pro rozpoznávání obličeje či pohybu. [37]

2.9.7 Neuronové sítě

Neuronové sítě napodobují skutečné neuronové sítě v lidském těle. Sítě tvoří množství neuronů, z nichž jsou vytvořeny jednotlivé vrstvy. Vstupní vrstva zajišťuje vstup dat do neuronové sítě, výstupní vrstva obsahuje výsledky a skrytá vrstva uchovává neurony, které obsahují danou logickou funkci. [49] Neuronové sítě mohou být v souvislosti s ověřením identity využity dvěma různými způsoby. První způsob spočívá v rozpoznání markantů nejrůznějšími způsoby, přičemž neuronové sítě jsou použity pouze pro konečnou klasifikaci tváře. Při druhém způsobu jsou neuronové sítě použity pro určení markantů i pro závěrečné rozpoznávání. [37]

Výhody metod rozpoznávání obličeje:

- V základním provedení při pořizování 2D snímků jsou pořizovací náklady nízké.
- Není vyžadován přímý fyzický kontakt se snímacím zařízením.
- Při použití 3D technologie nebo jakékoliv technologie v kombinaci s termokamerou je velmi obtížné systém obelstít.
- Může být využito pro hromadnou identifikaci.

Nevýhody rozpoznávání obličeje spatřujeme především:

- Rozpoznání může být zkomplikováno zakrytím obličeje, nasazením slunečních brýlí aj.
- Problém mohou způsobit i úrazy obličeje a plastické zásahy.
- Někteří lidé tuto metodu ověření identity odmítají.
- Osobní data uživatelů systému je nutné náležitě chránit.

3 HODNOCENÍ BIOMETRICKÝCH SYSTÉMŮ

Před realizací přístupového systému využívajícího konkrétní biometrickou metodu je nutné zvážit a zhodnotit všechny možné alternativy. Při hodnocení musíme brát v úvahu hned několik hledisek, kterými mohou být například náklady, spolehlivost, rychlost, akceptace uživateli, odolnost proti poškození, nadstandardní funkce atd. Jelikož je ovšem primárním úkolem biometrických systémů autentizace uživatele (tedy rozhodnutí o přijetí či odmítnutí přístupu), za nejdůležitější kritéria v souvislosti s hodnocením biometrických systému považujeme tzv. chybové míry. Chybové stavy nastávají, když [5]:

1. Jedna osoba předloží dva vzory, které jsou vyhodnocené jako odlišné – v tom případě dochází k chybné neshodě a tedy i k chybnému odmítnutí (False Reject).
2. Dvě osoby předloží dva vzory, které jsou vyhodnocené jako shodné – v tom případě dochází k chybné shodě a tedy i k chybnému přijetí (False Accept).

Na základě výše uvedeného byly definovány dva pojmy. Míra chybného odmítnutí (False Reject Rate – FRR) a Míra chybného přijetí (False Accept Rate – FAR). Dále lze sledovat například i Míru neschopnosti nasnímat (Failure To Acquire – FTA), Míru neschopnosti porovnat a další.

3.1 Míra chybného odmítnutí

Míra chybného odmítnutí je pravděpodobnost situace, při které biometrický systém vyhodnotí chybně dva biometrické vzorky od stejné osoby jako odlišné. Kvůli tomu nemusí být oprávněná osoba vpuštěna do kontrolované oblasti. [48] Hodnotu FRR lze snadno vypočítat pomocí vzorce [5]:

$$\mathrm{FRR} = \frac{počet\ porovnání\ vzorků\ osoby\ A\ vedoucí\ k\ \boldsymbol{neshodě}}{celkový\ počet\ porovnaní\ vzorků\ osoby\ A}$$

Oproti veličině FAR je Míra chybného odmítnutí chápána jako negativní hlavně z pohledu ověřované osoby. Jestliže je biometrické zařízení příliš přísné

a oprávněnou osobu vyhodnotí vícekrát jako neoprávněnou, je tato situace pro danou osobu nepříjemná a dochází ke ztrátě důvěry k danému zařízení. Tím klesá i ochota podstupovat ověření identity daným způsobem, což je pro vlastníka systému komplikace. [37]

3.2 Míra chybného přijetí

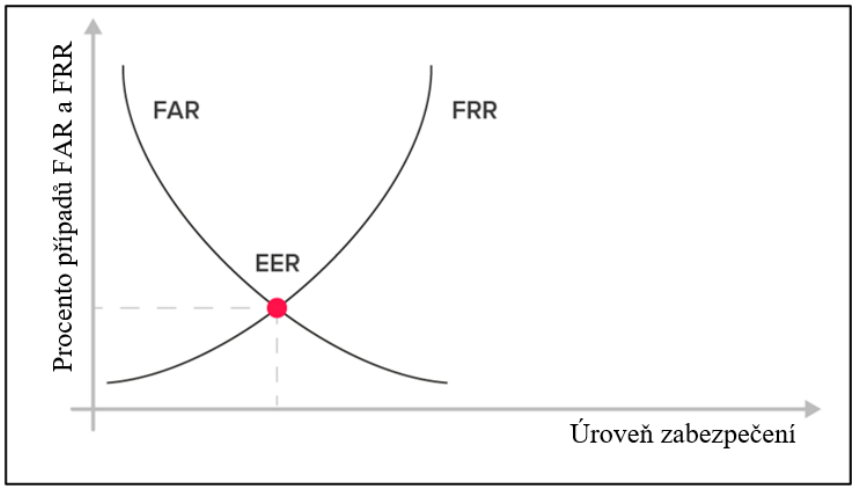
Míra chybného přijetí udává pravděpodobnost, že biometrický systém chybně posoudí dva odlišné předložené vzorky jako shodné. Kvůli této chybě může být neoprávněná osoba vpuštěna do střežené oblasti. [48] Míru chybného přijetí lze zjistit pomocí výpočtu [5]:

$$\text{FAR} = \frac{počet\ porovnání\ \boldsymbol{rozdílných}\ vzorků\ s\ výsledkem\ \boldsymbol{shoda}}{celkový\ počet\ porovnaní\ \boldsymbol{rozdílných}\ vzorků}$$

Bezpečnostní sílu biometrického systému dle hodnoty FAR (podle normy ISO/IEC 15480) považujeme za [5]:

- základní, když FAR ≤ 10^{-2},
- střední, když FAR ≤ 10^{-4},
- vysokou, když FAR ≤ 10^{-6}.

Vztah veličin FAR a FRR ukazuje Obrázek 3. Na obrázku lze vidět, že při snížení hodnoty FAR roste hodnota FRR a naopak. V průsečíku čar FAR a FRR se nachází bod EER, ve kterém jsou stejné procentuální hodnoty obou veličin.



Obrázek 3: Vztah FAR a FRR

Zdroj: vlastní zpracování dle [44]

3.3 Míra neschopnosti nasnímat

Míra neschopnosti nasnímat (zkratka FTA) udává podíl ověřovacích pokusů, při kterých systém selže z hlediska zachycení, či lokalizaci snímku nebo signálu v postačující kvalitě. Zjednodušeně řečeno je to podíl špatných záznamů daného zařízení, pořízených při automatickém snímaní, kvůli kterým je zaznamenání biometrické charakteristiky odmítnuto, i když je daná charakteristika k dispozici. Z uvedeného vyplývá, že čím vyšší je hodnota FTA, tím více je daný senzor nevhodný ke snímání vybrané biometrické charakteristiky. [5], [37] Hodnotu FTA bychom zjistili pomocí vzorce [5]:

$$\text{FTA} = \frac{\textit{neúspěšný počet pokusů o nasnímání dané charakteristiky}}{\textit{celkový počet pokusů o nasnímání dané charakteristiky}}$$

4 APLIKACE ROZPOZNÁVÁNÍ OBLIČEJE

Podle dat Českého statistického úřadu ověřovalo identitu uživatelů pomocí biometrických metod za účelem zajištění bezpečnosti informačních a komunikačních technologií v ČR v lednu roku 2019 celkem 11,2 % podniků, roku 2022 to bylo již 18 %. Nejvíce nasazovaly biometrické metody velké podniky (250+ zaměstnanců) z odvětví Informační a komunikační činnosti, dále odvětví Profesní, vědecké a technické činnosti a odvětví Činnosti v oblasti nemovitostí. Tabulka 3 zobrazuje prvních 10 států Evropské unie s více než deseti zaměstnanci, které v roce 2022 nejvíce využívaly biometrii k ověření identity. Nejvíce biometrických systému v praxi při ochraně informačních a komunikačních technologií využívalo Nizozemsko (24,4 %), naopak nejmenší podíl biometrických systémů byl zaznamenán v Bulharsku (6,2 %). Česká republika se s osmnácti procenty nachází na čtvrtém místě. [52], [53]

Tabulka 3: Využívání biometrických metod v EU v roce 2022

Pořadí	Stát	Podíl na celkovém počtu podniků v dané zemi (%)
1.	Nizozemsko	24,4
2.	Finsko	21,8
3.	Německo	19,0
4.	**Česko**	**18,0**
5.	Dánsko	17,3
6.	Španělsko	17,2
7.	Malta	16,0
8.	Švédsko	15,5
9.	Belgie	12,6
10.	Rumunsko	12,6

Zdroj: [52]

4.1 Rozpoznávání obličeje v ČR

V České republice se setkáváme s rozpoznáváním obličejů pouze na dvou veřejných místech. Jedná se o letiště Václava Havla v Praze a několik skiareálů. Zapojení těchto technologií např. do provozu v rámci městského kamerového systému hl. m. Prahy či využití technologie na fotbalových stadionech Úřad pro ochranu osobních údajů prozatím zamítl. Nejvíce jsou tyto technologie využívány pro kontrolu vstupu či ochranu aktiv ve firmách.

4.1.1 Letiště

Pravděpodobně nejznámějším místem v České republice, kde je rozpoznávání tváře využíváno, je letiště Václava Havla Praha. Zdroj [42] uvádí, že byl systém automatické detekce obličejů zřízen na základě usnesení vlády ČR č. 47/2015, o zvýšení bezpečnosti na mezinárodním letišti Václava Havla v Praze ze dne 19. ledna 2015. Od června 2018 je systém ve zkušebním provozu a k datu 19. srpna 2020 eviduje 189 pozitivních identifikací. Provozovatelem systému je Policie České republiky, zdrojová data k porovnání tváří jsou čerpána z informačního systému PATROS. Policie ČR dále udává, že k rozpoznávání obličeje zachyceného na kamerový záznam dochází až na serveru, protože v době zavedení systému nedisponoval trh kamerami, které by měly zabudovaný potřebný software v zařízení. Přístup do systému je povolen pouze bezpečnostním sborům, které na letišti působí (§ 11 odst. 1 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, § 14 a § 78 zákona č. 273/2008 Sb., o Policii České republiky a § 58 zákona č. 17/2012 Sb., o Celní správě České republiky). Aktuálně je do systému na letišti Václava Havla zapojeno 145 kamer, které monitorují převážně tranzitní prostor a veřejná místa s vysokou koncentrací lidí (např. prostor okolo informačních tabulí).

Doba uchování záznamu je dána následovně [14]:

- třídírna zavazadel – 5 dní,
- pevné a otočné kamery – 14 dní,
- kamery na bezpečnostní kontrole osob a vozidel – 30 dní.

Po uplynutí doby uložení jsou záznamy smazány přepisem. Monitorování a záznam probíhá v režimu 24/7. Údaje mohou být zpřístupněny nebo sdělovány pouze Policii ČR a dalším subjektům pouze na základě zákonného zmocnění. Údaje nejsou předávány do jiných států. [14]

Analýzu zajišťuje systém CertiConVis. K zajištění maximální bezpečnosti se využívají nejrůznější videoanalytické funkce. Společnost uvádí např. detekci výjezdů ze zásobovacího tunelu, detekci narušení perimetru, spuštění alarmu v případě pohybu v protisměru v jednosměrných prostorách, detekci odloženého zavazadla nebo detekci osob u vstupů do strategických místností. [19]

V rámci projektu zvyšování bezpečnosti na mezinárodních letištích vydalo ministerstvo vnitra v roce 2018 vyjádření, že do konce roku 2020 bude na letištích v Brně – Tuřanech, Pardubicích, Karlových Varech a Ostravě – Mošnově vybudován kamerový systém s automatickou detekcí obličejů a další bezpečnostní opatření. [25] Při kontaktování ministerstva vnitra za účelem zjištění aktuálního vývoje projektu bylo zjištěno, že je projekt prodloužen do poloviny roku 2024. K prodloužení doby realizace projektu došlo kvůli dopadům pandemie covidu-19, které zásadně omezily provoz a využívání regionálních letišť. Prodloužení projektu potvrdilo i Letiště Karlovy Vary s.r.o.

4.1.2 Skiareály

Dalšími místy v České republice, kde se setkáváme se systémy rozpoznávajícími lidskou podobu, jsou skiareály. V tomto případě je snahou provozovatelů skiareálů zabránit přenosu či zneužití poskytovaných služeb, typicky jde o kontrolu při přechodech přes turnikety, protože jsou lyžařské lístky prodávané jako nepřenosné.

Lyžařské středisko Skiareál Ještěd provozuje odbavovací systém s rozpoznáváním obličeje za účelem ochrany neoprávněného zneužití již zakoupeného skipasu. Skiareál na webových stránkách upozorňuje, že jsou skipasy nepřenosné a nesmí být tedy přeprodávány a půjčovány. Jestliže dojde k použití karty neoprávněnou osobou, bude skipas zablokován či odebrán

bez nároku na náhradu. Zneužití je znemožněno kamerami, které monitorují samoobslužné pokladny a odbavovací systémy. Monitorován je rovněž prostor turniketů. Při průchodu přes turniket je pořízena fotografie, kterou následně zpracovává a uchovává odbavovací systém. Pořízená fotografie je uchovávána po dobu platnosti skipasu, po ukončení platnosti je systémem vymazána. [32] Dále provozovatel na oficiálních webových stránkách zveřejňuje informace o kategorii zpracovávaných osobních údajů, účelu jejich zpracování, právním základu aj.

Jedná se například o následující údaje: [30]

- **Kategorie osobních údajů**: fotografie vaší podobizny při kontrole vstupu.
    - Záznam z přechodu turniketů, jméno, příjmení, GOPASS ID, datum a čas přechodu.
- **Účel zpracování**: zabránění zneužití služeb.
    - Verifikovat vaši podobiznu při přechodech turnikety v našich provozech, zejména lyžařských areálech. Jedná se o jediný možný prostředek, jak můžeme ověřit nezneužívání našich produktů, protože máme i takové zákazníky. Lístky se prodávají jako nepřenosné, a proto se kontroluje jejich nepřenosnost.
- **Právní základ**: smlouva, ve které vystupujete jako jedna ze smluvních stran a oprávněný zájem správce.
- **Doba zpracování**: přechody turnikety.
    - Vaše fotografie budou uchovávány následovně: při sezónních lístcích po celou dobu platnosti sezónního lístku, stejně jako při GOPASS kartě a při krátkodobých lístcích po dobu jejich platnosti a následujících 30 dní po skončení platnosti kvůli zabezpečení informací pro řešení reklamace. Při přechodech přes turnikety se během dne uchovávají všechny fotografie a po 23:59:59 zůstane uchována pouze první a poslední fotografie z přechodu přes turniket předchozí den.

Kamerový systém s rozpoznáváním obličeje provozuje také Skiareál Klínovec. V obchodních podmínkách skiareál upozorňuje na monitorování pokladního a odbavovacího systému kamerovým systémem. Dále uvádí, že při nákupu sezónního jízdného předkládá zákazník kromě jména, příjmení a dalších osobních údajů i aktuální fotografii a nákupem tohoto jízdného zákazník souhlasí se zpracováním osobních údajů v uvedeném rozsahu. Následně je při prvním průchodu turniketem jízdenka považována za použitou a je vázána s osobou, která ji použila, a dále je tedy jízdenka nepřenosná. Jestliže je jízdenka přenesena na jinou osobu, vyhrazuje si prodávající danou jízdenku vyloučit z dopravy bez náhrady. Výjimkou při přenosu je pouze situace při střídání rodičů u dítěte, kdy je jízdenka označená jako přenosná po prokázání rodinné příslušnosti či registrovaného partnerství v místě prodeje. [29] V dokumentu Informace o zpracování osobních údajů jako účel zpracování osobních údajů provozovatel skiareálu udává: „*Správce monitoruje vstupy, pohyb a aktivity v zařízeních správce, a to z důvodu zachování bezpečnosti, ochrany majetku správce a zabránění zneužívání služeb, které správce zákazníkům poskytuje. Právním základem je oprávněný zájem správce*.“ [15]

Podobné informace poskytují i další skiareály, které technologii rozpoznávání obličejů při svém provozu využívají. Jedná se například o SkiResort ČERNÁ HORA – PEC, Skiareál Rokytnice nad Jizerou, Skiareál Špindlerův Mlýn a další.

4.2 Rozpoznávání obličeje v zahraničí

V České republice je využití technologie rozpoznávání obličejů značně omezeno kvůli přísné ochraně osobních údajů. V některých zahraničních zemích je právní situace benevolentnější a rozpoznávání obličejů je nasazováno i na další místa, než jsou letiště a zimní sportovní areály.

Obchodní domy

Ve Velké Británii došlo v roce 2022 k nasazení kamerových systémů, které umí rozpoznat obličej, ve více než třiceti pobočkách maloobchodního řetězce Southern Co-Op, konkrétně v pobočkách s potravinami. Účelem tohoto rozhodnutí má být

identifikace osob, které byly v minulosti označené za pachatele nebo byly z prodejen vyloučeny. Po vstupu neoprávněné osoby do prodejny a její následné identifikaci zaměstnanci prodejny rozhodnou o dalších krocích. Řetězec na svých stránkách dále udává, že je systém v souladu s GDPR a neukládá fotografie jednotlivce, jestliže nebyl označen jako pachatel. Zákazníci daných prodejen jsou na využití této technologie upozorněni výrazným značením. [55] V USA bychom na technologii rozpoznávající obličeje narazili například v obchodech Macy's, Ace Hardware a dalších. [20], [34]

Policejní složky

Pro zvýšení veřejné bezpečnosti a udržování pořádku zapojují do svého systému funkce rozpoznávání obličeje i policejní složky. Jeden z takových rozsáhlých systémů funguje v Londýně pod záštitou Metropolitan Police. Metropolitan Police uvádí: „Technologii rozpoznávání obličeje může Met používat mnoha způsoby včetně prevence a odhalování zločinu, hledání hledaných zločinců, ochrany zranitelných osob a ochrany lidí před újmou – to vše proto, aby byli lidé, kterým sloužíme, v bezpečí.“ [9] Kvůli prevenci a odhalování zločinu a snaze chránit zranitelné využívá rozpoznávání obličeje i South Wales Police. [11] Dále tuto technologii využívá například New York Police Department. [8]

Veřejná doprava

S technologií rozpoznávání obličejů se setkáme i na Madrid South Bus Station, nejfrekventovanější autobusové stanici pro vnitrostátní i mezinárodní linky ve Španělsku. Prostor nádraží hlídá přes 100 kamer a software pro rozpoznání obličeje zajišťuje společnost Herta. Podle bezpečnostního manažera integrace systému rozpoznávání obličejů sdílení databázových dat a spolupráce se státními bezpečnostními úřady přispělo k výraznému snížení počtu incidentů a ke zvýšení celkové úrovně zabezpečení. [21]

Ve fázi testování je projekt společnosti Eurostar, která chce využít technologii rozpoznávání obličeje na trase z mezinárodního terminálu St Pancras v Londýně

do kontinentální Evropy. Projekt „Smartcheck lane“ je zaměřen na odbavovací a výstupní kontroly cestujících. Systém zahrnuje 2 skeny obličeje – první u vstupní brány, který slouží k ověření platnosti jízdenek, a druhý na výstupním kontrolním stanovišti, kde je kontrolována platnost údajů z pasu. [7], [10]

V roce 2021 spustilo metro v Moskvě systém umožňující zaplatit jízdné pomocí obličeje. Tzv. Face Pay systém byl implementován na více než 240 stanicích metra. K využívání tohoto systému je nutné mít mobilní aplikaci MosMetro, kam musí uživatelé nahrát svou fotografii, připojit údaje o bankovní a tranzitní kartě. Poté se stačí podívat do kamery umístěné nad turniketem a daná osoba je do kontrolované zóny vpuštěna. [26], [27]

Zdravotnická zařízení

Z důvodu ochrany pacientů, personálu a fyzického majetku využívá technologii rozpoznávání obličeje Raphael Hospital, zdravotní zařízení, které se nachází v Izraeli. Technologii zajišťuje společnost Oosto a díky tomuto řešení jsou zabezpečeny nejcitlivější části nemocnice (operační sály, personální zázemí, …), do kterých mohou vstoupit pouze oprávněné osoby, jako chirurgové či pomocný personál. Výhodou tohoto řešení je také omezení kontaminace na minimum, protože se daná osoba nemusí fyzicky dotýkat žádného povrchu při vstupu do zabezpečených míst. [39]

Společnost CETIFY Health zavedla identifikaci pacienta pomocí ověření obličeje na třech pobočkách společnosti Geisinger v Pensylvánii a dále plánuje tuto technologii zavádět do zdravotnického systému. V tomto případě slouží rozpoznávání obličeje pro rychlé a pohodlné ověření identity při návštěvách pobočky zařízení Geisinger. K tomu stačí naskenovat obličej pacienta při registraci do systému, sken uložit do elektronického lékařského záznamu pacienta a následně již pacienta při návštěvě centra bezkontaktně ověřit. [13]

4.3 Využití biometrie ve sportovním prostředí

Technologie s funkcí rozpoznávání obličeje na fotbalových či hokejových stadionech v ČR nenalezneme. V zahraničí využívá tuto technologii například dánský fotbalový stadion Brøndby a jedná se pravděpodobně o jeden z prvních systémů tohoto typu v EU. Fotbalový klub udává na svých oficiálních webových stránkách následující informace. [36] Účel zpracování osobních údajů:

- Při návštěvě stadionu Brøndby v souvislosti s fotbalovými zápasy nebo jinými událostmi o vás zpracováváme informace v souvislosti s kontrolou přístupu včetně biometrických informací v souvislosti s automatickým rozpoznáváním obličeje, abychom zajistili, že osoby, které mají dočasně nebo trvale zakázán přístup do Brøndby stadionu, nebyly do areálu stadionu vpuštěny.
- Kategorie osobních údajů, které zpracováváme: informace o vaší permanentce nebo vstupenkách (čárový kód atd.), které jste použili pro vstup na stadion. Dále informace o tom, který vchod jste použili, a také datum a čas skenování vstupenek/permanentek. Zpracovávány jsou také biometrické identifikátory ve spojení s kamerovým dohledem u vchodů.
- Právní základ pro naše zpracování osobních údajů pro uvedené účely:
    - Článek 6 Nařízení o ochraně osobních údajů, pododdíl 1, písmeno b, neboť zpracování je nezbytné pro splnění smlouvy s vámi (smlouva o přístupu k danému zápasu nebo akci).
    - Článek 6 Nařízení o ochraně osobních údajů, pododdíl 1, písmeno f, neboť zpracování je nezbytné k tomu, abychom mohli naplnit náš oprávněný zájem na účinné kontrole vstupu a zajistit tak klid a pořádek na stadionu.

- Právní základ zpracování citlivých osobních údajů:
    - § 7 pododdíl zákona o ochraně osobních údajů. 4, viz nařízení o ochraně údajů, článek 9, pododdíl g) a § 7 odst. 2 zákona o ochraně osobních údajů. 4, protože zpracování je nezbytné z důvodů významných společenských zájmů, viz povolení dánského úřadu pro ochranu údajů ke zpracování.
- Příjemci osobních údajů: informace jsou sdíleny s našimi IT dodavateli (zpracovateli dat), kteří pro nás informace ukládají a zpracovávají podle našich pokynů.

Kamerový systém s funkcí rozpoznání obličeje dále využívá například multifunkční velkokapacitní hala Madison Square Garden, která se nachází v centru Manhattanu v New Yorku. Provozovatel si v Zásadách ochrany osobních údajů vyhrazuje možnost shromažďovat biometrické informace, pokud se zúčastníte jakékoliv akce na některém z provozovaných míst. Dále uvádí možnost shromažďování zvukových nebo vizuálních informací, fyzických charakteristik aj. [35]

V roce 2021 bylo nasazeno několik stovek terminálů pro zajištění bezpečnosti při konání olympijských her v Tokiu. Systém zajistila firma Intel a japonská firma NEC. Systém byl nasazen především kvůli nutnosti zvýšené bezpečnosti související s rozšířením nemoci covid-19. Do systému byli lidé registrováni na základě fotografie ze státem vydaného průkazu totožnosti. Podle organizátorů bylo ověřování pomocí tváře 2x rychlejší než standardní kontroly ID. V případě olympijských her se jednalo o první využití této technologie. Aktuálně se diskutuje o využití obdobné bezpečnostní technologie i při konání olympijských her v roce 2024 v Paříži. [1], [17], [45]

5 AKCEPTACE NOVÉHO SYSTÉMU VEŘEJNOSTÍ

Při tvorbě této diplomové práce byla navázána spolupráce s firmou Enigoo, která se zabývá vývojem aplikačního ticketingového systému. Jejich systém umožňuje prodávat vstupenky přímo – na rozdíl od portálů typu GoOut či Ticketportal, které vstupenky pouze přeprodávají. Společnost Enigoo se zaměřuje převážně na odvětví sportu, přes ticketingový systém je možné prodávat vstupenky i permanentky, distribuovat je fyzicky i digitálně, spravovat platby, zajistit odbavení na vstupu, sledovat online statistiky aj. Mezi klienty společnosti patří AC Sparta Praha, České dráhy, HC Dynamo Pardubice, Mountfield HK, HC Motor České Budějovice a mnoho dalších. Enigoo je dceřinou firmou společnosti Deep Vision, která se zaměřuje na zakázkový vývoj softwaru a síťových technologií. Společnost Deep vision vyvinula vlastní all-in-one systém SAFEGOO – systém určený k identifikaci osob či bezkontaktní měření teploty. Jedná se o unikátní český projekt, který výrazně pomáhal v boji s pandemií covidu-19.

Vzhledem k zaměření společnosti i zájmům autorky bude dále zkoumáno řešení přístupových systémů na hokejových stadionech v ČR.

5.1 Specifika hokejového prostředí

Při sportovních utkáních se nachází v jeden časový interval na jednom místě několik stovek až tisíc lidí, kteří musí projít přes bezpečnostní kontrolu a prokázat oprávněnost ke vstupu do areálu pomocí permanentky či vstupenky. Při ověřování na základě např. obličejových rysů by zcela odpadla potřeba permanentních vstupenek ve formě kartiček, které musí fanoušci nosit neustále u sebe na každý zápas. Fyzické permanentky mohou být odcizeny, ztraceny či poškozeny. S výrobou, výměnou a vydáváním fyzických permanentních lístků jsou spojeny výrobní i administrativní náklady.

Při konání hokejových akcí je nutné odbavit velké množství lidí v co nejkratším čase. Moderní systémy dokážou ověřit totožnost osoby za méně než jednu vteřinu na vzdálenost až tří metrů.

S konáním hromadných sportovních akcí vyvstává dále otázka bezpečnosti. Ta je narušena především výtržníky a neukázněnými fanoušky. Nevhodné chování návštěvníků zápasů může narušit průběh zápasu, mít negativní dopady na ostatní návštěvníky a ohrozit soukromý majetek provozovatele stadionu. Za nevhodné chování fanoušků jsou také klubům udělovány vysoké pokuty a další formy trestů. Při aktuálních bezpečnostních opatřeních však není zcela možné jednoznačně zabránit vstup výtržníkům na další zápasy, protože identity návštěvníků jsou ve většině případů kontrolovány pouze namátkově pracovníky bezpečnostní služby.

5.2 Výběr vhodné biometrické metody

Po zvážení všech specifik hokejového prostředí, především pak otázky bezpečnosti při zápasech a komfortu pro uživatele systému, bude navrženo řešení využívající biometrické metody. Při využití biometrických metod by došlo ke zvýšení pravděpodobnosti zamezení vstupu neoprávněným osobám. Dále by zcela odpadla potřeba fyzických permanentních lístků a nehrozila by jejich ztráta, poškození či zneužití.

Z hlediska komfortu pro uživatele systému bylo vybíráno z biometrických metod zaměřených na fyziologické vlastnosti, aby nebylo nutné při autentizaci provádět žádnou speciální akci (předkládání podpisu, ověřování hlasu). Z fyziologických vlastností lze ověřovat např. obličej, charakteristiky oka, otisk prstu či dlaně, termogram a další. Technologie zaměřené na ověření osoby na základě charakteristik oka jsou finančně nákladné a pro uživatele méně příjemné než ostatní biometrické metody. Při otisku prstu či dlaně je zase nutný přímý fyzický kontakt se snímacím zařízením. Po zvážení všech těchto aspektů byla za optimální metodu pro tento případ užití zvolena metoda ověření obličejových rysů, která nevyžaduje přímý fyzický kontakt, dokáže rozeznat osobu i na větší vzdálenost a náklady na pořízení nejsou příliš vysoké (oproti ostatním metodám).

Zavedení nového přístupového systému by mělo největší dopad na prvotní uživatele tohoto systému – tedy na fanoušky hokejových zápasů (permanentkáře), kteří do této doby využívali zcela jiný přístupový systém. Aby mohla být implementace nového systému považována za úspěšnou, musí být (mimo jiné) kladně přijata. Za účelem zjištění akceptace navrženého systému potencionálními uživateli byl proveden průzkum mezi fanoušky vybraného hokejového klubu.

5.3 Cíl výzkumu

Primárním cílem výzkumu je zjištění míry akceptace navrženého systému v konkrétním prostředí. Pro lepší pochopení problematiky z pohledu uživatelů systému má být dále zjištěno povědomí respondentů o využití metody rozpoznávání obličeje v ČR, způsobu uchovávání dat z těchto systémů či o výhodách a nevýhodách tohoto řešení.

5.4 Počáteční předpoklady

Před zahájením dotazníkového šetření byly stanoveny následující předpoklady.
Předpoklad 1: Předpokládám, že více než 60 % respondentů bude proti zavedení přístupového systému využívajícího technologii rozpoznávání obličeje.
Předpoklad 2: Předpokládám, že 50–70 % respondentů netuší, že při procesu ověřování obličeje nemusí být uchovávána jejich fotografie.
Předpoklad 3: Předpokládám, že minimálně 20 % respondentů si neuvědomuje, že tuto technologii v ČR využívají skiareály či letiště.

5.5 Metodika výzkumu

Pro potřeby sběru většího množství dat a následnou analýzu těchto dat bylo vybíráno z kvantitativních metod výzkumu. Konkrétně byla zvolena metoda dotazování, což je metoda, při které jsou pokládány otázky předem vybraným respondentům. Z důvodu časové náročnosti, která je spojena s osobním dotazováním, bylo dotazování prováděno písemně za použití dotazníkového formuláře.

Dotazníkový formulář byl sestaven tak, aby nebyl příliš obsáhlý a respondentům nezabral více než 3 minuty času. Dotazník obsahoval devět povinných uzavřených otázek a jednu otevřenou dobrovolnou otázku, v rámci které bylo možné rozvinout názor na řešenou problematiku. První 3 otázky byly zaměřeny na osobní údaje respondentů – mělo být zjištěno, zda je respondent žena či muž, v jaké věkové kategorii se nachází a jak často navštěvuje hokejové zápasy. Zbylé otázky se týkaly názorů respondentů na technologie využívající biometrické metody, možností ukládání dat ve formě identifikačních markantů namísto fotografie, využití rozpoznávání obličeje na veřejných místech v ČR, výhod a nevýhod zavedení systémů s rozpoznáváním obličeje na hokejových akcích. Stěžejní otázka zjišťovala ochotu respondentů podstoupit ověření obličeje při vstupu na hokejový zápas.

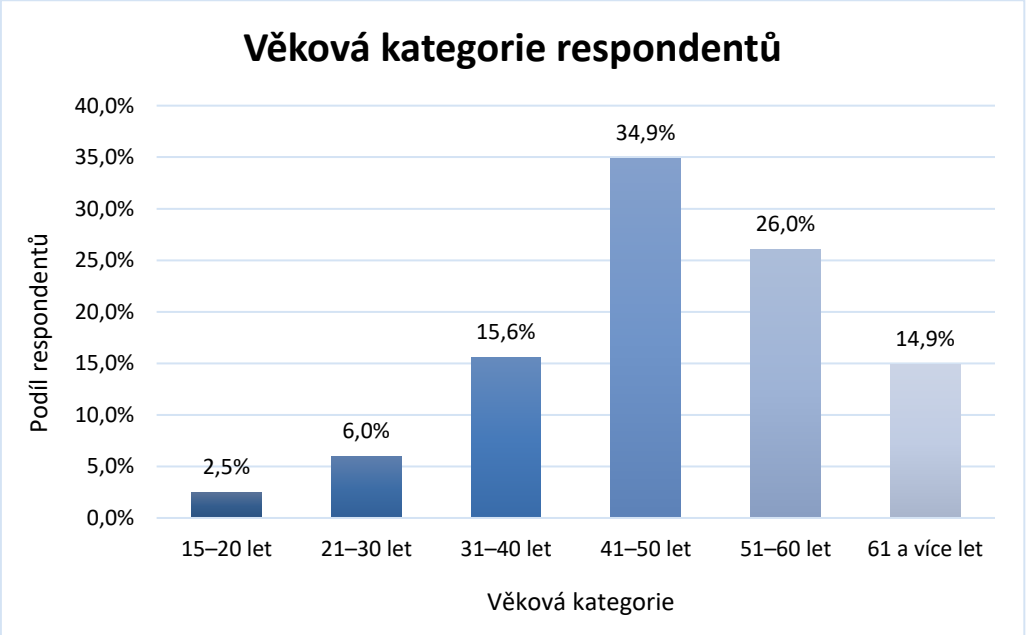
Po sestavení pilotní verze dotazníkového šetření byla jeho podoba konzultována s Ing. Petrem Mazánkem z firmy Enigoo kvůli obsahové stránce a rovněž byla následně testována dvaceti vybranými lidmi, kteří se o danou problematiku aktivně nezajímají, za účelem zjištění, zda jsou sestavené otázky dostatečně jednoznačné a snadno pochopitelné.

5.6 Charakteristika zkoumaného vzorku

Poslední fáze přípravy průzkumu spočívala ve výběru vhodného vzorku respondentů. Nutnou podmínkou výběru bylo vlastnictví permanentky na zápasy některého ze současných extraligových klubů v České republice. Jelikož jsou informace o vlastnících permanentních vstupenek citlivé a nelze je z veřejně dostupných zdrojů získat, bylo nutné některý z klubů oslovit a požádat jej o spolupráci. Oslovený extraligový klub byl vybrán na základě doporučení pana Ing. Petra Mazánka. Komunikace s vybraným klubem probíhala telefonicky a přes e-mail, a aby nebyla porušena ochrana osobních údajů dotčených osob, rozeslal klub vypracovaný dotazníkový formulář všem svým kontaktům z databáze vlastníků permanentek z vlastní e-mailové adresy. V databázi se nacházelo 1000 kontaktů.

5.7 Výsledky šetření

Dotazníkové šetření bylo vyhodnoceno po měsíci od rozeslání na adresy vybraných kontaktů a zúčastnilo se ho celkem 315 respondentů. Z toho 85,7 % respondentů tvořili muži a 14,3 % tvořily ženy. Věkové rozložení respondentů lze vidět na Obrázek 4.

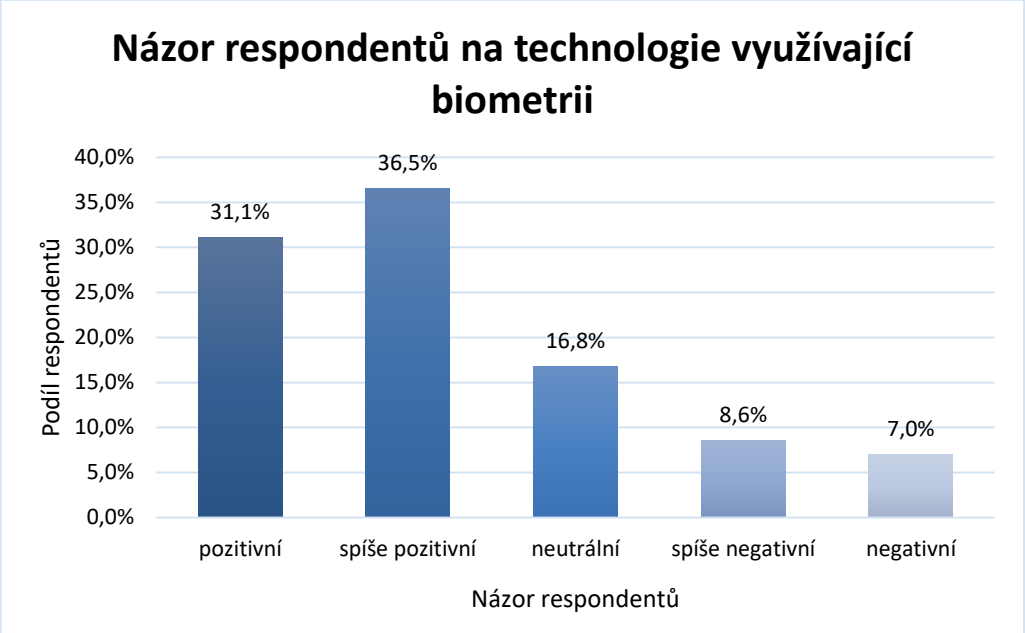


Obrázek 4: Graf rozložení věkové kategorie respondentů

Zdroj: vlastní zpracování

Následně byla zjišťována frekvence navštěvování hokejových zápasů. Celkem 240 respondentů uvedlo, že navštěvují hokejové zápasy minimálně 21krát ročně. Dále 44 respondentů chodí na zápasy 16–20krát ročně, 18 respondentů 11–15krát ročně a 13 respondentů navštěvuje zápas 10krát a méně za rok.

První z otázek, týkající se biometrických metod, zkoumala názor hokejových fanoušků osloveného klubu na technologie využívající biometrické metody obecně (rozpoznávání obličeje, otisk prstu, analýza hlasu aj.). Výsledek zobrazuje Obrázek 5.



Obrázek 5: Graf rozložení názorů respondentů na biometrii

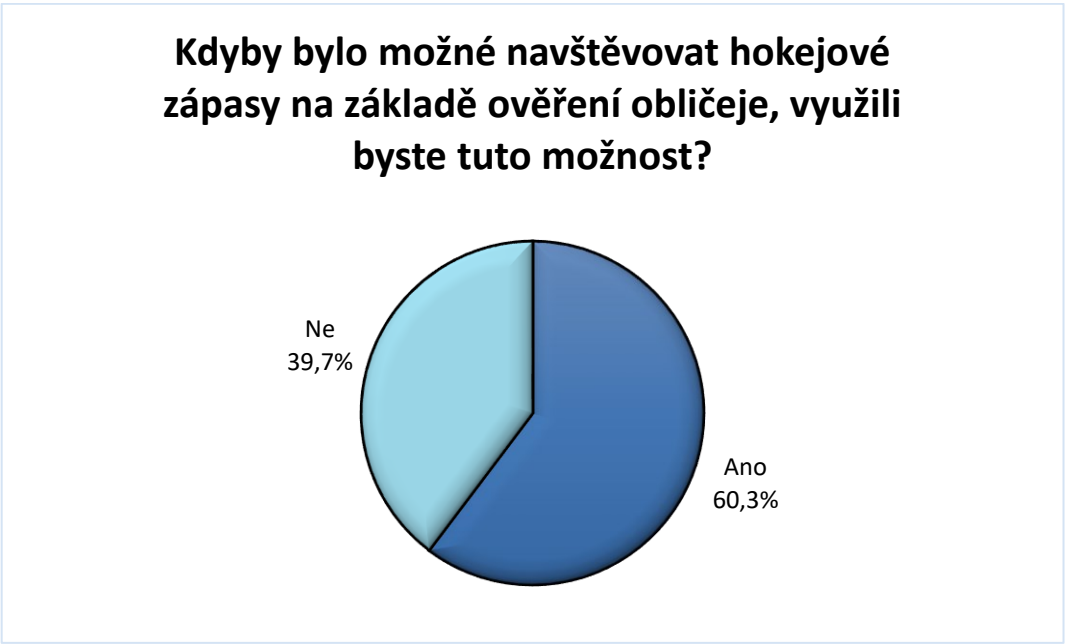
Zdroj: vlastní zpracování

Druhá otázka zjišťovala informovanost respondentů o možném způsobu uchovávání získaných údajů prostřednictvím softwaru, který ověřuje identitu osoby na základě charakteristik obličeje. Otázka zněla: „*Věděli jste, že některé systémy rozpoznávající obličej osob neukládají jejich fotografie? Tyto systémy pouze uchovávají informace o vzdálenosti určitých bodů – například od ucha ke špičce nosu – z čehož není zpětně možné zrekonstruovat přesnou podobu osob*.“ Celkem 37,8 % dotazovaných uvedlo, že tuto skutečnost vědělo, 62,2 % respondentů naopak uvedlo, že o této možnosti uchování dat dosud neslyšelo.

Účelem následující otázky bylo zjistit, zda dotazovaní vědí o veřejných místech v ČR, kde se technologie s rozpoznáváním obličejů využívá. Znění otázky bylo: „*Věděli jste, že rozpoznávání obličeje je v ČR běžné ve skiareálech, na letištích či v některých firmách?*“ Z výsledků dotazníkového šetření vyplývá, že o tomto

využití biometrie ví 76,5 % dotazovaných a 23,5 % dotazovaných o využití této technologie na uvedených místech nevědělo.

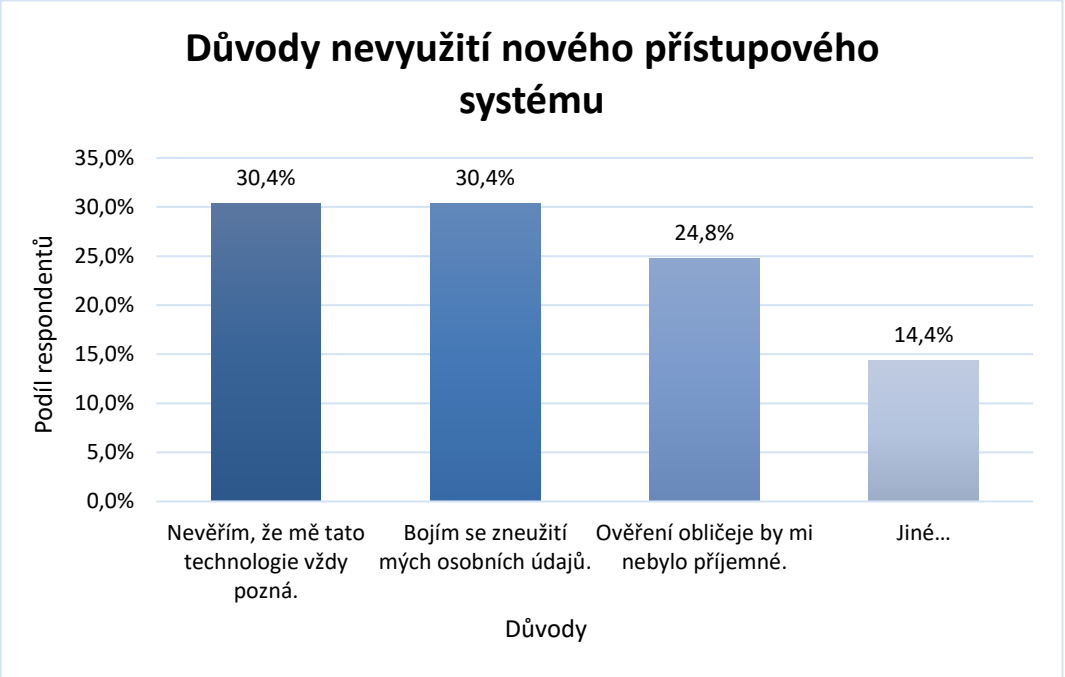
Stěžejní otázka šetření zjišťovala ochotu oslovených hokejových fanoušků využívat při vstupu na zápas technologii rozpoznávající obličej. Otázka zněla: „*Kdyby bylo možné navštěvovat hokejové zápasy na základě ověření obličeje, využili byste tuto možnost?*“ Výsledek této otázky lze vidět na Obrázek 6. Celkem 190 dotázaných (tedy 60,3 %) by při vstupu na zápasy nový přístupový systém využilo, naopak 125 tázaných (39,7 %) by raději zůstalo u stávajícího přístupového systému.



Obrázek 6: Graf využití nového přístupového systému

Zdroj: vlastní zpracování

Část respondentů, kteří uvedli, že by tuto technologii nevyužili, byli dále dotázáni na důvod. Výsledek představuje Obrázek 7.



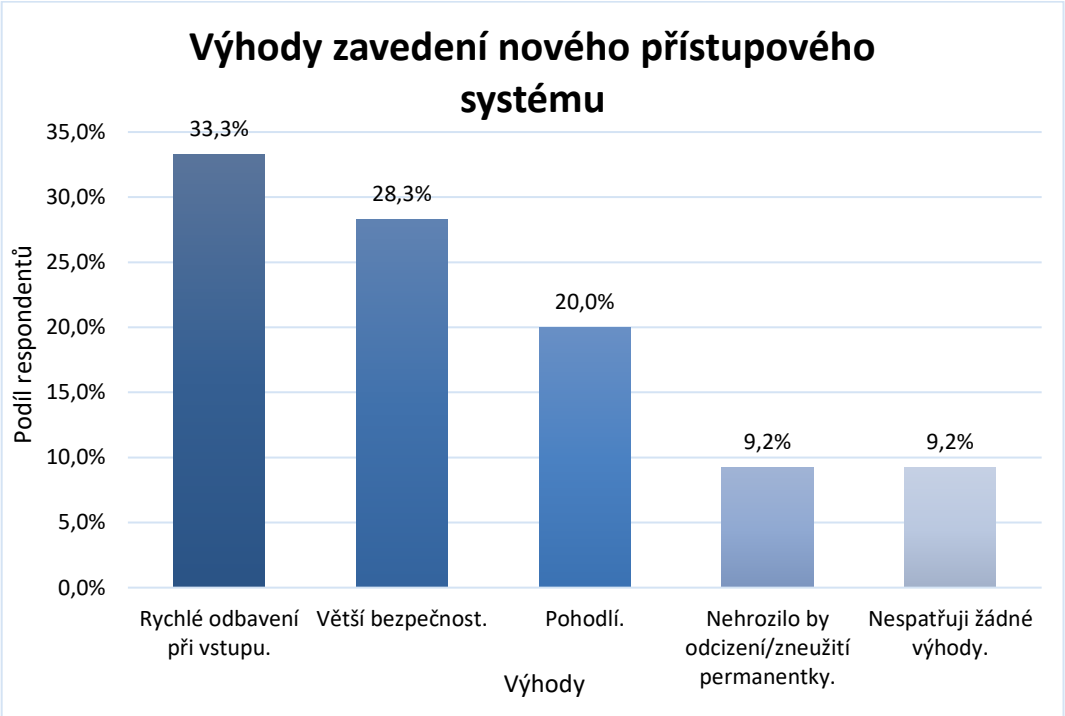
Obrázek 7: Graf důvodů nevyužití nového systému

Zdroj: vlastní zpracování

V rámci odpovědi „Jiné“ se vyskytovaly tyto odpovědi:

- Nebylo by možné permanentku přenést na někoho jiného.
- Současný přístupový systém je vyhovující.
- Permanentku mám nahranou v mobilu, který nosím neustále u sebe.
- Jde o zbytečnou investici.
- Nejsem příznivcem těchto technologií.

Předposlední otázka zkoumala subjektivní názor respondentů na výhody zavedení systémů s rozpoznáváním obličeje na hokejových akcích. Každý respondent mohl označit pouze jednu odpověď (viz Obrázek 8).



Obrázek 8: Graf výhod zavedení nového přístupového systému

Zdroj: vlastní zpracování

Poslední otázka zaměřená na rozšíření problematiky byla pouze dobrovolná, otevřená, a zjišťovala naopak největší nevýhody/nedostatky, které tento systém podle účastníků šetření má. Nejčastěji se odpovědi týkaly těchto bodů:

- Finanční náklady na zavedení systému a nákup technického vybavení (cena zařízení se promítne do ceny permanentky).
- Strach spojený s nepřesností rozpoznávání. Přesnost rozpoznávání při změně vizáže či při úrazu obličeje.
- Situace, která by nastala při výpadku systému či nerozpoznání oprávněné osoby.
- Přenosnost permanentky.
- Bezpečnost osobních údajů/identity.
- Narušení soukromí.

5.8 Posouzení předpokladů

Na základě získaných výsledků mohou být nyní počáteční předpoklady potvrzeny či vyvráceny.

Předpoklad 1: Předpokládám, že více než 60 % respondentů bude proti zavedení přístupového systému využívajícího technologii rozpoznávání obličeje.

Na otázku, která se týkala akceptace nového přístupového systému, založeného na metodě rozpoznávání obličeje, celkem 60,3 % respondentů uvedlo, že by tento systém využilo. Pouze 39,7 % respondentů naopak uvedlo, že by tento systém spíše nevyužilo.

Předpoklad 1 byl vyvrácen.

Předpoklad 2: Předpokládám, že 50–70 % respondentů netuší, že při procesu ověřování obličeje nemusí být uchovávána jejich fotografie.

Výsledky související s tímto tvrzením jsou následující: 62,2 % respondentů uvedlo, že o způsobu uložení dat v podobě identifikačních markantů namísto fotografie nevědělo, zbylých 37,8 % respondentů o této možnosti uložení dat již slyšelo.

Předpoklad 2 byl potvrzen.

Předpoklad 3: Předpokládám, že minimálně 20 % respondentů si neuvědomuje, že tuto technologii v ČR využívají skiareály či letiště.

Na otázku, která zněla „Věděli jste, že rozpoznávání obličeje je v ČR běžné ve skiareálech, na letištích či v některých firmách?“, odpovědělo 74 respondentů, že o využití technologií rozpoznávající obličej na uvedených místech nevědělo. V relativním vyjádření se tento počet respondentů rovná 23,5 %.

Předpoklad 3 byl potvrzen.

5.9 Vyhodnocení výzkumu

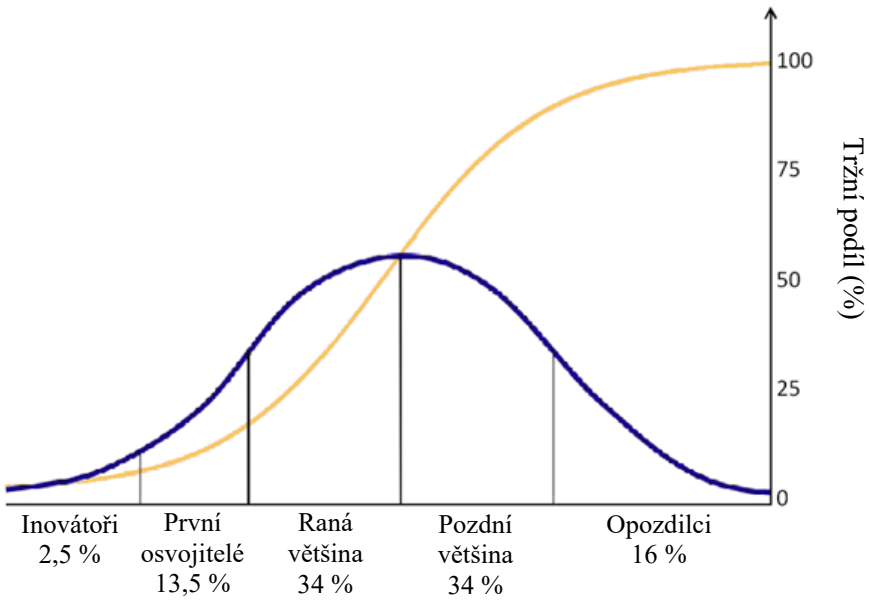
Dotazníkový formulář byl zaslán na tisíc e-mailových adres držitelů permanentních vstupenek osloveného hokejového klubu. Za sledovaný měsíc dotazník navštívilo 352 respondentů, z čehož 315 respondentů dotazník dokončilo. Úspěšnost vyplnění dotazníku je vzhledem k počtu návštěv rovna 89,5 %.

Převážnou většinu respondentů tvořili muži ve věkovém rozmezí 41–60 let, kteří navštěvují hokejové zápasy alespoň 21× ročně. Mezi respondenty převažuje spíše pozitivní názor na technologie využívající biometrické metody. O možnosti ukládání pořízených dat ve formě identifikačních markantů namísto celé fotografie nevědělo 62,2 % dotazovaných. Využití systémů rozpoznávajících obličej ve skiareálech, na letištích či v některých firmách si je vědomo 76,5 % respondentů.

Akceptace nového přístupového systému je v 60,3 % případech kladná (190 případů z celkových 315) a tito permanentkáři by nově zavedený systém využili. V kontextu celkového počtu vlastníků permanentních vstupenek klubu, tedy i těch, kteří se dotazníkového šetření nezúčastnili, je výsledná míra akceptace nového přístupového systému 19 %.

Další vývoj akceptace systému lze odvodit např. na základě teorie šíření inovací. Teorie šíření inovací, též teorie difúze inovací, je teorie vytvořená E. Rogersem, kterou publikoval roku 1962 v knize Diffusion of Innovations. Tato teorie se zabývá šířením inovací, technologií a myšlenek ve společnosti. Základem teorie je myšlenka, že se přijetí nové inovace/technologie/myšlenky neděje najednou, ale že mají naopak různé skupiny lidí tendenci přijímat technologii v různých časových úsecích. [4] Na tomto základu byla vytvořena tzv. kategorizace osvojitelů (viz Obrázek 9). První kategorií jsou inovátoři, kteří tvoří prvních 2,5 % skupiny a kteří přijímají novou technologii jako první. Druhou kategorií jsou tzv. early adopters, v překladu první/raní osvojitelé, tvořící dalších 13,5 % skupiny. První osvojitelé přijímají nové inovace pozitivně a jsou obvykle respektovaní svými vrstevníky, takže díky nim dochází k úspěšnému využívání

nové technologie dalšími lidmi. Následujících 34 % označujeme jako „raná většina“. Lidé označováni jako raná většina si nové myšlenky osvojují dříve než průměrná část skupiny a obvykle potřebují nejprve vidět důkazy, že daná inovace opravdu funguje, a až poté jsou ochotni tuto inovaci přijmout (tj. po určitém čase následují skupinu první osvojitelé). Dalších 34 % tvoří další skupina, nazývaná „pozdní většina“, přičemž lidé spadající do této skupiny bývají obvykle skeptičtí a jsou ochotni inovaci přijmout až po přijetí/vyzkoušení většiny. Posledních 16 % skupiny je považováno za tzv. opozdilce a je velmi obtížné je do procesu přijetí inovace zapojit. [3], [4]



Obrázek 9: Křivka difúze inovací

Zdroj: [40]

Dle popsané teorie je výsledek dostatečný pro postupné přijetí systému i ostatními uživateli, kteří nejsou v tuto chvíli o přijetí technologie rozhodnuti nebo tuto technologii odmítají (s předpokladem pozitivní zkušenosti skupiny early adopters s implementovaným systémem).

6 NÁVRH IMPLEMENTACE PŘÍSTUPOVÉHO SYSTÉMU

V následující kapitole bude provedena SWOT analýza projektu a budou specifikovány požadavky na nový přístupový systém. Následně bude popsán a navrhnut možný způsob implementace nového přístupového systému, který zahrnuje využití metod rozpoznávání obličeje.

6.1 SWOT analýza projektu

Před samotným návrhem konkrétního řešení byla provedena SWOT analýza připravovaného řešení. SWOT analýza je analytická metoda zaměřená na hodnocení vnitřních i vnějších vlivů, které ovlivňují úspěšnost projektu. [23] V rámci SWOT analýzy se analyzují silné a slabé stránky projektu, příležitosti a hrozby (viz Tabulka 4).

Tabulka 4: SWOT analýza projektu

	Pozitivní vlivy	**Negativní vlivy**
Interní vlivy	**Silné stránky** • první nasazení biometrie pro kontrolu vstupu v hokejovém prostředí v ČR • zvýšení bezpečnosti při pořádání sportovních akcí • rostoucí akceptace biometrie koncovými uživateli	**Slabé stránky** • závislost na kvalitě HW • vysoké pořizovací náklady • určitá míra chybovosti (FAR, FRR)
Externí vlivy	**Příležitosti** • zvyšování bezpečnostních požadavků pořadatelů • na českém trhu existuje pouze málo alternativ • rychlý vývoj HW a technologií	**Hrozby** • vstup konkurence na trh • zvýšené riziko hackerského útoku na datová úložiště • legislativní omezení

Zdroj: vlastní zpracování

6.2 Specifikace požadavků na systém

Před samotným návrhem konkrétního řešení bylo nutné stanovit požadavky, které jsou kladeny na přístupový systém ve sportovním prostředí. Jinak řečeno, následující požadavky na systém jsou zároveň nutnými kritérii, která musí nový systém splňovat.

1. Počet odbavení – systém musí být schopen odbavit několik stovek až tisíců uživatelů v krátkém časovém úseku. Vzhledem k dostupným informacím o množství prodaných permanentek některých extraligových klubů v uplynulých letech byla potřebná kapacita záznamů stanovena na 10 tisíc (v případě menších klubů postačuje i 5000 záznamů).
2. Rychlost odbavení – odbavení uživatelů musí být rychlé. Nový přístupový systém by měl splňovat dobu odbavení jednoho uživatele ≤ 2 sec.
3. Bezpečnost přístupového systému – přístupový systém musí být bezpečný, při zvláštních bezpečnostních incidentech nesmí být překážkou (musí umožňovat oboustranný/poplachový chod).
4. Přesnost systému musí být nejméně 99 %.
5. Intuitivní a snadné použití systému.

Po provedení analýzy současné podoby přístupových terminálů na hokejových stadionech a rozhovoru s odborníkem na bezpečnostní a přístupové systémy byla za optimální řešení zvolena kombinace přístupového turniketu s integrovaným terminálem, který bude zprostředkovávat vybraný software.

6.3 Turniket

Na trhu existuje velké množství výrobců, kteří nabízejí nejrůznější druhy turniketů. V České republice se výrobě turniketových systémů věnuje například firma ELVIS ze Žďáru nad Sázavou, COMINFO a.s. či Detomatic s.r.o.

6.3.1 Druhy turniketů

Tripodové/trnové turnikety jsou otočné turnikety nejčastěji se třemi rameny. Jedná se o nejrozšířenější typ turniketů, který lze implementovat téměř do jakéhokoliv prostředí venku i uvnitř. Tento typ turniketů obvykle mívá odolnou robustní konstrukci v celonerezovém provedení. Při bezpečnostních incidentech je standardně možné ramena turniketů sklopit.

Branky je možné nasadit ve vnitřních i vnějších prostorách. Nejčastěji se s nimi setkáváme např. při vstupu do obchodů. Jejich největší výhodou je především šíře vstupního prostoru, která je dostatečná pro invalidní vozíky nebo maminky s kočárky. Křídla branek mohou být celonerezová, s plexisklem, s tvrzeným sklem aj. Branka může být ovládána automaticky, bez potřeby zásahu procházející osoby, nebo může být ovládána pomocí určité akce (tlačení ramena před sebou).

Plnoprůchodové/plnorozměrné turnikety jsou turnikety velkých rozměrů, určené do ztížených podmínek s intenzivním zatížením. Součástí rotačního kříže jsou nejčastěji 3 nebo 4 ramena. Díky elektromagnetické brzdě je zajištěna úplná ochrana před neoprávněným vstupem. Podle požadavků zákazníka je standardně tento turniket vyráběn v nerezovém, žárově zinkovaném či lakovaném provedení.

Rotační turnikety jsou obvykle vyrobeny z nerezu nebo v kombinaci nerezu a skla/plexiskla. Standardní provedení rotačního turniketu má také 3 nebo 4 ramena. Rotační turnikety jsou vhodné především do obchodů, protože umožňují vyšší kontrolu návštěvníků, a také spolehlivě zabraní odchodu s odcizeným zbožím skrz vstupní prostory.

Dále se můžeme setkat se speedgate turnikety, turnikety s platebním automatem (součástí je platební terminál či mincovník), turnikety pro speciální využití aj.

6.3.2 Výběr turniketu

Z důvodu omezeného místa v hokejových halách a nákladů spojených s pořízením několika turniketů pro zajištění rychlého odbavení fanoušků byl za optimální druh turniketu pro tento účel zvolen tripodový turniket.

Při výběru tripodových turniketů sledujeme především tyto parametry: kapacita průchodu, provedení (jednosměrné/obousměrné), šíře průchodu či délka ramena. Pro účely implementace turniketů na hokejových stadionech byla stanovena minimální kapacita průchodu 30 osob/min., provedení oboustranné, minimální šířka průchodu 500 mm. Samozřejmostí musí být možnost bezpečnostního sklopení ramen turniketu (antipanik mód) a možnost úpravy turniketu podle požadavků na integraci terminálu pro rozpoznávání obličeje. Uvedené parametry splňují například tyto turnikety:

- tripodový turniket TRISTAR – výrobce Detomatic, kapacita průchodu až 40 osob/min., šířka průchodu 600 mm, přibližná cena v základním provedení: 99 729 Kč vč. DPH,
- tripodový turniket TTB07 – výrobce Elvis, kapacita průchodu 30 osob/min., šířka průchodu 500 mm, přibližná cena v základním provedení: 86 890 Kč vč. DPH,
- tripodový turniket TS2100 – výrobce ZKTeco, kapacita průchodu 30 osob/min., šířka průchodu 520 mm, přibližná cena v základním provedení: 52 818 Kč vč. DPH.

Z důvodu velkého množství turniketů i terminálů na trhu je vždy nutné kontaktovat výrobce/prodejce turniketů a zkonzultovat s ním možnosti instalace terminálu, který bude zajišťovat rozpoznávání osob na základě obličeje, případně i další požadované funkce a doplňky. Požadovaný turniket je následně vyroben na míru a je stanovena individuální cenová kalkulace.

6.4 Přístupový terminál

Stěžejní jednotkou navrhovaného řešení je terminál v podobě displeje se softwarem zajišťujícím kontrolu vstupu na základě ověření obličeje.

Terminály nabízí např. společnosti HikVision, ZKTeco, HFSecurity. V případě terminálů sledujeme parametry: rozlišení a velikost displeje, rozlišení a typ kamery, CPU a paměť, termokamera – ANO/NE + rozsah teplot, doplňky atd. Velmi často jsou na trhu k dostání terminály se softwarem v rámci jednoho produktu. Při výběru softwaru jsou nejdůležitějšími informacemi především rychlost rozpoznání obličeje, vzdálenost, na kterou je možné obličej rozpoznat, a kapacita obličejů, se kterou je systém schopný pracovat.

V zahraničí poskytují systém, který odpovídá požadavkům stanoveným v kapitole 6.2, firmy HikVision (terminály MinMoe), TKTeco (systémy ZKBioAccess, ZKBioSecurity), IDEMIA (systém VisionPass), Uniview a mnoho dalších. V České republice je počet vývojářů tohoto druhu systému značně nižší, především kvůli vysokým nákladům, které jsou s vývojem systému spojeny. Vlastní biometrický systém v kombinaci se vstupním terminálem nabízí například společnost Enigoo (systém SAGEGOO), SYSDO (systém SYSDO), Sevitech CZ (terminál Horečkomat) či společnost C H Complex Systém (systém Adam).

6.4.1 Specifika výběru terminálu

Při výběru vhodného řešení byly vybrány 3 systémy různých společností, které splňují stanovené požadavky z kapitoly 6.2, a nachází se v obdobné cenové kategorii. Tyto požadavky tvoří nutná omezující kritéria, která musí splňovat všechny porovnávané systémy.

Nutná omezující kritéria:

- Minimální kapacita je 10 000 obličejů.
- Rychlost odbavení musí být ≤ 2 sec.
- Přesnost systému musí být alespoň 99 %.
- Cena systému se musí pohybovat okolo 50 000 Kč (± 10 000 Kč).
- Terminál je vhodný k instalaci na turniket.

Dále byla zvolena vhodná kritéria, podle kterých bude vybíráno finální řešení. Kritéria byla vybrána na základě konzultace s technickým pracovníkem a odborníkem na kamerové systémy ze společnosti Euroalarm.

Vhodná kritéria jsou:

- Cena bez DPH [Kč] – minimalizační kritérium. Cena je uváděna v korunách českých.
- Kapacita obličejů – maximalizační kritérium.
- Rychlost [sec] – minimalizační kritérium. Rychlost je uváděna v sekundách.
- Termokamera – termokamera je výhodou.
- Velikost displeje [″] – maximalizační kritérium (dáváme přednost velkému displeji). Velikost displeje je uváděna v palcích.

Popis alternativ

Do procesu výběru vhodného přístupového systému byly vybrány tyto alternativy:

1. Hikvision DS-K1T607TEF – přístupový terminál s funkcí rozpoznání obličeje, se čtečkou otisku prstů a čtečkou karet. Terminál obsahuje kameru s duálním objektivem, která dokáže rozpoznat osobu na vzdálenost 1,5 metru. Terminál lze připojit k zámku, odchodovému tlačítku a dveřnímu kontaktu. [6]
2. SAFEGOO – all-in-one systém termální kamery a identifikace obličeje uživatelů české společnosti Enigoo. Terminál je vhodný jako nadstavba pro docházkové systémy, systémy kontroly vstupu do objektů a systémy návštěvnosti. Při ověřování osob systém nepracuje s celou fotografií, nýbrž s identifikačními markanty. [41]
3. Uniview OET-213H-BTM32 – terminál pro přesnou a rychlou digitální detekci obličeje, který obsahuje rovněž i detekční modul pro rychlé zjištění tělesné teploty. Koncové zařízení obsahuje dotykový displej, systém je ovládán počítačovou aplikací. Terminál lze instalovat na zeď, stojan či turniket. [31]

Metoda výběru vhodného řešení

Aby mohlo být zhodnoceno několik výběrových kritérií najednou, a zároveň byla zohledněna důležitosti těchto kritérií (protože všechna kritéria nemají stejnou váhu), byla pro výběr vhodného řešení zvolena metoda vícekriteriálního rozhodování. Konkrétně byla vybrána tzv. Fullerova metoda, která využívá pro zjištění vah kritérií párové porovnání. Princip Fullerovy metody spočívá v postupném porovnávání dvou kritérií, kdy z každé dvojice kritérií vybereme to důležitější (pro lepší přehlednost sestavujeme při porovnávání tzv. Fullerův trojúhelník). [50]

6.4.2 Výběr terminálu

V prvním kroku Fullerovy metody byl nejprve sestaven přehled zvolených kritérií a alternativ (viz Obrázek 10).

		k1	k2	k3	k4	k5
		Cena bez DPH [Kč]	**Kapacita obličejů**	**Rychlost [sec]**	**Termo-kamera**	**Velikost displeje [”]**
a1	**Hikvision DS-K1T607TEF**	42 109	20 000	0,5	ne	7
a2	**SAFEGOO**	49 050	20 000	0,7	ano	8
a3	**Uniview OET-213H-BTM32**	53 070	10 000	0,2	ano	7

Obrázek 10: Přehled alternativ a kritérií

Zdroj: vlastní zpracování

Fullerův trojúhelník, porovnávající dvojice kritérií, zobrazuje Obrázek 11. Hodnota fi je celkový počet preferencí, hodnota fi+1 je upravený počet preferencí o jedna a hodnota wi je upravená normovaná váha, označující výsledné váhy kritérií.

	k1	**k2**	**k3**	**k4**	**k5**	**fi**	**fi+1**	**wi**
k1		0	0	1	1	2	3	0,20
k2			1	1	1	4	5	0,33
k3				1	1	3	4	0,27
k4					1	1	2	0,13
k5						0	1	0,07
							15	**1**

Obrázek 11: Ohodnocení kritérií

Zdroj: vlastní zpracování

Výsledné pořadí vybraných kritérií s příslušnými normovanými váhami lze vidět na Obrázek 12.

pořadí	kritérium	wi
1.	kapacita obličejů	0,33
2.	rychlost [sec]	0,27
3.	cena bez DPH [Kč]	0,20
4.	termokamera	0,13
5.	velikost displeje [”]	0,07

Obrázek 12: Pořadí kritérií

Zdroj: vlastní zpracování

Dalším krokem v hledání optimálního řešení bylo porovnávání alternativ v rámci každého kritéria. Porovnávání proběhlo stejným způsobem jako v případě porovnávání kritérií. Výsledné tabulky lze vidět níže.

k1	a1	a2	a3	fi	fi+1	wi
a1		1	1	2	3	0,50
a2			1	1	2	0,33
a3				0	1	0,17
				3	**6**	**1**

Obrázek 13: Kritérium „cena bez DPH“

Zdroj: vlastní zpracování

k2	a1	a2	a3	fi	fi+1	wi
a1		0,5	1	2	3	0,43
a2			1	2	3	0,43
a3				0	1	0,14
				4	**7**	**1**

Obrázek 14: Kritérium „kapacita obličejů“

Zdroj: vlastní zpracování

k3	a1	a2	a3	fi	fi+1	wi
a1		1	0	1	2	0,33
a2			0	0	1	0,17
a3				2	3	0,50
				3	**6**	**1**

Obrázek 15: Kritérium „rychlost“

Zdroj: vlastní zpracování

k4	a1	a2	a3	fi	fi+1	wi
a1		0	0	0	1	0,14
a2			0,5	2	3	0,43
a3				2	3	0,43
				4	**7**	**1**

Obrázek 16: Kritérium „termokamera“

Zdroj: vlastní zpracování

k5	a1	a2	a3	fi	fi+1	wi
a1		0	0,5	1	2	0,29
a2			1	2	3	0,43
a3				1	2	0,29
				4	**7**	**1**

Obrázek 17: Kritérium „velikost displeje“

Zdroj: vlastní zpracování

Pro získání konečného pořadí jednotlivých alternativ byly vynásobeny upravené normované váhy kritérií s příslušnými upravenými normovanými váhami alternativ pro příslušné kritérium. Výsledek zobrazuje Obrázek 18.

Pořadí alternativ		
Hikvision DS-K1T607TEF	**0,37**	**1.**
SAFEGOO	**0,34**	**2.**
Uniview OET-213H-BTM32	**0,29**	**3.**

Obrázek 18: Výsledek Fullerovy metody

Zdroj: vlastní zpracování

Metoda Fullerova trojúhelníku označila za vhodné řešení alternativu Hikvision DS-K1T607TEF. Za druhou nejlepší alternativu bylo označeno řešení SAFEGOO, poslední alternativou je terminál Uniview OET-213H-BTM32.

6.5 Kritické zhodnocení navrženého systému

V rámci kritického zhodnocení nového přístupového řešení byla identifikována následující pozitiva a negativa implementace.

- Zvýšení bezpečnosti a zamezení vstupu nepovolaným osobám – na bezpečnost při konání hromadných akcí se kladou vysoké nároky. Nový přístupový systém by plnil preventivní funkci, jelikož není příliš

snadné jej obelstít, případně nápravnou funkci po bezpečnostním incidentu (formou zákazu vstupu neukázněného fanouška na další zápas/y).

- Komfort pro uživatele – nový přístupový systém by zajistil rychlé odbavení fanoušků bez nutnosti předkládání permanentní vstupenky, ať již ve fyzické podobě či ve virtuální podobě. Permanentku by tak nebylo možné zapomenout, ztratit či poškodit. Při ztrátě či poškození permanentky je často nutné uhradit stanovený poplatek.
- Zamezení zneužití permanentek – při ztrátě/odcizení fyzické permanentky lze lístek zneužít, jestliže nedojde ke včasnému nahlášení ztráty příslušnému klubu. Využití biometrických charakteristik by tyto situace eliminovalo.
- Méně administrace – s vydáváním, prodlužováním, blokováním a vydáváním nových permanentek po ztrátě/odcizení se pojí množství administrace. Těchto administrativních úkonů by bylo s nasazením navrhovaného systému značně méně.
- Další funkcionality – potřeba sofistikovanějšího přístupového systému se projevila především v době pandemie covidu-19, kdy mohla být díky biometrickým systémům měřena teplota uživatelů systému, detekována nasazená rouška/respirátor aj.

Nasazení přístupového systému s rozpoznáváním obličejů by mělo i svoje nevýhody, které bychom mohli spatřovat především v těchto bodech:

- velké počáteční náklady – s pořízením kompletně nového přístupového vybavení v podobě turniketů a terminálů by se pořizovací náklady pohybovaly v řádech statisíců až milionů podle počtu zařízení, druhu zvoleného hardwaru apod. Značně menší náklady by byly vynaloženy v případě úpravy stávajícího přístupového zařízení (úprava turniketů a instalace terminálů).
- Určitá míra chybovosti – žádný biometrický systém není 100%. Vždy bude přítomna určitá hodnota FAR a FRR. Uživatel systému může být

po operaci obličeje, může mít úraz v oblasti obličeje apod. Řešením by mohla být mobilní aplikace, v rámci které by se nahrála fotografie do databáze přístupového systému, a zároveň by aplikace obsahovala virtuální permanentku, kterou by se uživatel mohl prokázat v případě chybného zamítnutí přístupu.

- Situace v případě výpadku systému – pro případy dočasného selhání systému by bylo nutné stanovit alternativní scénář. Řešením by i v tomto případě mohla být virtuální permanentka v telefonu, která by sloužila jako záložní důkaz pro prokázání oprávněného uživatele.
- Závislost na kvalitě HW – navržený systém by byl tvořen nepostradatelnými hardwarovými prvky, jejichž selhání by mělo za následek neplnění cíle přístupového systému. Kvůli předejití selhání některého prvku systému by bylo nutné vybírat kvalitní hardware od ověřených prodejců a pravidelně všechny prvky systému servisovat, případně po určité době obměňovat.
- Vysoké nároky na ochranu dat – jelikož se jedná o biometrické údaje, které spadají do zvláštní kategorie osobních údajů, je nutné disponovat technologiemi, které zajistí nejvyšší ochranu dat proti ztrátě a odcizení. Také by bylo nutné zajistit omezení přístupu k těmto údajům třetím stranám a nepovolaným osobám.

7 PRÁVNÍ ASPEKTY NAVRŽENÉHO ŘEŠENÍ

Z pohledu právní regulace je umělá inteligence a strojové učení výzvou pro právo ochrany soukromí, především pak pro ochranu osobních údajů. Důvodem je zpracovávání a nakládání s velkým množstvím údajů o lidech a lidském chování. Na problematiku ochrany soukromí a osobních údajů poukazuje nejenom Evropská unie, ale i národní úřady pro ochranu osobních údajů, právní odborníci, neziskové organizace a další. [43]

Nakládání s osobními údaji podléhá Nařízení evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Biometrické údaje spadají do zvláštní kategorie osobních údajů, které popisuje Článek 9 Zpracování zvláštních kategorií osobních údajů, jehož celé znění přináší Příloha *A*, a je převzato z [47].

Roku 2019 vydal Úřad pro ochranu osobních údajů (ÚOOÚ) stanovisko týkající se možné identifikace a zamezení vstupu neoprávněným osobám na fotbalové stadiony. Ve stanovisku se odkazuje na uvedený článek 9 GDPR o zpracování zvláštních kategorií osobních údajů, který „*vyžaduje pro zpracování biometrických údajů i v případě významného veřejného zájmu výslovné zákonné zmocnění, které musí být přiměřené sledovanému cíli, musí dodržovat podstatu práva na ochranu údajů a poskytovat vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů*“. [46] Požadovaná právní úprava (zákonné zmocnění) se dle ÚOOÚ nenachází ani ve stávajícím zákonu o podpoře sportu, ani v českém zákonu o zpracování osobních údajů či jiných právních předpisech. V roce 2020 ÚOOÚ zveřejnil nové stanovisko k aktuálnímu návrhu nových opatření proti násilí na fotbalových stadionech. V něm zdůrazňuje především skutečnost: „*Každý návrh na použití biometrické technologie a automatizovaného vyhodnocování biometrických údajů musí obsahovat podrobné odůvodnění, včetně posouzení vlivu na ochranu osobních údajů (DPIA)*

podle článku 35 odst. 3 písm. b) GDPR, jestliže jde o rozsáhlé zpracování zvláštní kategorie údajů.“ [51] Součástí posouzení vlivu na ochranu osobních údajů musí být i analýza rizik, která je s využitím této technologie spojena (např. předávání či neoprávněné zpracování údajů). Dále musí na připravovaná legislativní opatření ministerstva vnitra navazovat technická a organizační opatření a musí být stanoveny omezení a záruky, které zamezí snaze využít biometrické informace i pro nežádoucí účely. [51]

ZÁVĚR

V úvodu této diplomové práce byla vypracována rešerše přístupových systémů a biometrických metod spolu s analýzou aplikace metody rozpoznávání obličeje na veřejných místech v ČR i v zahraničí. Při analýze bylo zjištěno, že je rozpoznávání obličeje v ČR aktuálně využíváno ve skiareálech, na letišti Václava Havla v Praze (s plánovaným rozšířením i na další mezinárodní letiště) či v nejrůznějších firmách (např. Metrostav).

Dále byl realizován průzkum akceptace nového přístupového systému mezi hokejovými fanoušky, kterých by se případná implementace systému týkala jako první – jde o fanoušky, kteří vlastní permanentní vstupenku na hokejové zápasy. Za tímto účelem byl osloven vybraný hokejový extraligový klub, s nímž byla navázána spolupráce. Pro potřeby sběru a následné analýzy množství dat byla pro průzkum zvolena metoda dotazníkového šetření.

Dotazníkové šetření se zúčastnilo 315 respondentů, z čehož 85,7 % tvoří muži a 14,3 % ženy. Více než 240 respondentů uvedlo, že navštěvují hokejové zápasy minimálně 21× ročně. První z otázek, týkající se biometrických metod, zkoumala názor hokejových fanoušků osloveného klubu na technologie využívající biometrické metody. Celkem 213 dotazovaných uvedlo, že mají k těmto technologiím pozitivní nebo spíše pozitivní názor, 53 respondentů zastává neutrální názor a 49 dotazovaných zastává názor negativní/spíše negativní. Další otázka zjišťovala, zda již respondenti slyšeli o možnosti ukládání identifikačních markantů namísto fotografie v biometrických systémech. Na tuto otázku 37,8 % dotazovaných uvedlo, že jsou s touto skutečností seznámeni, 62,2 % respondentů naopak uvedlo, že o této možnosti uchování dat dosud neslyšelo. Účelem další z otázek bylo zjistit, zda dotazovaní vědí o veřejných místech v ČR, kde se technologie s rozpoznáváním obličejů využívá (skiareály, letiště, firmy). Z výsledků dotazníku vyplývá, že o využití biometrie na těchto místech vědělo 76,5 % dotazovaných a 23,5 % dotazovaných o využití na uvedených místech nevědělo.

Výsledek stěžejní otázky, která zjišťovala ochotu dotazovaných hokejových fanoušků navštěvovat hokejové zápasy na základě ověření obličeje, dopadl následovně: 190 dotazovaných fanoušků (tedy 60,3 %) by při vstupu na zápasy nový přístupový systém využilo, naopak 125 tázaných (39,7 %) by raději zůstalo u stávajícího přístupového systému. Vzhledem k celkovému počtu permanentkářů daného klubu (klub má aktuálně 1000 permanentkářů) je výsledná míra akceptace navrhovaného přístupového systému rovna 19 %.

Primární cíl této diplomové práce spočíval ve vypracování návrhu implementace přístupového systému, který využívá k řízení přístupu biometrickou metodu rozpoznávání obličeje, pro hokejové prostředí. Před návrhem implementace byla provedena SWOT analýza řešení pro posouzení vlivů působících na zamýšlený projekt. Dále byly specifikovány požadavky, které by měl nový přístupový systém splňovat, aby mohl být považován za úspěšný.

Za nejvhodnější řešení byla označena kombinace tripodového turniketu a terminálu se softwarem zajišťujícím identifikaci osob. Z turniketů splňují stanovené požadavky např. turniket TRISTAR od výrobce Detomatic, turniket TTB07 od výrobce Elvis či turniket TS2100 od výrobce ZKTeco. Pro potřeby instalace přístupového terminálu jsou tyto turnikety po domluvě s výrobcem standardně upraveny na míru. Stěžejní jednotku přístupového systému tvoří terminál, jehož součástí je systém provádějící porovnávání získaných obličejových rysů s databází. Pro výběr vhodného řešení byla v tomto případě použita Fullerova metoda, která porovnávala kritéria: „cena bez DPH“, „kapacita obličejů“, „rychlost“, „termokamera“ a „velikost displeje“. Alternativy (terminály) vstupující do rozhodovacího procesu, které splnily nutné omezující podmínky, byly: Hikvision DS-K1T607TEF, SAFEGOO a Uniview OET-213H-BTM32. Po vyhodnocení procesu Fullerovy metody byl za vhodné řešení označen terminál DS-K1T607TEF od společnosti Hikvision.

POUŽITÁ LITERATURA

[1] AI-assisted security at the Paris 2024 olympic games. *AI-Regulation.com* [online]. [cit. 2023-04-11]. Dostupné z: https://ai-regulation.com/ai-driven-systems-paris-olympics/

[2] BURDA, Karel. *Základy elektronických zabezpečovacích systémů*. Brno: Akademické nakladatelství CERM, 2017. ISBN 978-80-7204-967-7.

[3] Diffusion of Innovation Theory. *MPH Online Learning Modules: Teaching and Digital Learning* [online]. Boston: Boston University School of Public Health, © 2016 [cit. 2023-04-11]. Dostupné z: https://sphweb.bumc.bu.edu/otlt/mph-modules/sb/behavioralchangetheories/behavioralchangetheories4.html

[4] Diffusion of Innovation Theory. *The University of Oklahoma* [online]. Oklahoma: The University of Oklahoma, © 2023 [cit. 2023-04-11]. Dostupné z:https://www.ou.edu/deptcomm/dodjcc/groups/99A2/theories.htm

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

[6] DS-K1T607TEF. *Hikvision* [online]. Hangzhou: Hikvision Digital Technology Co., © 2023 [cit. 2023-04-11]. Dostupné z: https://www.hikvision.com/my/products/Access-Control-Products/Face-Recognition-Terminals/Ultra-Series/ds-k1t607tef/

[7] Eurostar begins facial recognition trials in London. *International Railway Journal* [online]. Simmons-Boardman Publishing, © 2023 [cit. 2023-04-11]. Dostupné z: https://www.railjournal.com/technology/eurostar-begins-facial-recognition-trials-in-london/

[8] Facial Recognition. *City of New York* [online]. New York: City of New York, © 2023 [cit. 2023-04-11]. Dostupné z: https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page

[9] Facial Recognition. *Metropolitan Police* [online]. © 2023 [cit. 2023-04-11]. Dostupné z: https://www.met.police.uk/advice/advice-and-information/fr/facial-recognition

[10] Facial Recognition System Tested on London Train Station. *IT World Canada* [online]. IT World Canada, © 2023 [cit. 2023-04-11]. Dostupné z: https://www.itworldcanada.com/post/facial-recognition-system-tested-on-london-train-station

[11] Facial Recognition Technology. *South Wales Police* [online]. © 2023 [cit. 2023-04-11]. Dostupné z: https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/

[12] Fingerprint recognition. *Biometric Solutions* [online]. Biometric Solutions, 2016 [cit. 2023-04-11]. Dostupné z: https://www.biometric-solutions.com/fingerprint-recognition.html

[13] Geisinger Utilizes CERTIFY Facial Recognition. *Certify Health* [online]. CERTIFY Global, ©2022 [cit. 2023-04-11]. Dostupné z: https://www.certifyhealth.com/geisinger-utilizes-certify-facial-recognition/

[14] Informace ke zpracování osobních údajů. In: *Letiště Praha* [online]. Praha: Letiště Praha, © 2023 [cit. 2023-04-11]. Dostupné z: https://www.prg.aero/sites/default/files/obsah/soubory/informace-ke-zpracovani-osobnich-udaju/informace-ke-zpracovani-osobnich-udaju-v-cctv.pdf

[15] Informace o zpracování osobních údajů. In: *Skiareál Klínovec* [online]. Skiareál Klínovec, © 2023 [cit. 2023-04-11]. Dostupné z: https://klinovec.cz/stahnout/gdpr2018.pdf

[16] Introduction to Iris Recognition. *University of Cambridge* [online]. Cambridge: University of Cambridge, © 2023 [cit. 2023-04-11]. Dostupné z: https://www.cl.cam.ac.uk/~jgd1000/iris_recognition.html

[17] Japan turns to face biometrics for safe and secure Olympics amid COVID-19. *Biometric Update.com* [online]. Biometrics Research Group, © 2023 [cit. 2023-04-11]. Dostupné z: https://www.biometricupdate.com/202103/japan-turns-to-face-biometrics-for-safe-and-secure-olympics-amid-covid-19

[18] KISKU, Dakshina Ranjan, Phalguni GUPTA a Jamuna Kanta SING. *Advances in Biometrics for Secure Human Authentication and Recognition*. Boca Raton: CRC Press, 2014. ISBN 978-1-4665-8243-9.

[19] Letiště Václava Havla. *CertiConVis* [online]. CertiCon [cit. 2023-04-11].

Dostupné z: https://www.certiconvis.cz/pripadove-studie/letiste-vaclava havla/

[20] Macy's and macys.com Notice of Privacy Practices. *Macy's* [online]. New York: Macy's, © 2023 [cit. 2023-04-11]. Dostupné z: https://customerservice-macys.com/articles/macys-and-macyscom-notice-of-privacy-practices-2#collect.info

[21] Madrid's South Bus Station uses Herta's facial recognition software to monitor incidents. *SourceSecurity.com* [online]. Notting Hill Media Limited, © 2000 - 2023 [cit. 2023-04-11]. Dostupné z: https://www.source security.com/news/madrid-south-bus-station-herta-facial-recognition-softwa re-co-8419-ga.1616065060.html

[22] MALTONI, Davide. *Handbook of fingerprint recognition*. London: Springer, 2009. ISBN 978-1-84882-253-5.

[23] MÁCHAL, Pavel, Martina KOPEČKOVÁ a Radmila PRESOVÁ. *Světové standardy projektového řízení: pro malé a střední firmy : IPMA, PMI, PRINCE2*. Praha: Grada, 2015. Manažer. ISBN 978-80-247-5321-8.

[24] MICHAEL, Katina a M. G. MICHAEL. *Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants*. The United States of America: Information Science Reference, 2009. ISBN 978-1-59904-795-9.

[25] Ministerstvo vnitra pokračuje ve zvyšování bezpečnosti na mezinárodních letištích. *Ministerstvo vnitra České republiky* [online]. Ministerstvo vnitra České republiky, © 2023 [cit. 2023-04-11]. Dostupné z: https://www.mvcr. cz/clanek/ministerstvo-vnitra-pokracuje-ve-zvysovani-bezpecnosti-na-mezi narodnich-letistich.aspx

[26] Moscow adds facial recognition payment system. *The Verge* [online]. Vox media, © 2023 [cit. 2023-04-11]. Dostupné z: https://www.theverge.com/ 2021/10/15/22728667/russia-face-pay-system-moscow-metro-privacy

[27] Moscow Metro Introduces 'World's First' Pay-by-Face System. *The Moscow Times* [online]. The Moscow Times [cit. 2023-04-11].

Dostupné z: https://www.themoscowtimes.com/2021/10/15/moscow-metro-introduces-worlds-first-pay-by-face-system-a75300

[28] NORMAN, Thomas. *Electronic Access Control*. Oxford: Elsevier, 2012. ISBN 978-0-12-382028-0.

[29] Obchodní podmínky skiareál Klínovec. In: *Skiareál Klínovec* [online]. Skiareál Klínovec, © 2023 [cit. 2023-04-11]. Dostupné z: https://klinovec.cz/wp-content/uploads/2022/10/A01-OP-AREAL-ZIMA-23-CJ.pdf

[30] Ochrana osobních údajů. *Ještěd* [online]. TATRY MOUNTAIN RESORTS, © 2005 - 2023 [cit. 2023-04-11]. Dostupné z: https://www.skijested.cz/info/ochrana-osobnich-udaju-gdpr

[31] OET-213H-BTM32. In: *Uniview* [online]. Zhejiang Uniview Technologies Co., © 2011-2023 [cit. 2023-04-11]. Dostupné z: https://global.uniview.com/th/res/202207/14/20220714_1842106_UNV%20Face%20Recognition%20Access%20Control%20Terminal%20With%20Digital%20Detection%20Module%20OET-213H-BTM32%20Datasheet-V1.03%20EN_940885_362420_0.pdf

[32] On-line nákup skipasů. *Ještěd* [online]. TATRY MOUNTAIN RESORTS, © 2005 - 2023 [cit. 2023-04-11]. Dostupné z: https://www.skijested.cz/cenik-zima/skipasy/denni-skipasy

[33] PEARSON, Robert. *Electronic Security Systems: A Manager's Guide to Evaluating and Selecting System Solutions*. Oxford: Elsevier, 2007. ISBN 978-0-7506-7999-2.

[34] Privacy Policy. *Ace The helpful place* [online]. Ace Hardware, © 2023 [cit. 2023-04-11]. Dostupné z: https://www.acehardware.com/customer-service?page=privacy-policy#child_WhatTypeofPersonalInformation

[35] Privacy Policy. *Madison Square Garden Entertainment Corp*. [online]. MSG Entertainment Group, © 2023 [cit. 2023-04-11]. Dostupné z: https://www.msgentertainment.com/privacy

[36] PRIVATLIVSPOLITIK. *BRØNDBY IF* [online]. Brøndby IF [cit. 2023-04-11]. Dostupné z: https://brondby.com/privatlivspolitik/

[37] RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita*

člověka ve forenzních a komerčních aplikacích. Praha: Grada, 2008. Profesionál. ISBN 978-80-247-2365-5.

[38] RANKL, Wolfgang a Wolfgang EFFING. *Smart card handbook*. 4th ed. Přeložil Kenneth COX. Chichester: John Wiley, 2010. ISBN 978-0-470-74367-6.

[39] Raphael Hospital. In: *Oosto* [online]. Oosto, © 2023 [cit. 2023-04-11]. Dostupné z: https://oosto.com/wp-content/uploads/2022/08/oosto-case-study-raphael-hospital.pdf

[40] ROGERS, Everett M. *Diffusion of Innovations*. Fifth edition. New York: Simon & Schuster, 2003. ISBN 978-0743222099.

[41] SAFEGOO. *Roy Billing* [online]. ROY BILLING, © 2023 [cit. 2023-04-11]. Dostupné z: https://www.roybilling.cz/safegoo.html

[42] Systém detekce obličejů. *Policie České republiky* [online]. Policie ČR, © 2023 [cit. 2023-04-11]. Dostupné z: https://www.policie.cz/clanek/zverejnene-informace-2020-system-detekce-obliceju.aspx

[43] ŠTĚDROŇ, Bohumír a kol. *Právo a umělá inteligence*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2020. ISBN 978-80-7380-803-7.

[44] The False Rejection Rate. *RecFaces* [online]. Dubai: RecFaces [cit. 2023-04-11]. Dostupné z: https://recfaces.com/articles/false-rejection-rate

[45] Tokyo 2020 Olympics using facial recognition system from NEC, Intel. *CNET* [online]. CNET, © 2023 [cit. 2023-04-11]. Dostupné z: https://www.cnet.com/tech/computing/tokyo-2020-olympics-using-facial-recognition-system-from-nec-intel/

[46] ÚOOÚ k biometrické identifikaci nežádoucích osob na fotbalových stadionech. *Úřad pro ochranu osobních údajů* [online]. Praha: Úřad pro ochranu osobních údajů, © 2013 [cit. 2023-04-11]. Dostupné z: https://www.uoou.cz/uoou-k-nbsp-biometricke-identifikaci-nezadoucich-osob-na-fotbalovych-stadionech/d-35541

[47] Úplné znění GDPR. *Úřad pro ochranu osobních údajů* [online]. Praha: Úřad pro ochranu osobních údajů, © 2013 [cit. 2023-04-11]. Dostupné z: https://www.uoou.cz/uplne-zneni-gdpr/ds-6607/archiv=0&p1=3938

[48] VACCA, John R. *Biometric technologies and verification systems*. Oxford: Butterworth-Heinemann / Elsevier, 2007. ISBN 978-0-7506-7967-1.

[49] VOCHOZKA, Marek. *Metody komplexního hodnocení podniku*. 2. aktualizované vydání. Praha: Grada Publishing, 2020. Finance (Grada). ISBN 978-80-271-1701-7.

[50] Vyhodnocení variant. In: *Vláda ČR* [online]. Praha: Vláda ČR, © 2009-2023 [cit. 2023-04-11]. Dostupné z: https://www.vlada.cz/assets/ppov/lrv/ria/Vzdelavaci-manual-pro-RIA-UV-2017-priloha-Vyhodnoceni-variant_1.pdf

[51] Vyjádření ÚOOÚ k návrhu regulace násilí na fotbalových stadionech. *Úřad pro ochranu osobních údajů* [online]. Praha: Úřad pro ochranu osobních údajů, © 2013 [cit. 2023-04-11]. Dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=40780&n=vyjadreni%2Duoou%2Dk%2Dnavrhu%2Dregulace%2Dnasili%2Dna%2Dfotbalovych%2Dstadionech&p1=3383

[52] Využívání informačních a komunikačních technologií v podnikatelském sektoru - 2022. *Český statistický úřad* [online]. Praha [cit. 2023-04-11]. Dostupné z: https://www.czso.cz/csu/czso/vyuzivani-informacnich-a-komunikacnich-technologii-v-podnikatelskem-sektoru-2022

[53] Využívání informačních a komunikačních technologií v podnikatelském sektoru - rok 2018, leden 2019. *Český statistický úřad* [online]. Praha [cit. 2023-04-11]. Dostupné z: https://www.czso.cz/csu/czso/pouzivani-3d-tisku-a04qsy29py

[54] WAYMAN, James, Anil JAIN, Davide MALTONI a Dario MAIO, ed. *Biometric systems: technology, design and performance.* London: Springer-Verlag, 2005. ISBN 18-523-3596-3.

[55] Working to protect our store colleagues. *Southern Co-op* [online]. Portsmouth: The Southern Co-operative Limited [cit. 2023-04-11]. Dostupné z: https://southern.coop/news/store-update-protecting-our-colleagues

SEZNAM PŘÍLOH

Příloha A *Obecné nařízení o ochraně osobních údajů (GDPR) - Článek 9*

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679
ze dne 27. dubna 2016
o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Článek 9

Zpracování zvláštních kategorií osobních údajů

1. Zakazuje se zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.
2. Odstavec 1 se nepoužije, pokud jde o některý z těchto případů:
    a. subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů, s výjimkou případů, kdy právo Unie nebo členského státu stanoví, že zákaz uvedený v odstavci 1 nemůže být subjektem údajů zrušen;
    b. zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany, pokud je povoleno právem Unie nebo členského státu nebo kolektivní dohodou podle práva členského státu, v němž se stanoví vhodné záruky týkající se základních práv a zájmů subjektu údajů;
    c. zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas;
    d. zpracování provádí v rámci svých oprávněných činností a s vhodnými

zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy tohoto subjektu nebo na osoby, které s ním udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt;

e. zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů;

f. zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo pokud soudy jednají v rámci svých soudních pravomocí;

g. zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů;

h. zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče na základě práva Unie nebo členského státu nebo podle smlouvy se zdravotnickým pracovníkem a při splnění podmínek a záruk uvedených v odstavci 3;

i. zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění přísných norem kvality a bezpečnosti zdravotní péče a léčivých přípravků nebo zdravotnických prostředků, na základě práva Unie nebo členského státu, které stanoví odpovídající a zvláštní opatření pro zajištění práv a svobod subjektu údajů, zejména služebního tajemství;

j. zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely v souladu s čl. 89 odst. 1 na základě práva Unie nebo členského státu,

které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů.

3. Osobní údaje uvedené v odstavci 1 mohou být zpracovávány pro účely uvedené v odst. 2 písm. h), jsou-li tyto údaje zpracovány pracovníkem vázaným služebním tajemstvím podle práva Unie nebo členského státu nebo pravidel stanovených příslušnými vnitrostátními orgány nebo na jeho odpovědnost nebo jinou osobou rovněž vázanou povinností mlčenlivosti podle práva Unie nebo členského státu nebo pravidel stanovených příslušnými vnitrostátními orgány.
4. Členské státy mohou zachovat nebo zavést další podmínky, včetně omezení, pokud jde o zpracování genetických údajů, biometrických údajů či údajů o zdravotním stavu.