Metodika bezpečnosti biometrických systémů pro státní správu

Průzkum a edukace občanů České republiky v oblasti biometrie

TL02000134

Autoři: Ondřej Kanich, Alžběta Krausová, Marcela Petrová Kafková, Martin Drahanský, Tomáš Doseděl, Ján Matejka

Tento projekt je spolufinancován se státní podporou Technologické agentury ČR v rámci Programu ÉTA.

www.tacr.cz

Výzkum užitečný pro společnost.

Verze 1.2 (2022-06-29)

Úvod

Do rukou se vám dostává metodika popisující čím dál tím více využívané biometrické systémy. Jejím cílem je představit vám nejen jak biometrické systémy fungují, ale také jaká jsou jejich úskalí a nebezpečí. Metodika nabízí pohledy ze tří stran – technologického (zaměřeného na to „jak to funguje“), sociologického (zaměřeného na to „jak se k tomu lidí staví“) a právního (zaměřeného na to „jak s takovými daty legálně nakládat“). Metodika byla vytvořena na základě informací získaných z průzkumu mezi obyvateli ČR ohledně využívání biometrických systémů. I přesto, že biometrické systémy podstatně zvyšují bezpečnost, je nutné si na některé věci dávat pozor. Díky informacím z této metodiky by pro vás mělo být mnohem snadnější tato nebezpečí rozpoznávat, avšak především jim předcházet.

Úvod do biometrických systémů

Jako úplně první informace musí zaznít, co to vlastně biometrický systém je. Slovo biometrie je původem z řečtiny a skládá se ze slov „*bios*“ a „*metron*“, přičemž slovo „*bios*“ znamená život a slovo „*metron*“ znamená měřítko. Jedná se tedy o jakési „měření života“. Biometrický systém zajišťuje **automatizované rozpoznávání lidských jedinců** na základě jejich charakteristických anatomických rysů (např. obličej, otisk prstu, duhovka, sítnice) a behaviorálních rysů (tedy chování; např. dynamické vlastnosti podpisu, chůze) [1]. V biomedicínské oblasti však má slovo biometrie poněkud jiný význam – označuje statistické výpočty v biologii či medicíně (např. pravděpodobnosti vzniku nové generace po mutování, podklady pro genetické obory). Text celé této části týkající se biometrických systémů se opírá o [1] [2] [3] a mnohaleté zkušenosti v oboru.

Zatímco automatizované rozpoznání je záležitostí posledních 60 let, tak manuální je řádově starší. Nejstarší dochované informace o použití biometrie pocházejí z Číny ze 14. století n.l. Jedná se však o nepřímé důkazy biometrie – dochované kresby na skalních stěnách znázorňovaly strukturu podobnou otiskům prstů nebo na keramice byly nalezeny otisky prstů autora této keramiky (možná jako důkaz o autorství). První průkazné materiály o použití biometrie pocházejí z 19. století našeho letopočtu. Jedná se například o potvrzení výplaty otiskem prstu koloniální Indii. Na přelomu 19. a 20. století se biometrie začala používat v kriminalistice (antropometrie následovaná otisky prstů).

Pro následující text je nutné vyjasnit si několik pojmů. Prvním z nich je **identita**, to je jednoznačná charakteristika každého z nás. Je však třeba rozlišovat fyzickou a elektronickou identitu. Fyzickou identitu máme pouze jednu, tato identita je definována naším vzhledem a chováním. Na světě neexistuje člověk, který má shodnou fyzickou identitu s někým jiným (např. DNA je i u jednovaječných dvojčat odlišná). U elektronické identity to ovšem neplatí. V elektronickém světě si můžeme vytvořit identit tolik, kolik chceme – může se jednat např. o účty na e-mailových portálech či různé identifikační karty. Úkolem biometrických systémů je pak na základě předloženého biometrického vzorku potvrdit, že se jedná o danou identitu. K tomu se využívá buď proces verifikace nebo identifikace. V případě **verifikace** uživatel (osoba) sdělí systému svoji elektronickou identitu a na základě ní dojde k ověření fyzické identity. Jedná se tak o potvrzení 1:1, výsledkem je potvrzení nebo vyvrácení dané identity. **Identifikace** slouží ke zjištění identity osoby. Jedná se o situaci, kdy osoba zadá systému pouze svoji biometrickou vlastnost, ale nesdělí svoji identitu. Úkolem systému je pak rozpoznat identitu uživatele. Dojde k porovnání vzorku ze vstupu s celou databází uložených vzorků, přičemž výstupem je buď nalezená identita anebo výsledek „identita nenalezena“.

Existují tři varianty, jak můžeme svoji identitu prokázat, těmi jsou: prokázat *něco co víme* (znalost), *něco co máme* (vlastnictví) a *něco co jsme* (biometrie). Do první kategorie patří např. tajné tlačítko, předepsaný postup, heslo či PIN. Ideou tohoto přístupu je náhodná a lehce zapamatovatelná informace, což v sobě bohužel skrývá úskalí relativně lehkého získání této tajné skutečnosti nepovolanou osobou. Druhou kategorií je vlastnictví např. klíč, čipová karta, token, RFID-tag. Ideou tohoto přístupu je vlastnictví něčeho, co nemá nikdo jiný. Zde opět existuje varianta získání tohoto majetku nepovolanou osobou a rovněž i varianta zapomenutí nebo zkopírování. Poslední možností je biometrie, kdy prokazujeme něco, co jsme např. vzhled, chování, projevy v různých situacích). Ideou je skutečnost, že jsme sami nositeli identifikačního klíče. Samozřejmě i zde je jistá možnost zkopírování, zapomenutí však nehrozí. Na základě těchto variant je možné zhodnotit výhody a nevýhody biometrie. K výhodám biometrie

řadíme, že odrazuje útočníky od podvodů, zvyšuje bezpečnost, nemůže být lehce přenesena, zapomenuta či ztracena, eliminuje pokusy o popření identity, zvyšuje pohodlí. Naopak k nevýhodám patří skutečnost, že výstupem je nejednoznačné skóre porovnání (viz dále), nemůže být anulována v případě prozrazení, samotný biometrický systém je napadnutelný, nezachovává soukromí.

Přehled biometrických systémů

Jak již bylo naznačeno, biometrický systém může snímat různé části lidské anatomie nebo chování, zpracování těchto biometrických charakteristik je však podobné. Po nasnímání je biometrický vzorek zpracován extraktorem rysů. Cílem je ze vzorku získat jen relevantní údaje důležité pro verifikaci/identifikaci. Tato data nazýváme **biometrickou šablonou**, ta se následně uloží do databáze v případě, že do systému registrujeme nového uživatele. Pokud má proběhnout verifikace nebo identifikace, je z databáze vyvolána určená vzorová šablona. Následně proběhne porovnání vyvolané šablony (z databáze) a nové (získané) šablony.

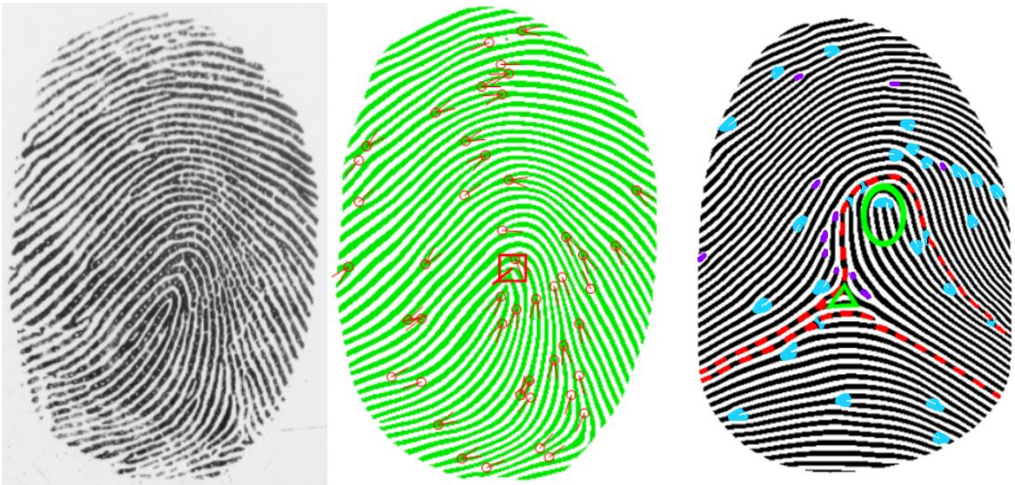
Porovnání je další velmi specifická část biometrického systému. U biometrie nelze předpokládat, že dvě šablony budou totožné. Zatímco heslo do systému musíme zadat úplně stejně, u biometrie porovnáváme, jak moc jsou si šablony podobné. Výsledkem je tak **skóre porovnání**, které určuje, nakolik vyhodnotil systém jejich shodnost. Z pohledu zabezpečení je důležité, kde je uchovávána databáze všech uživatelů systému. Nejjednodušší a nejbezpečnější variantou je **lokální uložení** (např. RFID, biometrický pas). V takovém případě systém přečte údaje (např. z pasu na letišti), nasnímá uživatele a šablony porovná. Data nejsou nikde dále ukládaná, a tak nehrozí jejich zneužití (nutno doplnit, že informace v biometrickém pasu jsou uchovávány i centrálně). Další varianta je uložení šablon v **centrální databázi**. V takovém případě existuje k danému biometrickému systému databáze, ta je propojena se všemi zařízeními. Můžeme hovořit o on-line a off-line centrálním systému. On-line je neustále připojen k centrálnímu serveru a ověřuje uživatele oproti aktuálně načteným informacím. U off-line centrálního systému dojde např. v noci k synchronizaci oprávněných uživatelů a databáze je pak uložena vlastně centrálně. Rozdíly jsou v přenosu dat a způsobu využití těchto odlišných způsobů realizací. Centrální databáze umožňuje např. evidenci docházky do budovy s několika vchody (např. zaměstnání). Nasnímané údaje uživatele jsou porovnány s těmi zaregistrovanými v databázi, a v tomto příkladu pokud odpovídají, uloží se i čas příchodu/odchodu. Nezáleží tak na použitém vchodu do budovy, všechny jsou propojeny pomocí centrální databáze. Ta je obvykle propojena jen s danými zařízeními a nedá se tak k ní připojit z internetu. Nicméně šablony tam jsou uložené a jisté riziko úpravy šablony tu je. Poslední možností je uložení databáze na **cloud**. Takové řešení může být potřeba v situacích, kde není jednoduše možné všechna zařízení propojit. Příklady takového využití mohou být evidence žadatelů o sociální dávky, evidence docházky pro několik poboček nadnárodní korporace atp. V takovém příkladu je databáze uložena na internetu (obvykle jako cloudové řešení). Biometrické údaje jsou tak přístupné všude kde je internetové připojení, ale stejně tak může být databáze napadnuta z internetu.

Biometrické charakteristiky

V úvodu bylo řečeno, že pro potvrzení identity je možné využít velkého množství biometrických charakteristik. Nicméně jen zlomek z nich se prakticky používá. Každá charakteristika má trochu jiné vlastnosti. Mezi tyto vlastnosti patří univerzalita (každá osoba by měla mít danou charakteristiku), jedinečnost (kolik osob je od sebe možné odlišit), konstantnost (jak moc se mění v čase), získatelnost (jak snadno se dá měřit), výkonnost (nesmí být příliš variabilní), akceptaci (jak moc je přijatelná pro uživatele), bezpečnost (jak obtížně se dá falzifikovat), ale i finanční náklady (na pořízení i údržbu) a některé další. Příkladem, sítnice oka je velmi jedinečná, bezpečná a konstantní, bohužel je drahá a uživatelsky nepříliš přívětivá, a tak ji vídáme spíše ve filmech než v praxi. Na druhé straně může stát obličej, u kterého je jedinečnost, bezpečnost, a hlavně konstantnost výrazně horší než u sítnice, nicméně je velmi přívětivý a levný, a tak ho vídáme čím dál častěji. Popsané budou tyto charakteristiky: otisk prstu, obličej, duhovka a podpis, neboť jsou nejčastěji používané a akceptované společností.

Otisky prstů

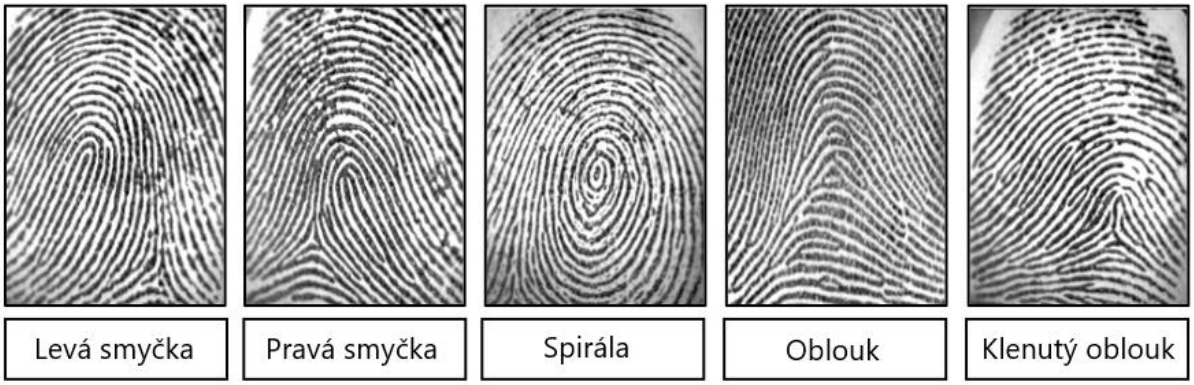
Otisky prstů patří mezi anatomické biometrické charakteristiky a jsou nejznámějším zástupcem. Otisky prstů excelují v jedinečnosti a konstantnosti a nemají vyloženou slabinu. Otisk prstu je obraz vzoru, který vytvářejí vrcholy (a údolí) na povrchu špičky prstu. Spojení a rozpojení těchto vrcholů nazýváme markanty a jen z nich je obvykle tvořena biometrická šablona. Na obrázku 1 vidíme nasnímaný otisk, ten stejný otisk zpracovaný určený k porovnání (červeně jsou vyznačeny markanty) a ukázkový otisk. Na něm jsou také vyznačeny markanty: rozdvojení modře a fialově ukončení. V některých systémech je šablona tvořena jen zakřivením vrcholů v přiložené části prstu. Každý prst každého člověka je unikátní (tedy i jednovaječná dvojčata mají unikátní otisky).



Obrázek 1: Nasnímaný, zpracovaný a ukázkový otisk prstu (ukázkový je převzat z [3]).

Otisky prstů je možné klasifikovat do 3-6 skupin (závisí na použitém systému) podle zobecněného tvaru vrcholů na daném prstu. Ke klasifikaci se využívají dva významné body jádro a delta. Jádro je nejspodnější vyklenutí papilárních linií („střed otisku“ na obrázku 1 naznačeno červeným čtvercem na prostředním otisku a zelenou elipsou na pravém otisku). Delta je místo v otisku kde linie probíhají do tří směrů (na obrázku 1 vpravo označeno zeleným trojúhelníkem). Každý otisk může mít jeden až dvě jádra a žádnou až dvě delty. Na základě jejich vzájemných pozic pak rozlišujeme třídy: *oblouk*, *klenutý oblouk*, *spirála*, *levá smyčka* a *pravá*

smyčka (viz obrázek 2). Otisk prstu je jedna z biometrických charakteristik uložených na biometrických dokladech (pasu a občanském průkazu).



Obrázek 2: Ukázka pěti základní tříd otisků prstů [4].

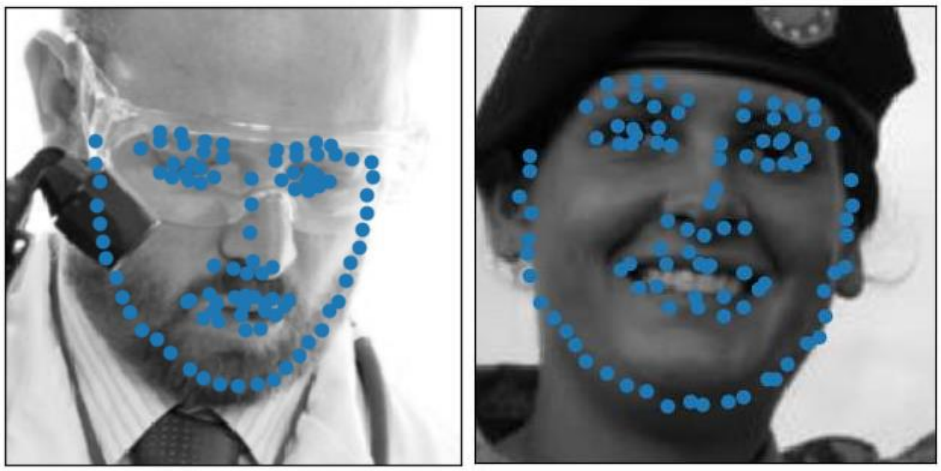
Pro snímání otisků se v dnešní době používají tři technologie: optická, kapacitní a ultrazvuková. **Optická** využívá přítlaku otisku na plochu senzoru, díky čemuž jde poměrně snadno a kvalitně oddělit papilární linie. Optický snímač je možné zabudovat pod displej. Některé řešení využívají rovnou pro snímání otisků fotoaparátu (a následně složitějších algoritmů zpracování). Optické snímače patří k nejlevnějším, trochu problematičtější je jejich zabezpečení proti falzifikátům. **Kapacitní** technologie snímá otisk pomocí malých plošek měřících elektrické vlastnosti prstu. Donedávna byla právě tato technologie nejlevnější, a tedy i nejčastěji používaná často v kombinaci jako s průtahovým snímáním. **Ultrazvukové** snímání bylo dlouhou dobu drahé, rozměrné ale velmi přesné. Aktuálně je nabízeno pouze jedním výrobcem a přesné detaily nejsou známé (tedy není ani jasné, nakolik se např. snížila přesnost při zmenšení rozměrů a ceny). V některých případech jsou otisky snímání pomocí **inkoustu a papíru** (prst se namočí do inkoustu a obtiskne na papír). Typicky používané policií na tzv. daktyloskopickou kartu. Ta se pak případně pro digitální využití skenuje.

Prakticky se využívají dva přístupy k rozpoznání podle otisků prstů. Jsou jimi porovnání založené na **markantech** a **rozpoznání vzorů**. Pozice, směr (udávaný tím, kam by pokračovala linie při rozdvojení a předchozí směr u ukončení) a obvykle i typ markantu se používá pro rozpoznání. Dostatečné množství markantů musí být na podobných pozicích. Tato metoda je využívána i daktyloskopickými experty, ti musejí nalézt 10-12 shodných markantů pro přístup do systému. **Rozpoznáním vzorů** je v dnešní době míněno využití neuronových sítí. Ty jsou často využity tam, kde není dostatek informací pro hledání markantů. To může nastat např. u senzoru jehož plocha pro snímání otisků je příliš malá na zachycení dostatečného množství markantů.

Obličej

Rozpoznávání podle obličeje je nejpřirozenějším způsobem rozpoznání osob u lidí. Každý z nás je schopen velmi přesně rozeznávat obličeje našich známých, rodiny a to i ve velmi složitých podmínkách. Automatizované rozpoznání pracuje na základě význačných bodů v obličeji (např. oči, pusa, nos, atd.), jak je vidět na obrázku 3. V poslední době se obličeje zpracovávají pomocí hlubokých neuronových sítí, jejichž rozhodování není úplně přesně popsané. Každým rokem se objevují nové (či úspěšně upravené) architektury neuronových sítí zajišťující čím dál tím robustnější a přesnější identifikaci. Jak již bylo zmíněno, silnou stránkou rozpoznání podle

obličeje je přívětivost a cena, slabší je hlavně konstantnost. Obličeje dvojčat jsou velmi podobné a tvoří tak velkou výzvu pro biometrické systémy. Fotka obličeje je nedílnou součástí různých identifikačních karet, a tak nepřekvapí, že jsou i součástí biometrických cestovních dokladů.



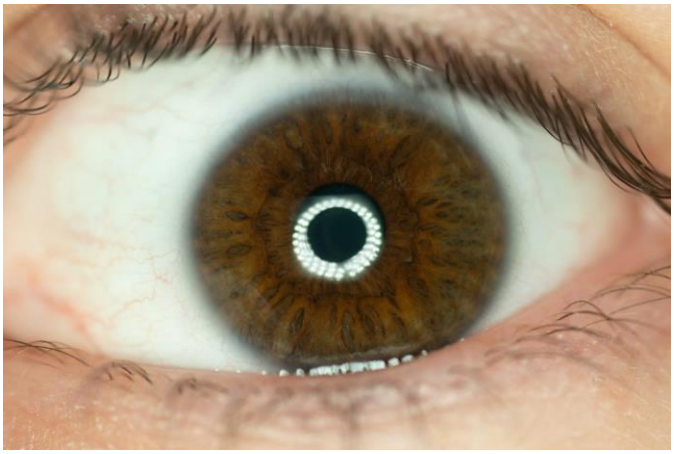
Obrázek 3: Ukázky obličejů s detekovanými význačnými obličejovými body.

Pro snímání obličeje lze využit jakákoliv kamera s dostatečným rozlišením. Obličej se dá snímat ve 2D (pouze fotka), 3D (obsahuje informaci o hloubce) a jistou možností je i snímat termokamerou a získat tak termosnímek. Velkým problémem termokamer je jejich cena, naopak zařízení schopná projektovat mřížku na obličej v „neviditelném“ NIR osvětlení jsou poměrně levná. Velmi často se tak setkáváme s rozpoznáním podle obličeje ve 3D pomocí strukturovaného světla. U obličeje máme dva zásadní problémy při snímání: okolní osvětlení a natočení**. Okolní osvětlení** může výrazně snížit úspěšnost verifikace. Při instalaci je potřeba to vzít v úvahu a vyhnout se tak pozicím, kde bude např. přímé slunce svítit do obličeje nebo do kamery. Většina databází obsahuje pouze fotky z čelního (frontálního pohledu). To ovšem znamená, že spolehlivost neuronových sítí (a tedy i porovnání) výrazně klesá, pokud uživatel není ve stejném čelním pohledu, ale má **natočenou hlavu**. Odolnost vůči natočení je jednou z hlavních výzev aktuálních algoritmů na rozpoznání obličeje.

Duhovka

Duhovka oka (tedy přední barevná část oka) se rovněž používá pro rozpoznání. Možná překvapivě spíše než samotná barva, se využívá textura (vzory, obrazce, čáry viditelné na duhovce). V průběhu tvorby šablony je duhovka změněna na seznam čísel. Ukázka duhovky je na obrázku 4. Každá duhovka je jiná, tedy i dvojčata mají duhovku odlišnou. Duhovka je velmi konstantní, bezpečná, a její silnou stránkou je jedinečnost, horší to je naopak s cenou. Také duhovka je součástí biometrických cestovních dokladů.

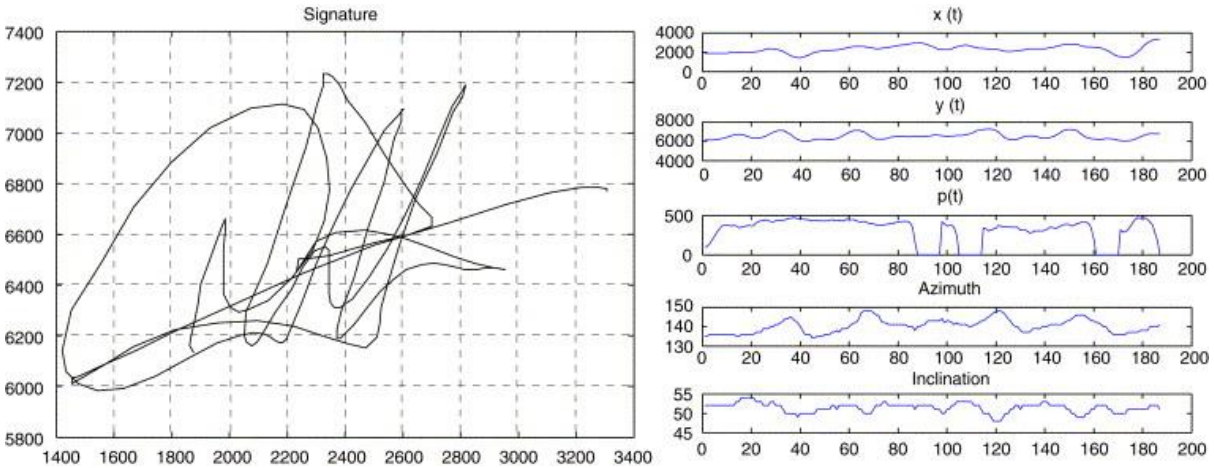
Snímání duhovky může probíhat pomocí viditelného světla (pak je snímač víceméně obyčejný foťák s kvalitním rozlišením) nebo pomocí NIR (*near infra-red*) osvětlení. Druhá varianta je preferovanější, protože potlačuje barvu duhovky, přičemž zvýrazňuje texturu. Nejznámější algoritmus rozpoznávání podle duhovky ji prvně lokalizuje a oddělí od zbytku oka i víček. Následně je „rozbalena“ do pásu na němž se vyznačí významné texturní body, podle kterých se následně porovnává. Používají se i metody založené na analýze vlastních komponent nebo metody založené na genetických algoritmech.



Obrázek 4: Detailní obrázek duhovky.

Podpis

Podpis zastává v biometrii speciální pozici. Dají se totiž porovnávat nejen jeho statické vlastnosti (pak by se řadil mezi anatomické charakteristiky), ale dá se snímat i samotný vznik podpisu (přesné tahy pera, naklonění, rychlost atp.), pak se řadí tyto vlastnosti do dynamických charakteristik. Jedná se o jednu z nejčastěji používaných forem potvrzení identity v každodenním životě. Systém na rozpoznání podpisu se však často drží pouze statických vlastností (tedy bez časového rozměru). V tomto směru je bohužel podpis jednou z nejhorších charakteristik mající velmi špatnou jedinečnost i bezpečnost, excelující pouze v přívětivosti a ceně. V takové podobě je uložen i v biometrických dokladech. Využití dynamických vlastností však může jeho vlastnosti rapidně zlepšit. Pro snímání takového podpisu je však potřeba speciálního pera nebo alespoň podložky, příp. využití vhodného tabletu. Snímek podpisu je na obrázku 5.

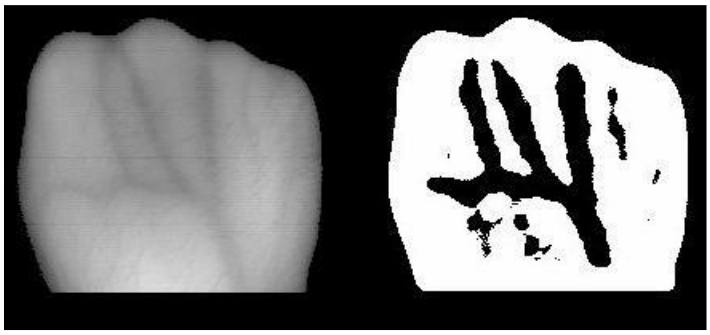


Obrázek 5: Ukázka statického podpisu a jeho dynamických vlastností [4].

Žíly ruky/dlaně/prstu

V reálných situacích se lze setkat i s dalšími charakteristikami. Rozpoznání podle žil ruky (dlaně, hřbetu ruky nebo i prstu) se využívá v některých zemích při verifikaci u bankomatu a u některých notebooků. Principiálně se jedná buď o prosvícení (transmisivní metoda) nebo odraz (reflexivní metoda), kdy pomocí NIR (*near infra-red*) osvětlení získáme snímek žil. Nastavením vlnové délky je možné od sebe dokonce odlišit okysličenou a neokysličenou krev.

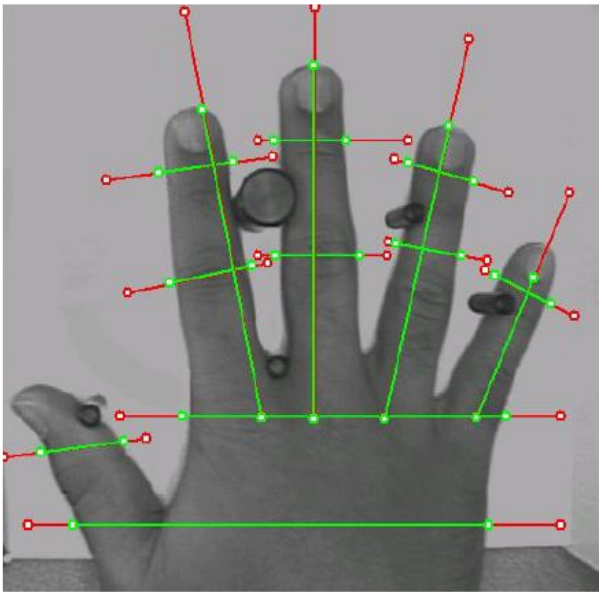
Ukázka snímku a zpracovaných žil je na obrázku 6. Žilní řečiště je poměrně konstantní a bezpečné. Problém je trochu v unikátnosti a výkonnosti (obzvlášť u žil prstu – kde jich je poměrně málo).



Obrázek 6: Ukázka snímku hřbetu ruky a extrahovaného žilního řečiště [1].

Geometrie ruky

Pro vstup do některých budov či kontrolu docházky se využívá geometrie (tvar) ruky. Její využití je limitováno nižším počtem uživatelů (protože jedinečnost je u geometrie ruky nižší). Snímá se obvykle kamerou zaměřenou na distanční sloupky, o které se opírají prsty. Z nich se pak zjistí délky prstů, zápěstí, šířky prstů a podle nich a metodou zarovnání kontury dlaně pak probíhá porovnání. Některé špatné vlastnosti geometrie ruky je možné částečně překonat s využitím 3D. Zisk dalšího rozměru pro porovnání je jen výhoda (je možné posuzovat i výšku prstů a navíc lze snímek přesněji proměřit).



Obrázek 7: Ukázka snímku ruky včetně naznačených bodů pro rozpoznávání [1].

Další biometrické charakteristiky

Při policejním vyšetřování je pak možné se setkat s rozpoznáním podle DNA, chůze, dentálního obrazu a dalších, které spadají spíše do forenzní oblasti. **DNA** funguje na základě poměrně malého množství genetické informace (kapička krve, vlas s kořínkem apod.). Z něj se namnoží DNA a u takto namnožených provedou testy. DNA je tak možno využít v policejní praxi. Přes perfektní přesnost je tato metoda velmi drahá na použití.

Rozpoznání podle **chůze** vyžaduje záznamy např. z kamerového systému. Není třeba příliš vysoké rozlišení. Sleduje se pohyb středu těla nebo siluety. Chůze je vysoce individuální a jen problematicky se mění. Problémem však může být různé oblečení, hlavně volnější.

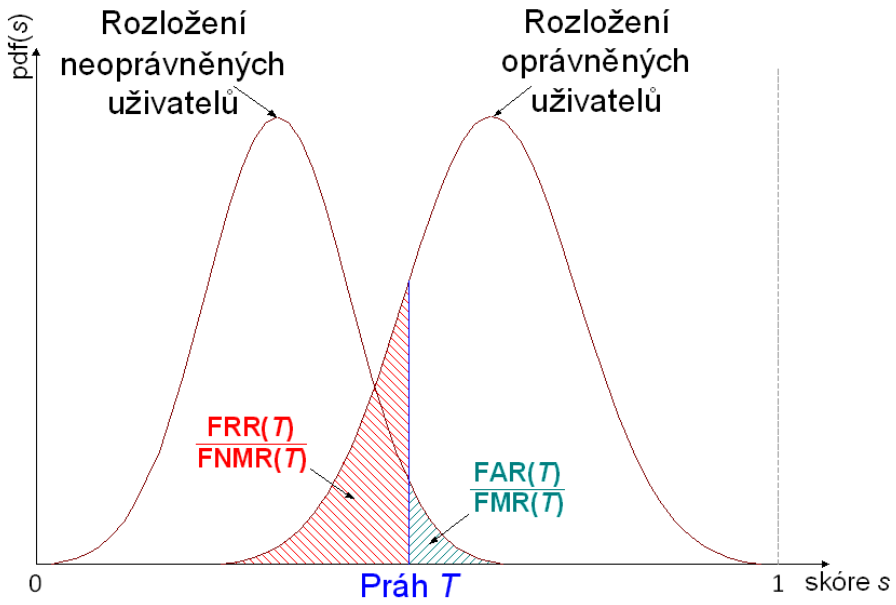
Dentální obraz je již čistě forenzní záležitost využívaná převážně při katastrofách pro ztotožnění.

Některé mobilní telefony a jiné asistenční systémy využívají hlasové příkazy, některé z těchto zařízení reagují pouze na hlasové příkazy daného uživatele (rozpoznávají-li i uživatele, tak provádějí tedy verifikaci na základě **hlasu**). Velmi dobré vlastnosti má **sítnice**, nicméně potýká se z nízkou akceptací a vysokou cenou. Z pohledu bezpečnosti a unikátnosti jde však o jednu z nejlepších charakteristik. Pro zvýšení úrovně bezpečnosti existují i **multimodální biometrické systémy**, tedy biometrické systémy požadující pro přístup několika biometrických charakteristik (např. obličej a duhovka), avšak tyto mohou kombinovat více různých senzorů stejné biometrické charakteristiky, algoritmů či způsobů práce s biometrickou charakteristikou. Výhodou je zvýšení bezpečnosti biometrického systému a dále umožnění přístupu jednou charakteristikou, když je druhá poškozena (např. řezná rána na bříšku prstu), nicméně na druhou stranu zvyšují čas potřebný k rozpoznání a rovněž navyšují cenu biometrického řešení.

Hodnocení výkonnosti biometrických systémů

Již víme, že biometrický systém může fungovat na základě různých biometrických charakteristik, které jsou různě vhodné pro rozličné účely. Víme také, že výsledkem není rovnou potvrzení nebo vyvrácení identity, ale skóre porovnání. Je tedy vůbec možné nějakým způsobem ohodnotit výkonnost biometrických systémů? A dále určit, který je lepší a který je horší? Možné to samozřejmě je, ale není to tak jednoduché jako například sdělení, že bezpečné heslo musí mít alespoň 8 znaků. Cílem tohoto textu je vysvětlit základy pro pochopení proč je skóre porovnání problematické a podle čeho lze systémy porovnávat. Vysvětlení všech detailů by pravděpodobně bylo delší než celá metodika.

Biometrický systém jako takový ohodnocuje, jak moc jsou si biometrické šablony podobné pomocí **skóre porovnání**. Pro zjednodušení si ho představíme jako pravděpodobnost toho, že jsou šablony totožné. V takovém případě 0 je nulová podobnost a 1 (nebo 100 %) je maximální podobnost. Šablony však nikdy totožné nejsou, nejedná-li se o tentýž soubor hodnot. Porovnáváme totiž části těla nebo naše chování – příklady: nikdy na senzor nepřitlačíme prst úplně stejným tlakem (kůže se rozpíná, otisk bude trochu jiný), nikdy se nepodepíšeme úplně stejně (zasekne se nám pero, roztřese ruka), atd. Vlivy okolního prostředí, uživatele samotného, ale i použitého senzoru mohou biometrický vzorek dostatečně ovlivnit. Musíme tedy určit práh, přičemž veškeré hodnoty skóre porovnání nižší než práh systém odmítne, naopak veškeré hodnoty stejné a vyšší přijme. Ideálně by se nám nemělo nikdy stát, že systém přijme neoprávněného (“špatného”) uživatele, jenže tak to bývá málokdy. Výsledek je pak podobný grafu 1 (vodorovná osa je skóre porovnání, svislá pravděpodobností rozložení daného uživatele). Některým neoprávněným uživatelům se povede přihlásit, a naopak některým oprávněným bude přístup zamítnut.



Graf 1: Rozložení oprávněných a neoprávněných uživatelů s chybovými mírami.

Tak získáváme dvě chyby, které systém může provést. Jsou jimi chybné přijetí (pustím do systému podvodníka/útočníka) a chybné odmítnutí (nepustím do systému právoplatného uživatele). U systému se tak často uvádí chybová míra **FAR** – *False Accept Rate* (míra chybného přijetí) nebo **FRR** - *False Reject Rate* (míra chybného odmítnutí). Obě dvě hodnoty by měly být co nejnižší. Co se však stane, když posuneme práh více vpravo směrem k 1? V určité fázi nepustíme žádného neoprávněného uživatele (tzn. FAR bude 0), nicméně to také znamená, že často odmítneme právoplatného uživatele (FRR bude vysoké). Takové nastavení bude vhodné pro vysoce střežený objekt, kde nevadí, že se i právoplatný uživatel bude muset pokoušet přihlašovat několikrát, avšak je jistota, že se tam nedostane útočník. Snížením prahu naopak dosáhneme toho, že se každý právoplatný uživatel přihlásí napoprvé bez problému, ale občas se do systému dostane “omylem” i podvodník/útočník. Takové nastavení může být vhodné např. pro přístup do mobilního telefonu, kde se očekává časté přihlašování právoplatných uživatelů, kteří chtějí být rozpoznáni napoprvé, ale nedá se očekávat, že přístup do telefonu bude zkoušet větší množství útočníků.

Mimo tyto dvě základní chyby je možné se setkat ještě s dalšími selháními samotného systému před provedením porovnání a to je: míra selhání snímání (**FTA** – *Fail To Acquire*; používá se i **FTC** – *Fail To Capture* ve stejném významu) je podíl verifikací či pokusů, u kterých systém selže při snímání či lokalizaci vzorku s dostatečnou kvalitou. Míra selhání snímání zahrnuje:

- pokusy, kde systém není schopen lokalizovat biometrický vzorek, přestože je prezentován,
- pokusy, u nichž selže segmentace, a
- pokusy, ve kterých nesplňuje nalezený vzorek práh kontroly kvality samotného snímače.

Míra selhání snímání závisí na prazích pro kvalitu vzorku, stejně jako povolená doba trvání snímání vzorku či povolený počet prezentací. Tato nastavení by měla být obsažena ve zprávě

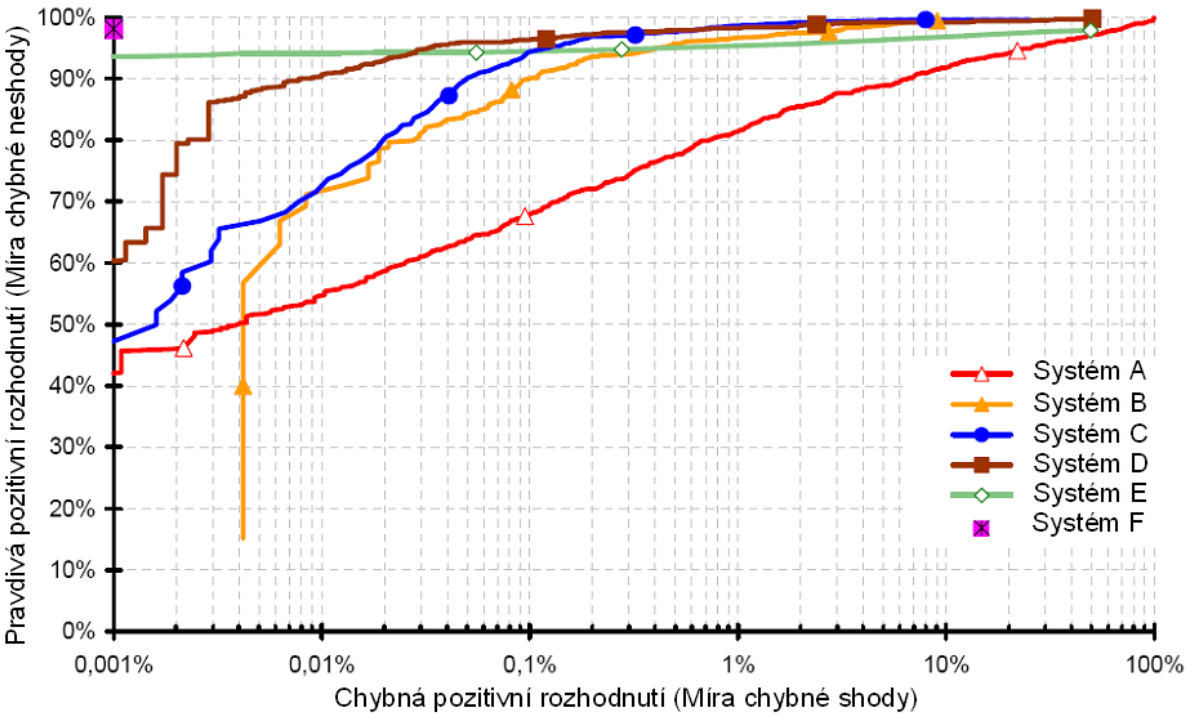
současně s pozorovanou mírou selhání snímání. Tato míra tak primárně ukazuje kvalitu použitého senzoru.

Druhou metrikou selhání před porovnáním je pak míra selhání registrace (**FTE** – *Fail To Enroll*; významově téměř totožný je i název **FTX** – *Fail To eXtract*) je podíl populace, pro kterou systém selže při kompletaci procesu registrace. Míra selhání registrace zahrnuje takové jedince:

- z jejichž nasnímaného biometrického vzorku není možné extrahovat rysy používané daným systémem,
- kteří nejsou schopni vyprodukovat vzorek s dostatečnou kvalitou při registraci (což zahrnuje i ty kteří selžou vlivem nezkušenosti s používáním daného zařízení), a
- kteří nemohou spolehlivě vyprodukovat rozhodnutí shody s jejich nedávno vytvořenou šablonou během pokusů o potvrzení použitelnosti registrace.

Míra selhání registrace závisí na registrační politice, která řídí práh kvality vzorku pro registraci, práh rozhodnutí pro potvrzení použitelnosti registrace (tedy úspěšnost extrakce rysů používaným systémem) a počet pokusů nebo času přípustných pro registraci v registrační transakci. Politika registrace by měla být popsána společně s pozorovanou mírou selhání registrace.

Místo, kde se na grafu 1 protnou rozložení oprávněných a neoprávněných uživatelů, se nazývá míra vyrovnání chyb (**EER** – *Equal Error Rate*). Pokud je práh *T* nastaven na tuto hodnotu, pak platí, že míra chybného přijetí a míra chybného odmítnutí dosahují stejné hodnoty. Mezi výrobci systémů se pak vžil přenesený význam, a to je přímo hodnota FAR (a FRR) pro práh nastavený na EER. Toto označení není přesné, ale bývá využíváno, a proto je zde zmíněno. Pomocí této hodnoty je pak možné systémy vůči sobě porovnávat. Nicméně je třeba vzít vždy v úvahu, že nastavení prahu na EER není vždy žádoucí a vhodné. Velmi záleží na očekávaném využití systému.



Graf 2: Ukázky ROC křivek.

Pokud od tvůrců biometrického systému zjistíme jen FAR nebo jen FRR, tak bohužel o systému samotném příliš nevíme. Tvůrce systému totiž mohl posunutím prahu zajistit lepší výsledky. Aby se zamezilo možnosti takové úpravy, používá se pro hodnocení **ROC křivka** (*Receiver Operating Curve*). Ta není závislá na prahu, a tak je ideální pro porovnání výkonnosti dvou systémů. Jak je vidět na příkladu v grafu 2, na vodorovné ose je FAR a na svislé FRR křivka, tudíž je ukázána závislost obou metrik bez rozhodovacího prahu. Ideální systém by se tady zobrazil jako "levý horní roh" (systém F). Dále je vidět, že pro různá nastavení jsou poměry FAR a FRR různé – vzhledem k plánovanému použití je tak možné přesněji vybrat, který systém je ideální. Pro představu, podle normy [6] jsou hodnoty FAR menší než 10^{-2} pro základní bezpečnostní sílu, menší než 10^{-4} pro střední zabezpečení a hodnoty menší než 10^{-6} pro vysoké zabezpečení.

Standardy a certifikace

Tato část stručně popisuje standardy týkající se biometrických systému a přehled certifikátů využívaných u biometrických systémů mobilních telefonů.

Standardy

Ve světě jsou používány standardy od dvou mezinárodních organizací, kterými jsou **ANSI** (*American National Standards Institute*) – **INCITS** (International Committee for Information Technology Standards), jehož podkomise zahrnují mj. B10 (identifikační karty), M1 (biometrie) a T4 (bezpečnostní techniky), dále potom **ISO/IEC** (*International Organization for Standardization*/*International Electrotechnical Commission*), s obdobnými podkomisemi SC 17 (karty a osobní identifikace), SC 37 (biometrie) a SC 27 (bezpečnostní techniky IT). V České republice se o normy stará Česká agentura pro standardizaci (https://www.agentura-cas.cz/), přičemž české normy v oblasti biometrie, identifikačních karet a bezpečnosti v IT se opírají v drtivém množství případů o normy ISO/IEC, tedy vzniknou české překlady s označením ČSN ISO/IEC následované číslem normy, příp. verzí a rokem vydaní.

Testování biometrických systémů na základě norem a platných předpisů by měly provádět nezávislé instituce – nejčastěji univerzity či výzkumné organizace (v Německu např. Fraunhofer Gesellschaft).

V případě testování biometrických systémů je třeba definovat typ **scénáře**, podle kterého se bude testovat. Tyto jsou definovány v normě ČSN ISO/IEC 19795 a rozlišujeme tři: *hodnocení technologie* (primárně testování pouze v laboratoři přímo vývojáři a znalými uživateli v přesně definovaných podmínkách), *hodnocení scénáře* (cílem je co nejvíce se přiblížit reálnému prostředí a reálné skupině osob, která bude daný systém používat) a *provozní hodnocení* (kdy se jedná již o reálnou instalaci u zákazníka, avšak v prvních několika měsících dochází ke sběru log souborů a optimalizaci veškerých procesů, aby se zajistila co nejvyšší výkonnost systému).

V případě testování výkonnosti systému využitím nasbíraných datasetů (šablon různých uživatelů a více instancí od stejného uživatele), tak je třeba stanovit **velikost datasetu**. Zde je třeba zahrnout *vlivy vnitro- a mezitřídní variability* (jak moc se nám mění vlastní biometrická charakteristika v čase a jak moc jsme si podobní v dané biometrické charakteristice s jinými jedinci), *vlivy okolního prostředí* (např. sluneční svit může na obličeji vytvořit stín) a v neposlední řadě i kolik *porovnání* chceme provést *v rámci jedné osoby* (tomu odpovídá počet uložených záznamů v různých sezeních totožné osoby) a kolik *porovnání* chceme provést *mezi*

různými osobami (kolik osob celkem nasnímáme a v kolika sezeních). V případě porovnávání většího počtu různých osob a máme-li zároveň uložen větší počet šablon z mnoha instancí u každé osoby, může počet kombinací narůst do obrovských výšin, kdy potom porovnávání bude trvat dny či týdny.

Mezi nejvýznamnější normy, které by měly být zmíněny, řadíme (kompletní seznam na webu „ISO/IEC JTC 1/SC 37 – Biometrics“):

- ISO/IEC 19784 – Biometric application programming interface
- ISO/IEC 19785 – Common biometric exchange formats framework
- ISO/IEC 19794 – Biometric data interchange formats
- ISO-IEC 19795 – Biometric performance testing and reporting
- ISO/IEC 24709 – Conformance testing for the biometric application programming interface (BioAPI)
- ISO/IEC 24713 – Biometric profiles for interoperability and data interchange
- ISO/IEC 24779 – Cross-jurisdictional and societal aspects of implementation of biometric technologies
- ISO/IEC 29109 – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794
- ISO/IEC 29794 – Biometric sample quality
- ISO/IEC 30107 – Biometric presentation attack detection
- ISO/IEC 30137 – Use of biometrics in video surveillance systems
- ISO/IEC 39794 – Extensible biometric data interchange formats

Přehled certifikátů mobilních telefonů

Dle zprávy [7] jsou standardy, kromě ISO/IEC a ANSI v jednotlivých trzích tyto:

- Amerika a Evropa – Google, Microsoft, EMVCO, FIDO Alliance, GlobalPlatform a další
- Střední východ – Aadhaar
- Japonsko, Korea, Čína – Alipay, UnionPay, FIDO Alliance

Z hlediska autentizace mohou být mobilní telefony certifikovány aliancí FIDO (*Fast IDdentity Online*). Tato aliance se zaměřuje na certifikování autentizačního procesu, tzn. i biometrických systémů v mobilním zařízení.

Pro biometrickou certifikaci FIDO vyžaduje:

- *False Reject Rate* (FRR) menší než 3:100 pro horní hranici 80% intervalu spolehlivosti. FRR je měřeno na úrovni transakcí. Pro odhad hodnoty musí být použita rovnice uvedená v ČSN ISO/IEC-19795-1 8.3.2. [8]
- *False Accept Rate* (FAR) menší než 1:10.000 pro horní hranici 80% intervalu spolehlivosti. FRR je měřeno na úrovni transakcí. Odhad této hodnoty se provádí podle ČSN ISO/IEC-19795-1 8.3.3. [8]

FIDO Presentation Attack Detection Criteria – pro jednotlivé kategorie útoku (podle ISO/IEC 30107, část 3 [9]) se vyhodnocuje *Impostor Attack Presentation Match Rate* (IAPMR). Například pro falzifikáty kategorie A musí platit, že 5 ze 6 falzifikátů dosahují hodnoty IAPMR menší než 20 % a zároveň při použití všech falzifikátů kategorie A musí být hodnota IAPMR menší než 50 %.

Pro hodnocení odolnosti certifikovaného systému proti prezentačnímu útoku rozdělilo konsorcium FIDO prezenční útoky podle požadavku na čas, vybavení a znalosti do 3 kategorií – viz tabulka 1.

Tabulka 1: Kritéria pro hodnocení certifikovaného systému dle FIDO.

		Otisk prstu	**Obličej**	**Duhovka/Oko**	**Hlas**
Úroveň A	**Čas**: < 1 den **Expertíza**: laik **Vybavení**: standardní	papírový výtisk, přímé použití latentního otisku na skeneru	papírový výtisk obličeje, zobrazení obličeje na mobilním zařízení	papírový výtisk obličeje, zobrazení obličeje na mobilním zařízení	přehrávání zvukového záznamu
	Zdroj biometrické charakteristiky: okamžitý, snadný	získání otisku prstu ze zařízení	fotografie ze sociálních médií	fotografie ze sociálních médií	záznam hlasu
Úroveň B	**Čas**: < 7 dnů **Expertíza**: profesionál **Vybavení**: standardní, specializované	otisky prstů z umělých materiálů, jako je želatina, silikon	papírové masky, video zobrazení obličeje (s pohybem a blikáním)	video zobrazení duhovky (s pohybem a blikáním); tištěná duhovka s kontaktními čočkami / okem panenky	přehrávání zvukového záznamu konkrétního hesla, hlasové mimiky
	Zdroj biometrické charakteristiky: střední	latentní tisk, odcizený obrázek otisku prstu	video subjektu, vysoce kvalitní fotografie	video subjektu, vysoce kvalitní fotografie	záznam hlasu konkrétní fráze, vysoce kvalitní záznam
Úroveň C	**Čas**: > 7 dnů **Expertíza**: expert **Vybavení**: specializované, na zakázku	3D tištěné podvrhy	silikonové masky, divadelní masky	kontaktní čočka / protetické oko se specifickým vzorem	hlasový syntetizátor
	Zdroj biometrické charakteristiky: obtížný	3D otisky prstů od subjektu	vysoce kvalitní fotografie, 3D informace o obličeji od subjektu	vysoce kvalitní fotografie v blízké IR	několik nahrávek hlasu pro výcvik syntetizátoru

Kompletní popis FIDO certifikace a průběhu testování je k nalezení v [10]. U mobilních telefonů certifikuje konsorcium FIDO operační systém (např. Android má od verze 7.0 certifikaci

FIDO2 (pro možnost přihlašování bez hesla [11]), tak i biometrické komponenty [12]. Prvními telefony, které získaly tuto certifikaci na senzor otisků prstů, byly Samsung Galaxy S10 a S10+.

Souhrnně lze konstatovat, že kromě FIDO neexistuje certifikační autorita biometrických systémů v mobilních telefonech.

Ochranný systém KNOX od společnosti Samsung byl certifikován v některých zemích:

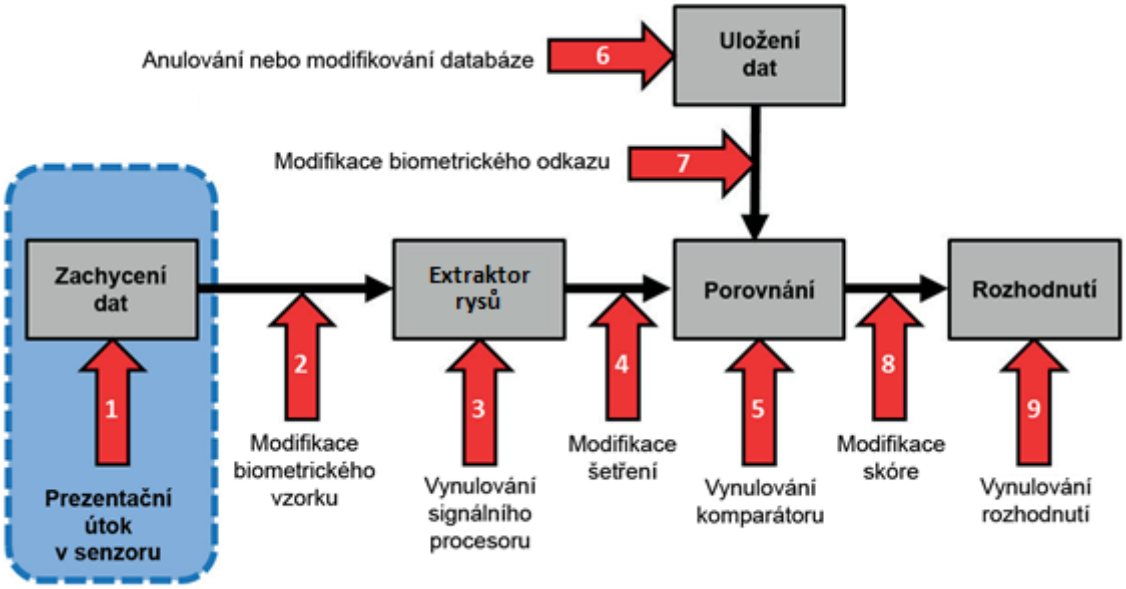
- USA/Kanada: Federal Information Processing Standard 140-2 Certification – Level 1 certification for both data-at-rest (DAR) and data-in-transit; National Institute of Standards and Technology (NIST)
- USA: Security Technical Implementation Guides (STIGs), DISA Approved Product List; Defense Information Systems Agency (DISA)
- USA: Common Criteria Certification for Mobile Device Fundamental Protection Profile (MDFPP); National Information Assurance Partnership (NIAP) USA: US Department of Defense Approved Products List; National Information Assurance Partnership (NIAP)
- Velká Británie: End User Devices (EUD) Security Guidance; Communications and Electronics Security Group (CESG)
- Finsko: Finnish National Security Auditing Criteria (KATAKRI II); Finnish Communications Regulatory Authority (FICORA)
- Austrálie: Protection Profile for Mobile Device Fundamentals; Australian Signals Directorate (ASD)

Bezpečnost

Obecně zabezpečení biometrických systémů sdílí mnoho prvků se zabezpečením jakéhokoliv informačního systému. Některé prvky zabezpečení jsou však specifické a funkčnost dalších z nich závisí na uživateli, tedy na každém z nás. Právě na tyto prvky primárně míří následující text. Na úvod budou vypsány všechny problematické části (přehledně jdou vidět na obrázku 8):

1. Předložení falzifikátu biometriky snímači (tzv. prezentační útok).
2. Opětovné zaslání již dříve použitých biometrických údajů (tzv. *replay attack*). Biometrický signál, který již byl použit biometrickým zařízením nebo je uložen v databázi, je opětovně předložen na vstupu. Případně úplná modifikace přenesených dat do extraktoru rysů.
3. Ovlivnění extraktoru rysů. Například Trojský kůň může zapříčinit vygenerování předem určené množiny rysů, která je následně (chybně) použita pro vygenerování šablony.
4. Změna biometrických rysů. Během přenosu dat mezi modulem extrakce rysů a porovnávacím modulem může dojít k záměně přenášených dat.
5. Ovlivnění porovnávacího modulu. Například Trojský kůň může zapříčinit vygenerování předem definovaného skóre porovnání pro určitou událost, pomocí čehož útočník může proniknout do systému.

6. Změna biometrické šablony. Šablona uložená v databázi může být pozměněna na šablonu útočníka, čímž se útočník může dostat do systému jako falešný oprávněný uživatel.
7. Útok na přenosový kanál mezi porovnávacím (nebo registračním) modulem a databází (uloženými šablonami). Během přenosu dat může dojít k záměně šablony.
8. Změna finálního rozhodnutí. Výsledek vygenerovaný v závislosti na zvoleném prahu a vypočteném skóre porovnání může být znegován.
9. Útok na samotnou aplikaci. Samotná aplikace, která si vyžádala autentizaci, může být také přímým terčem útoku, tj. dojde k vyřazení biometrické autentizace.



Obrázek 8: Příklady možných útoků na biometrický systém.

Body 2, 3, 4, 5, 7, 8, 9 se týkají samotných modulů biometrického systému, přenosu dat mezi těmito moduly, případně zastřešující aplikací. Tyto části by měly být zabezpečeny samotnými tvůrci biometrického systému a aplikace. Tedy přenos a některé údaje by měly být rozhodně šifrovány. Systémy by měly být maximálně aktualizovány, a tedy šance nabourání např. Trojského koně by tak měla být minimální. Samozřejmě je třeba poznamenat, že vyšší úrovně zabezpečení vyžadují vyšší nároky jak na cenu, tak na rychlost a spolehlivost. Je tedy potřeba najít vhodný kompromis mezi bezpečností a uživatelskou přívětivostí (např. nastavením vhodného prahu skóre porovnání). Běžný uživatel tak musí na toto myslet při pořizování biometrického systému a ujistit se, že jeho dodavatel zajišťuje bezpečnost na požadované úrovni. Podobně je na tom bod 6 (šablona v databázi) – tady je potřeba také myslet na to, jakým způsobem bude realizována databáze (a k čemu všemu bude připojena). Tento problém lokální, centrální a cloudové databáze již byl vysvětlen výše. Výběr řešení hraje roli při pořizování biometrického systému. Stejně tak je dobré zjistit, jestli jsou šablony šifrované (samotný fakt, že to není přímý snímek ale “jen” šablona nestačí).

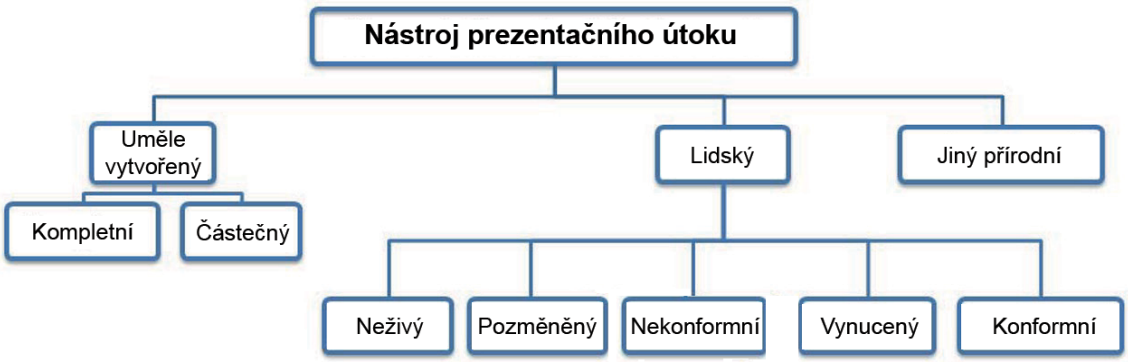
Jedním z možných problémů může představovat bod 2. **Replay útok** počítá standardně s obnovou opakováním komunikace na spojnici mezi moduly. U dotykových snímačů otisků prstů hrozí riziko reaktivace předchozího otisku. Za určitých okolností je možné přesvědčit některé senzory, že otisk, který zůstal na sklíčku senzoru, je nové snímání. V tu chvíli dochází

k podobným efektům jako u replay útoku. Tomu se dá zabránit očištěním sklíčka senzoru po jeho použití.

Největším rizikem tak zůstává modrá část, tj. **prezentační útok**. Ten se dá provést dvěma způsoby. První z nich závisí na nastavení systému, jak bylo popsáno v části Hodnocení výkonnosti. Při nastaveném nízkém prahu je možné, že při předložení biometriky bude uživatel potvrzen jako jiný (tento typ útoku se jmenuje *low-effort*). Při vhodném nastavení a vhodné biometrické charakteristice (nedostatečná jedinečnost by mohla vést také k nesprávnému přijetí) by k něčemu takovému nemělo docházet. Zbývá tedy druhý způsob, kdy se útočník připravuje a zcela vědomě se snaží systém prolomit.

Prezentační útok

Nehledě na očekávání, které v nás zanechává filmová produkce, je prakticky možné obejít systém jen dvěma způsoby, a to (a) připravením falzifikátu (neboli nástrojem prezentačního útoku) nebo (b) donucením uživatele k verifikaci/identifikaci (kompletní přehled útoku je na obrázku 9). Druhá možnost se běžného obyvatelstva příliš netýká, stejně tak jako destrukční varianty (např. uříznutí prstu), které ani nemusejí fungovat. I takové situace ovšem mají řešení. Pomocí metod na detekci okysličené a neokysličené krve je například možné detekovat uříznutý prst. Situace je řešitelná i pro odemčení z donucení. V některých systémech je možné při použití speciálního hesla nebo při přiložení specifického prstu vyvolat tzv. tichý poplach. Ten upozorní bezpečnostní složky, zatím co biometrický systém může (ale také nemusí pracovat dále).



Obrázek 9: Přehled možných nástrojů prezentačního útoku.

Smutným faktem zůstává, že biometrické systémy se dají prolomit vytvořením **falzifikátu** (*nástroje prezentačního útoku*). Jak již bylo zmíněno, tvorba falzifikátů je u některých biometrických charakteristik velmi obtížná, u některých snadnější. Nemá asi smysl popisovat metody pro tvorbu falzifikátů pro všechny charakteristiky. Zaměříme se na ty dvě nejpoužívanější, tj. obličej a otisky prstů.

Primitivní metody tvorby **falzifikátu** (nástroje prezentačního útoku) **pro obličej** jsou prostě vytištění fotky nebo prezentování fotku na mobilním telefonu. Jak již bylo zmíněno, většina zařízení používá pro rozpoznání obličeje metodu pracující s 3D povrchem. Za takových podmínek nutně nemůže stačit pouze fotka. Poměrně robustní falzifikát tak lze vytvořit pomocí 3D tisku. Vytištěný obličej je vhodné upravit (především doplnit oči, nos, pusu a uši), případně je možné jej potáhnout latexem a následně plně nalíčit.

U přípravy **falzifikátu** (nástroje prezentačního útoku) **pro otisků prstů** je situace o něco složitější. Jako první je totiž potřeba získat vzor, ten se na rozdíl od obličeje obvykle nedá jen tak snadno někde vyfotit. Je tedy potřeba připravit si půdu a donutit oběť zanechala někde svůj latentní otisk, ten zviditelnit, naskenovat a pak s ním pracovat v digitálním formátu. Dalším obvyklým krokem je příprava formy (obvykle deska plošných spojů) na ni se nanese vzor. Přidáváním materiálu jako je např. latex, želatina, silikon. Je zřejmé, že každý senzor se chová trochu jinak a je potřeba tvorbu falzifikátu upravit.

Aby se prezentačnímu útoku předešlo, je nutné v průběhu snímání provést také kontrolu živosti (neboli detekci prezentačního útoku). To je víceméně samostatný modul s tímto jediným cílem. Stejně jako při tvorbě falzifikátů, existuje mnoho různých metod na **detekci živosti** (*detekci prezentačního útoku*). Obě tyto činnosti jsou velmi úzce spjaté s použitou biometrickou charakteristikou, resp. typem snímání. Navíc jsou velmi propojené, neprolomitelné detekce jsou prolamovány sofistikovanějšími falzifikáty a na ty se připravují dokonalejší metody detekce. V oblasti **detekce živosti obličeje** se primárně příliš mnoho metod nepoužívá (nebo jsou dobře utajené), každopádně zde se nabízí poměrně jednoduché řešení = mimika. Zapojení mimických svalů se na falzifikátu jen velmi problematicky simuluje. U **otisku prstů** je to jiné tam se poměrně často používají kapacitní kroužky ověřující elektrické vlastnosti prstu (zároveň tak částečně brání sepnutí snímače v kapse). Sofistikované řešení je pak např. využití multispektrálních vlastností. V průběhu snímání otisku, je otisk osvětlen několika vlnovými délkami. Jednotlivé vrstvy kůže mají specifickou odezvu na vlnové délky. V dalším kroku pak běží potvrzení, že jsou všichni registrovaní biometrickými vlastnostmi (rysy).

Samozřejmě existují i další možnosti pro ztížení prolomení systému. Mezi ně patří například využití **multimodálního** systému. Tedy systému, který kombinuje několik různých charakteristik (příp. různých snímačů nebo způsobu zpracování). Myšlenka je jednoduchá na prolomení takového systému bude potřeba připravit větší počet kvalitních falzifikátů a každý musí při verifikaci uspět. Podobně pak lze postupovat i s metodami mimo biometrii, tj. kombinaci hesla a biometrie apod. Důležité však je, že falzifikát se nedá připravit bez znalosti dané biometriky. Neexistuje nic jako univerzální klíč, pokud útočník bude chtít přístup do systému, musí získat data navázaná na daný biometrický vzorek (tj. např. otisk prstu levého palce daného uživatele, pravou duhovku daného uživatele, …). A právě této části se dá do jisté míry předcházet.

Získat data může útočník pouze dvěma způsoby, a to (a) *prolomením databáze* a získáním dané šablony, nebo (b) *přímo od uživatele*. Prolomením a získáním dat z databáze nepřipadá v úvahu. Jak bylo řečeno výše, databáze bývají kvalitně zabezpečené, data v ní uložená by měly být pouze šablony, a ty by měly být zašifrované. I kdyby bylo prolomeno šifrování (což je velmi nepravděpodobné), u většiny biometrických charakteristik se nedá ze šablony připravit falzifikát.

Zbývá tak jediná možnost získání dat **přímo od uživatele**, tedy přímo od nás. Je možné tomu nějakým způsobem předcházet? Odpověď záleží na dané biometrické charakteristice. Pravděpodobnost, že vám někdo nasnímá sítnici (oční pozadí) bez vašeho vědomí je téměř nulová. Pravděpodobnost, že se někomu povede získat alespoň částečný otisk prstu u vás doma je poměrně vysoká (nutno dodat, že částečný otisk nemusí na tvorbu falzifikátu postačovat). Předcházet takovým možnostem získání biometrických dat je téměř nemožné (ano jistě, dá se chodit pořád v rukavicích, se zakrytým obličejem atd.). Je ale ještě jedno místo, kde většina z nás bez jediného zaváhání vloží biometrické údaje v perfektní kvalitě, a ještě se spokojeným výrazem. A to jsou sociální sítě nebo internet obecně. Těžko zabráníme tomu, aby na internetu

byl náš obličej (a nutno dodat, že ten si může poměrně snadno kdokoliv na ulici vyfotit bez našeho vědomí), ale vzpomeňte si, až příště budete ukazovat vztyčený palec nebo symbol vítězství ("véčko"). Dnešní mobilní telefony mají velmi kvalitní foťáky, přidáme dobré osvětlení a neštěstí je hotovo. Na obrázku 6 je vidět vlevo obrázek stažený z internetu a vpravo po drobných úpravách.

Podobně by se dalo postupovat s velkým množstvím biometrických charakteristik. Tím se dostáváme k poslední velké nevýhodě biometrie. Nemůžete ji zapomenout, ale **nemůžete ji** také **změnit**. Pokud jsou jednou biometrická data na internetu, vždy bude pro případné útočníky možné si je najít a zneužít. Vědecká komunita bádá nad možnostmi takzvané zrušitelné (odvolatelné) biometrie, aby bylo možné podobně jako heslo si změnit zabezpečení biometrickými údaji, ale není to vůbec jednoduché a nejlepším řešením je prostě si své biometrické údaje chránit – vždyť se jedná o naše osobní údaje.

Obrázek 6: Příklad zveřejnění vlastních biometrických údajů.

Postup vyřazování biometrických záznamů

Přesné možnosti práv v souladu s GDPR budou popsány dále. Tato část se pouze věnuje technickému zajištění vyřazování biometrických záznamů. Je možné se setkat s třemi způsoby uložení informovaných souhlasů, a tedy i různými způsoby, jak osoby z databází mazat.

První přístup je, že **informovaný souhlas je zcela anonymní**. Nikdy zpětně nelze dohledat, komu konkrétní souhlas patří. V případě žádosti o vyřazení je nutné vyřadit celou databázi a provést snímání a podepisování souhlasu znova.

Druhou variantou je, že **informovaný souhlas je uložen pod průběžných číslem**. Tedy první souhlas má číslo 1, druhý 2, atd. V takové situaci je možné uložit si tabulku převodního vztahu konkrétní osoby na konkrétní číslo. Tu má typicky pouze správce údajů, a tak standardně nelze z informovaného souhlasu nic vyčíst. V případě, že přijde požadavek na vyřazení tak se správce podívá, jaké číslo dané osobě patří. Její souhlas pak může zničit a stejně tak všechna data uložena pod tímto pořadovým číslem.

Třetí variantou je, že **informovaný souhlas obsahuje všechny informace**. V tu chvíli již není anonymní, ale na druhou stranu z obsahu zjistíme rovnou vše co je potřeba pro zrušení záznamu daného uživatele. V případě, že osoba požádá o vyřazení z databáze, je vyhledán její informovaný souhlas a následně je se všemi daty zničen.

Popis zjištění chování občanů ČR v letech 2020-2021

Tato část vychází z uveřejněné souhrnné výzkumné zprávy [13]. Ta se primárně týká výsledků výzkumu mezi obyvateli České republiky ohledně využívání technologií včetně biometrických systémů.

Metodologie sběru dat

Data, na jejichž základě popisuje vztah a znalosti obyvatel České republiky o biometrických systémech a obecně bezpečném ovládání moderních technologií, pocházejí z reprezentativního šetření obyvatel České republiky, kterým byl získán soubor (*n* =) 2341 respondentů 18letých a starších. Ten je doplněn daty z dětské populace získané od žáků základních a středních škol ve věku 12 až 19 let v celkovém počtu (*n* =) 363 žáků. Data pro dospělou populaci (18 a více let) jsou z výběrového šetření realizovaného od srpna 2020 do listopadu 2020. Data mladších respondentů pocházejí z výzkumu realizovaného ve školách v lednu až dubnu 2021. U dotazníků pro oba typy sběrů dat byla zachována co největší shoda, tak aby bylo možné sledovat rozrůznění znalostí a postojů dle věku respondentů. Zadavatelem výzkumu dospělých, realizátorem výzkumu nezletilých a garantem odborné části výzkumu je Katedra sociologie fakulty sociálních studií Masarykovy univerzity v Brně.

Nejprve byl realizován výzkum dospělé populace České republiky. Výzkumný vzorek byl konstruován kvótním výběrem jako reprezentativní pro obyvatele ČR ve věku 18 a více let. Kvóta byla vypočítána na základě dat poskytovaných ČSÚ dle SLDB2011. Kvótními znaky bylo pohlaví, věk, vzdělání, velikost obce a kraj. Struktura populace byla dle kvótních parametrů následně přepočítána na požadovanou velikost výběrového souboru. Sběr proběhl metodou standardizovaných rozhovorů tváří v tvář (face-to-face) s využitím elektronického dotazníku v notebooku (CAPI). Všem respondentům byl po ukončení rozhovoru tazateli předán edukační letáček shrnující základní fakta o biometrii „Biometrie není jen otisk prstu. Dávejte pozor, komu své údaje poskytnete“, který je zároveň výstupem projektu – popularizačním textem.

Data z populace mladší 18 let byla sbírána přímo členy výzkumného týmu. Sběr dat zkomplikovala opatření proti nemoci COVID-19. Pro získání dat proto byly využity osobní kontakty ve školách, což nám umožnilo vstup do terénu v podobě připojení do on-line výuky a tím možnost sesbírání dat on-line. Návazná přednáška VUT se při tomto způsobu odkládá na dobu, kdy bude možné žáky ve škole navštívit. Bezprostředně po ukončení vyplňování on-line dotazníku byli žáci edukováni videem vytvořeným týmem z řešitelského pracoviště VUT. Při volbě tříd a škol jsme v maximální možné míře dbali na variabilitu z hlediska věku, velikosti obce a typu školy. Celkově jsme ve čtyřech školách získali data ze 14 tříd, což nám přineslo (N=) 363 vyplněných dotazníků.

Struktura vzorku

Náš výzkumný vzorek v konečné podobě čítá 2 704 respondentů ve věku od 12 do 88 let. Z hlediska pohlaví mírně převažují ženy (52 %) oproti mužům (48 %). Žáci tvoří 13 %, respondenti se základním vzděláním pak 14 %, se středoškolským vzděláním bez maturity 31 %, se středoškolským vzděláním s maturitou 29 % a s vysokoškolským vzděláním 13 %. Ještě jednou bychom rádi upozornili, že se žáky sice pracujeme jako se vzdělanostní kategorií, nicméně největší vliv má u těchto respondentů vzhledem k jejich specifickému postavení v životní dráze jejich věk. Poměrně rovnoměrně jsou respondenti zastoupeni podle velikosti místa bydliště, tak jak to odpovídá i podílu populace v těchto různých typech sídel.

Hlavní zjištění

V následujících částech budou postupně rozebrány hlavní zjištění a výsledky provedeného výzkumu. Konkrétně z pohledu vlastnictví technologií, expertnosti v jejich užívání, užívání internetu, aktivního používání emailu, nákupů na internetu, zabezpečení mobilního telefonu, rizikovosti chování na internetu, zkušenosti se zneužitím hesel, legitimity využívání biometrie a reálnosti hollywoodských scénářů.

Vlastnictví technologií

Základním předpokladem bezpečného užívání moderních technologií je jejich vlastnictví. Zjišťovali jsme proto, které s technologií, u kterých se dnes mohou běžně setkat s biometrií (počítáme zde i cestovní pas, jelikož biometrické údaje jsou povinnou součástí cestovních pasů) obyvatelé České republiky vlastní. Naším cílem bylo také zjistit, jak jsou na tom Češi s vlastnictvím vybraných technologií. "Chytrý" telefon je v naší populaci vlastněný již téměř univerzálně, vlastní jej 81 % respondentů, viz tabulka 2. Výrazně rozšířené jsou i další technologie. Notebook vlastní 74 % respondentů, stolní počítač a tablet cca 40 % respondentů. Televizi s internetovým připojením vlastní přesně polovina respondentů. Bankovnictví v mobilu dnes využívá 53 % Čechů. Cestovní pas je pak součástí výbavy dvou třetin dotázaných (66 %).

Tabulka 2. Relativní četnost vlastněných technologií obyvateli České republiky.

Vlastním…	**%**
notebook	74
stolní počítač	41
tablet	38
„chytrý" telefon	81
bankovnictví v mobilu	53
TV s internetovým připojením	50
cestovní pas	66

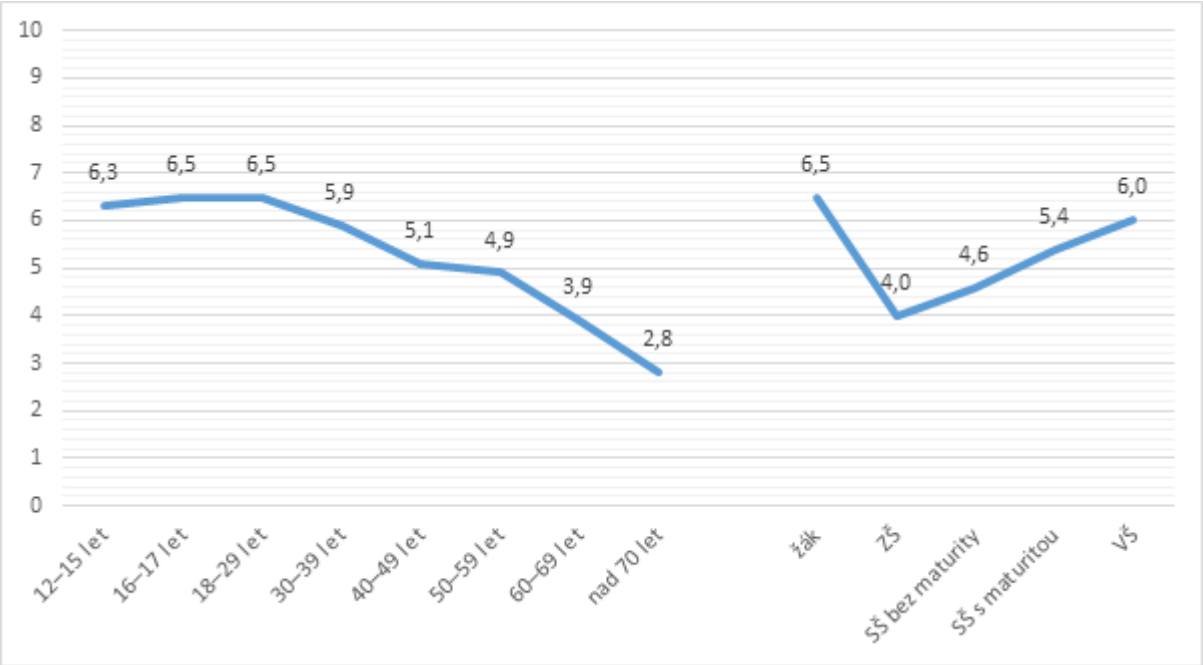
Pozn. Dopočet do 100 % tvoří lidé, kteří danou technologii nevlastní.

Vlastnictví technologií je výrazně stratifikováno věkem a vzděláním. Lidé do 18 let jsou nejčastějšími uživateli technologií (kromě internetového bankovnictví, které výrazně méně využívají děti do 15 let – pouze 47 % z nich), přičemž až do věkové kategorie 50–59 let nejsou mezi věkovými kategoriemi zásadní rozdíly. Je zde patrný pouze velice mírný pokles od věkové kategorie 18–29 let. K výraznému poklesu dochází od 60 let a k dalšímu pak od 70 let. Lidé v těchto seniorských věkových kategoriích výrazně méně vlastní notebook (52 %, 34 %), stolní počítač (37 %, 26 %), tablet (20 %, 12 %), chytrý telefon (56 %, 32 %), bankovnictví v mobilu (26 %, 11 %) a televizi s internetovým připojením (33 % a 19 %). Nejčastěji vlastněnou technologií mezi dvěma nejstaršími kategoriemi (ačkoli stále méně často než u mladších) je cestovní pas, který vlastní přes polovinu respondentů ve věku 60–69 let (52 %) a 38 % dotázaných nad 70 let. Další trend je možné sledovat u lidí vlastnících stolní počítač a televizi s

internetovým připojením, kdy jsou vlastníky výrazně častěji lidé ve věku 12–17 let, poté ve věku 18–59 let nejsou patrné téměř žádné rozdíly a od 60 let opět dochází k poklesu. Z hlediska vzdělání jsou největšími vlastníky technologií lidé s vysokoškolským vzděláním, s klesajícím vzděláním klesá i podíl vlastníků. Muži a ženy se v tom jaké technologie vlastní nijak neliší. V seniorských kategoriích jsou mírně častějšími vlastníky ženy než muži.

Expertnost v užívání technologií

Kromě toho, jestli lidé doma mají vybrané technologie, nás také zajímalo, nakolik jsou experty v používání technologií. To jsme zjišťovali otázkou na sebepojetí respondenta jako experta na 10bodové škále, od (1) *úplného neználka* po (10) *experta/profesionála*. Průměrně se lidé zařazovali do středu škály (hodnota 5,2 na stupnici od 1 do 10), přičemž pohlaví ani velikost bydliště nehrály roli. Jejich technologické sebevědomí tedy není příliš vysoké. Opět zde však byl patrný rozdíl mezi věkovými a vzdělanostními kategoriemi (graf 3). Subjektivní expertnost je poměrně stabilní ve třech nejmladších věkových kategoriích (12–29 let) na hodnotách 6,3–6,5, nicméně od věkové kategorie 30–39 let dochází k mírnému poklesu (rozdíl 0,6 bodu oproti předchozí kategorii) až do kategorie 50–59 let (pokles o 1 bod vůči kategorii 30–39 let). Výrazný pokles je pak viditelný u kategorie 60–69 let (pokles o 1 bod vůči kategorii 50–59 let) a 70 a více let (pokles o 1,1 bodu vůči kategorii 60–69 let). Subjektivní expertnost tak klesá od věkové kategorie 30–39 let a je nejmenší u lidí nad 60 let.



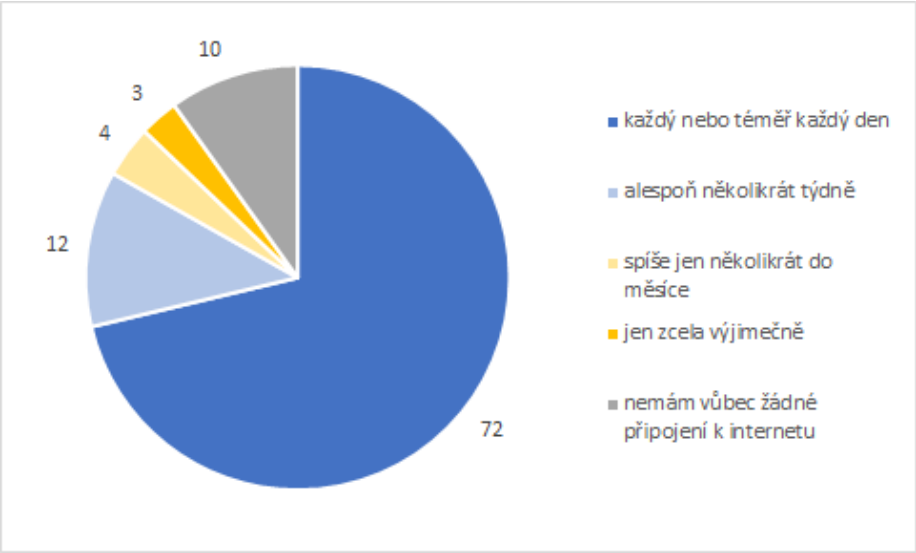
Graf 3. Vliv věku a vzdělání na subjektivní expertnost (průměr; 1 = úplný neználek, 10 = expert).

Vliv vzdělání je opět téměř lineární, jako tomu bylo u vlastnění technologií. S vyšším dosaženým vzděláním subjektivní expertnost roste a tyto rozdíly jsou značné. Nicméně i zde platí, že za největší experty se považují žáci.

Užívání internetu

Dostupné internetové připojení je dalším základním předpokladem pro možnost moderní technologie používat, v našem výzkumu jsme nehodnotili dostupnost internetu, ale pouze samotné používání. Aktivními uživateli internetu je v Česku přes 80 % lidí (72 % jej užívá každý nebo

téměř každý den a 12 % alespoň několikrát do týdne). Nejmenší podíl představují lidé, kteří internet užívají jen několikrát do měsíce nebo výjimečně (4 % a 3 %). Lidí, kteří v Česku vůbec nemají připojení k internetu, je 10 %. Vše shrnuje graf 4. Používání internetu je tedy výrazně rozšířené a můžeme také konstatovat, že lidé jsou buď v podstatě každodenními uživateli, nebo se bez internetového připojení téměř či úplně obejdou. A právě tato skupina lidé, kteří internet nepoužívají vůbec si vzhledem k rozvoji e-governmentu a e-health zaslouží specifickou pozornost.



Graf 4. Frekvence užívání internetu.

Na to, jak často Češi využívají internet, má opět vliv věk a vzdělání. Pro potřebu této části jsme kategorie sloučili na aktivní uživatele (užívají alespoň několikrát týdně), výjimečné uživatele (několikrát do měsíce nebo výjimečně) a na ty, co nemají připojení k internetu vůbec. Z tabulky 3 je jasně patrné, že nejméně často používají internet lidé nad 60 let, přičemž je i velký rozdíl mezi kategorií 60–69 let a 70 a více let, kdy nejstarší uživatelé jsou aktivními uživateli jen v 39 %. V těchto dvou věkových kategoriích navíc narůstá podíl těch, kteří jsou zcela bez připojení k internetu, v kategorii 60–69 let je to 23 % lidí a v kategorii nad 70 let dokonce 47 % lidí. K výraznému poklesu však dochází již od kategorie 50–59 let. Podstatné je přitom, že i v nejstarší věkové kategorii se podíl aktivních uživatelů internetu přibližuje polovině. Mezi nezletilými je pak podíl aktivních uživatelů v podstatě absolutní.

Tabulka 3. Frekvence užívání internetu podle věku (%).

Věk uživatele	**12–15**	**16–17**	**18–29**	**30–39**	**40–49**	**50–59**	**60–69**	**70+**
aktivní uživatel	100	99	96	96	92	85	64	39
výjimečný uživatel	0	1	3	3	7	9	13	14
bez připojení k internetu	0	0	0	1	1	6	23	47
celkem	100	100	100	100	100	100	100	100

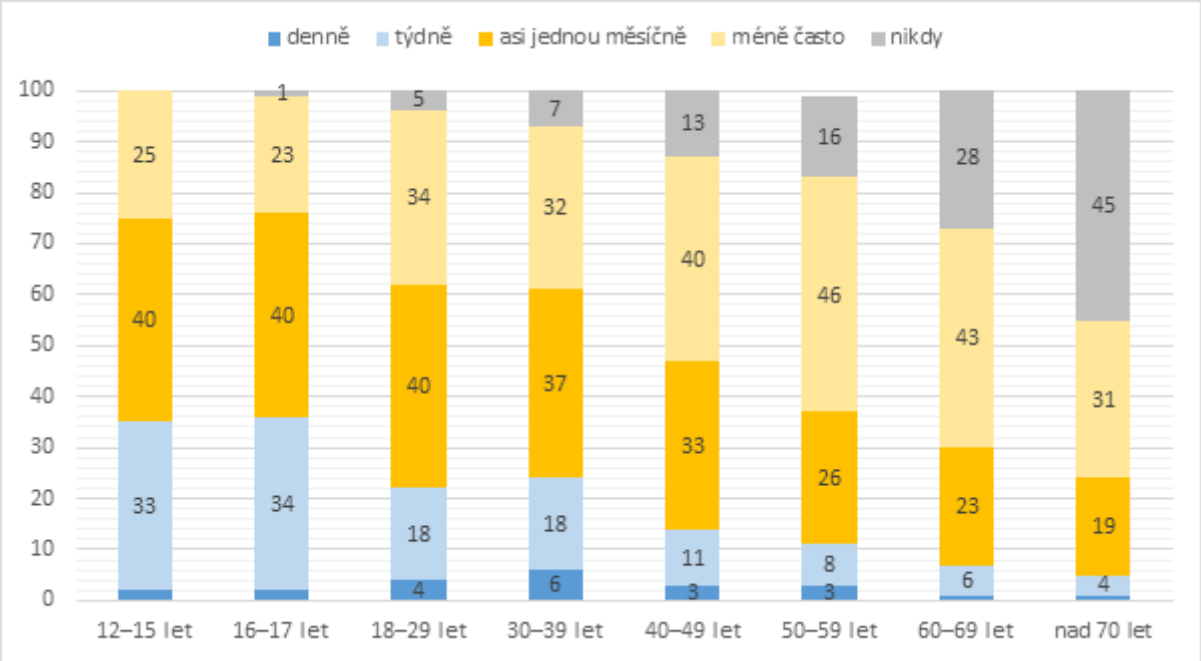
Vzdělání v tomto případě poskytuje jako dělicí hranici maturitu. Mezi aktivní uživatele se řadí pouze 55 % lidí se základní školou a 78 % středoškoláků bez maturity, kdežto mezi středoškoláky s maturitou je to 92 % a mezi vysokoškoláky 94 %. Pokles intenzity používání internetu s nižším vzděláním se především projevuje větším podílem těch, kteří internet nepoužívají vůbec. Mezi lidmi se základním vzděláním je to 30 % lidí, co nemají žádné připojení, mezi středoškoláky bez maturity 13 % a s maturitou a vysokoškolským diplomem jsou to už jen 3–4 %.

Aktivní používání e-mailu

V Česku využívá e-mailovou adresu průměrně 88 % lidí a tento podíl se podle věku a vzdělání liší spíše mírně. Mírné rozdíly jsou mezi věkovými kategoriemi, kdy ji používají téměř všichni lidé mezi 16. a 17. rokem (94 %), zatímco lidé starší 70 let ji používají nejméně (72 %). V ostatních věkových kategoriích je podíl uživatelů e-mailu v rozmezí 80–90 %. Rozdíly nejsou velké ani mezi vzdělanostními skupinami, největší je mezi lidmi se základním vzděláním (75 %) a vysokoškoláky (95 %), a to 20 procentních bodů. Používání e-mailu přitom vzrůstá s dosaženým vzděláním. Žáci jsou v tomto ohledu na úrovni vzdělanější části populace (93 % z nich e-mail aktivně používá).

Nákup zboží a služeb na internetu

Z hlediska ochrany osobních údajů a vlastních finančních zdrojů představuje nakupování na internetu potenciálně rizikovou činnost. Třetina Čechů takto nakupuje asi jednou do měsíce (33 %), další třetina pak méně často než jednou do měsíce (36 %). Zbylá třetina se dělí na ty, co na internetu nenakupují vůbec (13 %), a na ty, co v tomto stylu nakupování našli zalíbení a nakupují buď týdně (15 %), nebo denně (3 %).



Graf 5. Frekvence nakupování či objednávání zboží a služeb na internetu podle věku (%).

Lze však pozorovat, že nakupování na internetu je výrazně častější u lidí ve věku 12–15 let (33 %) a 16–17 let (34 %), kdy takto týdně nakupuje třetina z nich (graf 5). U dvou starších věkových skupin (18–39 let) takto týdně nakupuje pětina z nich (18 %) a u lidí ve věku 40–49 let jedna desetina (11 %). Lidé starší 50 let využívají nákup na internetu méně než v 10 % případů. Mezi lidmi ve věkových skupinách mezi 12. a 49. rokem na internetu nakupuje asi jednou do měsíce zhruba 30–40 %. Jednou do měsíce na internetu také nakoupí mezi 20 a 25 % lidí nad 50 let. Nejvyšší podíl těch, kteří na internetu nenakupují vůbec, najdeme mezi respondenty ve věku 60–69 let (28 % z nich) a nad 70 let (45 % z nich).

Mezi těmi, co nakupují na internetu týdně, jsou nejvýraznější žáci, tento způsob nákupu totiž využívá 35 % z nich. Je důležité upozornit, že data pro žákovskou populaci byla sbírána v době lockdownu kvůli nemoci covid-19, což mohlo frekvenci nákupu na internetu podstatně ovlivnit. Naproti tomu lidé se základním vzděláním a středoškoláci bez maturity nakupují přes internet týdně jen v 9 % a nikdy tento způsob nákupu nevyužívá 20–30 % z nich. Lidé, co nakupují na internetu týdně, se lišili také podle velikosti místa bydliště, kdy takto často nakupovala pětina lidí z obcí o velikosti 1 000 – 4 999 obyvatel (21 %) a jenom necelá desetina lidí z obcí o velikosti 20 000 – 99 999 obyvatel (9 %). On-line nákupy se tak zdají být fungující strategií kompenzující horší dostupnost zboží a služeb v menších obcích.

Platba kartou na internetu

Používání platební karty při nákupech na internetu s sebou přináší řadu rizik. Proto nás zajímalo, zda Češi rozlišují, na jakých webech svou kartu použijí. Výsledky jsou vidět na tabulce 4. Běžně na všech webech platí kartou pětina Čechů (20 %), zatímco dvakrát tolik Čechů (43 %) si dává větší pozor a kartou platí pouze na osvědčených webech. Pouze na českých webech platí 13 % lidí a svou kartu při placení na internetu vůbec nevyužívá 24 % lidí.

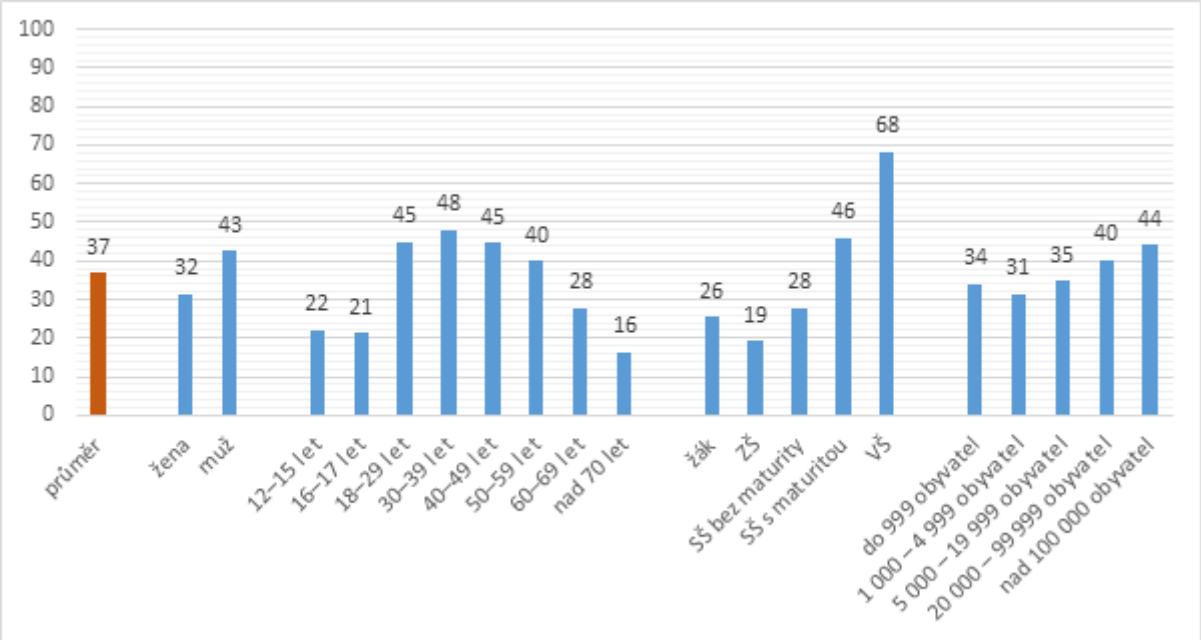
Nicméně, i zde jsou mezi lidmi rozdíly, zejména u věku a vzdělaní. Největší podíl lidí, kteří na internetu kartou neplatí vůbec, je mezi lidmi ve věku 60–69 let (43 %) a 70 a více let (52 %). Naopak nejvíce na internetu kartou platí lidé v mladém dospělém věku do 29 let (86 % z nich). Zároveň se však tito lidé nejméně zajímají o to, zdali je web, na kterém kartou platí, ověřený, protože 30 % z nich platí běžně kartou na všech webech. Dalo by se říci, že nejobezřetnější skupinou při platbách na internetu jsou dvě nejmladší věkové skupiny, kdy ve skupině 12–15 let platí jen na osvědčených webech 59 % a ve skupině 16–17 let 64 %. Pokud nejstarší lidé (70 a více let) platí na internetu kartou, nejčastěji preferují české weby (23 %) a jsou tak jedinou skupinou, ve které je toto chování převažující. Ostatní věkové skupiny klidně zaplatí kartou i na zahraničních webech, ale musí být ověřené.

Tabulka 4. Platba kartou na internetu.

Platíte na internetu kartou?	**%**
Ano, běžně na všech webech	20
Jen na osvědčených webech	43
Jen na českých webech	13
Nikdy	24
celkem	100

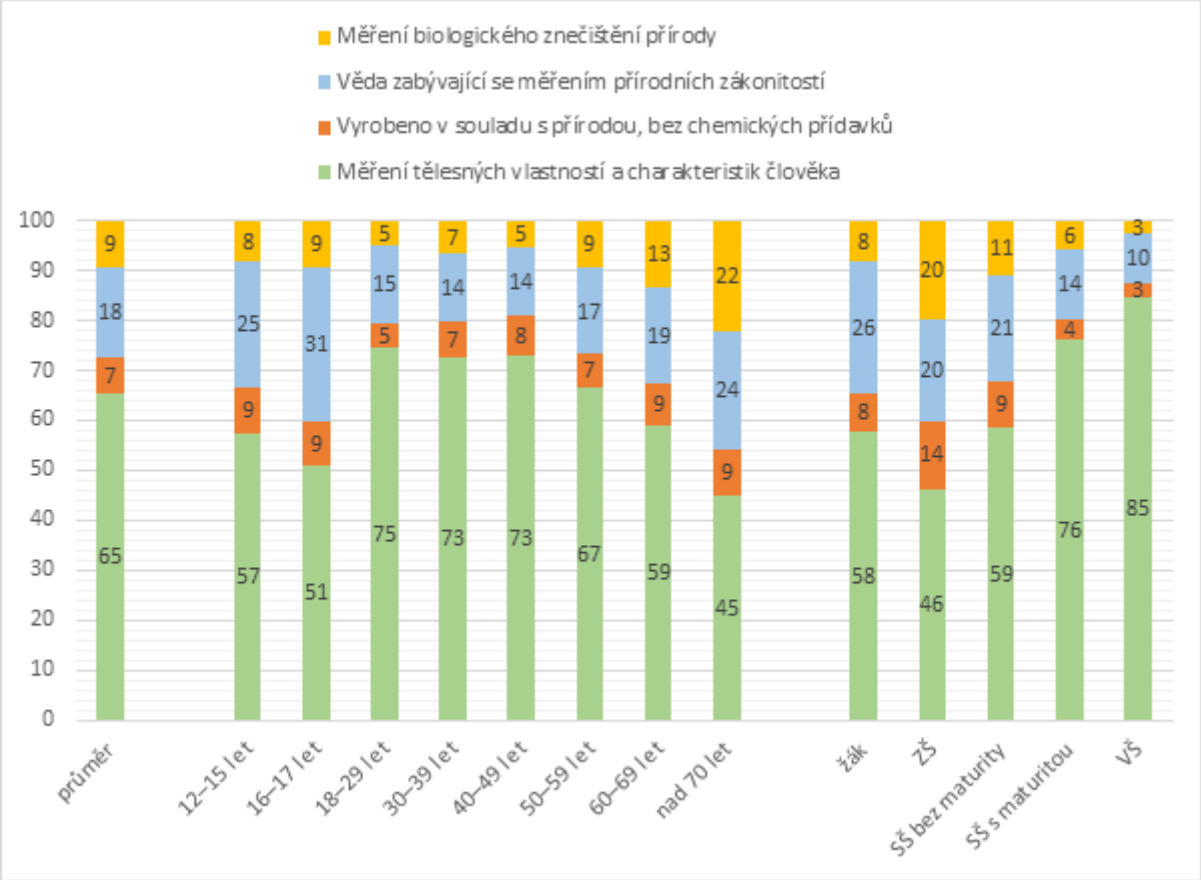
Znalost pojmu biometrie

Přestože je biometrická autentizace ve formě otisku prstu už delší dobu součástí všech nově prodávaných smartphonů, znalost tohoto pojmu v české populaci není příliš vysoká. Nějakou formu setkání se se slovem biometrie deklaruje 37 % respondentů (graf 6). Je však mezi nimi více mužů (43 %) než žen (32 %). Nejčastěji deklarují zkušenost s tímto slovem lidé mezi 18 a 59 lety (kolem 45 %), zatímco nezletilí a lidé nad 60 let se s ním setkali jen zhruba ve 20 % případů. Vzdělání představuje nejsilnější prediktor, jelikož od základního vzdělání (19 %) zkušenost se slovem biometrie výrazně roste, nejvíce ji deklarují vysokoškoláci (68 %). Žáci v tomto ohledu tvoří spíše méně obeznámenou skupinu (26 %), což vzhledem k jejich intenzivnímu používání technologií představuje značný problém. Vyšší obeznámenost se slovem biometrie je deklarována také ve velkých městech (nad 100 000 obyvatel 44 %) než v menších sídlech.



Graf 6. Podíl lidí, kteří se již setkali se slovem „biometrie“ podle pohlaví, věku, vzdělání a velikosti místa bydliště (%). *Pozn. Dopočet do 100 % tvoří lidé, kteří si nejsou jisti, nebo se se slovem „biometrie“ nesetkali.*

Co to ta biometrie ale je? Na to jsme se respondentů také zeptali. Z nabízených možností většina (65 %) odpověděla správně, že biometrie znamená *měření tělesných vlastností a charakteristik člověka*. Druhou nejčastěji volenou možností (i když výrazně méně – 18 %) bylo označení biometrie za *vědu zabývající se měřením přírodních zákonitostí*. Další dvě možnosti (*vyrobeno v souladu s přírodou, bez chemických přídavků* a *měření biologického znečištění vody)* byly voleny opravdu velmi zřídka (méně než 10 %). Nejvyšší znalost pojmu měli mladší lidé ve věku 18–49 let (kolem 75 %) a také lidé s vysokoškolským vzděláním (85 %). Nejnižší pak lidé nad 70 let a starší (45 %) a lidé se základním vzděláním (46 %). (graf 7) Výrazným zlomem je tedy věk 50 let a také děti mají výrazně nižší znalosti než ostatní populace.



Graf 7. Znalost významu slova „biometrie“ nebo „biometrický“ podle věku a vzdělání (%). *Pozn. Dopočet do 100 % tvoří lidé, kteří si nejsou jisti, nebo se se slovem „biometrie“ nesetkali.*

Znalost pojmu biometrie jsme také ověřovali pomocí výčtu tělesných rysů, u kterých měli respondenti rozhodnout, zda mohou sloužit k biometrické identifikaci či nikoliv. Všechny tělesné vlastnosti v první části tabulky 5, jako tělesná výška nebo délka vousů, nemohou být využity k bezpečné identifikaci člověka. Kromě barvy očí, kterou za vhodnou k biometrické identifikaci považuje 47 % respondentů, dokázali Češi poměrně dobře odhadnout, že tyto vlastnosti pravděpodobně nebudou nejlepšími biometrickými znaky (tělesná výška byla označena za vhodnou ve 33 %, barva vlasů ve 21 %, hmotnost v 18 %, délka vlasů ve 14 % a délka vousů ve 12 %).

Nejčastěji měli tendenci označovat nesprávné tělesné vlastnosti za vhodné nejmladší respondenti, ve věku 12–17 let. Lze pozorovat mírně klesající trend špatného označování s dosaženým vzděláním.

Tabulka 5. Označení dané vlastnosti člověka jako vhodné k biometrické identifikaci.

V současnosti lze využít k bezpečné identifikaci člověka…	**%**
barva očí	47
tělesná výška	33
barva vlasů	21
hmotnost	18

délka vlasů	14
délka vousů	12
otisk prstu	93
DNA (genetická informace)	87
obraz oka (sítnice, duhovka)	77
podpis	63
hlas	62
tvar obličeje	61
styl psaní rukou	54
tvar ruky	43
styl chůze	37
rozložení cév v částech těla (kardiovaskulární řečiště)	37
styl psaní na stroji nebo počítači	17

Zabezpečení mobilního telefonu

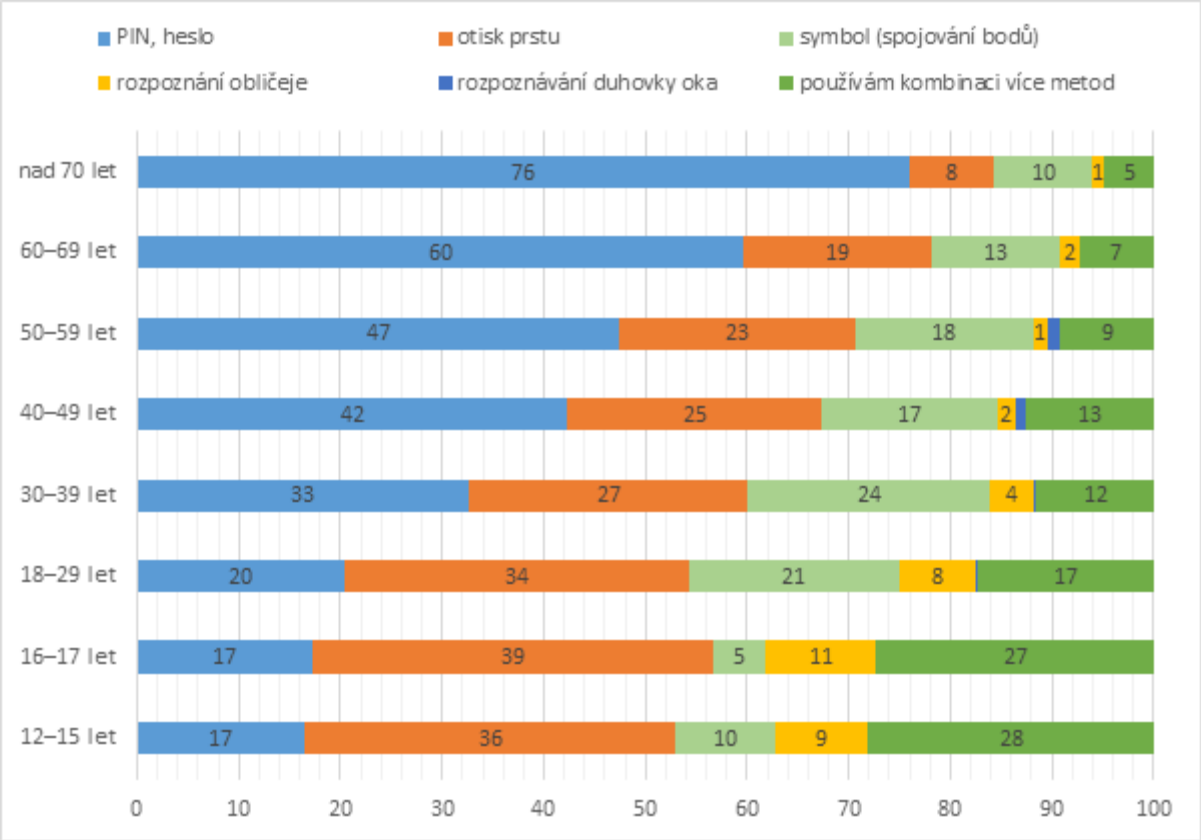
Biometrické systémy zabezpečení jsou již běžnou součástí naprosté většiny mobilních telefonů. Část lidí ale z různých důvodů používá telefon tlačítkový, který umožňuje pouze zabezpečení pomocí PINu / hesla. Samozřejmě je také možné nechat telefon zcela bez zabezpečení. Tuto variantu volí celých 32 % občanů, což je vysoký podíl. V preferenci pro to nechat svůj mobilní telefon zcela bez zabezpečení vidíme obvyklý trend, kdy tuto možnost volí především lidé starší a s nižším vzděláním. Zatímco mezi nezletilými je takových méně než dvě procenta, v nejstarší skupině 70letých a starších je jich 72 %. Nárůst této preference je přitom s věkem v podstatě lineární. Silný je i vliv vzdělání. Více než polovina (57 %) lidí se základním vzděláním svůj mobilní telefon nezabezpečuje, mezi vyučenými je to 40 %, mezi středoškoláky s maturitou 29 % a mezi vysokoškolsky vzdělanými čtvrtina (24 %). Můžeme tedy konstatovat, že dospělí a zejména starší lidé k zabezpečení svého telefonu nepřistupují ve srovnání s dětmi příliš zodpovědně.

Pokud respondenti svůj mobil zabezpečují, je biometrická autentizace oblíbeným způsobem. Jak se ukazuje, pro téměř třetinu respondentů je otisk prstu nejčastějším způsobem zabezpečení mobilního telefon. Stále však vede zabezpečení pomocí PIN kódu či hesla, které využívá 35 % Čechů. 17 % využívá symbol (spojování bodů) a 15 % kombinuje více metod. Jen 5 % respondentů využívá rozpoznání obličeje a téměř nikdo nevyužívá rozpoznání duhovky oka k zabezpečení mobilního telefonu.

Typ převážně používané metody zabezpečení mobilního telefonu se liší napříč věkovými skupinami (viz graf 8). Mladší lidé spíše preferují zabezpečení pomocí otisku prstu nebo kombinaci více metod, přičemž obě preference s věkem klesají. Tento pokles je patrný již od věku 30 let a výrazný je pak v obou seniorských kategoriích. Naproti tomu s přibývajícím věkem

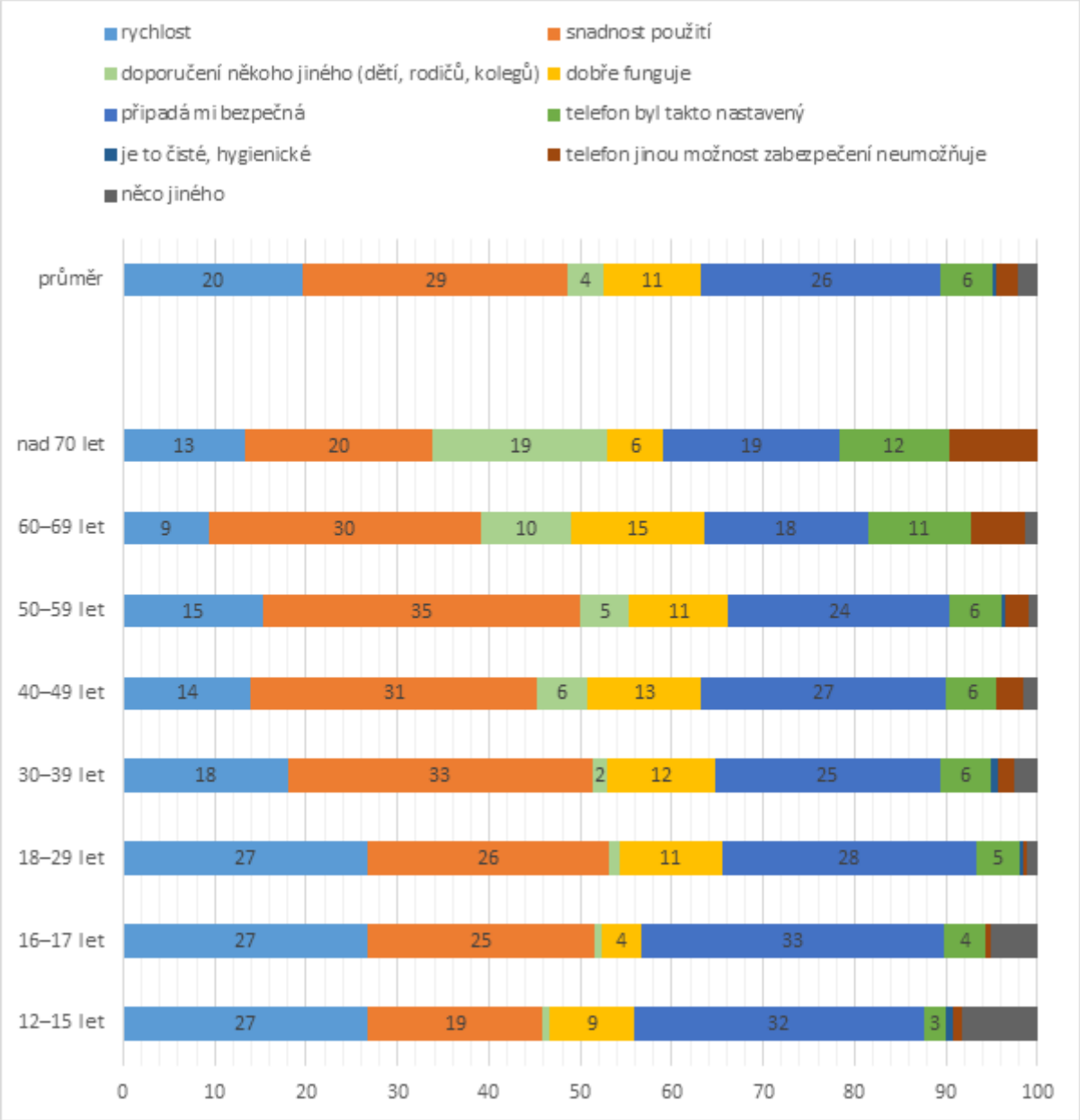
stoupá oblíbenost PIN kódů a hesel, které využívá přes 70 % lidí nad 70 let. Dané je to i vyšším podílem vlastníků tlačítkových mobilních telefonů ve starších věkových skupinách, které jiný způsob autentizace než kód neumožňují.

Žáci v největší míře využívají otisk prstu (41 %) a kombinaci více metod (28 %), PIN kód jen v 15 %. Vysokoškoláci využívají nejčastěji PIN kód (29 %) a otisk prstu (30 %). Ostatní vzdělanostní skupiny se od sebe příliš neliší, nejčastěji využívají PIN kód (cca 40 %) a otisk prstu (cca 25 %). Mezi dospělými je také populární symbol (spojování bodů) (cca 20 %), pro žáky už však atraktivní není (jen 6 %).



Graf 8. Nejčastější způsob zabezpečení mobilního telefonu podle věku (%).

Také jsme se zajímali o to, co ty, kteří si změnili způsob zabezpečení svého mobilního telefonu, vedlo k výběru této nové metody zabezpečení. Tato zjištění jsou vidět na grafu 9. Pro mladé lidi do 29 let byla nejdůležitějším faktorem rychlost a bezpečnost nové metody zabezpečení. Pro starší věkové skupiny to taktéž byla bezpečnost, ale na rozdíl od mladších lidí pro ně hrála velkou roli také snadnost použití. Nejstarší lidé (70 a více let) také dali poměrně často na doporučení někoho jiného (19 %).



Graf 9. Nejčastější důvod pro změnu způsobu zabezpečení mobilního telefonu podle věku (%).

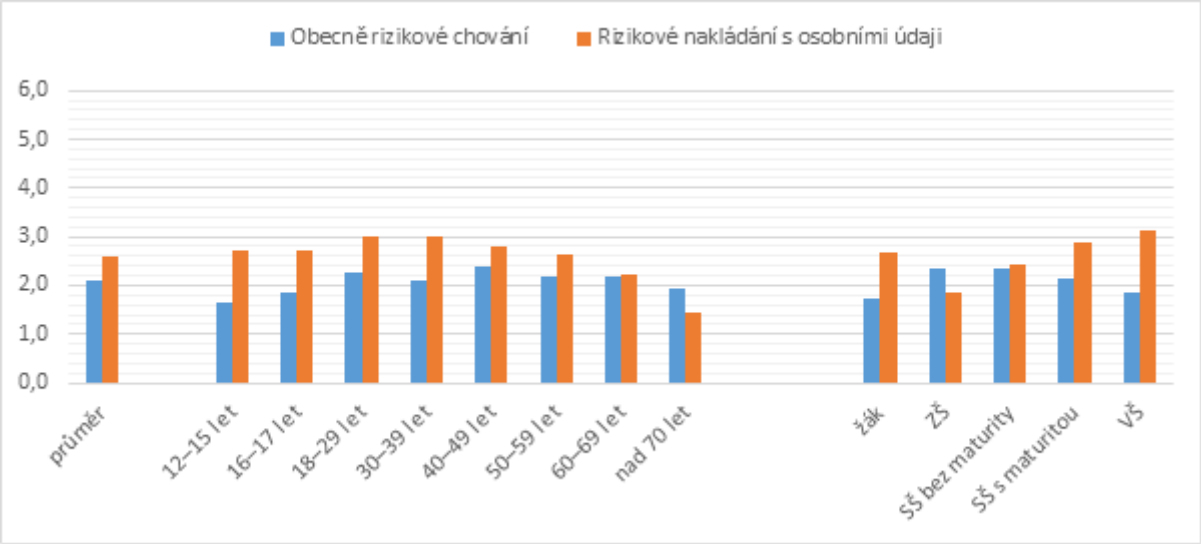
Rizikovost chování na internetu a při zabezpečování

Chovají se tedy Češi obecně nezodpovědně? A jak nakládají se svými osobními údaji (nebo hesly)? Na to nám pomohou odpovědět dva indexy rizikovosti. Respondenti měli vždy z dvojice výroků označit ten, který na ně lépe sedí. Pokud respondent označil ten, co znamená menší riziko, dostal jeden bod. Mohl tak celkem získat 0–6 bodů u každého indexu. Pokud získal 6 bodů, ukazuje to na vysokou míru zodpovědnosti obecně nebo při nakládání s osobními údaji. V případě zisku 0 bodů se respondent chová vysoce rizikově. Dvojice výroků, ze kterých respondenti vybírali, jsou vypsány v tabulce 6.

Tabulka 6. Výroky, ze kterých byly sestaveny indexy obecně rizikového chování a rizikového nakládání s osobními údaji.

Obecně rizikové chování	
Snižování rizika	**Zvyšování rizika**
Když kupujete nějakou dražší věc (např. počítač, porovnáváte ceny v několika obchodech).	I když kupujete nějakou dražší věc, nakupujete spíš tam, kde to máte blízko nebo je to prostě nejjednodušší.
Každý měsíc si velmi podrobně zkontrolujete výpisy z účtů.	Výpisy nekontrolujete, věříte, že to má banka správně.
Drobný tisk na jakémkoli důležitém dokumentu vždy (pokaždé) dopodrobna pročítáte.	Drobné písmo na dokumentech, jako je pronájem, pojistka nebo žádost o půjčku, nečtete, je to zbytečné.
Pravidelně zálohujete všechny důležité soubory v počítači, a osobní dokumenty máte uloženy v dobře přístupných složkách.	Pravidelné zálohování a organizování počítačových složek nebo dokumentů neprovádíte.
Nikdy nenakupujete oblečení, aniž byste je vyzkoušeli.	Někdy nakoupíte oblečení bez toho, že byste si jej vyzkoušel(a).
Na cesty do zahraničí si vždy dokupujete cestovní pojištění.	I na zahraniční cesty si určitě vystačíte s domácí modrou kartičkou zdravotní pojišťovny.
Rizikové nakládání s osobními údaji	
Snižování rizika	**Zvyšování rizika**
Zadávám hesla vždy znovu při každém přihlášení.	Ukládám si hesla do počítače.
Volím pro každý systém nové heslo.	Mám jedno stejné heslo na všechno.
Hesla pravidelně měním.	Mám stále stejné zapamatovatelné heslo.
Všechny platební karty mám uložené v telefonu	Platební kartu mám ve formě plastové kartičky.
Vyplňuji jen zcela povinné údaje.	Do formulářů či objednávek vždy vyplňuji všechna data.
Vyplňuji své údaje vždy znovu.	Ukládám údaje ve formulářích na e-shopech (nechávám si údaje předvyplněné).

Jak je možné vidět v grafu 10, Češi se průměrně chovají spíše rizikově, jelikož se hodnota obou indexů drží spíše v nižších hodnotách. Co se týče rozdílu mezi obecně rizikovým chováním a rizikovým nakládáním s osobními údaji, dávají si respondenti větší pozor, když dojde konkrétně na jejich osobní údaje. Obecně se nejrizikověji chovají žáci do 17 let spolu s vysokoškoláky. Naopak nejopatrnějšími jsou lidé ve věku 40–49 let a také lidé se základním vzděláním a středoškoláci bez maturity. Při nakládání s osobními údaji je situace odlišná. Obezřetnost je v tomto případě nejnižší u lidí nad 70 let a u lidí se základním vzděláním.



Graf 10. Indexy obecně rizikového chování a rizikového nakládání s osobními údaji podle věku a vzdělání. (0 = vysoké riziko, 6 = nízké riziko).

Zkušenost se zneužitím hesel nebo jiných přístupových údajů

To, že strach ze zneužití technologií není tak častý, může být také do jisté míry způsobeno malou zkušeností s reálným kybernetickým ohrožením, jako je krádež hesla nebo identity. V Česku s nimi má zkušenost méně než 10 % lidí a když už, tak se většinou jedná o jednorázovou krádež hesla do méně důležitého systému (tabulka 7).

Tabulka 7. Zkušenost s kybernetickým ohrožením.

	Ne, nikdy	Ano, jednorázově	Ano, opakovaně
krádež hesla do méně důležitého systému	92	7	1
krádež hesla do středně důležitého systému	96	3	1
krádež hesla do velmi důležitého systému	99	1	0
krádež identity (někdo se za vás vydával a psal vaším jménem e-maily, zprávy…)	95	4	1

Nicméně pokud se podíváme na zkušenost napříč věkovými a vzdělanostními skupinami, jasně zde vyčnívají lidé v žákovském věku. S jednorázovou krádeží hesla do méně důležitého systému má zkušenost 32 % žáků. Do 15 let je to 26 % a ve skupině 16–17 let dokonce 33 %.

Legitimita využívání biometrie institucemi/soukromými subjekty

Biometrické systémy jsou používány v různých situacích, potenciál jejich využití je značný, nicméně snadné je i jejich zneužití pro omezování práv občanů, jak známe z některých totalitních režimů. Ptali jsme se respondentů, jaké způsoby použití soukromými i státními institucemi považují za legitimní a to bez ohledu abychom specifikovali aktuální omezení daná le-

gislativou. Každou z potenciálních možností použití měli respondenti hodnotit z hlediska legitimity využití na stupnici 1–10, kdy 1 znamenalo, že toto použití je zcela v pořádku a 10 naopak, že není vůbec v pořádku. Jak se zdá, Češi a Češky spíše považují využívání biometrie institucemi nebo soukromými subjekty jako legitimní, nicméně stále se na bodové škále pohybují blízko středu. Výsledky i postupy, při nichž je biometrie využívána, jsou shrnuty v tabulce 8. Nejméně se respondentům zamlouvá, aby děti ve školách používaly pro vstup a výdej obědů otisk prstu. Nejvíce se v akceptaci všech použití liší nejmladší respondenti ve věku 12–15 let a žáci, kteří obecně s postupy souhlasí více než dospělí respondenti.

Tabulka 8. Legitimita využívání biometrie institucemi / soukromými subjekty (Průměr, 1 = zcela v pořádku; 10 = vůbec není v pořádku).

Nakolik souhlasíte s následujícími postupy…	
děti ve školách používají pro vstup a výdej obědů otisk prstu	4,9
celoplošný kamerový systém státu automaticky vyhledává přestupky	4,3
město používá (pojízdné) kamery pro záznam poznávacích značek zaparkovaných automobilů	4,2
stát provozuje celoplošný kamerový systém s automatickým rozpoznáváním obličejů, aby vyhledával hledané osoby	4,1

Reálnost hollywoodských scénářů

Ve filmech se často objevují různé scénáře zneužití biometrických údajů. Zajímalo nás, které Češi a Češky považují za reálné. Přehled scénářů a základní výsledky poskytuje tabulka 9. Nejvíce reálné se respondentům zdá donucení člověka pod hrozbou násilí, aby použil svůj otisk prstu nebo oko (80 %). Kolem 60 % Čechů považuje za reálné vytvoření kopie prstu a obličeje na základě dat ukradených z biometrického systému a vytvoření kopie otisku prstu na základě otisku zanechaného např. na skleničce. 50 % Čechů si myslí, že je možné oddělení příslušné části (prst, oko) od těla odříznutím/vydloubnutím a použití této části pro vstup např. do budovy. Podobně 43 % považuje za reálné vytvoření kopie obličeje jen podle fotografie a její využití pro vstup do zabezpečeného místa.

Tabulka 9. Podíl respondentů, kteří souhlasí s reálností daného scénáře.

Scénáře	**%**
donucení člověka pod hrozbou násilí, aby použil svůj otisk prstu / oko	80
vytvoření kopie otisku prstu na základě dat ukradených z biometrického systému	63
vytvoření kopie otisku prstu na základě otisku zanechaného např. na skleničce	61
vytvoření kopie obličeje na základě dat ukradených z biometrického systému	60
oddělení příslušné části (prst, oko) od těla odříznutím/vydloubnutím a použití této části pro vstup např. do budovy	50
vytvoření kopie obličeje jen podle fotografie a její využití pro vstup do zabezpečeného místa	43

Důvěra v reálnost filmových scénářů se liší napříč věkovými a vzdělanostními skupinami a také podle toho, v jak velké obci člověk žije. Zejména mladí lidé v žákovském věku mají větší tendenci věřit daným scénářům a jejich odlišnost od dospělé populace je značná. Výjimkou je vytvoření kopie obličeje jen podle fotografie a její využití pro vstup do zabezpečeného místa, tam jsou naopak nejskeptičtější.

Závěry analýzy

Podstatným výsledkem je relativně malé technologické sebevědomí našich respondentů a respondentek. To je sice výrazně ovlivněno věkem a vzděláním v obvyklém směru poklesu s věkem a nižším vzděláním, ovšem i ti, kteří v hodnotách technologické sebepercepce skórovali nejvýše, se pohybují jen mírně nad průměrem možného rozsahu škály.

U většiny znalostních otázek jsme zaznamenali srovnatelnou úroveň znalostí v populaci 18–49 let. Mírně nižší znalosti IT technologií, IT bezpečnosti i biometrií vykazovaly ženy než muži. Velikost místa bydliště nehrála v tomto směru žádný výrazný vliv. **Ve věkové skupině 50–59 let dochází u obou pohlaví k výraznému zlomu, poklesu průměrných znalostí**. Tento klesající trend je pak ještě prohlouben ve všech starších věkových skupinách.

Tito starší a vzhledem ke svým nižším znalostem ohroženější lidé obecně dokončili své (zejména středoškolské) vzdělání před rokem 1990, kdy bylo rozšíření výpočetní techniky v České republice v podstatě nulové. Jak ukazují naše zjištění, velká část z nich se s moderními technologiemi dostatečně neseznámila ani v průběhu následující pracovní kariéry.

Na druhou stranu nelze tyto osoby z digitalizace společnosti vynechávat. Pokud až doposud nenašly důvod či motivaci k používání informačních technologií, můžeme konstatovat, že digitalizace okolního světa je dohnala. I lidé starší 50 let používají chytré mobilní telefony, mobilní či internetové bankovnictví a objednávají služby a zboží po internetu. Cestují s biometrickými cestovními pasy a pohybují se v prostorech snímaných bezpečnostními kamerami. Je však třeba si uvědomit, že používání těchto technologií a jejich dostatečná uživatelská znalost není zcela všeobecně rozšířena a že zejména mezi lidmi ve vyšším věku a také s nižším vzděláním je nezanedbatelná skupina těch, kteří ICT a biometrické technologie aktivně nevyužívají (mají tlačítkové telefony a nepoužívají internet).

Pokud se zaměříme výhradně na **vliv vzdělání**, dochází k **lomu v trendu znalostí na úrovni maturity**. Lidé, kteří ukončili svou vzdělávací dráhu na základní škole nebo střední škole bez maturity, mají znalosti IT výrazně menší než lidé s úplným středoškolským nebo vysokoškolským vzděláním. Vysvětlujeme si to odlišným osudem na trhu práce. Lidé s nižším vzděláním získávají spíše pozice kvalifikovaných či polokvalifikovaných manuálních pracovníků a ke své práci moderní IT technologie (zatím) příliš nevyužívají. Oproti tomu lidé s maturitou či vysokoškolským vzděláním působí do velké míry v nemanuálních povoláních, kde je rutinní zvládání IT považováno za samozřejmost.

V souvislosti s ostatními charakteristikami respondentů má ale **vyšší vzdělání tzv. kompenzační roli**. Podíváme-li se například na respondenty a respondentky ve věkové skupině 50–59 let, u nichž, jak bylo zmíněno výše, dochází k prvnímu výraznému poklesu IT znalostí, vyčnívají mezi nimi lidé s vyšším vzděláním jako ti, kdo pracují s IT technologiemi častěji a mají o nich lepší znalosti. **Dosažení alespoň středoškolského vzdělání s maturitou tak posouvá znalosti starších respondentů a respondentek na úroveň lidí o 5–10 let mladších**. Naopak získání nižšího než maturitního vzdělání posouvá respondenty v IT znalostech o jednu až dvě věkové skupiny směrem k horším výsledkům.

Nejvíce ohroženy nízkými znalostmi o informačních technologiích, jejich bezpečném používání a biometriích jsou v současné České republice osoby vyššího věku a s nízkým vzděláním, častěji ženy než o muži. U žen bez maturity je riziková již skupina starší 50 let, u mužů bez maturity výrazně klesají znalosti po dosažení 55. roku života. U vyšších vzdělanostních skupin se snížení znalostí projevuje až po 60. roce života.

Upozorňujeme, že se jedná o vliv kohorty, nikoliv věku, a že uvedené údaje jsou platné pro českou populaci v roce 2020, kdy byla data sbírána, a pro konkrétní typ technologické kvalifikace. S tím, jak se respondenti posouvají do vyšších věkových skupin, se bude posouvat i zmíněná hranice poklesu znalostí. Pokud je např. v roce 2020 tato hranice na úrovni 50 let, bude v roce 2030 na úrovni 60 let. Přitom se bude jednat o tytéž respondenty (narozené před rokem 1970). Platí to však pouze pro aktuálně používané technologie, při rozšíření výrazně inovativních technologií můžeme opět předpokládat výhodu mladší a vzdělanější části populace.

V našich analýzách jsme záměrně oddělovali skupinu respondentů a respondentek, jejichž odpovědi jsme získali prostřednictvím sond na základních a středních školách. Jednak se, na rozdíl od zbytku výzkumu, nejedná o reprezentativní vzorek populace, jednak mají několik specifik. Předně jde o osoby s nedokončeným či dokončeným základním vzděláním, které tedy spadají do nejnižší vzdělanostní kategorie. Od jiných příslušníků této kategorie se ale liší zejména tím, že ještě nemají ukončenou vzdělávací dráhu, a nemůžeme tedy predikovat, v jaké vzdělanostní kategorii nakonec skončí. Zbytečně by proto deformovali výsledky platné pro kategorii dospělých, kteří své vzdělání ukončili základní školou.

Celkově můžeme na základě našich analýz konstatovat, že žáci mají výrazně nadprůměrné ukazatele využívání moderních technologií. Podle očekávání pracují s mobilními telefony, tablety, internetem i sociálními sítěmi mnohem častěji než příslušníci vyšších věkových kategorií. S tím ale překvapivě nejsou spojeny vyšší znalosti. V tomto směru žáci za ostatními často zaostávají, výrazně patrné je to u jejich nízké znalosti biometrie. Na rozdíl od ostatních pak mají častější zkušenost s krádeží digitální identity, ať už za ni považují svůj e-mailový účet, profil na sociálních sítích, nebo postavu v počítačové hře.

Z hlediska znalostí o biometriích se ukázalo, že respondenti nechápou princip fungování biometrických systémů. Z velké části se domnívají, že v systému je uložena kompletní biometrická informace (např. sken otisku prstu), kterou je možno ze systému získat a vyrobit její kopii. V rámci edukace by proto bylo vhodné zaměřit se na proces, jak je s biometrickou informací nakládáno. Dalším výrazným nedostatkem je neznalost tzv. testu živosti, kdy systém různými metodami ověřuje, zda je předložená biometrická charakteristika spojena se skutečným člověkem. V případě otisku prstu může jít např. o měření tělesné teploty nebo elektrického odporu kůže, v případě skenu obličeje zase může systém vyžadovat provedení různých mimických úkonů. Statické neživé kopie jsou správně fungujícím systémem odmítnuty. V rámci edukace by proto bylo vhodné popsat proces ověřování biometrické informace.

Právní pravidla zpracování biometrických údajů

Biometrické systémy zpracovávají biometrické údaje. Rozmach užívání biometrických systémů znamenal i potřebu tyto údaje v některých případech zvlášť chránit.

Biometrické osobní údaje

Pro Českou republiku, stejně jako pro členské státy Evropské unie, je zásadním právním dokumentem 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 známé pod zkratkou GDPR. Podle čl. 4 písm. 1) se osobními údaji rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě, subjektu údajů; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

GDPR obsahuje v čl. 4 písm. 14) i zvláštní definici biometrických údajů. Jsou jimi osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.

Biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby jsou považovány za zvláštní kategorii údajů podle čl. 9 GDPR (dříve citlivé údaje). Jejich zpracování podléhá zvláštním, zpřísněným podmínkám. Zpracovávání osobních údajů patřících do této kategorie je zakázáno, pokud nemá správce, tedy osoba, která určuje účel a prostředky zpracování, nemá pro toto zpracování speciální důvod.

Principy zpracování osobních údajů

Zpracování osobních údajů, ať již běžných nebo zvláštních, se řídí zásadami uvedenými v čl. 5 GDPR. Osobní údaje musejí být

- ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem (zásada zákonnosti, korektnosti a transparentnosti),
- shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný (zásada účelového omezení),
- přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány (zásada minimalizace údajů),
- přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny (zásada přesnosti),
- uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány (zásada omezení uložení) a
- zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením (zásada integrity a důvěrnosti).

Za dodržení zásad zpracování osobních údajů odpovídá správce, a to i přesto, že některé úkony zpracování pro správce vykonává zpracovatel.

Právní důvody pro zpracování osobních údajů

Zásada zákonnosti znamená, že osobní údaje smí být zpracovávány jen z důvodů stanovených zákonem. Správce může osobní údaje zpracovávat, jen pokud

- subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů,
- zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů,
- zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje,
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce, nebo
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

Přestože je zpracovávání biometrických údajů jako zvláštní kategorie údajů zakázáno, existují z toho zákazu výjimky. Zpracování je možné

- subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů,
- 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,
- 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,
- 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,
- zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů,
- zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků, nebo pokud soudy jednají v rámci svých soudních pravomocí.
- 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;

- 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
- 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;
- 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 GDPR 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.

I když vztah mezi zákonnými důvody zpracování (čl. 6 odst. 1 GDPR) a výjimkami ze zákazu zpracování zvláštních kategorií údajů (čl. 9 odst. 2) není ze samotného nařízení zcela jasný, komentářová literatura se kloní k závěru, že podmínky obou ustanovení je třeba splnit kumulativně. To znamená, že správce musí mít pro zpracování zvláštních kategorií údajů zákonný důvod a zároveň musí doložit, že mu ke zpracování osobních údajů svědčí některá z výjimek zákazu. Tento názor podporuje i stanovisko č. 3/2019 k otázkám a odpovědím týkajícím se vzájemného působení nařízení o klinických hodnoceních a obecného nařízení o ochraně osobních údajů (čl. 70 odst. 1 písm. b)), které takto zákonné důvody a výjimky pro zvláštní kategorie údajů aplikuje. Zpracování biometrických údajů pro proto mělo být nezbytné pro plnění smlouvy. Například plnění smlouvy je takového charakteru (finanční služby, zdravotní služby), že ověření uživatele prostřednictvím jeho biometrických znaků je vzhledem k povaze služby přiměřené. Nezbytnost znamená, že neexistují vhodné alternativy.

Souhlas se zpracováním biometrických údajů

Pro komerčně využívané biometrické systémy bude nejčastější výjimkou ze zákazu zpracování výslovný souhlas subjektu údajů (čl. 9 odst. 2 písm. a) GDPR) Právním základem zpracování může být buď souhlas subjekt údajů (čl. 6 odst. 1 písm. a) GDPR) nebo plnění smlouvy (čl. 6 odst. 1 písm. b) GDPR). Poskytovatel služby s biometrickým ověřením identity uživatele bude mít s uživatelem uzavřenu smlouvu o poskytování služby. Pro využití biometrických údajů musí mít zároveň výslovný souhlas. Plnění smlouvy samo o sobě k využití biometrických údajů neopravňuje.

Souhlas musí být svobodný, konkrétní, informovaný a jednoznačný (čl. 4 písm.) 11 GDPR). U zvláštních kategorií údajů musí subjekt údajů souhlas vyjádřit výslovně. Evropský sbor pro ochranu osobních údajů doporučuje ve svých pokynech k souhlasu souhlas písemný, nebo elektronický za použití dvoufázového ověření. Ani ústní forma souhlasu není vyloučena. U ní bude mít však správce při kontrole problematické dokázat, že souhlas byl udělen.

Text souhlasu musí být od případného ostatního textu jasně oddělen. Pokud je souhlas subjektu údajů vyjádřen písemným prohlášením, které se týká rovněž jiných skutečností, musí být podle čl. 7 odst. 2 GDPR žádost o vyjádření souhlasu předložena způsobem, který je od těchto jiných skutečností jasně odlišitelný, a je srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků. V opačném případě není souhlas závazný.

Subjekt údajů má podle čl. 7 odst. 3 GDPR právo svůj souhlas kdykoli odvolat. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Podle Evropského sboru to znamená, že po odvolání souhlasu, zůstávají zákonné všechny operace zpracování údajů, jež byly na souhlasu založeny a konaly se před jeho odvoláním. Správce ale musí zpracování zastavit, a pokud neexistuje žádný jiný právní základ zpracování, měl by je správce vymazat.

Odvolat souhlas musí být stejně snadné jako jej poskytnout, např. přes stejné elektronické rozhraní, jedním kliknutím apod.

Souhlas je svobodný, má-li subjekt údajů možnost volby souhlas udělit. Pokud takovou volbu nemá, o platný souhlas se jednat nebude. Souhlas není svobodný ani tehdy, pokud ho subjekt údajů nemůže odmítnout nebo odvolat, aniž by utrpěl škodu nebo újmu. Biometrické systémy se často využívají ke kontrole docházky zaměstnanců. Evropský sbor však považuje souhlas zaměstnance se zpracováním jeho údajů za platný pouze výjimečně, a to v situacích, kdy má zaměstnance skutečnou možnost volby. Zpracovávání biometrických údajů v docházkových systémech bude protizákonné, pokud zaměstnance nebude mít možnost evidence docházky jiným způsobem.

Souhlas subjektu údajů musí být udělen pro jeden či více konkrétních účelů. Pokud je účelů zpracování více, měl by mít subjekt údajů možnost udělit souhlas ke každému z nich zvlášť. Požadavek jednoznačnosti souhlasu spojuje Evropský sbor s aktivním jednáním subjektu údajů. Neplatně udělený souhlas by byl takový, kdy políčko pro vyjádření souhlasu by bylo předzaškrtnuto. Subjekt údajů musí vyjádřit svůj souhlas jednoznačným potvrzením.

S konkrétností souhlasu souvisí i informovanost subjektu údajů. GDPR požaduje po správci, aby subjektu údajů sdělil informace vyčtené v čl. 13 a čl. 14 GDPR. První ustanovení se týká informování o zpracování osobních údajů, které má správce přímo od subjektu údajů. Druhé ustanovení dopadá na situaci, kdy má správce osobní údaje z jiného zdroje. U zpracovávání biometrických údajů v biometrických systémech na základě souhlasu bude mít správce osobní údaje přímo od subjektu údajů.

Informace o zpracování

Správce musí v okamžiku získání osobních údajů poskytnout subjektu tyto informace:

- totožnost a kontaktní údaje správce a jeho případného zástupce,
- případně kontaktní údaje případného pověřence pro ochranu osobních údajů,
- účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování,
- oprávněné zájmy správce nebo třetí strany, pokud jsou tyto důvodem zpracování,
- případné příjemce nebo kategorie příjemců osobních údajů,
- případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Komise o odpovídající ochraně nebo, v případech předání uvedených v článcích 46 nebo 47 nebo čl. 49 odst. 1 GDPR, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny,

- dobu, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby,
- existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů,
- pokud je zpracování založeno na souhlasu, existence práva odvolat kdykoli souhlas,
- existence práva podat stížnost u dozorového úřadu,
- skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů,
- skutečnost, že dochází k automatizovanému rozhodování, včetně profilování podle čl. 22 GDPR včetně smysluplných informací týkajících se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

GDPR neurčuje, v jaké podobě musí být údaje poskytnuty. Mohou být subjektu údajů sděleny písemně včetně elektronicky podoby nebo i ústně. Poskytnutí informací ústní formou bude mít správce ovšem problematické doložit.

Subjekt údajů musí mít vždy aktuální informace. Správce ho tedy musí upozornit na každou změnu zpracování osobních údajů, nejlépe před účinností změny. I když to GDPR výslovně nestanoví, měl by správce subjektu údajů při oznámení změny upozornit subjekt údajů na možnost odvolat souhlas.

U biometrických systémů je zvláště důležité, aby správce poskytl informace subjektu údajů srozumitelně a pokud možno jednoduše. Informace by měly být srozumitelné průměrnému člověku, ne pouze specialistům. Subjekt údajů by se na základě informací měl mít možnost rozhodnout, zda svoje osobní údaje správci poskytne, či nikoliv. V biometrických systémech může být obtížné poskytnout všechny informace požadované GDPR jednoduchým způsobem. Evropský sbor připouští rozvrstvené poskytnutí informací. V první „vrstvě“ by mohly být informace poskytované subjektu jednodušší. Ve druhé „vrstvě“ by pak byly informace o zpracování osobních údajů detailněji popsány. Informace by měly být subjektu údajů snadno přístupné, např. prostřednictvím viditelného odkazu. V prostředí chytrého telefonu by informace měly být poskytnuty písemně v elektronické podobě. V prostředí bez displeje (internet věcí) by informace měly být poskytnuty prostřednictvím QR kódů, po spuštění v podobě pokynů, SMS zprávou nebo emailem.

Výjimkou z poskytnutí informací je situace, kdy subjekt údajů již informace má. Pak správce musí subjektu údajů poskytnout informace, které subjekt údajů ještě neobdržel a nemůže je mít (čl. 13 odst. 4 GDPR).

Práva subjektu údajů

Při zpracování osobních údajů má subjekt údajů práva uvedená v kapitole III. GDPR.

Subjekt údaj má

- právo na informace (čl. 13 a 14),
- právo na přístup k osobním údajům (čl. 15),
- právo na opravu (článek 16);
- právo na výmaz, také nazývané právo být zapomenut (čl. 17),
- právo na omezení zpracování (článek 18),

- právo na přenositelnost údajů (čl. 20),
- právo vznést námitku (čl. 21) a
- právo nebýt předmětem automatizovaného rozhodování včetně profilování (čl. 22).

Právo na přístup k údajům

Subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud zpracovávány jsou, má subjekt údajů právo získat k nim přístup. Subjekt údajů má také právo na informace, jejichž výčet je totožný s čl. 13 GDPR.

Správce musí subjektu údajů poskytnout jejich kopii. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob.

Právo na opravu

Subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení.

Některé zpracovávané biometrické údaje se mohou v průběhu času změnit. Otisky prstů nebo podoba obličeje se může změnit ku příkladu po úraze. V takovém případě má subjekt údajů právo na to, aby správce biometrický údaj aktualizoval.

Právo na výmaz („právo být zapomenut“)

Subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se ho týkají. Správce má povinnost osobní údaje vymazat, jestliže to GDPR stanoví. Správce je povinen osobní údaje vymazat, pokud

- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
- subjekt údajů odvolal svůj souhlas, na jehož základě byly a neexistuje žádný další právní důvod pro zpracování,
- subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování nebo subjekt údajů vznese námitky proti zpracování pro marketingové účely,
- osobní údaje byly zpracovány protiprávně,
- osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu EU nebo členského státu a osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti dítěti.

Jestliže správce osobní údaje zveřejnil a je povinen je vymazat, musí podniknout přiměřené kroky, aby informoval další správce, kteří tyto osobní údaje zpracovávají, že subjekt údajů uplatnil právo na výmaz.

I přes žádost subjektu údajů nemusí být osobní údaje vymazány, pokud je zpracování nezbytné:

- pro výkon práva na svobodu projevu a informace,

- pro splnění právní povinnosti, jež vyžaduje zpracování podle práva EU nebo členského státu, které se na správce vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen,
- z důvodů veřejného zájmu v oblasti veřejného zdraví, pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely v souladu s čl. 89 odst. 1 GDPR, pokud je pravděpodobné, že by právo na výmaz znemožnilo nebo vážně ohrozilo splnění cílů zpracování pro tyto účely,
- pro určení, výkon nebo obhajobu právních nároků.

Biometrické údaje, které správce zpracovává na základě souhlasu subjektu údajů, musí být podle komentářové literatury vymazány po odvolání souhlasu bez další žádosti subjektu údajů o výmaz. Správce nemusí vymazat údaje o žádosti, informace o podrobnostech jejího vyhovění a další informace, kterými může v budoucnu prokázat splnění své povinnosti.

Právo na omezení zpracování

Subjekt údajů má právo na to, aby správce omezil zpracování pokud

- subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit;
- zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;
- správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;
- subjekt údajů vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.

Právo na přenositelnost údajů

Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil, a to v případě, že zpracování je založeno na souhlasu nebo na plnění smlouvy a zároveň se zpracování provádí automatizovaně.

Při výkonu svého práva na přenositelnost údajů podle odstavce 1 má subjekt údajů právo na to, aby osobní údaje byly předány přímo jedním správcem správci druhému, je-li to technicky proveditelné.

Právo na přenositelnost se týká pouze údajů, které subjekt údajů správci poskytl. Toto právo nelze uplatnit v případě osobních údajů, které správce odvodil, nebo které získal sám, např. analýzou dat. Samotné biometrické údaje zpravidla správce získá přímo od subjektu údajů. Jsou-li biometrické údaje zpracovávané správcem na základě výsledného souhlasu a automatizovaně, má subjekt údajů právo na jejich přenos.

Právo vznést námitku

Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které se jej týkají, na základě zpracování z důvodu oprávněného zájmu a z důvodu splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci včetně. Správce osobní údaje nesmí dále zpracovávat, pokud neprokáže závažné

oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků. Námitce proti zpracování pro účely přímého marketingu včetně profilování musí subjekt údajů vyhovět vždy.

Jelikož právo na námitku má subjekt údajů, jehož údaje jsou zpracovávány z důvodu oprávněného zájmu nebo ve veřejném zájmu nebo pro výkon veřejné moci, nebudete toto právo ve vztahu k biometrickým údajům často uplatňováno, ledaže by byly biometrické údaje zpracovávány z důvodu podle čl. 6 odst. 1 písm. e) (veřejný zájem, výkon veřejné moci) ve spojení s čl. 9 odst. 2 písm. g) (výjimka významného veřejného zájmu) nebo (písm. i) (výjimka veřejného zájmu v oblasti veřejného zdraví), nebo by po splnění podmínek čl. 22 GDPR bylo na jejich základě prováděno profilování.

Automatizované individuální rozhodování, včetně profilování

Subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká.

Výjimkou ze zákazu je nezbytnost takového zpracování k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem údajů, povolení právem EU nebo členského státu, které stanoví vhodná opatření zajišťující ochranu práv a svobod a oprávněných zájmů subjektu údajů; nebo pokud dal subjekt údajů k takovému zpracování výslovný souhlas.

provést vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů, alespoň práva na lidský zásah ze strany správce, práva vyjádřit svůj názor a práva napadnout rozhodnutí.

Automatizované zpracování nesmí být založeno na zvláštních kategoriích údajů, tedy i biometrických údajů, pokud k tomu nedal subjekt údajů svůj výslovný souhlas nebo zpracování je nezbytné z důvodu významného veřejného zájmu. I v případě, že je takové zpracování možné musí správce zavést vhodná opatření pro zajištění práv a svobod a oprávněných zájmů subjektu údajů.

Zpracování biometrických údajů pro účely automatizovaného individuálního rozhodování je tedy možné jen

- existuje-li výjimka ze zákazu automatizovaného individuálního rozhodování (čl. 22 odst. 2 GDPR) a
- existuje-li výjimka ze zákazu zpracování zvláštních kategorií údajů v podobě výslovného souhlasu nebo z důvodu významného veřejného zájmu a
- správce přijal vhodná opatření pro zajištění práv a svobod a oprávněných zájmů subjektu údajů (alespoň práva na lidský zásah ze strany správce, práva vyjádřit svůj názor a práva napadnout rozhodnutí), přičemž osoba, která přezkoumává rozhodnutí, by měla mít k přezkumu oprávnění, stejně tak jako by měla mít oprávnění rozhodnutí změnit.

Způsob výkonu práv subjektu údajů

Správce musí vyhovět žádosti subjektu údajů pro, pokud u správce svá práva uplatní. Výjimkou je situace,

- kdy správce nemůže zjistit totožnost subjektu údajů; GDPR po správci nepožaduje, aby totožnost subjektu údajů zjišťoval (čl. 11 GDPR),

- kdy konkrétní ustanovení GDPR umožňuje správci za určitých podmínek nevyhovět, nebo mu přímo neumožňuje vyhovět;
- kdy jsou žádosti o výkon práv až šikanózního charakteru (zjevně nepřiměřené či nedůvodné, nebo opakující se).

Ať již správce žádosti musí vyhovět, nebo ji může nebo musí zamítnout, musí každopádně bez zbytečného odkladu, nejpozději do jednoho měsíce od obdržení žádosti poskytnout subjektu údajů informace o přijatých opatřeních (čl. 11 GDPR). Jednoměsíční lhůtu lze prodloužit v případě potřeby až o dva měsíce s ohledem na složitost a počet žádostí. Správce informuje subjekt údajů o jakémkoliv takovém prodloužení do jednoho měsíce od obdržení žádosti spolu s důvody pro tento odklad. Jestliže subjekt údajů podal žádost v elektronické formě, poskytnou se informace v elektronické formě, je-li to možné, pokud subjekt údajů nepožádá o jiný způsob.

Pokud správce nepřijme opatření, o něž subjekt údajů požádal, informuje bezodkladně a nejpozději do jednoho měsíce od přijetí žádosti subjekt údajů o důvodech nepřijetí opatření a o možnosti podat stížnost u dozorového úřadu a žádat o soudní ochranu.

Pokud má správce důvodné pochybnosti o totožnosti fyzické osoby, která podává žádost o výkon svých práv, může požádat o poskytnutí dodatečných informací nezbytných k potvrzení totožnosti subjektu údajů. Pokud by správce ku příkladu umožnil jiné osobě přístup k osobním údajům, bylo by toto být považováno za porušení zabezpečení osobních údajů.

Informace o zpracování osobních údajů podle čl. 13 a 14 GDPR, stejně tako jako reakce na žádosti týkající se výkonu jejich práv, musí správce učinit bezplatně. Přiměřený poplatek zohledňující administrativní náklady spojené poskytnutím informací nebo s výkonem práv může správce požadovat, je-li žádosti zjevně nepřiměřená, nedůvodná nebo opakující se. Z takového důvodu nemusí žádosti ani vyhovět.

Povinnosti správce

Správce je odpovědný za dodržování GDPR během procesu zpracování osobních údajů. Má především povinnost dodržovat zásady ochrany osobních údajů (čl. 5 GDPR), povinnost informovat subjekt údajů o zpracování (čl. 13 a čl. 14 GDPR) a reagovat na žádosti subjektu údajů o výkon jeho práv (čl. 12, čl. 15 až čl. 22 GDPR), a v případě, že je žádosti možno vyhovět, učinit tak. Některé z těchto povinností dopadají pouze na správce, jiné má vedle správce i zpracovatel osobních údajů.

Kromě těchto povinností, má správce řadu dalších, specifických povinností. Některé z nich se přímo týkají zvláštních kategorií údajů, tedy i biometrických údajů. Těmito povinnostmi jsou:

- zavést záměrnou a standardní ochranu osobních údajů,
- vést záznamy o činnostech zpracování,
- uzavřít písemnou dohodu se zpracovatelem,
- provést posouzení vlivu na ochranu osobních údajů,
- jmenovat pověřence pro ochranu osobních údajů,
- přijmout vhodná opatření k zabezpečení osobních údajů,
- ohlásit porušení zabezpečení osobních údajů,
- povinnost spolupráce s dozorovým úřadem.

Povinnost zavést záměrnou a standardní ochranu osobních údajů

Záměrná a standardní ochrana osobních údajů je v angličtině přiléhavěji označována jako data protection by design and by default (čl. 25 GDPR). Dodržování těchto povinností je spojené s povinností přijmout vhodná opatření k zabezpečení osobních údajů (záměrná ochrana) a povinností dodržovat zásadu minimalizace (standardní ochrana)

Záměrná ochrana osobních údajů znamená, že správce zavede vhodná technická a organizační opatření a nezbytné záruky, aby splnil požadavky subjektů údajů a ochránil jejich práva a svobody. GDPR nespecifikuje, co jsou vhodná technická a organizační opatření. Pouze uvádí, že tato opatření závisí na stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob. Vhodnost opatření se posuzuje podle konkrétního zpracování. Záměrnou ochranu osobních údajů zavede správce před započetím zpracování a posuzuje ji i během samotného zpracování. Záměrnou ochranou může být např. detekce malwaru (technické opatření) nebo vnitřní směrnice o bezpečnosti informací (organizační opatření).

Při zpracování biometrických údajů je třeba před i během zpracování je třeba záměrnou ochranu obzvláště respektovat, neboť se jedná o osobní údaje citlivé povahy, u nichž narušení integrity může znamenat závazné riziko pro subjekty údajů. Opatření je třeba v průběhu zpracování průběžně kontrolovat, doplňovat a měnit, aby byla záměrná ochrana osobních údajů neustále dodržována.

Standardní ochranou osobních údajů se rozumí zpracovávání pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Toto se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti. Pro zajištění standardní ochrany je správce povinen přijmout technická a organizační opatření stejně jako v předchozím případě. Tato opatření by měla zohledňovat konkrétně naplňování zásady minimalizace.

Povinnost vést záznamy o činnostech zpracování

Správce, který zpracovává mimo jiné zvláštní kategorie údajů, tedy i biometrické údaje, je povinen vést písemné (elektronické) záznamy o činnostech zpracování (čl. 30 GDPR). Tyto záznamy musí obsahovat informace, které jsou v GDPR uvedeny. Jsou jimi:

- jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů;
- účely zpracování,
- popis kategorií subjektů údajů a kategorií osobních údajů,
- kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích,
- informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci,
- je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů,
- je-li to možné, obecný popis technických a organizačních bezpečnostních opatření.

Zpracovatel má též povinnost vést záznamy o činnostech zpracování. I u zpracovatele uvádí GDPR jejich povinný výčet. Správce a zpracovatel jsou povinni tyto údaje předložit na žádost Úřadu pro ochranu osobních údajů.

Povinnost uzavřít smlouvu se zpracovatelem

Správce a zpracovatel jsou povinni uzavřít spolu písemnou (elektronickou) smlouvu. Zpracovatel je fyzická nebo právnická osoba, která pro správce vykonává určité činnosti, které jsou spojené se zpracováním osobních údajů (čl. 28 GDPR). Tyto činnosti mohou být přímo spojené s nakládáním s osobními údaji (služby analýzy osobních údajů a profilování) nebo je nakládání s osobními údaji vedlejší, ale nezbytný aspekt poskytované služby (poskytování softwaru, při jehož používání se data ukládají na serverech poskytovatele, Software as a Service).

Správce si může zvolit pouze takového zpracovatele, který je schopen zajistit vhodná technická a organizační opatření tak, aby zpracování splňovalo požadavky GDPR a zajišťovalo ochranu práv subjektů údajů. Správce je povinen před uzavřením smlouvy se zpracovatelem zvážit, zda zpracovatel takové to požadavky splňuje. V průběhu smluvního vztahu je povinen a oprávněn tyto požadavky kontrolovat. Zpracovatel má povinnost mu kontroly a audity umožnit. Za porušení povinností zpracovatele je odpovědný správce. Zpracovatel by měl být správcem informován, že mezi osobními údaji, které pro správce zpracovává, jsou i biometrické údaje, aby tomu přizpůsobil svá technická a organizační opatření.

Správce je osobou, která určuje účel a prostředky zpracování, i když zpracovatel může některá méně důležitá rozhodnutí ve vztahu k osobním údajům činit sám. Zpracovatel musí jednat postupovat podle pokynů správce. Pokud se zpracovatel domnívá, že některý pokyn je v rozporu s GDPR nebo jinými předpisy na ochranu osobních údajů, je povinen toto správci sdělit.

GDPR opět vypočítává body, které musí zpracovatelská smlouva obsahovat. Ve vztahu k biometrickým údajům jsou zvláště důležité body týkající se kategorie osobních údaj, která musí být ve smlouvě uvedena, a povinnost přijmout vhodná opatření k zabezpečení osobních údajů. Zabezpečení osobních údajů musí zohledňovat zvláštní povahu zpracovávaných údajů. Pokud má zpracovatel v úmyslu zapojit dalšího zpracovatele, musí o tom správce informovat a získat od něho předem písemné povolení. Další zpracovatel (subzpracovatel) má stejné povinnosti jako primární zpracovatel, zejména poskytnutí dostatečných záruk týkajících se vhodných technických a organizačních opatření, které by rovněž měla reflektovat zvláštní povahu biometrických údajů.

Povinnost provést posouzení vlivu na ochranu osobních údajů

Před zahájením zpracování je správce povinen provést posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů (posouzení vlivu na ochranu osobních údajů neboli DPIA, Data Protection Impact Assessment) (čl. 35 GDPR). Správce nemá tuto povinnost při každém zpracování. Posouzení vlivu se provádí pouze, pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob. GDPR poté uvádí, kdy je vypracování posouzení vlivu zejména povinné. Je to:

- systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad,

- rozsáhlé zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů, nebo
- rozsáhlé systematické monitorování veřejně přístupných prostorů.

Pokud jsou biometrické údaje zpracovávány rozsáhle, je vypracování posouzení vlivu povinné. Podle pokynů k tomuto článku se rozsáhlé zpracování posoudí na základě počet dotčených subjektů údajů, objemu údajů nebo rozsahu jednotlivých zpracovávaných údajů, délky nebo trvání činnosti zpracování údajů a zeměpisném rozsahu zpracování.

I když by nebylo zpracování biometrických údajů vyhodnoceno jako rozsáhlé, je správce povinen posouzení vlivu vypracovat, jestliže zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických. Riziko pro práva a svobody může znamenat technologický produkt, který bude využívat biometrické údaje, byť jejich zpracování nebude rozsáhlé.

Kromě zpracování, které podléhají posouzení vlivu na ochranu osobních údajů přímo na základě GDPR, Úřad pro ochranu osobních údajů sestaví a zveřejní seznam druhů operací zpracování, které podléhají požadavku na posouzení vlivu. Tento seznam operací může konkretizovat obecné podmínky pro posouzení vlivu, které jsou v GDPR uvedeny. Úřad pro ochranu osobních údajů může naopak sestavit i seznam operací, která posouzení vlivu nepodléhají. Úřad vypracoval v listopadu roku 2020 Metodiku obecného posouzení vlivu na ochranu osobních údajů, která obsahuje seznam operací, které posouzení vlivu podléhají a které naopak nepodléhají. Posouzení vlivu podléhají podle metodiky operace zpracování kritických údajů, údajů umožňujících přímou identifikaci a/nebo údajů vysoce osobní povahy subjektů údajů, přičemž mezi kritické údaje se řadí biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby (včetně biometrických kamer a dalších podobných zařízení).

Podle GDPR není správce posouzení povinen provést, pokud zpracování probíhá na základě právní povinnosti správce nebo jeho úkolu ve veřejném zájmu, nebo při výkonu veřejné moci, za předpokladu, že posouzení vlivu na ochranu osobních údajů bylo již provedeno jakožto součást obecného posouzení dopadů v souvislosti s přijetím právního základu pro takové zpracování.

Posouzení vlivu na ochranu osobních údajů musí obsahovat především tyto body:

- systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce,
- posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů;
- posouzení rizik pro práva a svobody subjektů údajů
- plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

Pokud z posouzení vlivu na ochranu osobních údajů vyplývá, že by zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal opatření k jeho zmírnění, je podle čl. 36 GDPR povinen konzultovat toto zpracování před jeho zahájením s Úřadem pro ochranu osobních údajů.

Zákon 110/2019 Sb., o zpracování osobních údajů v § 10 uvádí, že posouzení vlivu se netýká zpracování, které správce provádí ze zákona.

Povinnost jmenovat pověřence pro ochranu osobních údajů

Správce a zpracovatel mají povinnost jmenovat pověřence pro ochranu osobních údajů v případech stanovených GDPR (čl. 37 a násl. GDPR). Správce a zpracovatel mají tuto povinnost, pokud

- jsou orgánem veřejné moci či veřejným subjektem,
- jejich hlavní činnosti spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů, nebo
- jejich hlavní činnosti spočívají v rozsáhlém zpracování zvláštních kategorií údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

Jestliže hlavní činností správce nebo zpracovatel bude (mimo jiné) rozsáhlé zpracovávání biometrických údajů, musí pověřence jmenovat. Bod odůvodnění 97 vykládá hlavní činnost jako činnost související se základními činnostmi a nevztahují se na zpracování osobních údajů jakožto pomocnou činnost. Podle pokynů týkajících se pověřenců jsou hlavní činnosti klíčové operace nezbytné pro dosažení cílů správce nebo zpracovatele.

Rozsáhlé zpracování vykládají tyto pokyny shodně s pokyny týkajícími se posouzení vliv na ochranu osobních údajů, tedy počet dotčených subjektů údajů, objemu údajů nebo rozsahu jednotlivých zpracovávaných údajů, trváním činnosti zpracování údajů a zeměpisném rozsahu zpracování. Skupina podniků může jmenovat jediného pověřence pro ochranu osobních údajů.

GDPR stanoví, že pověřenec pro ochranu osobních údajů musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a musí mít schopnosti plnit své úkoly. Těmi jsou zejména:

- poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle GDPR a dalších předpisů na ochranu osobních údajů,
- monitorování souladu s GDPR a dalšími předpisy na ochranu osobních údajů,
- poskytování poradenství týkající se posouzení vlivu na ochranu osobních údajů a monitorování jeho uplatňování,
- spolupráce s dozorovým úřadem a
- působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování.

Pověřenec pro ochranu osobních údajů může být pracovníkem správce či zpracovatele, nebo může úkoly plnit na základě smlouvy o poskytování služeb. V každém případě správce nebo zpracovatel zajistí, aby byl pověřenec náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů a aby nedostával žádné pokyny týkající se výkonu svých úkolů. V souvislosti s plněním svých úkolů nesmí být pověřenec propuštěn ani sankcionován. Pověřenec údajů musí být přímo podřízen vrcholovým řídícím pracovníkům správce nebo zpracovatele. Pověřenec pro ochranu osobních údajů může plnit i jiné úkoly a povinnosti. Správce nebo zpracovatel zajistí, aby žádné z těchto úkolů a povinností nevedly ke střetu zájmů.

Subjekty údajů se mohou obracet na pověřence pro ochranu osobních údajů ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem svých práv. Proto musí

být pověřenec pro subjekty údajů snadno dostupný. Jeho kontaktní údaje musí být uvedeny v informacích, které subjekt údajů dostává před zahájením zpracování.

Pověřenec musí brát při plnění svých úkolů patřičný ohled na riziko spojené s operacemi zpracování a současně přihlíží k povaze, rozsahu, kontextu a účelům zpracování, tedy musí zohlednit to, že správce nebo zpracovatel zpracovává biometrické údaje a pro jaký účel je zpracovává, stejně tak jako jaké hrozí z tohoto zpracování rizika pro subjekty údajů.

Povinnost přijmout vhodná opatření k zabezpečení osobních údajů

Jednou ze zásadních povinností správců a zpracovatelů je osobní údaje vhodně zabezpečit. Vhodné zabezpečení vybírá správce a zpracovatel podle

- stavu techniky,
- nákladům na provedení,
- povaze, rozsahu, kontextu a účelům zpracování a
- různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob.

Správce a zpracovatel mají povinnost zajistit úroveň zabezpečení, které odpovídá riziku pro práva a svobody subjektu údajů. Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

GDPR nestanoví, jaká opatření má správce nebo zpracovatel přijmout. Důležitý je výsledek, tedy vhodné zabezpečení. Jako příklad uvádí GDPR pseudonymizaci a šifrování integritu, dostupnost a odolnost systémů a služeb zpracování, schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů, procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování, schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování, schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů, procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Opatření jsou technická a organizační. Technickými opatřeními se rozumí zabezpečení sítě, šifrování, volba hesel, přístupových oprávnění, ukládání logů apod. Organizačními opatřeními jsou pak školení zaměstnanců nebo vnitřní směrnice o ochraně osobních údajů. Jako příklad může sloužit zákon č. 181/2024 Sb., o kyberbezpečnosti, který uvádí příklady organizačních a technických opatřen v § 5. Správce a zpracovatel přijmou opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

Čím citlivější povahy osobní údaje jsou a čím větší újma by v případě porušení zabezpečení mohla subjektům údajů vzniknout, tím komplexnější zabezpečení by měl správce nebo zpracovatel přijmout. Bude-li správce nebo zpracovatel zpracovávat biometrické údaje, měl by zavést tomu odpovídající opatření.

Povinnost ohlásit porušení zabezpečení osobních údajů

Správce má povinnost porušení zabezpečení ohlásit dozorovému úřadu. Ohlášení by měl správce učinit bez zbytečného odkladu. GDPR stanoví, že lhůta k ohlášení je 72 hodin od okamžiku, kdy se o porušení zabezpečení správce dozvěděl. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění. Zpracovatel ohlašuje porušení zabezpečení správci.

Prošením zabezpečení se podle pokynů k ohlašování případů porušení zabezpečení osobních údajů p rozumí porušení integrity, porušení dostupnosti nebo porušení důvěrnosti. Bod 75 odůvodnění uvádí, že rizika pro práva a svobody fyzických osob mohou vyplynout ze zpracování osobních údajů, které by mohlo vést k fyzické, hmotné nebo nehmotné újmě, zejména v případech, kdy by zpracování mohlo vést k diskriminaci, krádeži či zneužití identity, finanční ztrátě, poškození pověsti, ztrátě důvěrnosti osobních údajů chráněných služebním tajemstvím, neoprávněnému zrušení pseudonymizace nebo jakémukoliv jinému významnému hospodářskému či společenskému znevýhodnění, kdy by subjekty údajů mohly být zbaveny svých práv a svobod nebo možnosti kontrolovat své osobní údaje.

Povinnost provést ohlášení správce nemá, pokud vyhodnotí, že je nepravděpodobné, že by porušení mělo za následek riziko pro práva a svobody fyzických osob. Správce musí zvážit rizika podle konkrétních okolností porušení. Vodítkem by měl být podle pokynů k porušení typ porušení, povaha citlivost a objem osobních údajů, možnost zjištění totožnosti fyzických osob, závažnost následků pro fyzické osoby a zvláštní charakteristiky správce a fyzické osoby, počet dotčených fyzických osob nebo všeobecné aspekty (např. potenciální dopady a pravděpodobnost, že k nim dojde).

Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, musí správce toto porušení podle čl. 34 GDPR bez zbytečného odkladu subjektu údajů. Pokyny k ohlášení zabezpečení uvádí, že v případě porušení zabezpečení zvláštních kategorií údajů (např. krádeže identity) by měl správce bez zbytečného odkladu oznámit toto porušení dotčeným fyzickým osobám, v odůvodněných případech i dříve než dozorovému úřadu.

Povinnost spolupracovat s dozorovým úřadem

Správce a zpracovatel, případně jejich zástupci mají na požádání podle čl. 31 GDPR povinnost spolupracovat s dozorovým úřadem při plnění úkolů tohoto úřad. V České republice je dozorovým úřadem Úřad pro ochranu osobních údajů. Dozorový úřad může požadovat spolupráci a součinnost je v případech uvedených v GDPR nebo v jiném zákoně. Součinnost může dozorový úřad požadovat mimo jiné při monitorování a vymáhání dodržování nařízení, vyřizování stížností, provádění šetření, monitorování vývoje ochrany osobních údajů v relevantních oblastech apod.

Role Úřadu pro ochranu osobních údajů

Úřad pro ochranu osobních údajů je nezávislý orgán, který monitoruje a vymáhá plnění povinností správců podle GDPR. Na základě podnětů nebo kontrolních plánů provádí u správců kontroly zpracování osobních údajů a v případě pochybení uloží správci sjednat nápravu, případně mu udělí pokutu.

Úřad pro ochranu osobních údajů:

- monitoruje a vymáhá uplatňování tohoto nařízení,
- zvyšuje povědomí veřejnosti o rizicích, pravidlech, zárukách a právech v souvislosti se zpracováním a podporuje porozumění těmto otázkám. Zvláštní pozornost se přitom věnuje akcím, které jsou určeny speciálně pro děti,
- v souladu s právem členského státu poskytuje poradenství vnitrostátnímu parlamentu, vládě a dalším orgánům a institucím ohledně legislativních a správních opatření týkajících se ochrany práv a svobod fyzických osob v souvislosti se zpracováním,
- podporuje povědomí správců a zpracovatelů o jejich povinnostech podle tohoto nařízení,
- na požádání poskytuje všem subjektům údajů informace ohledně výkonu jejich práv podle tohoto nařízení a, je-li to vhodné, spolupracuje za tímto účelem s dozorovými úřady v jiných členských státech,
- zabývá se stížnostmi, které mu podá subjekt údajů nebo subjekt, organizace či sdružení, a ve vhodné míře prošetřuje předmět stížnosti a v přiměřené lhůtě informuje stěžovatele o vývoji a výsledku šetření, zejména v případech, kdy je zapotřebí další šetření nebo koordinace s jiným dozorovým úřadem,
- s cílem zajistit jednotné uplatňování a prosazování tohoto nařízení spolupracuje s dalšími dozorovými úřady, mimo jiné formou sdílení informací, a s těmito úřady si vzájemně poskytuje pomoc,
- provádí šetření o uplatňování tohoto nařízení, mimo jiné na základě informací obdržených od jiného dozorového úřadu či jiného orgánu veřejné moci,
- monitoruje vývoj v relevantních oblastech, pokud má vliv na ochranu osobních údajů, zejména vývoj informačních a komunikačních technologií a obchodních praktik,
- přijímá standardní smluvní doložky,
- připravuje a udržuje seznam v souvislosti s požadavkem provádět posouzení vlivu na ochranu osobních údajů,
- poskytuje poradenství o některých operacích zpracování,
- podporuje vypracování kodexů chování, vydává stanoviska a schvaluje takové kodexy chování, které poskytují dostatečné záruky,
- vybízí k zavedení mechanismů pro vydávání osvědčení o ochraně údajů a pečetí a známek dokládajících ochranu údajů a schvaluje kritéria pro vydávání osvědčení,
- případně provádí pravidelný přezkum osvědčení,
- navrhuje a zveřejňuje kritéria pro schvalování subjektu pro monitorování kodexů chování a subjektu pro vydávání osvědčení
- provádí schvalování subjektu pro monitorování kodexů chování a subjektu pro vydávání osvědčení,
- schvaluje smluvní doložky,
- schvaluje závazná podniková pravidla,
- přispívá k činnostem Evropského sboru pro ochranu osobních údajů,
- vede interní záznamy o porušeních GDPR a o přijatých opatřeních,
- plní veškeré další úkoly související s ochranou osobních údajů.

Po provedené kontrole má Úřad pro ochranu osobních údajů možnost:

- upozornit správce či zpracovatele, že zamýšlené operace zpracování pravděpodobně porušují GDPR,
- udělit napomenutí správci či zpracovateli, jehož operace zpracování porušily GDPR,

- nařídit správci nebo zpracovateli, aby vyhověli žádostem subjektu údajů o výkon jeho práv,
- nařídit správci či zpracovateli, aby uvedl operace zpracování do souladu s GDPR, a to případně předepsaným způsobem a ve stanovené lhůtě,
- nařídit správci, aby subjektu údajů oznámil případy porušení zabezpečení osobních údajů,
- uložit dočasné nebo trvalé omezení zpracování, včetně jeho zákazu,
- nařídit opravu či výmaz osobních údajů nebo omezení zpracování a ohlašování takových opatření příjemcům, jimž byly osobní údaje zpřístupněny,
- odebrat osvědčení nebo nařídit, aby subjekt pro vydávání osvědčení odebral osvědčení, nebo aby osvědčení nevydal, pokud požadavky na osvědčení plněny nejsou nebo již přestaly být plněny,
- uložit správní pokutu vedle či namísto jiných opatření, podle okolností každého jednotlivého případu,
- nařídit přerušení toků údajů příjemci ve třetí zemi nebo toků údajů mezinárodní organizaci.

Soudní a správní ochrana

Subjekt údajů může podat podnět k Úřadu pro ochranu osobních údajů. Pokud má subjekt údajů za to, že jeho práva podle byla porušena v důsledku zpracování jeho osobních údajů v rozporu s GDPR může se domáhat nápravy žalobu proti správci u soudu.

Kdokoli, tedy teoreticky nejen subjekt údajů, kdo v důsledku porušení GDPR utrpěl hmotnou či nehmotnou újmu, má právo obdržet od správce nebo zpracovatele náhradu utrpěné újmy.

Správce zapojený do zpracování je odpovědný za újmu, kterou způsobí zpracováním, jež porušuje GDPR. Zpracovatel je za újmu způsobenou zpracováním odpovědný pouze v případě, že nesplnil povinnosti stanovené GDPR konkrétně pro zpracovatele nebo že jednal nad rámec zákonných pokynů správce nebo v rozporu s nimi. Správce nebo zpracovatel jsou této odpovědnosti zproštěni, pokud prokáží, že nenesou žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla.

Ukládání pokut

Úřad pro ochranu osobních údajů musí zajistit, aby ukládání správních pokut za porušení GDPR bylo účinné, přiměřené a odrazující.

Při rozhodování o tom, zda uložit správní pokutu, a rozhodování o výši správní pokuty v jednotlivých případech se řádně zohlední mimo jiné tyto okolnosti:

- povaha, závažnost a délka trvání porušení s přihlédnutím k povaze, rozsahu či účelu dotčeného zpracování, jakož i k počtu dotčených subjektů údajů a míře škody,
- zda k porušení došlo úmyslně nebo z nedbalosti,
- kroky podniknuté správcem či zpracovatelem ke zmírnění škod způsobených subjektům údajů,
- kategorie osobních údajů dotčené daným porušením,
- splnění předchozích opatření,
- způsob, jakým se dozorový úřad dozvěděl o porušení,
- spolupráce s dozorovým úřadem, nebo
- přijatá technická a organizační opatření.

Za porušení GDPR může správce uložit správní pokuty až do výše 10 000 000 EUR, nebo jedná-li se o podnik, až do výše 2 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší.

Úřad pro ochranu osobních údajů však musí být při ukládání pokut konzistentní, musí naplňovat zásadu legitimního očekávání účastníků řízení a zásahu rovného zacházení, neboli zásadu, aby v podobných případech nevznikaly neodůvodněné rozdíly mezi účastníky jednotlivých řízení.

Záruky a odchylky pro zpracování pro účely pro účely vědeckého výzkumu

Biometrické údaje mohou být zpracovávány pro účely vědeckého výzkumu. I na tento druh zpracování GDPR pamatuje. GDPR umožňuje oproti jinému zpracování určité výjimky. Těmito výjimkami jsou výjimky z účelového omezení, z omezení doby zpracování, ze zákazu zpracování zvláštních kategorií údajů, z informační povinnosti nebo z práva na výmaz.

Zpracování zvláštních kategorií údajů, tedy i biometrických údajů je možné, pokud je zpracování je nezbytné pro účely vědeckého výzkumu. V takovém případě se neuplatní zákaz zpracování zvláštních kategorií údajů.

Osobní údaje musí být zpracovávány pro určitý účel. GDPR pamatuje i na situace, kdy je možné se osobní údaje získané pro jiný účel zpracovávat pro jiný účel. Zpracovávání pro účely vědeckého výzkumu se nepovažuje za neslučitelné s původním účelem zpracování.

Správce nemusí informovat subjekt údajů o zpracování, pokud poskytnutí takových informací není možné nebo by vyžadovalo nepřiměřené úsilí.

Správce nemusí vyhovět žádosti subjektu údajů o právo na výmaz, pokud by bylo pravděpodobné, že by výmaz znemožnil nebo vážně ohrozil splnění cílů zpracovávání, tedy ohrožení pravdivosti a správnosti výsledků výzkumu.

Zpracování pro účely vědeckého výzkumu musí podléhat vhodným zárukám práv a svobod subjektu údajů. Důvodem jsou právě výše uvedené výjimky. Záruky musí zajistit, aby byla zavedena technická a organizační opatření, zejména s cílem zajistit dodržování zásady minimalizace údajů. Tato opatření mohou zahrnovat pseudonymizaci za podmínky, že lze tímto způsobem splnit sledované účely. Pokud mohou být sledované účely splněny dalším zpracováním, které neumožňuje nebo které přestane umožňovat identifikaci subjektů údajů, musí být tyto účely splněny tímto způsobem.

Případové studie (use-cases)

Případové studie jsou rozdělené na dvě části podle toho, zda je vyžadován souhlas subjektu údajů nebo zda je zpracování prováděno na základě jiného právního důvodu. V případě souhlasu se subjekt údajů může svobodně rozhodnout, zda si údaje přeje zpracovávat, či nikoliv. V některých případech má právě nemožnost se svobodně rozhodnout za následek neplatnost souhlasu. U jiných důvodů volbu ohledně zpracování nemá. Smyslem tohoto rozdělení jsou dále rozdílné nároky subjektu údajů ve vztahu k uplatnění svých práv. Subjekt údajů má kromě práva na odvolání souhlasu za dalších podmínek i právo na výmaz svých osobních údajů nebo právo na přenositelnost. Pokud je zpracovávání založeno na jiném právním důvodu, subjekt údajů taková práva nemá.

Zpracování biometrických údajů na základě souhlasu

Jako první budou popsány případy, které zpracovávají biometrické údaje na základě souhlasu. Tyto jsou mnohem četnější a obvyklejší než druhá kategorie.

Využití biometriky v mobilních zařízeních

Biometrika se v mobilních zařízeních využívá z důvodu bezpečnosti přihlášení a obsluhy zařízení. Biometrika tedy slouží k zabezpečení. Kvalitu zabezpečení zajišťují standardy a certifikace, které jsou popsány na začátku dokumentu. Prakticky se setkáváme s rozpoznáním podle obličeje (typicky 3D) a otisku prstu (optická, kapacitní nebo ultrazvuková technologie). Některá zařízení umějí obě charakteristiky kombinovat. Teoreticky bychom se v budoucnu mohli setkat s rozpoznáváním podle duhovky (v minulosti bylo používáno), podle specifického chování (např. styl kresby symbolu, ovládání zařízení), podle geometrie a otisku dlaně anebo žilního řečiště. Z pohledu zabezpečení mobilních telefonů jsou aktuálně nejspolehlivější metody založeny na otiscích prstů (velmi ovšem záleží na konkrétním provedení).

Právním důvodem zpracování je výslovný souhlas subjektu údajů podle čl. 9 odst. 2 písm. a) GDPR. Bez tohoto souhlasu nemůže správce biometrické údaje zpracovávat. Souhlas může uživatel mobilního telefon kdykoliv odvolat a požadovat výmaz svých biometrických údajů. Subjekt údajů má dále právo na přístup ke svým osobním údajům, právo na omezení zpracování a právo nebýt předmětem automatizovaného rozhodování. Teoreticky má subjekt údajů právo na přenositelnost, tedy přenos k jinému správci, nicméně protože biometrické údaje slouží zejména k zabezpečení mobilního zařízení, nebude mít toto právo praktické využití.

Správce musí dodržovat všechny povinnosti, které mu GDPR ukládá. Správce musí zpracovávat biometrické údaje v mobilních zařízeních transparentně, tj. musí poskytnout subjektu údajů všechny potřebné informace o zpracování.

Účel zpracování biometrických údajů musí být jasně vymezen a biometrické údaje nesmí být zpracovávány po dobu delší než je nezbytné ke splnění účelu.

Obzvláště důležitá je zásady integrity a důvěrnosti osobních údajů. Zabezpečení by mělo odrážet zvláště citlivou povahu biometrických údajů mimo jiné šifrování, zálohování, nebo pravidelné hodnocení přijatých technických a organizačního opatření.

Protože biometrika v mobilních zařízeních představuje rozsáhlé zpracování zvláštních kategorií údajů, bude muset správce vypracovat posouzení vlivu na ochranu osobních údajů. Zároveň se bude jednat o zpracování za využití nových technologií, které bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude za následek vysoké riziko pro práva a svobody fyzických osob.

Posouzení musí obsahovat alespoň:

- systematický popis zamýšlených operací zpracování a účely zpracování,
- posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů,
- posouzení rizik pro práva a svobody subjektů údajů uvedených v odstavci a
- plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s GDPR, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

Pokud bude možné posoudit zpracování biometrických údajů v mobilních zařízeních jako hlavní činnosti správce nebo zpracovatele, která spočívá v rozsáhlém zpracování těchto osobních údajů, bude muset správce, popřípadě zpracovatel muset jmenovat pověřence na ochranu osobních údajů.

Porušení zabezpečení biometrických údajů bude až na výjimky zakládat povinnost správce hlásit do 72 hodin od zjištění toto porušení Úřadu pro ochranu osobních údajů.

Toto ohlášení musí obsahovat zejména:

- popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů,
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace,
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů,
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Jelikož bude pravděpodobné, že porušení zabezpečení biometrických údajů v mobilních zařízeních bude mít za následek vysoké riziko pro práva a svobody fyzických osob, bude muset porušení zabezpečení oznámit správce bez zbytečného odkladu subjektům údajů.

Autentifikace bankovních transakcí pomocí biometriky

Biometrika se nejen v mobilních zařízeních využívá z důvodu bezpečnosti transakcí. Nejčastější použití v dnešní době je autentifikace pomocí otisku prstu při používání bankovních aplikací v mobilních telefonech. Dle certifikace a kvality použitého biometrického systému je samozřejmě možné k potvrzení identity využít i ostatní biometrické charakteristiky zmíněné v předchozí části ohledně mobilních zařízení. V některých zemích je využita autentifikace i při výběru z bankomatu kdy je možné doplnit nebo nahradit PIN biometrikou. Pro takové použití se např. v Polsku využívá rozpoznání podle žilního řečiště. Teoreticky by však do bankomatu mohlo být zabudováno jakékoliv zařízení s dostatečnou úrovní zabezpečení (viz další případ týkající se zaměstnání).

Biometrika slouží k zabezpečení transakce. Ověření pomocí biometrických údajů je jako jedna z možností silného ověření uvedeno v § 223 odst. 3 zákona č. 370/2017 Sb., o platebním styku. Banka sama biometrické údaje nezpracovává a nemá k nim přístup. Od třetí strany dostává pouze informaci, zda ověření proběhlo úspěšně nebo neúspěšně.

Právním důvodem zpracování je souhlas subjektu údajů podle čl. 9 odst. 2 písm. a) GDPR. Bez tohoto souhlasu nemůže správce biometrické údaje zpracovávat. Majitel účtu má stejná práva, jaké jsou uvedena výše, ve vztahu k biometrickým údajům v mobilním zařízení. Subjekt údajů má právo odvolat souhlas, právo na přístup ke svým osobním údajům, právo na omezení zpracování a právo nebýt předmětem automatizovaného rozhodování a právo na přenositelnost.

Správce, kterým bude poskytovatel služby autentifikace, musí dodržovat všechny povinnosti, které mu GDPR ukládá. Správce musí zpracovávat biometrické údaje transparentně, tj. musí poskytnout subjektu údajů všechny potřebné informace o zpracování.

Účel zpracování biometrických údajů musí být jasně vymezen a biometrické údaje nesmí být zpracovávány po dobu delší, než je nezbytné ke splnění účelu.

Musí být dodržovány zásady integrity a důvěrnosti osobních údajů. Zabezpečení by mělo odrážet zvláště citlivou povahu biometrických údajů mimo jiné šifrování, zálohování, nebo pravidelné hodnocení přijatých technických a organizačního opatření.

Protože zpracování biometrických údajů pro účely autentizace bankovních transakcí chování bude představovat rozsáhlé zpracování zvláštních kategorií údajů, bude muset správce vypracovat posouzení vlivu na ochranu osobních údajů. Zároveň se bude jednat o zpracování za využití nových technologií, které bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude za následek vysoké riziko pro práva a svobody fyzických osob.

Posouzení musí obsahovat alespoň:

- systematický popis zamýšlených operací zpracování a účely zpracování,
- posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů,
- posouzení rizik pro práva a svobody subjektů údajů uvedených v odstavci a
- plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s GDPR, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

Zpracování biometrických údajů pro účely autentizace bankovních transakcí bude hlavní činnosti správce – poskytovatele služby, která spočívá v rozsáhlém zpracování biometrických údajů, bude muset správce, jmenovat pověřence na ochranu osobních údajů.

Porušení zabezpečení biometrických údajů bude až na výjimky zakládat povinnost správce ohlásit do 72 hodin od zjištění toto porušení Úřadu pro ochranu osobních údajů.

Toto ohlášení musí obsahovat zejména:

- popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů,
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace,
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů,
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Jelikož bude pravděpodobné, že porušení zabezpečení biometrických údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, bude muset porušení zabezpečení oznámit správce bez zbytečného odkladu subjektům údajů.

Behaviorální biometrika

Behaviorální biometrika slouží jako analýza chování v reálném čase. Může sloužit jako silné ověření identity. Nejčastějšími sledované parametry jsou preference používaných zařízení, frekvence, lokalita a preferované časy připojení, způsob zadávání přihlašovacích údajů, průchod aplikací apod. Tento způsob verifikace aktuálně není příliš používán, může však probíhat i průběžně při používání zařízení (tj. pokud zařízení začne používat někdo jiný, automaticky

se zamkne). Dalším typickým zástupcem dynamických charakteristik je rozpoznání podle způsobu chůze (praktické využití je spíše u soudních sporů než např. jako přístupový systém) a rozpoznání podle podpisu (v tomto případě máme na mysli podpis včetně informací o tom, jak vznikal – tj. např. pozice pera v čase, rychlost podpisu, náklon pera, přítlak apod.). Je potřeba dodat že aktuálně ve valně většině případů je verifikace na základě podpisu založena pouze na jeho reprezentaci bez behaviorálních charakteristik (snímání dynamických vlastností je podmíněno speciálním perem – tj. i většina podpisů na tablet nebo speciální plochu aktuálně tyto dynamické vlastnosti nevyužívá).

Právním důvodem zpracování je souhlas subjektu údajů podle čl. 9 odst. 2 písm. a) GDPR. Bez tohoto souhlasu nemůže správce biometrické údaje zpracovávat. Subjekt údajů má právo odvolat souhlas, právo na přístup ke svým osobním údajům, právo na omezení zpracování a právo nebýt předmětem automatizovaného rozhodování a právo na přenositelnost.

Správce musí dodržovat všechny povinnosti, které mu GDPR ukládá. Správce musí zpracovávat biometrické údaje transparentně, tj. musí poskytnout subjektu údajů všechny potřebné informace o zpracování.

Účel zpracování biometrických údajů musí být jasně vymezen a biometrické údaje nesmí být zpracovávány po dobu delší než je nezbytné ke splnění účelu.

Musí být dodržovány zásady integrity a důvěrnosti osobních údajů. Zabezpečení by mělo odrážet zvláště citlivou povahu biometrických údajů mimo jiné šifrování, zálohování, nebo pravidelné hodnocení přijatých technických a organizačního opatření.

Protože zpracování biometrických údajů pro účely analýzy chování bude pravděpodobně představovat rozsáhlé zpracování zvláštních kategorií údajů, bude muset správce vypracovat posouzení vlivu na ochranu osobních údajů. Zároveň se bude jednat o zpracování za využití nových technologií, které bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude za následek vysoké riziko pro práva a svobody fyzických osob.

Posouzení musí obsahovat alespoň:

- systematický popis zamýšlených operací zpracování a účely zpracování,
- posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů,
- posouzení rizik pro práva a svobody subjektů údajů uvedených v odstavci a
- plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s GDPR, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

Pokud bude možné posoudit zpracování biometrických údajů pro účely analýzy chování jako hlavní činnosti správce nebo zpracovatele, která spočívá v rozsáhlém zpracování těchto osobních údajů, bude muset správce, popřípadě zpracovatel muset jmenovat pověřence na ochranu osobních údajů.

Porušení zabezpečení biometrických údajů bude až na výjimky zakládat povinnost správce ohlásit do 72 hodin od zjištění toto porušení Úřadu pro ochranu osobních údajů.

Toto ohlášení musí obsahovat zejména:

- popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů,

- jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace,
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů,
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Jelikož bude pravděpodobné, že porušení zabezpečení biometrických údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, bude muset porušení zabezpečení oznámit správce bez zbytečného odkladu subjektům údajů.

Využívání biometriky v zaměstnání (např. vstup do budovy, otevírání pokladny apod.)

Využívání biometriky v zaměstnání je problematické. Biometrické údaje jakožto zvláštní kategorie údajů mohou být zpracovávány pouze s výslovným souhlasem subjektu údajů podle čl. 9 odst. 2 písm. 1) GDPR. Z technologického hlediska se můžeme setkat s jakýkoliv (typicky zabudovaným nástěnným) biometrickým zařízením. Ty v dnešní době typicky využívají rozpoznání podle otisků prstů, obličeje, geometrii (tvaru) ruky, duhovky a žilního řečiště. Takové zařízení může být kombinováno i se systémem zaznamenávání docházky. Jako alternativu může takové zařízení využívat i zabezpečení pomocí klíče (obvykle tokenu RFID tj. pomocí čipu nebo karty).

Úřad pro ochranu osobních údajů sice v jednom případě neshledal v používání FaceID, tedy kontrolu vstupu pomocí rozeznávání obličeje, porušení GDPR, nicméně sám úřad prohlásil, že se jednalo o specifický případ. Zaměstnance nedával k použití svých biometrických údajů souhlas. Zpracování probíhalo na základě výjimky podle čl. 9 odst. 2 písm. b) (plnění povinnosti v oblasti pracovního práva) ve spojení s čl. 6 odst. 1 písm. c) GDPR (plnění povinností správce).

Souhlas se zpracováním osobních údajů musí být svobodný, jinak se nejedná o platný souhlas. Souhlas zaměstnance je málo kdy svobodný, protože zaměstnance může mít při jeho neudělení obavu z důsledků pro pracovněprávní vztah. Aby souhlas s použitím biometrických údajů mohl být považován za svobodný, měl by mít zaměstnanec alternativu, pokud se rozhodně souhlas nedělit. S využitím alternativy nesmí být spojené negativní následky pro zaměstnance.

Kontrola vstupu do škol

Kontrola vstupu pomocí biometriky se provádí za účelem zabezpečení vstupu do budovy. I přesto, že i v tomto případě by šlo využít jakéhokoliv nástěnného biometrického zařízení, je prakticky nutné myslet na využití dětmi. Zařízení by tak mělo snímat charakteristiku, která je i v nižším věku stabilní a snadno se snímá (nabízí se rozpoznání podle otisků prstů či duhovky).

Právním důvodem zpracování je souhlas subjektu údajů podle čl. 9 odst. 2 písm. a) GDPR. Bez tohoto souhlasu nemůže správce biometrické údaje zpracovávat. Správcem by v tomto případě byla škola. Pokud je souhlas odvolán, nesmí správce biometrické údaje dále zpracovávat. Jestliže by žák neměl možnost identifikovat se při vstupu jiným způsobem, byl by jeho souhlas, resp. souhlas udělený jeho zákonným zástupcem neplatný.

Úřad pro ochranu osobních údajů v případě kontroly ověřování identity pomocí biometriky, že souhlas se zpracováním biometrických údajů není platný, protože tento způsob ověření sloužil v konkrétním případě pouze pro usnadnění vstupu osobám, nikoliv k zabezpečení. Do budovy

mohly společně s osobou, jejíž identita byla ověřena pomocí biometriky, vstoupit i další osoby, které nebyly identifikovány.

Využívání biometrického klíče pro odemykání domu

Kontrola vstupu pomocí biometriky se provádí za účelem zabezpečení vstupu do budovy. Právním důvodem zpracování je souhlas subjektu údajů podle čl. 9 odst. 2 písm. a) GDPR. Správcem by bylo společenství vlastníků jednotek nebo majitel domu (právnická nebo fyzická osoba, případně bytové družstvo). Bez tohoto souhlasu nemůže správce biometrické údaje zpracovávat. Pokud je souhlas odvolán, nesmí správce biometrické údaje dále zpracovávat. Jestliže by majitel bytu nebo nájemce neměl alternativu k takovému ověřování identity, nebyl by jeho souhlas platný.

Biometrické systémy mohou pracovat i tak, že osobu přímo neidentifikují, pouze ji autentizují. Pokud v takovém případě dojde ke změně majitele nebo nájemce, bylo by nutné celou databázi biometrických údajů nahrát znovu, protože osobu, která se odstěhovala, nelze z databáze pouze jednoduše vyřadit. Zde je k dispozici plná škála možných biometrických řešení (nicméně opět je nutné uvažovat s potenciálně velkým věkovým rozpětím uživatelů takového systému).

Protože zpracování biometrických údajů pro účely odemykání domu nebude pravděpodobně představovat rozsáhlé zpracování zvláštních kategorií údajů, nicméně se bude jednat o zpracování za využití nových technologií, které bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude za následek vysoké riziko pro práva a svobody fyzických osob a správce bude muset vypracovat posouzení vlivu na ochranu osobních údajů.

Posouzení musí obsahovat alespoň:

- systematický popis zamýšlených operací zpracování a účely zpracování,
- posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů,
- posouzení rizik pro práva a svobody subjektů údajů uvedených v odstavci a
- plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s GDPR, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

Pokud by se vlastník domu rozhodl tento systém použít, nemusel by jmenovat pověřence pro ochranu osobních údajů, protože se pravděpodobně nebude jednat hlavní činnosti správce spočívající v rozsáhlém zpracování zvláštních kategorií údajů.

Rozpoznávání obličeje na sociálních sítích

Biometrické údaje se na sociálních sítích využívají k vyhledávání majitele profilu ve videích a na fotkách, k označování a mohou sloužit i k detekci krádeže identity. Z technologického hlediska je vhodné dodat, že, až na několik výjimek, jsou to právě firmy vlastnící sociální sítě, které mají aktuálně nejspolehlivější a nejvýkonnější systémy na rozpoznání obličeje.

Právním důvodem zpracování je souhlas subjektu údajů podle čl. 9 odst. 2 písm. a) GDPR. Správcem je poskytovatel sociální sítě. Bez tohoto souhlasu nemůže správce biometrické údaje zpracovávat. Pokud je souhlas odvolán, nesmí správce biometrické údaje dále zpracovávat.

Subjekt údajů má právo odvolat souhlas, právo na přístup ke svým osobním údajům, právo na omezení zpracování a právo nebýt předmětem automatizovaného rozhodování a právo na přenositelnost.

Správce musí dodržovat všechny povinnosti, které mu GDPR ukládá. Správce musí zpracovávat biometrické údaje transparentně, tj. musí poskytnout subjektu údajů všechny potřebné informace o zpracování.

Účel zpracování biometrických údajů musí být jasně vymezen a biometrické údaje nesmí být zpracovávány po dobu delší než je nezbytné ke splnění účelu.

Musí být dodržovány zásady integrity a důvěrnosti osobních údajů. Zabezpečení by mělo odrážet zvláště citlivou povahu biometrických údajů mimo jiné šifrování, zálohování, nebo pravidelné hodnocení přijatých technických a organizačního opatření.

Protože zpracování biometrických údajů pro účely rozpoznávání obličeje bude představovat rozsáhlé zpracování zvláštních kategorií údajů, bude muset správce vypracovat posouzení vlivu na ochranu osobních údajů. Zároveň se bude jednat o zpracování za využití nových technologií, které bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude za následek vysoké riziko pro práva a svobody fyzických osob.

Posouzení musí obsahovat alespoň:

- systematický popis zamýšlených operací zpracování a účely zpracování,
- posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů,
- posouzení rizik pro práva a svobody subjektů údajů uvedených v odstavci a
- plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s GDPR, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

Pokud bude možné posoudit zpracování biometrických údajů pro účely rozpoznávání obličejů jako hlavní činnosti správce nebo zpracovatele, která spočívá v rozsáhlém zpracování těchto osobních údajů, bude muset správce, popřípadě zpracovatel muset jmenovat pověřence na ochranu osobních údajů.

Porušení zabezpečení biometrických údajů bude určitě zakládat povinnost správce ohlásit do 72 hodin od zjištění toto porušení Úřadu pro ochranu osobních údajů.

Toto ohlášení musí obsahovat zejména:

- popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů,
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace,
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů,
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Jelikož bude pravděpodobné, že porušení zabezpečení biometrických údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, bude muset porušení zabezpečení oznámit správce bez zbytečného odkladu subjektům údajů.

Home assistants – Alexa, Google home, atd. (rozpoznávání hlasu)

Systémy rozpoznávání hlasu slouží pro pohodlnější vyhledávání informací, objednávání služeb a nastavování. Právním důvodem zpracování je souhlas subjektu údajů podle čl. 9 odst. 2 písm. a) GDPR. Firma Amazon v roce 2019 připustila, že uchovává záznamy hlasů po neomezenou dobu, pokud je uživatel sám nevymaže. Google naopak uvádí, že hlasové záznamy neuchovává, pokud uchovávání uživatel nezvolí. I přesto, že hlas není příliš spolehlivý pro identifikaci osob ve velkém rozsahu, jeho omezené použití (např. v jedné domácnosti = spíše jednotky uživatelů) bude spolehlivě dostatečně.

Subjekt údajů má právo odvolat souhlas, právo na přístup ke svým osobním údajům, právo na omezení zpracování a právo nebýt předmětem automatizovaného rozhodování a právo na přenositelnost.

Správce musí dodržovat všechny povinnosti, které mu GDPR ukládá. Správce musí zpracovávat biometrické údaje transparentně, tj. musí poskytnout subjektu údajů všechny potřebné informace o zpracování.

Účel zpracování biometrických údajů musí být jasně vymezen a biometrické údaje nesmí být zpracovávány po dobu delší než je nezbytné ke splnění účelu.

Musí být dodržovány zásady integrity a důvěrnosti osobních údajů. Zabezpečení by mělo odrážet zvláště citlivou povahu biometrických údajů mimo jiné šifrování, zálohování, nebo pravidelné hodnocení přijatých technických a organizačního opatření.

Protože zpracování biometrických údajů pro účely home assistants bude představovat rozsáhlé zpracování zvláštních kategorií údajů, bude muset správce vypracovat posouzení vlivu na ochranu osobních údajů. Zároveň se bude jednat o zpracování za využití nových technologií, které bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude za následek vysoké riziko pro práva a svobody fyzických osob.

Posouzení musí obsahovat alespoň:

- systematický popis zamýšlených operací zpracování a účely zpracování,
- posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů,
- posouzení rizik pro práva a svobody subjektů údajů uvedených v odstavci a
- plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s GDPR, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

Protože zpracování biometrických údajů bude hlavní činnosti správce, která spočívá v rozsáhlém zpracování těchto osobních údajů, bude muset správce jmenovat pověřence na ochranu osobních údajů.

Porušení zabezpečení biometrických údajů bude nepochybně zakládat povinnost správce ohlásit do 72 hodin od zjištění toto porušení Úřadu pro ochranu osobních údajů.

Toto ohlášení musí obsahovat zejména:

- popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů,
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace,
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů,
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Jelikož bude pravděpodobné, že porušení zabezpečení biometrických údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, bude muset porušení zabezpečení oznámit správce bez zbytečného odkladu subjektům údajů.

Zpracovávání biometrických údajů na základě jiného právního důvodu

Tyto případy podléhají specifickým (jiným) právním důvodům pro zpracování údajů. V takových případech jsou práva subjektů výrazně omezena.

Biometrické osobní doklady – občanské průkazy a cestovní pasy

K zpracovávání biometrických údajů se děje na základě právního předpisu, např. na základě zákona č. 269/2021 Sb. o občanských průkazech, nebo zákona č. 329/1999 Sb., o cestovních pasech) Zpracování je tedy nezbytné pro plnění právních povinností správce podle čl. 6 odst. 1) písm. c). Správce tedy nemůže uplatnit některá svá práva, u kterých to GDPR vylučuje, a to právo na výmaz, právo na přenositelnost a právo vznést námitku proti zpracování.

Biometrické údaje se uchovávají v občanských průkazech. Podle § 5 odst. 1 písm. a) bod 10 zákona č. 269/2021 Sb. o občanských průkazech se jedná o otisk prstu a zobrazení obličeje. Podle § 40 tohoto zákona Biometrické údaje uvedené v občanském průkazu lze použít pouze pro účely ověření pravosti občanského průkazu a totožnosti držitele občanského průkazu při překračování státních hranic.

Biometrické údaje jsou uchovávány i v cestovních pasech. Stejně jako u občanských průkazů se jedná o zobrazení obličeje a otisky prstů (§ 5 odst. 2 zákona č. 329/1999 Sb., o cestovních pasech. Biometrické údaje lze podle § 6 odst. 2 tohoto zákona použít výlučně pro ověřování pravosti cestovního dokladu a ověření totožnosti občana pomocí osobních údajů zapsaných v cestovním dokladu, popřípadě porovnání biometrických údajů zpracovaných v nosiči dat prostřednictvím technického zařízení umožňujícího srovnání aktuálně zobrazených biometrických údajů občana s biometrickými údaji zpracovanými v nosiči dat cestovního dokladu. Platné mezinárodní standardy dále počítají i s uchováváním duhovky a rozpoznáním podle ní.

Správce musí dodržovat všechny zásady, které GDPR stanoví. Nadto se ho týkají i pravidla pro zpracování daná zvláštním zákonem, na základě, kterého jsou osobní údaje zpracovávány.

Správce nemá povinnost před započetím zpracování vypracovat posouzení vlivu na ochranu osobních údajů. Důvodem je výjimka ze zpracování posouzení, pokud zpracování probíhá na základě zvláštního zákona. Toto posouzení by měl provést zákonodárce. Podle § 10 zákona č. 110/2019 Sb., nemusí správce provádět posouzení vlivu zpracování na ochranu osobních

údajů před jeho zahájením, pokud mu právní předpis stanoví povinnost takové zpracování osobních údajů provést.

Správce, který je orgánem veřejné moci má povinnost jmenovat pověřence pro ochranu osobních údajů.

I když je důvodem zpracování zvláštní zákon, neznamená to, že subjekt údajů, jehož biometrické údaje jsou zpracovávány, nemá žádná práva. Samozřejmě nemá právo odvolat souhlas.

Subjekt údajů má právo, aby se mu dostalo úplných informací o zpracování. Tyto informace mu může správce poskytnout i prostřednictvím internetu (§ 8 zákona č. 110/2019 Sb., o zpracování osobních údajů) Má také právo na přístup k osobním údajům a právo obdržet kopii osobních údajů, které správce zpracovává. Subjekt údajů má právo na opravu. Správce je povinen bez zbytečného odkladu opravit nepřesné osobní údaje.

Subjekt údajů nemá naopak právo na výmaz osobních údajů. Právo na výmaz by měl, pokud by byly osobní údaje zpracovány protiprávně. V takovém případě má subjekt údajů i právo na omezení zpracování.

Subjekt údajů nemá právo ani na přenositelnost a na námitku proti zpracování. Právo na přenositelnost má subjekt údajů pouze tehdy, pokud jsou osobní údaje zpracovány na základě smlouvy nebo souhlasu. Na námitku má subjekt údajů právo pouze tehdy, pokud jsou jeho osobní údaje zpracovávané na základě oprávněného zájmu správce nebo pro splnění úkolu prováděného ve veřejném zájmu.

Biometrické rozpoznávání obličeje, např. na letištích, na ulici

Systémy rozpoznávání obličeje slouží primárně policii při vyhledávání rizikových osob. Právním důvodem zpracování by v takovém případě byl důvod podle čl. 6 odst. 1 písm. e) (splnění úkolu prováděného ve veřejném zájmu), nebo c) GDPR (plnění právní povinnosti správce) spolu s čl. 9 odst. 2 písm. g) GDPR (zpracování z důvodu významného veřejného zájmu).

Oprávnění ke zpracování biometrického rozpoznávání obličejů má Vojenská policie podle § 11a odst. 1 zákona č. 300/2013 Sb., o Vojenské polici. Podle § 11a odst. 5 může Vojenská policie při plnění svých úkolů v zahraničních misích podle pravidel nasazení pořizovat a dále zpracovávat biometrické údaje také u jiných osob, než jsou fyzické osoby obviněné ze spáchání úmyslného trestného činu nebo fyzické osoby, které bylo sděleno podezření pro spáchání takového trestného činu.

Podle § 66a odst. 1 a 2 zákona č. 273/2008 Sb., o Policii České republiky a § 11c zákona č. 153/1994 Sb. o zpravodajských službách České republiky mohou tyto bezpečností složky zpracovávat digitální fotografie a agendové identifikátory fyzických osob získané z informačních systémů veřejné správy. Podle důvodové zprávy k novele by mělo být možné i softwarové vyhledání a rozpoznávání obličejů.

Systém biometrického rozpoznávání obličejů je instalován ve zkušebním režimu na letišti Václava Havla v Praze, a to na základě usnesení vlády České republiky č. 47/2015, o zvýšení bezpečnosti na mezinárodním letišti Václava Havla v Praze. Je vhodné dodat, že soustava kamer vhodná pro rozpoznávání obličejů je prakticky použitelná i pro rozpoznávání podle chůze a v některých případech by mohla být využita i pro rozpoznání podle duhovky.

Podle § 11 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů a čl. 23 GDPR se čl. 12 až 22 a v jim odpovídajícím rozsahu též čl. 5 GDPR se použijí přiměřeně nebo se splnění

povinností správce nebo zpracovatele nebo uplatnění práva subjektu údajů stanovených těmito články odloží, je-li to nezbytné a svým rozsahem přiměřené k zajištění chráněného zájmu uvedeného v § 6 odst. 2 výše uvedeného zákona. Chráněným zájmem jsou mimo jiné obranné nebo bezpečnostní zájmy České republiky, nebo veřejný pořádek a vnitřní bezpečnost, předcházení, vyhledávání nebo odhalování trestné činnosti, stíhání trestných činů, výkon trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech. Možnost takové výjimky připouští čl. 23 GDPR.

Právní předpis, který obsahuje omezení práv, musí obsahovat:

- účely zpracování nebo kategorie zpracování,
- kategorie osobních údajů,
- rozsah zavedených omezení,
- záruky proti zneužití údajů nebo protiprávnímu přístupu k nim či jejich protiprávnímu předání,
- specifikaci správců nebo kategorie správců,
- doby uložení a platné záruky s ohledem na povahu, rozsah a účely zpracování nebo kategorie zpracování,
- rizika z hlediska práv a svobod subjektů údajů a
- právo subjektů údajů být informováni o daném omezení, pokud toto informování nemůže být na újmu účelu omezení.

Takové informace obsahuje § 79 a násl. zákona o Policii České republiky, § 10 zákona o Vojenské policii

Použitá literatura

[1] Drahanský, M., Orság, F., Doležel, M., a kol. Biometrie. Computer Press a.s., 2011, p. 294. ISBN 978-80-254-8979-6.

[2] Drahanský, M.: Hand-Based Biometrics: Methods and Technology, IET 2018, p. 430, ISBN 978-1-78561-224-4.

[3] Jain, A. K., Flynn, P., Ross, A. A.: Handbook of Biometrics. Springer, 2008, s. 556, ISBN 978-0-387-71040-2.

[4] Krsička, T.: Extrakce podrobných informací z plastických otisků prstů. Bakalářská práce. FIT VUT, 2022, p. 54.

[5] Faundez-Zanuy M.: On-line signature recognition based on VQ-DTW. Pattern Recognition, Elsevier, 2007, pp. 981-992. DOI 10.1016/j.patcog.2006.06.007.

[6] ISO/IEC TR 29156:2015, Information technology — Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics

[7] Leading the market in biometric systems solutions, Dostupné na: https://www.fingerprints.com/uploads/corporate/2016/12/Fingerprints-Capital-Markets-Day-2016.pdf

[8] ČSN ISO/IEC 19795-1, Informační technologie – Testování a hodnocení výkonnosti biometrik – Část 1: Principy a základní struktura, 2008

[9] ČSN ISO/IEC 30107-3, Informační technologie – Detekce biometrického prezentačního útoku – Část 3: Testování a podávání zpráv, 2019

[10] FIDO Biometrics Requirements, [Online]. Dostupné na: https://fidoalliance.org/specs/biometric/Biometrics-Requirements-v1.0-wd-20190606.html

[11] Android Now FIDO2 Certified, Accelerating Global Migration Beyond Passwords, [Online]. Dostupné na: https://fidoalliance.org/android-now-fido2-certified-accelerating-global-migration-beyond-passwords/

[12] FIDO – Biometric Component Certification, [Online]. Dostupné na: https://fidoalliance.org/certification/biometric-component-certification/

[13] Kafková, M. P., Doseděl, T., a Reimerová, K.: Výzkumná zpráva: Průzkum a edukace občanů České republiky v oblasti biometrie, Masarykova univerzita, Brno, Česká republika, 2021. [Online]. Dostupné na: https://webcentrum.muni.cz/media/3338383/precobi_vyzkumna-zprava.pdf