Brožura pro obyvatele – biometrické systémy

Průzkum a edukace občanů České republiky v oblasti biometrie

TL02000134

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

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

www.tacr.cz

Výzkum užitečný pro společnost.

Úvod

Do rukou se vám dostává brožura 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. Brožura byla vytvořena na základě informací získaných z průzkumu mezi obyvateli ČR ohledně využívání biometrických systémů. Tyto výsledky si budete moci přečíst a sami si ověřit, jak na tom jste. I přesto, že biometrické systémy podstatně zvyšují bezpečnost, je nutné si na některé věci dávat pozor. Díky informacím z této brožury by pro vás mělo být mnohem snadnější tato nebezpečí rozpoznávat, avšak především jim předcházet. Poslední část se pak věnuje biometrickým údajům z právního pohledu. Doufáme, že na základě nabytých znalostí budete vy i vaši blízcí využívat biometrické systémy ještě efektivněji a bezpečněji.

Průzkum znalostí biometrických systémů mezi občany České republiky

Zdroj dat a metodologie výzkumu

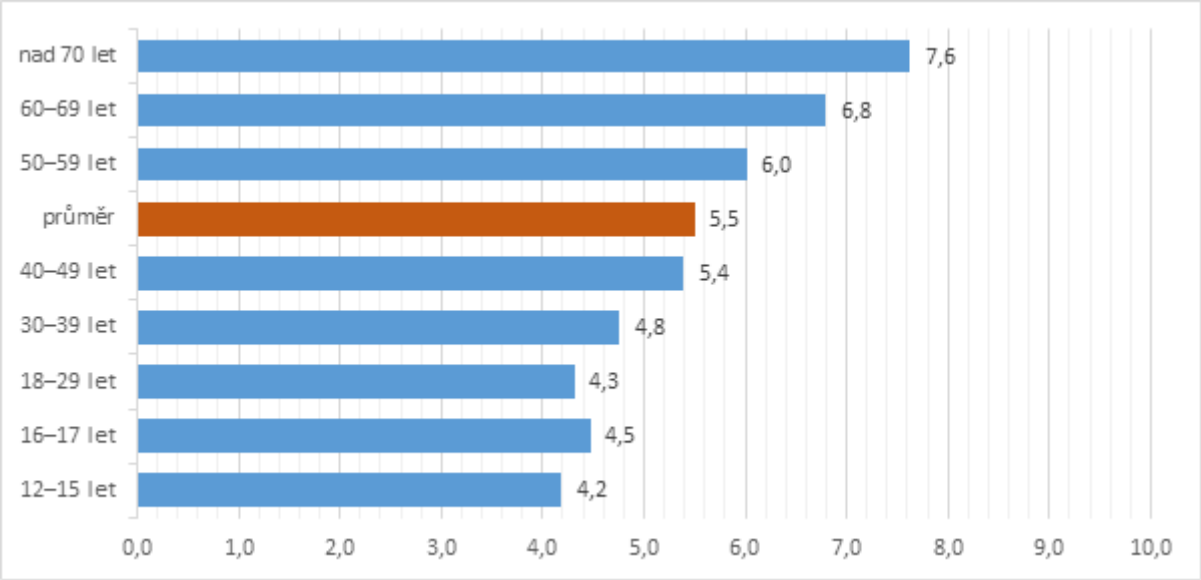
Moderní technologie jsou rychle se rozvíjející oblastí. Jejich výraznou akceleraci jsme zaznamenali zejména v reakci na opatření proti onemocnění COVID-19. Prezentované výsledky jsou proto platné pro dobu sběru dat (podzim 2020), populaci České republiky a soudobé technologie. Tato brožura obsahuje soubor zjištění o znalostech a způsobech používání ICT a biometrických technologií obyvatelstva České republiky. Prezentované výsledky představují absolutní počty, tedy procentuální podíly jednotlivých kategorií odpovědí. U všech otázek jsme analyzovali rozdíly mezi obyvateli podle věku (věkovými skupinami kategorizovanými po 10 letech), vzdělání (nejvyššího získaného vzdělání), pohlaví a velikosti bydliště. Vzhledem k tomu, že naše analýzy ukázaly zcela zásadní vliv věku na odpovědi respondentů a respondentek, je podstatná část grafů a tabulek věnována právě jim. Ostatním rozdílům se ve zprávě věnujeme pouze v případech, že existují a jsou z věcného hlediska významné.

Data pro tuto brožuru pocházejí ze dvou zdrojů. 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 sběru dat byla zachována co největší shoda, tak aby bylo možné sledovat rozrůznění znalostí a postojů dle věku respondentů a respondentek. 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. Kvótními znaky bylo pohlaví, věk, vzdělání, velikost obce a kraj. Celkově bylo nasbíráno (*N*=) 2 341 úplných dotazníků. Data z populace mladší 18 let byla sbírána přímo členy výzkumného týmu. Sběr dat zkomplikovala opatření proti nemoci COVID-19, kdy druhé stupně základních škol a střední školy musely přejít na on-line výuku a další způsob výuky byl dlouhodobě nejistý. 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 sbírání dat on-line. 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.

Vztah k moderním technologiím a jejich vlastnictví

Nejprve nás zajímalo, jaký je vztah respondentů k novinkám různého typu. Na škále 1–10 nám respondenti měli sdělit, zda (1) *velmi rádi zkouší všechny novinky* nebo (10) *novinky začnou používat, až je to zcela nezbytné*. Průměrně se respondenti pohybovali na hodnotě 5,5, což naznačuje, že Češi celkově nemají příliš vyhraněný přístup k novinkám. Ani je cíleně nevyhledávají, ani se jim nevyhýbají. V tomto ohledu se však výrazně odlišují jednotlivé věkové skupiny. Nejmladší respondenti holdují novinkám nejvíce ze všech, kdežto s přibývajícím věkem se nadšení z objevování nových věcí vytrácí, jak ukazuje následující graf 1.

Graf 1. Vztah k novinkám podle věku (průměr; 1 = velmi rád zkouším všechny novinky, 10 = novinky začnu používat, až je to zcela nezbytné).



Naším cílem bylo také zjistit, jak jsou na tom Češi s vlastnictvím vybraných zařízení a využíváním moderních technologií, u kterých se dnes mohou běžně setkat s biometrií. Do této kategorie počítáme i vlastnictví cestovního pasu, který obsahuje biometrické údaje. Z tabulky 1 je patrné, že nejčastěji vlastněnou technologií byl „chytrý“ telefon (81 %) následovaný notebookem (74 %), zatímco stolní počítač a tablet dnes využívá jen 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 1. 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

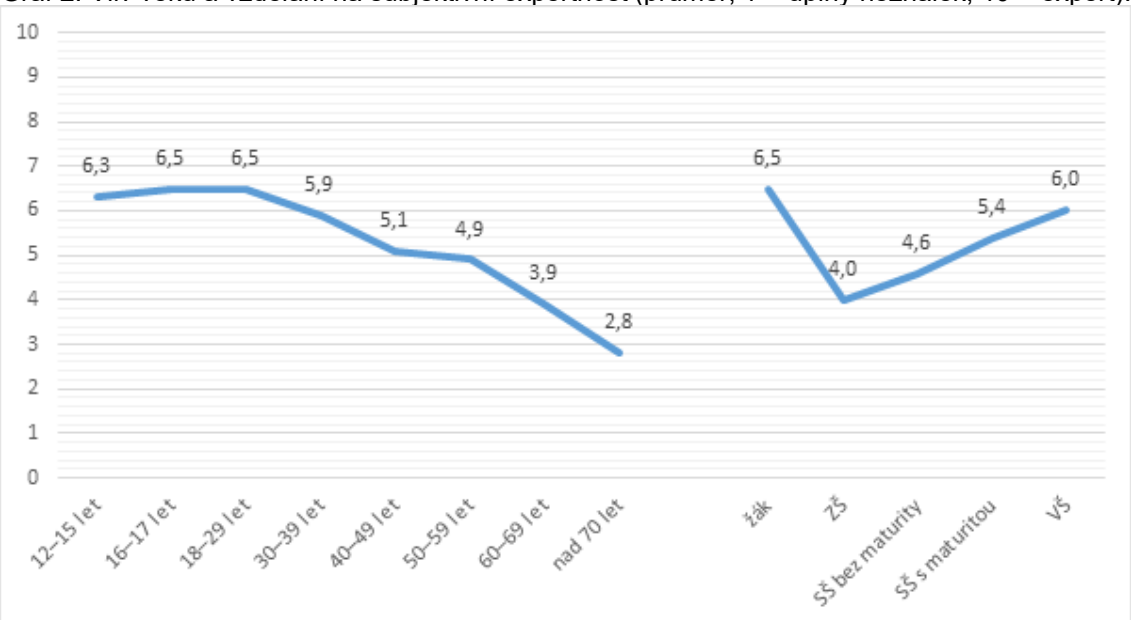
Pozn. Dopočet do 100 % tvoří v každém řádku lidé, kteří danou technologii nevlastní.

Vlastnictví technologií je nejvíce 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 starších 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 %, 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.

Expertnost v užívání technologií

Kromě toho, jestli lidé doma mají vybrané technologie, nás také zajímalo, zda se při jejich používání cítí jako experti. To jsme zjišťovali nejprve 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. Opět zde však byl patrný rozdíl mezi věkovými a vzdělanostními kategoriemi (graf 2). 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 klesání (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. 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.

Graf 2. Vliv věku a vzdělání na subjektivní expertnost (průměr; 1 = úplný neználek, 10 = expert).



Užívání internetu a typ připojení

V mapování užívání a znalostí technologií v Česku nám také slouží poznatky o užívání internetu. 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 používají jen několikrát do měsíce nebo výjimečně (4 % a 3 %). Lidí, kteří v Česku vůbec nemají připojení k internetu, je 10 %. Vše shrnuje tabulka 2.

Tabulka 2. Frekvence užívání internetu.

Internet užívám…	**%**
každý nebo téměř každý den	72
alespoň několikrát týdně	12
spíše jen několikrát do měsíce	4
jen zcela výjimečně	3
nemám vůbec žádné připojení k internetu	10
celkem	100

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. 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 už podíl aktivních uživatelů internetu přibližuje polovině a můžeme rozhodně očekávat i další nárůst. Mezi nezletilými je pak podíl aktivních uživatelů v podstatě absolutní.

Nákup zboží a služeb na internetu

Nákup nebo objednávání zboží a služeb na internetu není v Česku pro většinu lidí na denním pořádku. 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 %).

Tabulka 3. Frekvence nakupování či objednávání zboží a služeb na internetu (%).

Na internetu nakupuji nebo objednávám…	%
denně	3
týdně	15
asi jednou měsíčně	33
méně často	36
nikdy	13
celkem	100

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. 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).

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. 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 vzdělání. 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, zda je web, na kterém kartou platí, ověřený, protože 30 % z nich platí běžně kartou na všech webech. Dalo by se říci, že nejvíce obezřetnou 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

Zabezpečení mobilního telefonu

Celých 32 % obyvatel České republiky nemá svůj mobilní telefon vůbec zabezpečený, což je vysoký podíl. Častěji jsou to lidé starší a s nižším vzděláním. Zatímco mezi nezletilými je takových méně než dvě procenta, v nejstarší skupině sedmdesátiletých a starších je jich 72 %. Silný je i vliv vzdělání. Více než polovina (57 %) lidí se základním vzděláním svůj mobilní telefon nezabezpečuje, mezi vyučenými je to 40 %, mezi středoškolsky vzdělanými 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.

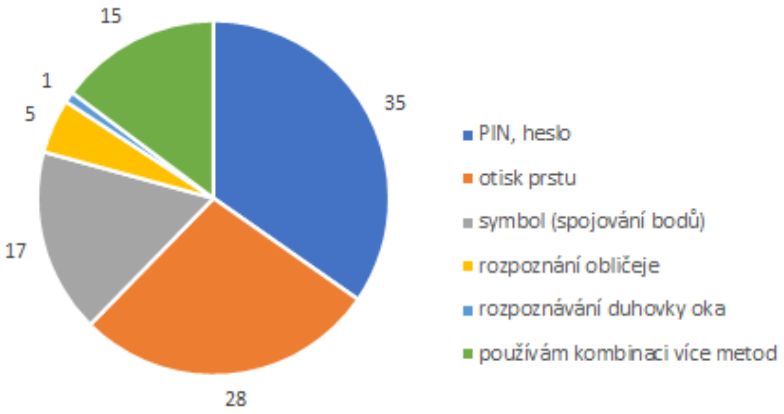
Pokud respondenti svůj mobil zabezpečují, je biometrická autentizace oblíbeným způsobem. Jak se ukazuje, pro téměř třetinu respondentů je otisk prstu nejčastějším způsobem zabezpečení mobilního telefonu. Stále však vede zabezpečení pomocí PIN kódu či hesla, které využívá 35 % Čechů. 17 % využívá symbol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

Mobil už přitom v dnešní době zdaleka neslouží jen k telefonování, ale stává se branou k řadě dalších služeb. Pomocí mobilu přistupujeme k bankovním údajům, ukládáme do něj své zdravotní informace a soukromé fotografie. S rozvojem bankovní identity může mobil posloužit také k prokázání totožnosti vůči státním orgánům. Pokud někdo získá nezabezpečený mobil, otevírá se mu tak celá řada možností.

Zabezpečení na základě znalosti (PIN, heslo, obrazec) má nevýhodu v tom, že si uživatel musí tajnou informaci pamatovat. Lidé proto volí jednoduchá hesla, která pak není problém uhodnout (např. 1234, datum narození). Složitější hesla si zase zaznamenávají a hrozí proto, že někdo ukradne mobil i s heslem.

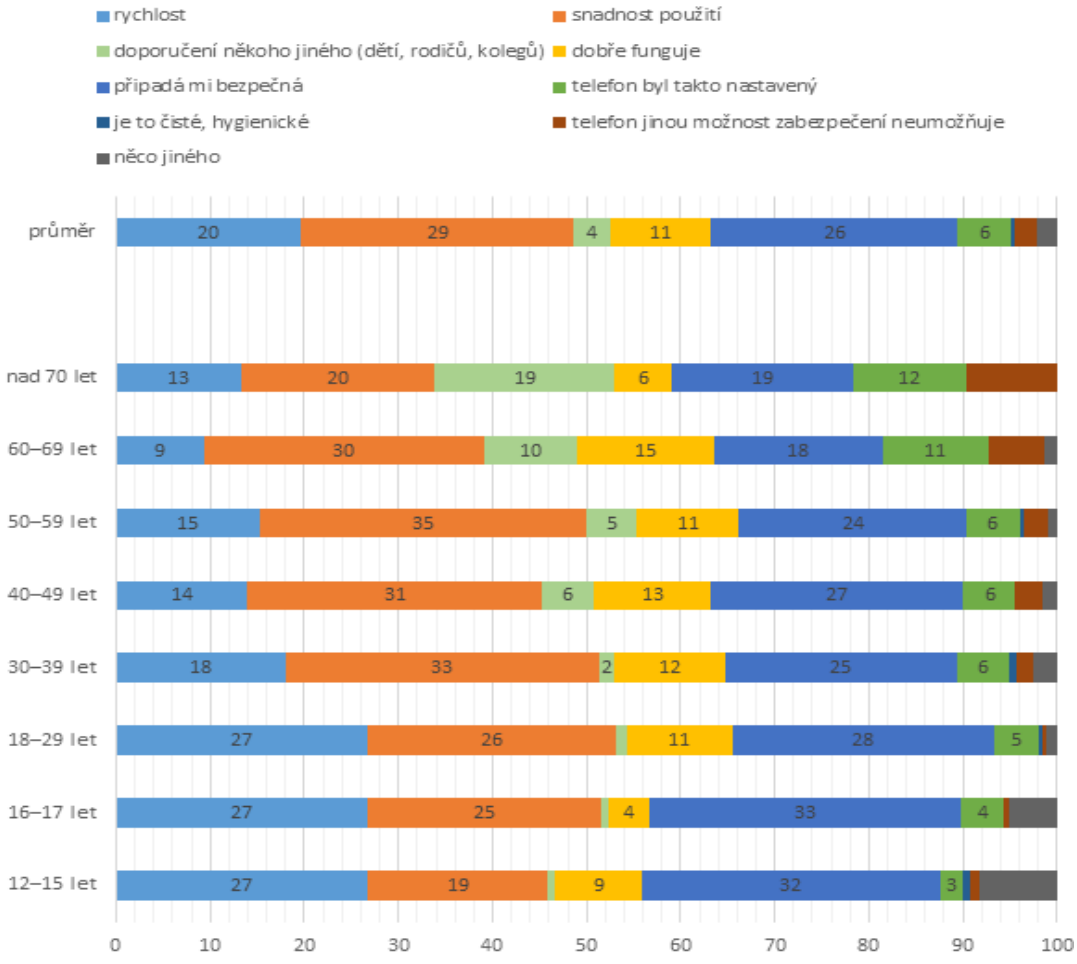
Biometrické zabezpečení založené na fyzických charakteristikách člověka většinu z těchto nedostatků odstraňuje. Uživatel si nemusí nic pamatovat, přitom používá relativně složitou informaci v podobě otisku prstu nebo skenu duhovky. Přitom nehrozí, že by mu někdo jeho otisk prstu ukradl.

Graf 3. K zabezpečení svého mobilního telefonu nejčastěji používám … (v %)



Také jsme se zajímali o to, co ty, kteří si změnili způsob zabezpečení svého mobilního telefonu, vedlo k této změně. Jak ukazuje graf 4, pro mladé lidi do 29 let byla největším faktorem vyšší rychlost a bezpečnost nové metody zabezpečení. Pro starší věkové skupiny to taktéž byla bezpečnost, ale na rozdíl od mladších respondentů a respondentek pro ně hrála velkou roli také snadnost použití. Nejstarší lidé (70 a více let) také dali poměrně často na doporučení někoho jiného (19 %). V obou případech jsou biometrické metody zabezpečení dobře použitelné. Jejich nastavení i rutinní používání je rychlé a snadné.

Graf 4. Nejčastější důvod pro změnu způsobu zabezpečení mobilního telefonu podle věku (%).



Z hlediska využívání biometrických metod tak můžeme konstatovat dva hlavní závěry. S postupnou obměnou starých zařízení a technologií se k biometrickému způsobu zabezpečení dostávají další skupiny obyvatel. Pro ty už není přítomnost biometrického zabezpečení technologickou novinkou, kvůli které by si pořizovali nový přístroj, ale samozřejmou součástí moderního zařízení. Jednou z mnoha technologií, které jejich mobil, tablet, počítač poskytuje. Odlišná situace je s využíváním těchto možností. Zejména starší uživatelé se necítí být experty a novinky využívají hlavně v případě, kdy jim jejich nastavení a následné používání bude připadat snadné.

Znalost pojmu biometrie

Nějakou formu setkání se se slovem biometrie deklaruje 37 % respondentů. 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 základních a středních škol v tomto ohledu tvoří spíše méně obeznámenou skupinu (26 %). Je přitom zajímavé, že tato skupina moderní technologie využívá nejvíce ze všech. Zdá se tedy, že mladá generace přijímá moderní vymoženosti tak, jak jsou jí nabízeny, a nepotřebuje o nich sáhodlouze uvažovat.

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 chybné 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 5: Znalost významu slova „biometrie“ nebo „biometrický“ podle věku a vzdělání (%).

Zkušenost se zneužitím hesel nebo jiných přístupových údajů

Strach ze zneužití technologií není tak častý, jak bychom mohli očekávat, což 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.

Nicméně pokud se podíváme na zkušenost napříč věkovými a vzdělanostními skupinami, jasně zde vyčnívají děti do 18 let. 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 %. Opět poukazujeme na to, že tato věková skupina používá moderní technologie nejintenzivněji ze všech, ale zjevně není dostatečně informovaná o souvisejících rizicích.

Jak již bylo uvedeno, s rostoucím významem mobilů jako přístupového bodu k řadě dalších služeb, a zařízení pro uchování většího a většího množství soukromých a citlivých informací, lze bohužel očekávat, že případů zneužití identity bude přibývat i v dalších skupinách.

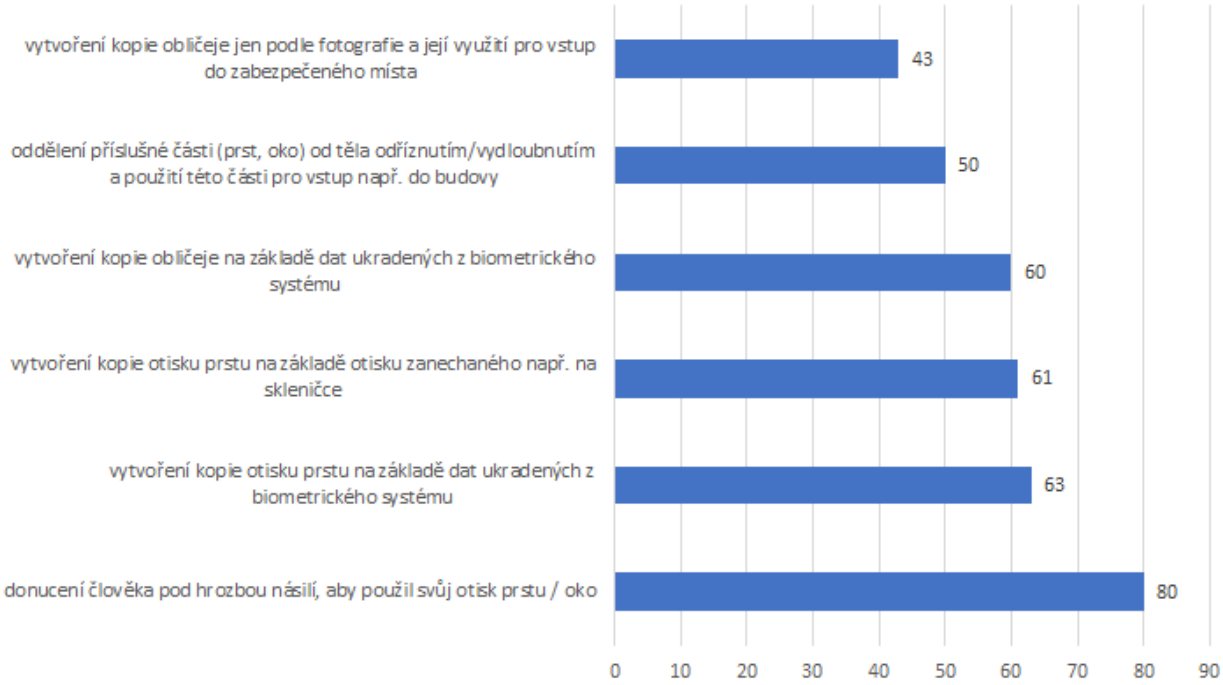
Reálnost hollywoodských scénářů

Už při přípravě výzkumu jsme pojali podezření, že zejména nejmladší generace má informace o biometrickém zabezpečení založené zejména na sledování filmů. V nich se často objevují různé scénáře zneužití biometrických údajů. Zajímalo nás proto, které scénáře Češi považují za reálné. Přehled scénářů a základní výsledky poskytuje graf 6. 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.

Dobře navržený biometrický systém by se přitom většinou z uvedených scénářů neměl nechat oklamat. Neukládá totiž kompletní kopii biometrické informace (např. celý otisk prstu), ale jen její vybrané charakteristiky (např. několik nejdůležitějších bodů či linií uložených v šabloně). Ty jsou navíc někdy matematicky upraveny tak, aby bylo znemožněno zrekonstruování původní informace. Proti umělým kopiím nebo využití prstů mrtvého člověka zase chrání takzvaná detekce prezentačního útoku (živosti). Snímač biometrických údajů při ní například u prstu zjišťuje, zda má prst správné prokrvení a elasticitu kůže či prověřuje multispektrální vlastnosti kůže. Při biometrickém ověřování identity prostřednictvím kamery mobilního telefonu, jaké dnes používají například banky, zase člověk musí podle pokynů systému otáčet hlavou na různé strany, měnit mimiku obličeje a podobně. Zneužití například statické fotografie je tak značně ztíženo, v ideálním případě znemožněno.

Důvěra v reálnost scénářů filmů se liší napříč věkovými a vzdělanostními skupinami. Obecně lze konstatovat, že zejména děti do 18 let mají větší tendenci věřit daným scénářům a že 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.

Graf 6: Podíl respondentů, kteří souhlasí s reálností daného scénáře (v %).



Při zlepšování informovanosti obyvatelstva o biometriích je proto vhodné zaměřit se jednak na vysvětlení, co to vlastně biometrické zabezpečení je, avšak rovněž vyvrátit řadu mýtů, které v tomto směru panují. Mezi nejsilnější patří možnost vytvoření kopie části lidského těla jen na základě informací ukradených z biometrického systému, nebo možnost zneužití biometrických údajů proti vůli jejich nositele či nositelky.

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] 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

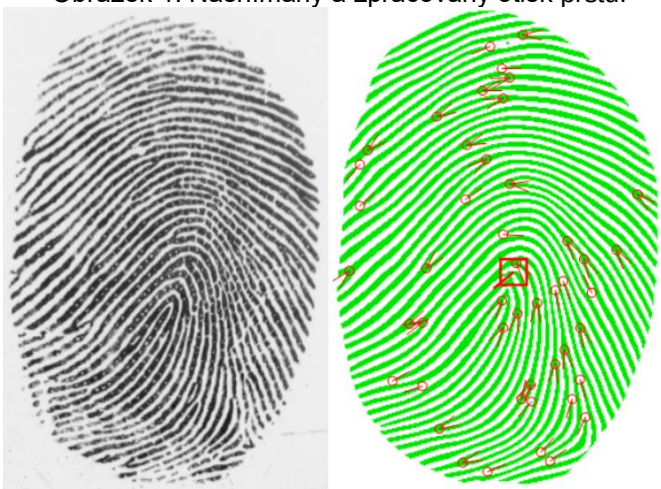
V úvodu bylo řečeno, že pro potvrzení identity je možné využít velkého množství biometrických charakteristik. Nicméně jen zlomek z nich se prakticky používá. Každá charakteristika má trochu jiné vlastnosti. Mezi tyto vlastnosti patří jedinečnost (kolik osob je od sebe možné odlišit),

konstantnost (jak moc se mění v čase), akceptaci (jak moc je přijatelná pro uživatele), bezpečnost (jak obtížně se dá falzifikovat), ale i finanční náklady a mnoho dalších. 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 (viz obrázek 1). 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). Otisky prstů je možné klasifikovat do 3-6 skupin podle zobecněného tvaru vrcholů na daném prstu. Otisk prstu je jedna z biometrických charakteristik uložených na biometrických dokladech (pasu a občanském průkazu).

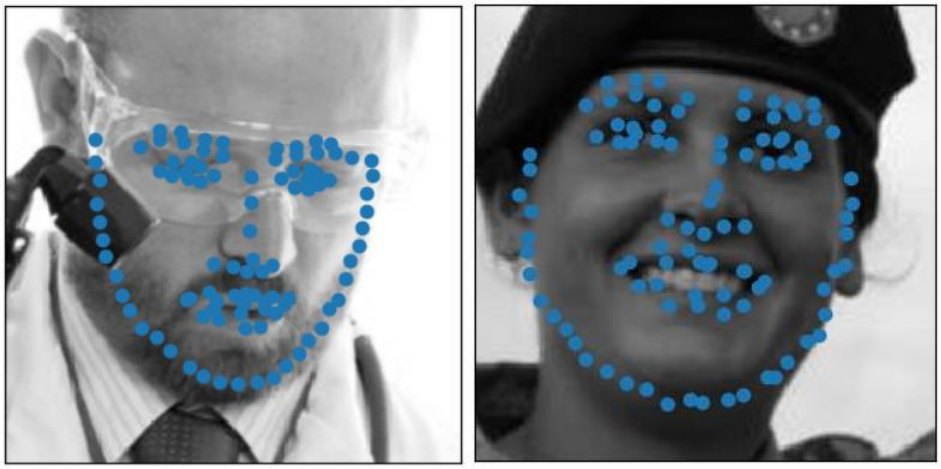
Obrázek 1: Nasnímaný a zpracovaný otisk prstu.



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, pusy, nos, atd.), jak je vidět na obrázku 2. V poslední době se obličeje zpracovávají pomocí hlubokých neuronových sítí, jejichž rozhodování není úplně přesně popsané. 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 kartiček, a tak nepřekvapí, že jsou i součástí biometrických cestovních dokladů.

Obrázek 2: Ukázky obličejů s detekovanými význačnými obličejovými body.



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 3. 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.

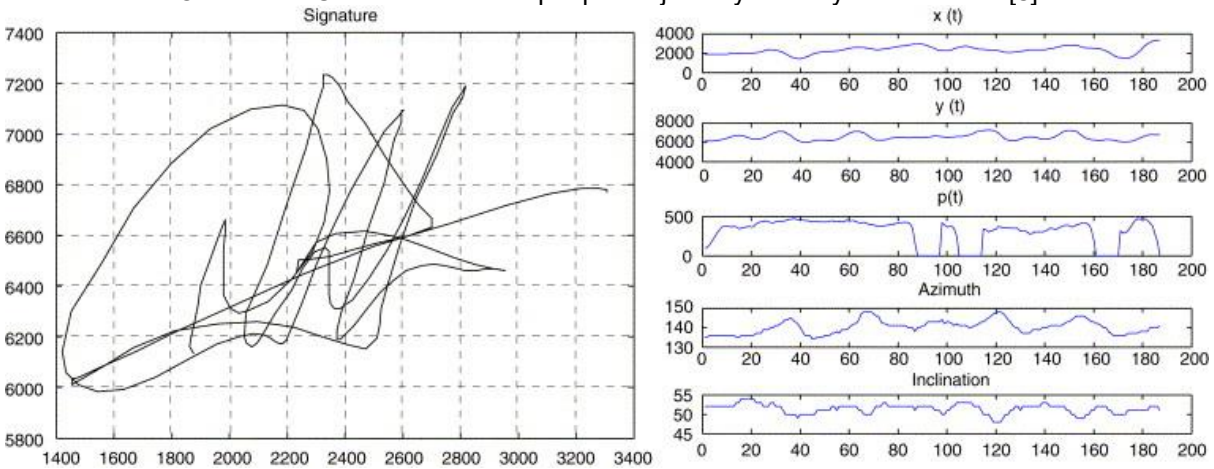
Obrázek 3: Detailní obrázek duhovky.

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 4.

Obrázek 4: Ukázka statického podpisu a jeho dynamických vlastností. [3]



Další biometrické charakteristiky

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. 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). Některé mobilní telefony a jiné asistenční systémy využívají hlasové příkazy, některé z těchto zařízení reagují pouze na hlasové příkazy daného uživatele (provádí tedy verifikaci na základě **hlasu**). Pro zvýšení úrovně bezpečnosti existují i **multimodální biometrické systémy**, tedy biometrické systémy požadující pro přístup několika biometrických charakteristik (např. obličej a duhovka). Při policejním vyšetřování je pak možné se setkat s rozpoznáním podle DNA, chůze a další, které spadají spíše do forenzní oblasti.

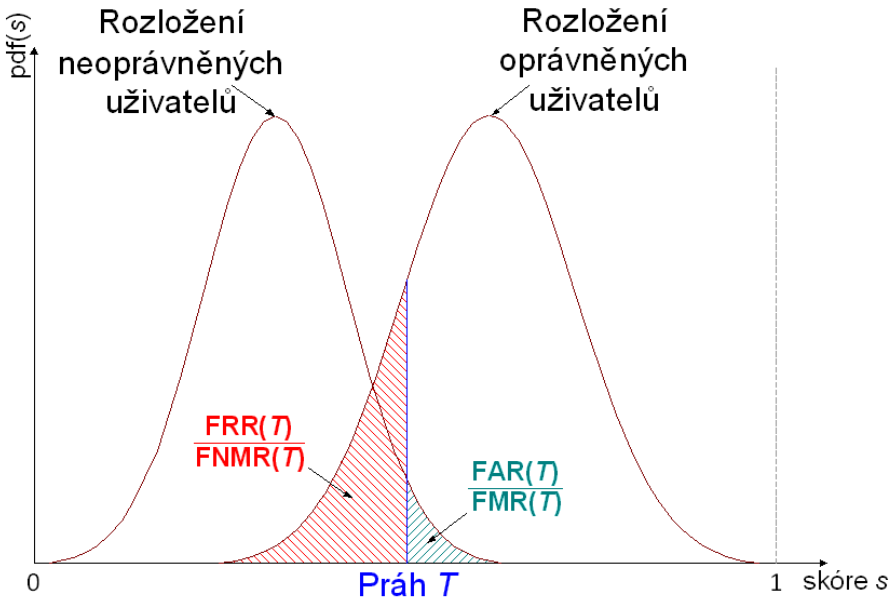
Hodnocení výkonnosti biometrických systémů

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 brožura.

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 7 (vodorovná osa je skóre porovnání, svislá pravděpodobností rozložení daného uživatele). Některým neoprávněným uživatelům se povede přihlásit, a naopak některým oprávněným bude přístup zamítnut.

Graf 7: Rozložení oprávněných a neoprávněných uživatelů s chybovými mírami.

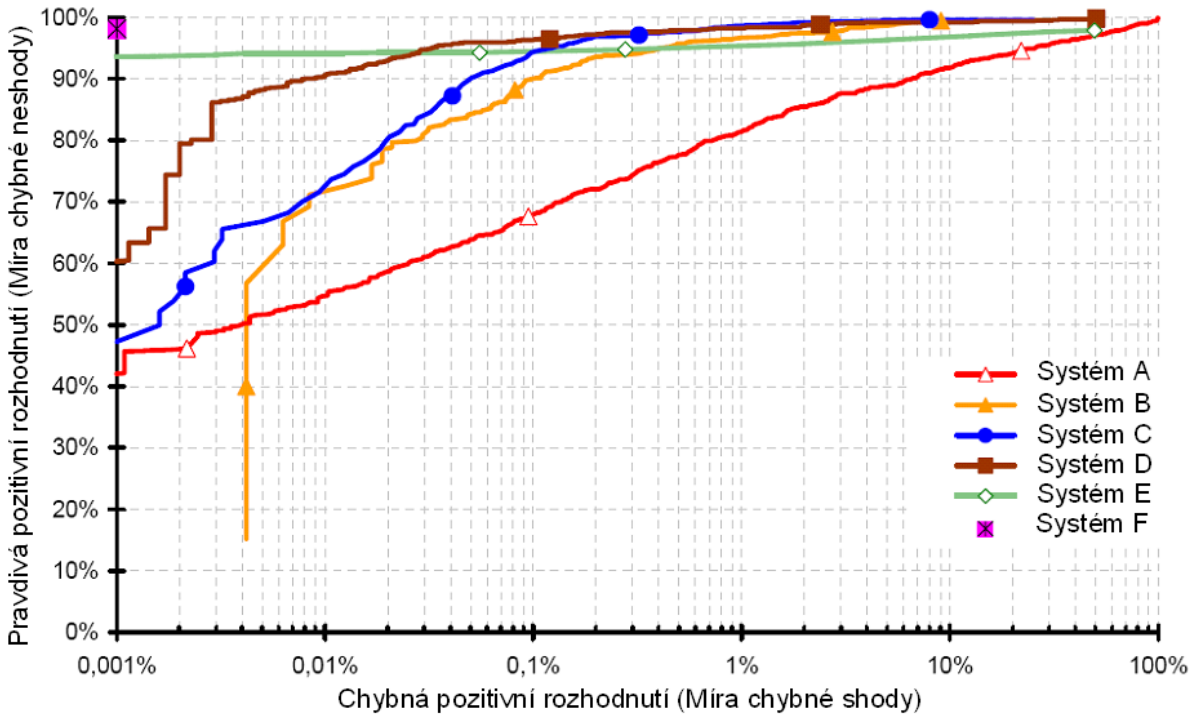


Tak získáváme dvě chyby, které systém může provést. Jsou jimi chybné přijetí (pustím do systému "útočníka") a chybné odmítnutí (nepustím do systému právoplatného uživatele). U systému se tak často uvádí chybová míra **FAR** - *false accept rate* (míra chybného přijetí) nebo **FRR** - *false reject rate* (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 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.

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 8, 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 [4] 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.

Graf 8: Ukázky ROC křivek.



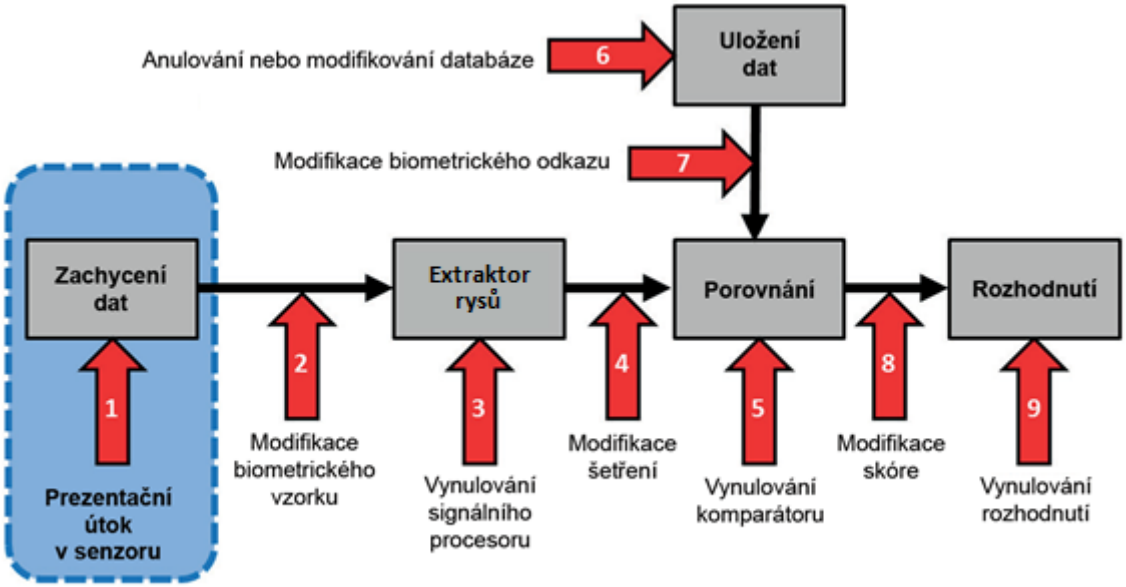
Bezpečnost

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 5):

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 5: 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. **Útok replay** 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. Druhá možnost se běžného obyvatelstva příliš netýká, stejně tak jako destrukční varianty (např. uříznutí prstu), které ani nemusejí fungovat. Smutným faktem zůstává, že biometrické systémy se dají prolomit vytvořením falzifikátu. Jak již bylo zmíněno, tvorba falzifikátů je u některých biometrických charakteristik velmi obtížná, u některých snadnější. 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.

Nemá smysl zacházet do detailů jak tvorby falzifikátů, tak různých metod na **detekci živosti**. 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. 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.

Právní regulace využívání biometrických systémů v České republice

Biometrika umožňuje jedinečnou identifikaci člověka. Údaje zjištěné měřením různých částí či projevů našeho těla přímo vypovídají o tom, kdo jsme (např. tvar obličeje a vzdálenosti mezi jednotlivými body na něm, barva a tón hlasu či způsob podpisu). Biometrické charakteristiky je zároveň nemožné jednoduše změnit. Jsou proto velmi spolehlivé při ověřování totožnosti. Při cestování do zahraničí se již běžně používají biometrické pasy, které obsahují informace pro automatizované rozpoznávání tváře. Kromě veřejných orgánů používají biometriku i soukromé firmy, a to například pro kontrolu vstupu na pracoviště nebo do sportovních center.

V případě, že dojde k získání biometrických údajů neoprávněnou osobou, mohou být tyto údaje zneužity různými způsoby. Typicky může jít o krádež identity, kdy jiná osoba použije elektronický záznam obsahující biometrické informace pro ověření identity pro umožnění přístupu, provedení platby atd. Biometrické údaje mohou být používány rovněž pro protiprávní identifikaci osob pohybujících se ve veřejném prostoru nebo pro získávání informací o osobách z různých databází, a to s vysokou mírou spolehlivosti. Obecně vzato může zneužití biometrických údajů vést například k fyzické újmě, újmě na pověsti, finanční ztrátě, či diskriminaci.

Vzhledem k tomu, že biometrické údaje nelze zpravidla jednoduše změnit (výjimkou je např. plastická operace) a jejich využívání proto vede k vyšší zranitelnosti člověka, stanoví právo kromě obecných podmínek pro ochranu soukromí a osobnosti i zvláštní podmínky a omezení při zpracovávání biometrických údajů. Tyto druhy právní ochrany se přitom vzájemně překrývají a ovlivňují. Ustanovení o ochraně osobnosti obecně chrání život člověka, jeho svobodu, důstojnost, zdraví, právo na příznivé životní prostředí, čest, soukromí a projevy osobní povahy. Tato pravidla se mohou doplňkově uplatnit například v situacích, kdy by v konkrétním případě selhala nebo byla zneužita ustanovení o zpracování osobních údajů a šlo by například o zachycení podoby člověka.

Obecné podmínky pro ochranu soukromí a osobnosti stanoví Listina základních práv a svobod České republiky (čl. 10) a různé mezinárodní úmluvy a dokumenty (např. Všeobecná deklarace lidských práv, Úmluva o ochraně lidských práv a základních svobod, Úmluva Rady Evropy č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních dat, Listina základních práv Evropské unie, Smlouva o fungování Evropské unie).

Obecná pravidla pro ochranu osobnosti obsahuje občanský zákoník, a to v § 81–117. Obecná a zvláštní pravidla pro zpracování osobních údajů a biometrických údajů pak obsahuje zejména přímo použitelné evropské Obecné nařízení o ochraně osobních údajů (zkráceně tzv. GDPR z angl. *General Data Protection Regulation*)[1] a český zákon č. 110/2019 Sb., o zpracování osobních údajů. Tento zákon mimo jiné implementuje do českého práva tzv. policejní směrnici[2], která v čl. 10 stanoví podmínky pro zpracování biometrických údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů.

[1] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

[2] Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či

Právní řád obsahuje rovněž zvláštní předpisy regulující zpracování biometrických údajů pro specifické účely. Konkrétně se jedná například o veřejné a cestovní doklady[3], pobyt cizinců na území ČR[4], práci Policie ČR[5], či využívání biometrie pro účely platebního styku[6].

Právní definice biometrických údajů

Biometrické údaje jsou zvláštní kategorií osobních údajů. Osobním údajem je v podstatě jakákoliv informace o živém člověku, jejíž identitu zná správce osobních údajů, tedy osoba, která tuto informaci zpracovává. Osobním údajem je však i informace o člověku, jejíž identitu správce osobních údajů může zjistit, a to například proto, že zná její jméno, rodné číslo, nebo jiné údaje, na základě nichž může tohoto člověka odlišit od ostatních osob.

V principu nezáleží na tom, zda správce osobních údajů zná jméno člověka, jehož osobní údaje zpracovává. Důležité je, zda jej správce může vyčlenit ze skupiny osob a jednat s ním jinak než s ostatními, například jej hodnotit a na základě tohoto hodnocení mu poskytovat jiné služby.

Biometrické údaje jsou takové osobní údaje, které dokáží člověka identifikovat jedinečným způsobem, tedy odlišit ho od všech ostatních osob, a to na základě jeho fyziologických znaků (podoba tváře, otisk prstu) nebo znaků chování (specifický způsob psaní na klávesnici). Aby mohly být uvedené znaky považovány za biometrický údaj, musejí být předem zvláštním způsobem technicky zpracovány.

Technické zpracování uvedených znaků člověka má typicky dvě fáze: měření a vytvoření biometrické šablony. V první fázi se pomocí určitého zařízení změří příslušný rys a elektronicky se odebere biometrický vzorek. Může jím být například fotografie otisku prstu, fotografie obličeje, záznam hlasu nebo záznam toho, jakým tempem člověk píše na klávesnici. Tento biometrický vzorek je následně zpracován pomocí různých algoritmů, které ze vzorku vyberou určité charakteristiky a z nich vytvoří biometrickou šablonu. Tato šablona se pak používá při ověřování identity. Jedním z nejběžnějších používání biometrických údajů je odemykání mobilních telefonů pomocí otisku prstu. Ten je při prvním použití telefonu získán pomocí senzoru a následně zpracován na biometrickou šablonu, která se pak používá pro porovnání.

Jenom takto zpracovaný otisk prstu je z hlediska práva považován za biometrický údaj. Samotná fotografie otisku prstu, která nebyla technicky zpracována na biometrickou šablonu, nebude za biometrický údaj považována.

---

stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV

[3] Zákon č. 197/2009 Sb., o certifikaci veřejných dokladů s biometrickými údaji a o změně některých zákonů, ve znění pozdějších předpisů; zákon č. 329/1999 Sb., o cestovních dokladech, ve znění pozdějších předpisů

[4] Zákon č. 325/1999 Sb., o azylu, ve znění pozdějších předpisů (viz zejm. § 52 a násl. a § 59 a násl.); zákon č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, ve znění pozdějších předpisů (viz zejm. § 5, § 44 a násl. či § 74); zákon č. 221/2003 Sb., o dočasné ochraně cizinců, ve znění pozdějších předpisů (viz zejm. § 35 a násl. a § 49); vyhláška č. 88/2011 Sb., o technických podmínkách a postupu při pořizování biometrických údajů a podpisu cizince pro účely vydání průkazu o povolení k pobytu

[5] Zákon č. 273/2008 Sb. o Policii České republiky, ve znění pozdějších předpisů (viz zejm. § 65); zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů (viz § 334b, § 360a); zákon č. 269/1994 Sb., o Rejstříku trestů, ve znění pozdějších předpisů (§ 10 odst. 5).

[6] Zákon č. 370/2017 Sb., o platebním styku, ve znění pozdějších předpisů (viz § 223 odst. 3 písm. c)).

Povinnosti osob zpracovávajících biometrické údaje

Biometrické údaje zpracovávají pro různé účely soukromé i veřejné subjekty. Primární odpovědnost za zpracování biometrických údajů má správce. To je osoba, která rozhoduje o účelu a způsobu zpracování. Jednoduše řečeno, správce říká, proč údaje zpracovává (účel) a jak je zpracovává (způsob). Právě jeho rozhodnutí má vliv na to, jaké údaje bude zpracovávat a jakým rizikům tak může fyzické osoby, které mu své osobní údaje poskytnou, případně vystavit. Tyto fyzické osoby označuje GDPR jako tzv. subjekty údajů.

Právě proto, že správce rozhoduje o míře rizika, má velké množství povinností, které musí splnit. Pokud tak neučiní, může dostat pokutu od Úřadu na ochranu osobních údajů, který je v těchto věcech dozorovým úřadem. Subjekty údajů se navíc mohou na správci dožadovat případných odškodnění, pokud jim porušením některé ze svých povinností způsobí škodu.

Základní povinností správce je dodržovat při zpracování osobních údajů tzv. Zásady zpracování, které stanoví čl. 5 odst. 1 GDPR.

První zásadou je, že správce musí údaje zpracovávat v souladu se zákonem, korektně a transparentně. Mimo jiné to znamená, že správce musí mít legitimní důvod pro zpracování údajů. Používání biometrických údajů pro účely jedinečné identifikace člověka GDPR obecně zakazuje. Biometrické údaje totiž zvyšují riziko pro samotný subjekt údajů. GDPR zároveň ale stanoví výjimky, kdy biometrické údaje zpracovávat lze. Je tomu tak zejména v následujících případech: a) subjekt údajů udělil se zpracováním výslovný souhlas, b) zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany, c) zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas. Kromě GDPR ale existují i jiné předpisy, které stanoví povinnost zpracovávat biometrické údaje, a to zejména veřejnými orgány. Zpracování těchto údajů je proto legitimní, protože jde o plnění právní povinnosti.

Druhou zásadou, je účelové omezení zpracování údajů. To znamená, že ještě před tím, než správce začne osobní údaje zpracovávat, musí jasně říci, proč to dělá a následně údaje nezpracovávat pro jiné účely. Když tedy například zpracovává biometrické údaje pouze za účelem umožnění vstupu do určitých prostor, nesmí tyto biometrické údaje používat i za účelem monitorování docházky a toho, kdo v daných prostorách strávil kolik času, nebo s kým společně odcházel. Pokud by chtěl zpracovávat údaje i pro tyto účely, musel by to dopředu sdělit a vyžádat si například souhlas nebo mít pro zpracování jiný právní titul.

Třetí zásadou je minimalizace údajů. Správce by neměl zpracovávat víc údajů, než je nezbytně nutné pro dosažení účelu, který si stanovil.

Čtvrtou zásadou je zásada přesnosti údajů, která spočívá v tom, že správce musí údaje průběžně aktualizovat a udržovat je přesné, nebo je bezodkladně vymazat či opravit.

Pátou zásadou je zásada omezení uložení údajů. To znamená, že správce by neměl údaje uchovávat déle, než je nezbytně nutné pro účel, pro nějž údaje zpracovává. Po uplynutí této lhůty musí údaje buď vymazat, nebo anonymizovat.

Poslední zásadou, je zásada integrity a důvěrnosti zpracování osobních údajů. Podle této zásady musí správce přijmout taková opatření, která zabrání neoprávněnému či protiprávnímu zpracování údajů a jejich náhodné ztrátě, zničení nebo poškození.

Dalšími povinnostmi správce jsou ty povinnosti, které má vůči subjektům údajů při zajišťování jejich práv. Ta jsou podrobně popsána v následující kapitole.

Správce má pak ještě řadu zvláštních povinností, z nichž budeme jmenovat jenom některé. Správce by měl již od začátku ke zpracování údajů přistupovat s tím, že má na mysli ochranu zájmů subjektů údajů a dopředu promyslí různá rizika a scénáře, které by mohly nastat, a přijde s řešeními, která budou rizikům předcházet. Zároveň nesmí správce subjektům nutit souhlas se zpracováním nebo jej předpokládat. Správce si také musí vést podrobnou dokumentaci o tom, jak údaje zpracovává. Tyto záznamy pak slouží i k prokázání toho, že jednal v souladu s právem, v případech, kdy jeho jednání prověřuje Úřad na ochranu osobních údajů. Pokud správce zpracovává biometrické údaje ve velkém rozsahu nebo takovým způsobem, že to může přinést pro subjekty údajů velké riziko, musí provést tzv. posouzení vlivu své činnosti na zpracování osobních údajů. Toto posouzení má předepsané náležitosti a v jeho rámci se provádí podrobné posouzení případných rizik a stanoví se plány pro řešení těchto rizik a odpovídající bezpečnostní opatření. Správce má vždy povinnost přijmout vhodná opatření k zajištění bezpečnosti osobních údajů. V určitých případech také musí jmenovat tzv. pověřence pro ochranu osobních údajů. Jedná se o specialistu, který má na starosti ochranu osobních údajů, pracuje relativně nezávisle, spolupracuje i s Úřadem na ochranu osobních údajů a je kontaktním bodem pro subjekty údajů. V případě porušení zabezpečení osobních údajů má správce rovněž povinnost ohlásit tento incident Úřadu na ochranu osobních údajů.

Správce může zpracování osobních údajů delegovat i na jiný subjekt, například na jinou firmu (tzv. zpracovatel). V tomto případě má ale povinnost vybrat firmu s dobrou reputací a kvalitním zázemím, které zaručí, že budou osobní údaje zpracovávány v souladu se zákonem. Správce musí se zpracovatelem uzavřít písemnou smlouvu, v níž budou specifikovány záruky ze strany zpracovatele.

Práva osob, jejichž biometrické údaje jsou zpracovávány

Obecné nařízení o ochraně osobních údajů (GDPR) zaručuje osobám, jejichž biometrické údaje jsou zpracovávány, řadu práv. Ta slouží zejména k tomu, aby mohl jednotlivec uplatňovat svou vůli ohledně toho, komu data zpřístupní, a také určitou kontrolu nad tím, jak jsou údaje zpracovávány.

Předpokladem výkonu vlastních práv je dostatečná informovanost osoby. Proto GDPR osobám zaručuje jednak právo na transparentní jednání správce (čl. 12 GDPR) a dále právo na informace (čl. 13 a 14 GDPR). Podle těchto ustanovení musí správce subjektům údajů poskytovat informace v takové formě, aby jim rozuměli. Správce proto musí zajistit, aby měl subjekt údajů snadný přístup ke všem informacím, které mu podle práva náleží a dále aby tyto informace byly napsány jasným a jednoduchým jazykem. To má zamezit praxi, kdy správci používali zbytečně složité právní formulace, kterým mohl porozumět zase jenom právník. V rámci práva na informace jsou pak subjektům údajů garantovány určité informace. Správce údajů by měl subjektům sdělit tyto informace:

a) jaká je totožnost a kontaktní údaje správce a jeho případného zástupce
b) případně jaké jsou kontaktní údaje případného pověřence pro ochranu osobních údajů
c) jaké jsou účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování
d) co jsou oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na právním titulu oprávněného zájmu

e) kdo jsou případní příjemci nebo kategorie příjemců osobních údajů
f) případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Komise o odpovídající ochraně údajů v dané zemi
g) jaká je doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby
h) to, že mají subjekty údajů právo 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 právo na přenositelnost údajů
i) to, že mají subjekty údajů právo odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním
j) to, že mají subjekty údajů právo podat stížnost u dozorového úřadu
k) 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
l) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

Subjekt údajů má dále právo na přístup k osobním údajům (čl. 15 GDPR). Správce by měl na žádost poskytnout subjektu údajů kopii jím zpracovávaných osobních údajů. Zpravidla tak učiní elektronicky.

Dalším právem je právo na opravu (čl. 16). Podle tohoto ustanovení má subjekt údajů 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.

Dále má subjekt údajů i právo na výmaz (tzv. právo být zapomenut, čl. 17 GDPR), na základě něhož může správce požádat, aby vymazal jeho osobní údaje – např. v případech kdy odvolá svůj souhlas se zpracováním nebo když už jeho údaje nejsou potřeba pro účel zpracování, nebo byly údaje zpracovány protiprávně.

Subjekt údajů má rovněž právo na omezení zpracování (čl. 18 GDPR), kdy správce musí omezit zpracování v některých případech – například když subjekt údajů namítá nepřesnost údajů.

V rámci práva na přenositelnost údajů (čl. 20 GDPR) musí správce subjektu údajů poskytnout jeho osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu, pokud se zpracování provádí automatizovaně nebo na základě souhlasu subjektu údajů nebo na základě plnění smlouvy. Důvodem je to, aby subjekty údajů mohly svá data snadno nahrát k jinému poskytovateli stejných služeb a změnit tak poskytovatele.

Dalším právem je právo vznést námitku proti zpracování osobních údajů (čl. 21 GDPR). Správce pak nesmí ve zpracování osobních údajů pokračovat, pokud neprokáže závažné oprávněné důvody pro zpracování osobních údajů subjektu.

A nakonec má subjekt údajů i právo nebýt předmětem automatizovaného rozhodování a profilování (čl. 22 GDPR), pokud by takové rozhodnutí výrazně ovlivnilo jeho zájmy nebo práva. Jde například o případ, kdy bankovní systém na základě analýzy platebního chování rozhodne o tom, že subjekt údajů nemá nárok na půjčku nebo na hypotéku. S takovým rozhodnutím by musel subjekt údajů výslovně souhlasit.

Svých práv se může člověk domáhat buď přímo u správce osobních údajů, u soudu nebo prostřednictvím Úřadu na ochranu osobních údajů.

Kompetence Úřadu na ochranu osobních údajů

Úřad na ochranu osobních údajů je nezávislým dozorovým orgánem v oblasti zpracování osobních údajů. Má v podstatě tři druhy pravomocí – vyšetřovací pravomoc, nápravnou pravomoc a povolávací a poradní pravomoc.

V rámci svých vyšetřovacích pravomocí může úřad zejména vyžadovat poskytnutí všech informací od správců a zpracovatelů, které potřebuje k výkonu svých úkolů, provádět vyšetřování formou auditů, nebo získat přístup do všech prostor, v nichž správce a zpracovatel působí, včetně přístupu k veškerému zařízení a prostředkům určeným ke zpracování údajů.

V rámci svých nápravných pravomocí může úřad například upozorňovat, že zamýšlené operace pravděpodobně porušují GDPR, udělovat napomenutí a správní pokuty, nařizovat určité činnosti správcům a zpracovatelům nebo ukládat omezení či zákaz zpracování.

V rámci povolovacích a poradních pravomocí pak úřad poskytuje poradenství správcům a zpracovatelům, vydává stanoviska a kodexy, nebo povoluje určité druhy zpracování údajů.

V rámci své činnosti zpracovává úřad zprávy o činnosti, které zveřejňuje. Na jeho webových stránkách www.uoou.cz je k dispozici velké množství veřejně přístupných materiálů.

Specifika využívání biometriky ve zvláštních případech

S biometrikou se setkáváme téměř každý den. Naše biometrické údaje mohou zpracovávat různé subjekty a činí tak zejména na základě našeho výslovného souhlasu. Je tomu tak zejména u mobilních aplikací a zařízení, u kterých typicky souhlasíme s využíváním biometriky v rámci zásad na ochranu osobních údajů, při využívání biometrických údajů pro vstup do budovy u zaměstnavatele nebo do školy, při rozpoznávání obličeje na sociálních sítích či při rozpoznávání hlasu pomocí inteligentních domácích asistentů. U těchto aplikací je důležité mít na paměti, že svůj souhlas s využíváním biometriky můžeme kdykoliv odvolat. Určitá služba nebo přístup by nám měly být poskytnuty i bez využívání biometriky. Pokud by totiž poskytnutí služby bylo podmíněno souhlasem s využíváním biometrických údajů, pak nelze takový souhlas považovat za svobodný, a tudíž platný.

Je třeba si uvědomit, že ale existují i systémy, které naše biometrické údaje zpracovávají bez našeho souhlasu, a to na základě zvláštních zákonů. Typicky jde o využívání biometriky v cestovních pasech, či pro účely předcházení nebo vyšetřování trestných činů.

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] 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.

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