PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29

00720/12/CS

WP 193

Stanovisko č. 3/2012 k vývoji biometrických technologií

Přijaté dne 27. dubna 2012

Shrnutí

Biometrické systémy jsou úzce spojeny s konkrétní osobou, jelikož mohou využívat určitou jedinečnou vlastnost jednotlivce k identifikaci a/nebo autentizaci. Zatímco biometrické údaje určité osoby lze vymazat nebo změnit, v případě zdroje, z něhož byly pořízeny, tomu tak obvykle není.

Biometrické údaje jsou úspěšně a účinně používány ve vědeckém výzkumu, jsou hlavním prvkem forenzních věd a cenným prvkem systémů kontroly přístupu. Pomáhají zvýšit úroveň bezpečnosti a zajišťují, aby byly postupy identifikace a autentizace snadné, rychlé a pohodlné. V minulosti bylo používání této technologie nákladné a v důsledku tohoto ekonomického omezení byl dopad na právo fyzických osob na ochranu údajů omezený. V posledních letech se toto výrazně změnilo. Analýza DNA je nyní rychlejší a cenově dostupná téměř pro každého. Technologický pokrok zlevnil datová úložiště a výkon počítačů; to umožnilo internetová fotoalba a sociální sítě s miliardami fotografií. Levnější jsou i čtečky otisků prstů a kamerové monitorovací systémy. Rozvoj těchto technologií přispěl k pohodlnějšímu provádění mnohých operací, k vyřešení mnoha trestných činů a větší spolehlivosti systémů kontroly přístupu, přinesl však s sebou i nové hrozby pro základní práva. Genetická diskriminace se stala reálným problémem. Krádež identity již není pouze teoretickou hrozbou.

Zatímco ostatní nové technologie, které jsou určeny široké veřejnosti a které nedávno vyvolaly obavy ohledně ochrany údajů, se nutně nezaměřují na vytvoření přímého spojení s určitou osobou (nebo vytvoření tohoto spojení vyžaduje značné úsilí), biometrické údaje jsou svou povahou přímo spojeny s určitou fyzickou osobou. To nepředstavuje vždy pouze klad, nýbrž to má i řadu stinných stránek. Vybavení kamerových monitorovacích systémů a inteligentních telefonů systémy rozpoznávání obličeje na základě databází v sociálních sítích by mohlo například znamenat konec anonymity a nesledovaného pohybu fyzických osob. Čtečky otisků prstů, čtečky struktury žil nebo pouhý úsměv do kamery mohou na druhou stranu nahradit karty, kódy, hesla a podpisy.

Toto stanovisko se zabývá tímto i jiným nejnovějším vývojem s cílem zvýšit informovanost dotčených osob a legislativních orgánů. Tyto technické inovace, které jsou velmi často představovány jako technologie, které pouze zlepšují uživatelské pohodlí při práci s aplikacemi, by mohly vést k postupné ztrátě soukromí, nebudou-li zavedena přiměřená ochranná opatření. V tomto stanovisku jsou proto určena technická a organizační opatření, která mají zmírnit rizika z hlediska ochrany údajů a soukromí a která mohou pomoci zamezit negativním dopadům na soukromí evropských občanů a jejich základní právo na ochranu údajů.

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995,

s ohledem na článek 29 a čl. 30 odst. 1 písm. a) a odst. 3 uvedené směrnice,

s ohledem na svůj jednací řád,

PŘIJALA TOTO STANOVISKO

1. Oblast působnosti stanoviska

Ve svém pracovním dokumentu o biometrických údajích z roku 2003 (WP 80) přezkoumala pracovní skupina zřízená podle článku 29 (dále jen „pracovní skupina“) otázky ochrany údajů, které jsou spojeny s využíváním nových technologií, jež jsou schopny elektronicky snímat a zpracovávat biometrické údaje. V letech, které od té doby uplynuly, bylo používání této technologie široce zaváděno ve veřejném i soukromém sektoru a byla vyvinuta řada nových služeb. Biometrické technologie, které kdysi vyžadovaly značné finanční nebo výpočetní zdroje, jsou nyní výrazně levnější a rychlejší. V současnosti je běžné používání čteček otisků prstů. Některé přenosné počítače jsou například vybaveny čtečkou otisků prstů za účelem biometrické kontroly přístupu. Pokroky v analýze DNA znamenají, že výsledky jsou k dispozici do několika málo minut. Některé z nově vyvíjených technologií, jako je rozpoznávání struktury žil nebo rozpoznávání obličeje, se již dostaly do fáze vyspělosti. Jejich použití v různých oblastech každodenního života je na dosah. Biometrické technologie jsou úzce spojeny s určitými vlastnostmi jednotlivce a některé z nich lze využít k zjištění citlivých údajů. Mnoho z nich mimoto umožňuje automatické sledování osob nebo vytváření jejich profilů, a jejich potenciální dopad na soukromí a právo fyzických osob na ochranu údajů je proto vysoký. Tento dopad se zvyšuje s rostoucím zaváděním těchto technologií. Každý jednotlivec bude pravděpodobně zaregistrován v jednom či více biometrických systémech.

Toto stanovisko má poskytnout revidovaný a aktualizovaný rámec jednotných obecných pokynů a doporučení k uplatňování zásad soukromí a ochrany údajů v biometrických aplikacích. Toto stanovisko je určeno evropským a vnitrostátním legislativním orgánům, odvětví biometrických systémů a uživatelům těchto technologií.

2. Definice

Biometrické technologie nejsou nové a již se jimi zabývala různá stanoviska pracovní skupiny. Cílem tohoto oddílu je shrnout příslušné definice a v případě potřeby je aktualizovat.

Biometrické údaje: Jak již bylo uvedeno ve stanovisku pracovní skupiny č. 4/2007 (WP 136), biometrické údaje lze definovat jako:

> *„biologické vlastnosti, behaviorální rysy, fyziologické rysy, znaky živého organismu nebo opakovatelné úkony, které jsou jedinečné pro daného jednotlivce a současně měřitelné, bez ohledu na to, že technické metody jejich měření používané v praxi zahrnují určitou míru pravděpodobnosti“.*

Biometrické údaje mění nevratně vztah mezi tělem a identitou, jelikož zajišťují, že jsou znaky lidského těla „strojově čitelné“ a mohou být dále použity.

Biometrické údaje lze uchovávat a zpracovávat v různých formách. Někdy jsou biometrické údaje získané od určité osoby uchovávány a zpracovávány v hrubé formě, která umožňuje rozpoznat bez zvláštních znalostí zdroj, z něhož pocházejí, například fotografie obličeje, fotografie otisku prstu nebo hlasový záznam. Jindy jsou zachycené prvotní biometrické údaje zpracovávány tak, že jsou vybrány pouze určité vlastnosti a/nebo znaky, které jsou uloženy jako biometrická šablona.

Zdroj biometrických údajů: Zdroje biometrických údajů se mohou velmi lišit a zahrnují fyzické, fyziologické, behaviorální nebo psychologické rysy jednotlivce. Podle stanoviska č. 4/2007 (WP 136):

> *„zdroje biometrických údajů (např. vzorky lidských tkání) samy biometrickými údaji nejsou, lze je však použít k získávání biometrických údajů (výběrem informací z těchto zdrojů)“.*

Jak je uvedeno v dokumentu WP 80, existují dvě hlavní kategorie biometrických technik:

- Za prvé existují techniky založené na fyzických a **fyziologických** rysech, které měří fyzické a fyziologické znaky určité osoby a zahrnují ověření otisků prstů, analýzu snímku prstů, rozpoznávání duhovky, analýzu sítnice, rozpoznávání obličeje, obraz tvaru ruky, rozpoznávání tvaru ucha, rozbor tělesného pachu, rozpoznávání hlasu, analýzu DNA a rozbor potu atd.
- Za druhé existují techniky založené na **behaviorálních rysech**, které měří chování určité osoby a zahrnují ověření vlastnoručního podpisu, analýzu úhozů na klávesnici, analýzu způsobu držení těla, chůze nebo pohybu, vzorce chování naznačující určité podvědomé myšlení, jako je lhaní atd.

V úvahu je nutno vzít rovněž nově vznikající oblast technik založených na **psychologických** rysech. Tyto techniky zahrnují měření odezvy na konkrétní situace nebo zvláštní testy k porovnání psychologického profilu.

Biometrická šablona: Z hrubé formy biometrických údajů (např. měření obličeje podle snímku) lze získat hlavní rysy a uchovávat je místo samotných prvotních údajů za účelem pozdějšího zpracování. To představuje biometrickou šablonu údajů. Zásadní otázkou je stanovení velikosti (množství informací) šablony. Velikost šablony by na straně jedné měla být dostatečná pro řízení bezpečnosti (a zamezit překrývání různých biometrických údajů nebo náhradním identitám), na druhou stranu by velikost šablony neměla být příliš velká, aby se zamezilo rizikům rekonstrukce biometrických údajů. Vytvoření šablony by mělo být jednosměrným procesem, to znamená, že by nemělo být možné obnovení hrubých biometrických údajů ze šablony.

Biometrické systémy: Podle dokumentu WP 80 jsou biometrické systémy:

> *„aplikace, které používají biometrické technologie umožňující automatickou identifikaci a/nebo autentizaci / ověření totožnosti určité osoby. Aplikace pro autentizaci / ověření totožnosti se často používají pro různé úkoly ve zcela odlišných oblastech, pro různé účely a v rámci odpovědnosti celé řady různých subjektů.“*

V důsledku nejnovějšího technologického rozvoje je nyní možné používat biometrické systémy rovněž ke kategorizaci/segregaci.

Rizika, která představují biometrické systémy, vyplývají ze samotné povahy biometrických údajů použitých při zpracování. Obecnější definicí by proto byl systém, který získává a dále zpracovává biometrické údaje.

Zpracovávání biometrických údajů v biometrickém systému obvykle zahrnuje různé postupy, jako je registrace, uchovávání a porovnávání:

– **Registrace biometrických údajů:** Zahrnuje veškeré postupy prováděné v rámci biometrického systému za účelem získání biometrických údajů ze zdroje biometrických údajů a spojení těchto údajů s určitou fyzickou osobou. Množství a kvalita údajů požadovaných během registrace by měla postačovat k přesné identifikaci, autentizaci, kategorizaci nebo ověření totožnosti této osoby bez zaznamenávání přílišných údajů. Množství údajů získaných ze zdroje biometrických údajů během fáze registrace musí být přiměřené účelu zpracování a úrovni výkonnosti biometrického systému.

Fáze registrace obvykle zahrnuje první kontakt jednotlivce s konkrétním biometrickým systémem. Registrace ve většině případů vyžaduje osobní účast jednotlivce (např. v případě pořízení otisků prstů), a může proto představovat vhodnou příležitost k poskytnutí informací a oznámení o korektním zpracovávání. Jednotlivce však lze zaregistrovat i bez jeho vědomí nebo souhlasu (např. kamerové systémy se zabudovanou funkcí rozpoznávání obličeje). Správnost a bezpečnost procesu registrace má zásadní význam pro výkonnost celého systému. Jednotlivec se může v biometrickém systému zaregistrovat znovu za účelem aktualizace zaznamenaných biometrických údajů.

– **Uchovávání biometrických údajů**: Údaje získané při registraci mohou být za účelem pozdějšího použití uchovávány lokálně v operačním centru, v němž došlo k jejich registraci (např. v čtečce), nebo v přístroji, který má u sebe jednotlivec (např. na inteligentní kartě), nebo mohou být odeslány a uloženy v centrální databázi, která je přístupná jednomu či více biometrickým systémům.

– **Porovnávání biometrických údajů**: Jedná se o postup srovnávání biometrických údajů/šablony (pořízených během registrace) s biometrickými údaji/šablonou, které byly získány z nového vzorku za účelem identifikace, ověření totožnosti / autentizace nebo kategorizace.

Biometrická identifikace: Identifikací jednotlivce pomocí biometrického systému je obvykle proces srovnávání biometrických údajů určité osoby (pořízených v době identifikace) s řadou biometrických šablon uložených v databázi (tj. proces porovnávání jedné šablony s mnoha jinými).

Biometrické ověřování totožnosti / autentizace: Ověřováním totožnosti jednotlivce pomocí biometrického systému je obvykle proces srovnávání biometrických údajů určité osoby (pořízených v době ověřování totožnosti) s jednou biometrickou šablonou uloženou v zařízení (tj. proces srovnávaní jedné šablony s jinou (jednou) šablonou).

Biometrická kategorizace/segregace: Kategorizací/segregací jednotlivce pomocí biometrického systému je obvykle proces zjišťování, zda biometrické údaje určité osoby patří do skupiny s určitou předem stanovenou charakteristikou za účelem provedení určitého úkonu. V tomto případě není důležité identifikovat nebo ověřit totožnost určitého jednotlivce, nýbrž jej automaticky zařadit do určité kategorie. Reklamní displej může například zobrazovat různé reklamy v závislosti na osobě, která jej sleduje, a to podle věku nebo pohlaví.

Multimodální biometrie: Tu lze definovat jako kombinaci různých biometrických technologií k zlepšení přesnosti nebo zvýšení výkonnosti systému (nazývá se rovněž víceúrovňovou biometrií). Biometrické systémy používají v procesu porovnávání dva či více biometrických znaků/podob téhož jednotlivce. Tyto systémy mohou pracovat různými způsoby a shromažďovat různé biometrické údaje pomocí různých snímačů, nebo shromažďovat více jednotek téhož biometrického údaje. Některé studie zařazují do této kategorie rovněž systémy, které fungují tak, že provádějí vícenásobné čtení stejného biometrického údaje, nebo systémy, které k získání prvků z téhož biometrického vzorku používají více algoritmů. K příkladům multimodálních biometrických systémů patří na úrovni EU elektronický cestovní pas a v USA program US-VISIT pro služby biometrické identifikace.

Přesnost: Při používání biometrických systémů je obtížné získat naprosto bezchybné výsledky. To může být způsobeno rozdíly v prostředí při pořizování údajů (osvětlení, teplota atd.) a rozdíly v použitém zařízení (kamery, skenovací zařízení atd.). Nejčastěji používanou tradiční metodou hodnocení výkonnosti je míra chybného přijetí a míra chybného odmítnutí, které lze přizpůsobit používanému systému:

– Míra chybného přijetí (*False Accept Rate* – FAR): Jedná se o pravděpodobnost, že biometrický systém nesprávně identifikuje určitou osobu nebo neodmítne podvodníka. Měří procentní podíl neplatných vstupů, které jsou nesprávně povoleny. Nazývá se rovněž falešně pozitivním výsledkem.

– Míra chybného odmítnutí (*False Reject Rate* – FRR): Jedná se o pravděpodobnost, že systém povede k chybnému odmítnutí. K chybnému odmítnutí dojde tehdy, není-li určitá osoba ztotožněna s existující biometrickou šablonou. Nazývá se rovněž falešně negativním výsledkem.

Při správném nastavení a seřízení systému lze kritické chyby biometrických systémů omezit na minimální úroveň, která je přípustná pro provozní použití, a to snížením rizik nesprávného posouzení. Dokonalý systém bude mít nulové míry chybného přijetí a chybného odmítnutí, častěji jsou však korelovány negativně. Zvýšení míry chybného přijetí často snižuje míru chybného odmítnutí.

Při posuzování toho, zda je přesnost určitého biometrického systému přijatelná, či nikoli je důležité vyhodnotit účel zpracování, míru chybného přijetí i míru chybného odmítnutí a velikost populace. Při posuzování přesnosti biometrického systému lze vzít v úvahu rovněž

schopnost odhalit živý vzorek. Je například možné okopírovat latentní otisky prstů a použít je k vytvoření falešných prstů. Čtečka otisků prstů nesmí být v tomto případě oklamána tak, aby provedla pozitivní identifikaci.

3. Právní analýza

Příslušným právním rámcem je směrnice o ochraně údajů (95/46/ES). Pracovní skupina již v dokumentu WP 80 uvedla, že biometrické údaje jsou ve většině případů osobními údaji. Mohou být proto zpracovávány pouze tehdy, existuje-li právní základ a je-li zpracování přiměřené, podstatné a nepřesahující míru s ohledem na účely, pro které jsou tyto údaje shromažďovány a/nebo dále zpracovávány.

Účel

Předpokladem pro používání biometrických údajů je jednoznačné stanovení účelu, pro které jsou biometrické údaje shromažďovány a zpracovávány, s přihlédnutím k rizikům z hlediska ochrany základních práv a svobod jednotlivců.

Biometrické údaje lze například shromažďovat s cílem zajistit nebo zvýšit bezpečnost systémů zpracování zavedením vhodných opatření na ochranu osobních údajů před neoprávněným přístupem. Pro zavedení vhodných bezpečnostních opatření založených na biometrických znacích osob pověřených zpracováváním v zájmu zajištění úrovně bezpečnosti, která odpovídá rizikům, jež vyvolává zpracování, a povaze osobních údajů, které mají být chráněny, v zásadě neexistují žádné překážky. Je však třeba mít na paměti, že používání biometrických prvků samo o sobě nezajišťuje větší bezpečnost, jelikož mnoho biometrických údajů lze shromažďovat bez vědomí dotyčné osoby. Čím vyšší je plánovaná úroveň bezpečnosti, tím méně budou samotné biometrické údaje schopny dosáhnout tohoto cíle.

Musí být dodržena zásada účelového omezení společně s ostatními zásadami ochrany údajů; při stanovování různých účelů použití je třeba mít na paměti zejména zásady přiměřenosti, nezbytnosti a minimalizace údajů. Je-li to možné, musí mít subjekt údajů na výběr mezi několika účely aplikace s více funkcemi, zejména v případě, že jedna či několik z nich vyžaduje zpracovávání biometrických údajů.

Příklad:
Používání elektronických přístrojů umožňujících zvláštní postupy autentizace na základě biometrických údajů bylo doporučeno v souvislosti s bezpečnostními opatřeními, která mají být přijata v případě:

- zpracovávání osobních údajů shromažďovaných telefonními operátory během odposlouchávání, které povolil soud;
- přístupu k provozním údajům (a údajům o umístění) uchovávaným pro soudní účely poskytovateli veřejně přístupných elektronických komunikačních služeb nebo veřejné komunikační sítě a přístupu do příslušných prostor, kde jsou tyto údaje zpracovávány;
- shromažďování a uchovávání genetických údajů a biologických vzorků.

Fotografie na internetu, v sociálních médiích, při správě fotografií na internetu nebo sdílení aplikací nesmí být dále zpracovávány za účelem získání biometrických šablon nebo jejich registrace v biometrickém systému k automatickému rozpoznávání osob na snímcích (rozpoznávání obličeje) bez zvláštního právního základu (např. souhlasu) pro tento nový účel. Existuje-li právní základ pro tento sekundární účel, musí být zpracovávání rovněž přiměřené, podstatné a nepřesahující míru s ohledem na tento účel. Pokud subjekt údajů souhlasil s tím, aby fotografie, na nichž se objevuje, mohly být pomocí algoritmu rozpoznávání obličeje zpracovány za účelem jeho automatického označení v internetovém fotoalbu, musí se toto zpracování uskutečnit způsobem zajišťujícím ochranu údajů: biometrické údaje, které po označení snímků jménem, pseudonymem či jiným textem stanoveným subjektem údajů již nejsou zapotřebí, musí být vymazány. Vytvoření stálé databáze biometrických údajů není za tímto účelem *a priori* nutné.

Přiměřenost

Používání biometrických údajů vyvolává otázku přiměřenosti každé kategorie zpracovávaných údajů s ohledem na účel zpracování údajů. Jelikož biometrické údaje lze použít pouze v případě, že jsou přiměřené, podstatné a nepřesahující míru, znamená to přísné posouzení nezbytnosti a přiměřenosti zpracovávaných údajů a toho, zda by určeného účelu bylo možno dosáhnout způsobem, který méně narušuje soukromí.

Při analýze přiměřenosti navrhovaného biometrického systému je první úvahou to, zda je systém nezbytný k uspokojení zjištěné potřeby, tj. zda je nutný pro uspokojení této potřeby, a nikoliv to, že je nejpohodlnější nebo nákladově nejefektivnější. Druhým faktorem, který je nutno vzít v úvahu, je skutečnost, zda bude systém při uspokojování této potřeby pravděpodobně účinný, a to s přihlédnutím k zvláštním charakteristikám plánované biometrické technologie, která má být používána[1]. Třetím aspektem, který je nutno uvážit, je skutečnost, zda je výsledná ztráta soukromí úměrná případné předpokládané výhodě. Je-li výhoda relativně malá, například větší pohodlí nebo mírná úspora nákladů, pak není ztráta soukromí přiměřená. Čtvrtým aspektem při posuzování přiměřenosti biometrického systému je skutečnost, zda by požadovaného účelu bylo možno dosáhnout prostředky, které méně narušují soukromí[2].

Příklad:
Ve zdravotním a fitness klubu je nainstalován centrální biometrický systém založený na shromažďování otisků prstů za účelem povolení přístupu do tělocvičny a k souvisejícím službám pouze zákazníkům, kteří uhradili příslušné poplatky.
K provozování tohoto systému bude zapotřebí uchovávání otisků prstů všech zákazníků a pracovníků klubu. Je zřejmé, že toto použití biometrických údajů není přiměřené potřebě kontroly vstupu do klubu a usnadnění správy předplatného. Lze si snadno představit, že by stejně praktická a účinná byla i jiná opatření, například jednoduchý kontrolní seznam nebo používání štítků RFID či magnetické karty, které nevyžadují zpracovávání biometrických údajů.

[1] Biometrické údaje budou používány pro účely ověření totožnosti nebo identifikace: biometrický identifikátor může být považován za technicky vhodný pro jeden účel, nikoli však pro druhý (např. v systémech, které mají být používány pro účely identifikace v oblasti vymáhání práva, by měly být upřednostněny technologie vyznačující se nízkými mírami chybného odmítnutí).

[2] Například inteligentní karty či jiné metody, které pro účely autentizace neshromažďují ani centrálně neuchovávají biometrické údaje.

Pracovní skupina upozorňuje na rizika spojená s používáním biometrických údajů pro účely identifikace ve velkých centrálních databázích vzhledem k případným negativním důsledkům pro dotyčné osoby.

Je nutno vzít v úvahu významný dopad těchto systémů na důstojnost subjektů údajů a důsledky pro základní práva. Na základě Evropské úmluvy o ochraně lidských práv a základních svobod a judikatury Evropského soudu pro lidská práva týkající se článku 8 Úmluvy pracovní skupina zdůrazňuje, že jakékoli narušení práva na ochranu údajů je přípustné pouze pod podmínkou, že je v souladu se zákonem a v demokratické společnosti je nezbytné pro ochranu důležitého veřejného zájmu[3].

Aby bylo zajištěno dodržení těchto podmínek, je nutno stanovit cíl sledovaný systémem a posoudit přiměřenost údajů, které mají být zadávány do systému, ve vztahu k zmíněnému cíli.

Za tímto účelem musí správce zjistit, zda je zpracování a jeho mechanismy, kategorie údajů, které mají být shromažďovány a zpracovávány, a předávání údajů obsažených v databázi nutné a nezbytné. Přijatá bezpečnostní opatření musí být přiměřená a účinná. Správce musí uvážit práva, která budou udělena fyzickým osobám, jichž se osobní údaje týkají, a zajistit, aby aplikace obsahovala náležitý mechanismus k uplatňování těchto práv.

Příklad:
Používání biometrických údajů pro účely identifikace. Systémy analyzující obličej osoby a rovněž systémy, které analyzují DNA osoby, mohou velmi účinně přispět k boji proti trestné činnosti a účinně zjistit totožnost neznámé osoby, která je podezřelá ze spáchání závažného trestného činu. Tyto systémy používané ve velkém měřítku však mohou mít závažné vedlejší účinky. V případě rozpoznávání obličeje, kdy lze biometrické údaje snadno získat bez vědomí subjektu údajů, by rozsáhlé používání ukončilo anonymitu ve veřejných prostorách a umožnilo by trvalé sledování fyzických osob. V případě údajů o DNA je použití této technologie spojeno s rizikem, že mohou být odhaleny citlivé údaje o zdraví dotyčné osoby.

Přesnost

Zpracovávané biometrické údaje musí být přesné a podstatné s ohledem na účely, pro které byly shromažďovány. Údaje musí být přesné při registraci a při zjišťování spojení mezi dotyčnou osobou a biometrickými údaji. Přesnost při registraci je důležitá rovněž pro předcházení zneužití identity.

Biometrické údaje jsou jedinečné a většina z nich vytváří jedinečnou šablonu nebo snímek. V případě širokého používání, zejména u značné části obyvatelstva, mohou být biometrické údaje považovány za identifikátor obecného významu ve smyslu směrnice 95/46/ES. Pak bude použitelné ustanovení čl. 8 odst. 7 směrnice 95/46/ES a členské státy budou muset určit podmínky jejich zpracování.

[3] Viz rozsudek Soudního dvora ze dne 20. května 2003 ve spojených věcech C-465/00, C-138/01 a C-139/01 (Rechnungshof v. Österreichischer Rundfunk a další), rozsudek Evropského soudu pro lidská práva ze dne 4. prosince 2008, žaloby č. 30562/04 a 30566/04 (S. a Marper v. Spojené království) a rozsudek ze dne 19. července 2011, žaloby č. 30089/04, 14449/06, 24968/07, 13870/08, 36363/08, 23499/09, 43852/09 a 64027/09 (Goggins a další v. Spojené království).

Minimalizace údajů

V této souvislosti se může objevit zvláštní problém, jelikož biometrické údaje často obsahují více informací, než je pro funkce porovnávání zapotřebí. Zásadu minimalizace údajů musí prosazovat správce údajů. To za prvé znamená, že by měly být zpracovávány, předávány nebo uchovávány pouze potřebné údaje, a nikoli všechny dostupné informace. Správce údajů by měl za druhé zajistit, aby standardní konfigurace podporovala ochranu údajů, aniž by ji bylo nutno vyžadovat.

Doba uchovávání údajů

Správce by měl stanovit dobu uchovávání biometrických údajů, která by neměla být delší, než je nezbytné pro účely, pro které byly údaje shromažďovány nebo dále zpracovávány. Správce musí zajistit, aby po uplynutí odůvodněné lhůty byly údaje nebo profily odvozené z těchto údajů trvale vymazány.

Musí být jasný rozdíl mezi obecnými osobními údaji, jež mohou být zapotřebí delší dobu, a biometrickými údaji, které se již nepoužívají, například v případě, že subjekt údajů již nemá přístup do určitých prostor.

Příklad:
Zaměstnavatel používá biometrický systém ke kontrole vstupu do vyhrazeného prostoru. Úloha zaměstnance již nevyžaduje přístup do vyhrazeného prostoru (např. změna odpovědnosti nebo pracovního úkolu). V tomto případě musí být jeho biometrické údaje vymazány, jelikož již neplatí účel, pro nějž byly shromážděny.

3.1. Oprávněný důvod

Zpracovávání biometrických údajů musí být založeno na jednom z oprávněných důvodů, které jsou stanoveny v článku 7 směrnice 95/46/ES.

3.1.1. Souhlas, čl. 7 písm. a)

Prvním takovým oprávněným důvodem uvedeným v čl. 7 písm. a) je případ, kdy subjekt údajů udělil souhlas se zpracováním. Podle čl. 2 písm. h) směrnice o zpracování údajů musí být souhlas svobodný, výslovný a vědomý projev vůle subjektu údajů. Musí být jasné, že tento souhlas nelze získat svobodně prostřednictvím závazného přijetí všeobecných podmínek nebo možností volby. Souhlas musí být mimoto odvolatelný. V tomto ohledu pracovní skupina ve svém stanovisku k definici souhlasu zdůrazňuje různé důležité aspekty tohoto pojmu: platnost souhlasu; právo fyzických osob na zpětvzetí souhlasu; souhlas udělený před tím, než zpracování začne; požadavky týkající se kvality a přístupnosti informací[4].

V mnoha případech, kdy jsou biometrické údaje zpracovávány bez platné alternativy, jako je heslo nebo magnetická karta, nelze souhlas považovat za svobodný. Například systém, který subjekty údajů odrazuje od toho, aby jej používaly (např. příliš mnoho zbytečného času vynaloženého uživatelem nebo příliš složitý systém), nelze považovat za platnou alternativu, a nevede tudíž k platnému souhlasu.

[4] WP 187, stanovisko č. 15/2011 k definici souhlasu.

Příklady:
V případě neexistence alternativních oprávněných důvodů lze biometrický systém autentizace použít ke kontrole vstupu do videoklubu pouze tehdy, mohou-li se zákazníci svobodně rozhodnout, zda tento systém využijí. To znamená, že vlastník videoklubu musí poskytnout alternativní mechanismy méně narušující soukromí. Takový systém umožní zákazníkovi, který kvůli své osobní situaci není ochoten nebo schopen podstoupit pořízení otisků prstů, souhlas neudělit. Volba pouze mezi nevyužíváním služby a poskytnutím biometrických údajů naznačuje, že souhlas nebyl udělen svobodně, a nelze jej považovat za oprávněný důvod.

V mateřské škole je nainstalován skener struktury žil k ověřování toho, zda jsou dospělé osoby přicházející do mateřské školy (rodiče a zaměstnanci) oprávněny ke vstupu, či nikoli. K provozování tohoto systému by bylo zapotřebí uchovávání otisků prstů všech rodičů a zaměstnanců. Souhlas by byl sporným právním základem zejména v případě zaměstnanců, jelikož ti nemusí mít skutečnou možnost odmítnout používání takovéhoto systému. Byl by sporný rovněž u rodičů, pokud neexistuje jiný alternativní způsob vstupu do mateřské školy.

I když může existovat silný předpoklad, že souhlas je kvůli typické nerovnováze mezi zaměstnavatelem a zaměstnancem slabým důvodem, pracovní skupina jej zcela nevylučuje, *„pokud je dostatečně zaručeno, že je souhlas skutečně svobodný“*[5].

Souhlas v rámci pracovního poměru musí být proto přezkoumán a řádně odůvodněn. Místo vyžadování souhlasu by měli zaměstnavatelé ověřit, zda je prokazatelně nutné používat biometrické údaje zaměstnanců k oprávněnému účelu, a posoudit tuto nezbytnost na základě základních práv a svobod zaměstnanců. Pokud lze nezbytnost přiměřeně odůvodnit, může být právní základ tohoto zpracování založen na oprávněném zájmu správce, jak je stanoveno v čl. 7 písm. f) směrnice 95/46/ES. Zaměstnavatel musí vždy hledat prostředky, které co nejméně narušují soukromí, a volit pokud možno postupy, jež nevyžadují zpracovávání biometrických údajů.

Jak je však popsáno v oddíle 3.1.3, mohou existovat případy, kdy je používání biometrického systému v oprávněném zájmu správce. V těchto případech není souhlas nutný.

Souhlas je platný pouze tehdy, jsou-li poskytnuty dostatečné informace o použití biometrických údajů. Jelikož biometrické údaje mohou být použity jako jedinečný a univerzální identifikátor, je nutno považovat poskytnutí jasných a snadno přístupných informací o způsobu použití konkrétních údajů za naprosto nezbytné, aby bylo zaručeno jejich korektní zpracování. Jedná se proto o zásadní požadavek, aby byl souhlas s použitím biometrických údajů platný.

Příklady:
Platný souhlas se systémem kontroly přístupu, který používá otisky prstů, vyžaduje informace o tom, zda biometrický systém vytváří šablonu, která je jedinečná pro tento systém, či nikoli. Pokud se používá algoritmus, který vytváří stejnou biometrickou šablonu v různých biometrických systémech, musí subjekt údajů vědět, že může být rozpoznán v několika různých biometrických systémech.

[5] WP 187, stanovisko č. 15/2011 k definici souhlasu.

Určitá osoba nahraje svůj snímek do fotoalba na internetu. Registrace tohoto snímku v biometrickém systému vyžaduje výslovný souhlas udělený na základě vyčerpávajících informací o tom, co se děje s biometrickými údaji, jak dlouho a pro jaké účely jsou zpracovávány.

Jelikož souhlas lze kdykoli odvolat, musí správci údajů zavést technické prostředky, které mohou zrušit používání biometrických údajů v jejich systémech. Biometrický systém fungující na základě souhlasu musí být proto schopen účinně zrušit veškerá spojení s identitou, která vytvořil.

3.1.2. Smlouva, čl. 7 písm. b)

Zpracovávání biometrických údajů může být nezbytné pro splnění smlouvy, kde je subjekt údajů jednou ze stran, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu. Je však třeba uvést, že to platí obecně pouze tehdy, jsou-li poskytovány čistě biometrické služby. Tento právní základ nelze použít k odůvodnění sekundární služby, která spočívá v registraci určité osoby v biometrickém systému. Pokud lze takovou službu oddělit od hlavní služby, nemůže smlouva týkající se hlavní služby odůvodnit zpracovávání biometrických údajů. Osobní údaje nejsou zbožím, které lze požadovat výměnou za určitou službu, proto smlouvy, které předpokládají nebo nabízejí službu pouze pod podmínkou, že dotyčná osoba souhlasí se zpracováváním svých biometrických údajů pro jinou službu, nemohou sloužit jako právní základ tohoto zpracování.

Příklady:
a) Dva bratři poskytnou laboratoři vzorky vlasů za účelem provedení testu DNA k zjištění, zda jsou skutečně bratry. Smlouva s laboratoří týkající se provedení tohoto testu je dostatečným právním základem pro registraci a zpracování biometrických údajů.

b) Určitá osoba nahraje fotografii do fotoalba na sociální síti, aby ji ukázala svým přátelům. Pokud smlouva (podmínky služby) stanoví, že používání služby je vázáno na registraci tohoto uživatele v biometrickém systému, není toto ustanovení dostatečným právním základem pro tuto registraci.

3.1.3. Právní povinnost, čl. 7 písm. c)

Dalším právním důvodem zpracovávání osobních údajů je situace, kdy je zpracování nezbytné pro splnění právní povinnosti, které podléhá správce. Tak je tomu v některých zemích například při vydávání a/nebo používání cestovních pasů[6] a víz[7].

---

[6] Otisky prstů byly do cestovních pasů zavedeny podle nařízení Rady (ES) č. 2252/2004 ze dne 13. prosince 2004 a do povolení k pobytu v souladu s nařízením Rady (ES) č. 1030/2002 ze dne 13. června 2002.

[7] Registrace biometrických identifikátorů ve Vízovém informačním systému (VIS) je stanovena v nařízení (ES) č. 767/2008 ze dne 9. července 2008 o Vízovém informačním systému (VIS) a o výměně údajů o krátkodobých vízech mezi členskými státy (nařízení o VIS). Viz rovněž stanovisko č. 3/2007 o návrhu nařízení Evropského parlamentu a Rady, kterým se mění Společná konzulární instrukce k vízům pro diplomatické mise a konzulární úřady v souvislosti se zavedením biometrických prvků, včetně ustanovení o organizaci přijímání a zpracování žádostí o víza (KOM(2006) 269 v konečném znění), WP 134; stanovisko č. 2/2005 o návrhu nařízení Evropského parlamentu a Rady o vízovém informačním systému (VIS) a výměně údajů o krátkodobých vízech mezi členskými státy (KOM(2004) 835 v konečném znění), WP 110; stanovisko č. 7/2004 o zahrnutí biometrických prvků v povoleních k pobytu a vízech, zohledňujícím zavedení Evropského informačního vízového systému (VIS), WP 96.

3.1.4. Oprávněné zájmy správce údajů, čl. 7 písm. f)

Podle článku 7 směrnice 95/46/ES může být zpracovávání biometrických osobních údajů oprávněné rovněž tehdy, pokud „je nezbytné pro uskutečnění oprávněných zájmů správce nebo třetí osoby či osob, kterým jsou údaje sdělovány, za podmínky, že nepřevyšují zájem nebo základní práva a svobody subjektu údajů“.

To znamená, že existují případy, kdy je použití biometrických systémů v oprávněném zájmu správce údajů. Takový zájem je však oprávněný pouze tehdy, může-li správce prokázat, že jeho zájem objektivně převyšuje právo subjektu údajů nebýt registrován v biometrickém systému. Je-li například třeba zajistit bezpečnost vysoce rizikových prostor pomocí mechanismu, který může přesně ověřit, zda jsou osoby oprávněny vstupovat do těchto prostor, může být použití biometrického systému v oprávněném zájmu správce. V níže uvedeném příkladě týkajícím se biometrického systému kontroly přístupu do laboratoře nemůže správce nabídnout zaměstnanci alternativní mechanismus, aniž by to mělo přímý dopad na bezpečnost vyhrazeného prostoru, jelikož neexistují žádná alternativní, méně rušivá opatření, která jsou vhodná k dosažení odpovídající úrovně bezpečnosti tohoto prostoru. Je proto v jeho oprávněném zájmu zavést takový systém a zaregistrovat omezený počet zaměstnanců. Při tom nemusí získat jejich souhlas. I v případě, že je platným právním důvodem zpracování oprávněný zájem správce, platí jako vždy všechny ostatní zásady ochrany údajů, zejména zásady přiměřenosti a minimalizace údajů.

Příklad:
Ve společnosti, která provádí výzkum nebezpečných virů, je laboratoř zajištěna dveřmi, které se otevírají pouze po úspěšném ověření otisků prstů a snímku duhovky. To má zajistit, aby s těmito nebezpečnými materiály mohly experimentovat pouze osoby, které jsou obeznámeny se zvláštními riziky, byly vyškoleny ohledně příslušných postupů a společnost je považuje za důvěryhodné. Oprávněný zájem společnosti zajistit, aby do vyhrazeného prostoru mohly vstupovat pouze příslušné osoby, s cílem zaručit, že lze významně omezit bezpečnostní rizika spojená se vstupem do tohoto prostoru, převyšuje přání dotyčných osob, aby jejich biometrické údaje nebyly zpracovávány.

Používání biometrických údajů pro obecné požadavky týkající se bezpečnosti majetku a osob nelze obvykle považovat za oprávněný zájem převyšující zájmy nebo základní práva a svobody subjektu údajů. Naopak, zpracovávání biometrických údajů může být jako nástroj potřebný k zajištění bezpečnosti majetku a/nebo osob odůvodněné pouze tehdy, existují-li důkazy o konkrétní existenci značného rizika, které jsou založeny na objektivních a zdokumentovaných případech. Za tímto účelem musí správce prokázat, že dané okolnosti vyvolávají značné konkrétní riziko, které musí správce posoudit zvlášť obezřetně. Aby byla dodržena zásada přiměřenosti, musí správce v případě existence takových vysoce rizikových situací ověřit, zda by s ohledem na sledované cíle mohla být případná alternativní opatření stejně účinná, avšak méně rušivá, a vybrat takové alternativy.
Je rovněž nutné pravidelně přezkoumávat existenci dotyčných okolností. Na základě výsledku tohoto přezkumu musí být zpracování údajů, s ohledem na něž bylo zjištěno, že již není odůvodněné, ukončeno nebo pozastaveno.

3.2. Správce údajů a zpracovatel údajů

Směrnice 95/46/ES ukládá správcům údajů povinnosti v souvislosti se zpracováváním osobních údajů. V rámci zpracovávání biometrických údajů mohou být správci údajů různé subjekty, například zaměstnavatelé, donucovací orgány nebo migrační orgány.

Pracovní skupina připomíná pokyn uvedený v jejím stanovisku k pojmům „správce“ a „zpracovatel“[8], které náležitě objasňuje způsob výkladu těchto základních definic směrnice.

3.3. Automatizované zpracovávání (článek 15 směrnice)

Jsou-li používány systémy, které jsou založeny na zpracovávání biometrických údajů, je nutno věnovat zvláštní pozornost možným diskriminačním důsledkům pro osoby, které systém odmítne. K ochraně práva fyzické osoby nestat se subjektem opatření, které se ho dotýká, přijatého výlučně na základě automatizovaného zpracování údajů, je nutno zavést odpovídající ochranná opatření, jako je lidský zásah, nápravná opatření nebo mechanismy, které umožňují, aby subjekt údajů vyjádřil svůj názor.

Podle článku 15 směrnice 95/46/ES *„členské státy přiznají všem osobám právo nestat se subjektem rozhodnutí, které vůči nim zakládá právní účinky nebo které se jich významně dotýká, přijatého výlučně na základě automatizovaného zpracování údajů určeného k hodnocení určitých rysů jejich osobnosti, například pracovního výkonu, důvěryhodnosti, spolehlivosti, chování atd.“*

3.4. Transparentnost a informování subjektu údajů

Podle zásady korektního zpracování musí být subjekty údajů informovány o shromažďování a/nebo používání jejich biometrických údajů (článek 6 směrnice 95/46/ES). Je třeba zamezit systému, který takové údaje shromažďuje bez vědomí subjektů údajů.

Správce údajů musí zajistit, aby byly subjekty údajů v souladu s článkem 10 směrnice o ochraně údajů náležitě informovány o hlavních prvcích zpracování, jako je totožnost správce, účely zpracování, druh údajů, doba trvání zpracování, právo subjektu údajů na přístup, opravu nebo výmaz údajů a právo na zpětvzetí souhlasu a údaje o příjemci nebo kategoriích příjemců, kterým jsou údaje sdělovány. Jelikož správce biometrického systému je povinen informovat subjekt údajů, nesmí být biometrické údaje určité osoby pořízeny bez jejího vědomí.

3.5. Právo na přístup k biometrickým údajům

Subjekty údajů mají právo získat od správců údajů přístup ke svým údajům, včetně biometrických údajů. Subjekty údajů mají rovněž právo na přístup k případným profilům založeným na těchto biometrických údajích. Pokud správce údajů musí za účelem udělení tohoto přístupu zjistit totožnost subjektů údajů, je nezbytné, aby byl tento přístup umožněn bez zpracování dalších osobních údajů.

3.6. Bezpečnost údajů

Správci údajů musí přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení, náhodné ztrátě, úpravám, neoprávněnému sdělování nebo přístupu, jakož i proti jakékoli jiné podobě nedovoleného zpracování[9].

Veškeré shromážděné a uložené údaje musí být náležitě zabezpečeny. Tvůrci systémů musí navázat kontakty s odpovídajícími odborníky na bezpečnost, aby bylo zajištěno náležité odstranění bezpečnostních problémů, zejména v případě, že se stávající systémy přesouvají na internet.

---

[8] WP 169, stanovisko č. 1/2010 k pojmům „správce“ a „zpracovatel“.

[9] Čl. 17 odst. 1 směrnice 95/46/ES.

3.7. Ochranná opatření u osob se zvláštními potřebami

Používání biometrických údajů může mít významné dopady na důstojnost, soukromí a právo na ochranu údajů u zranitelných osob, jako jsou malé děti, starší osoby a osoby, které nejsou fyzicky s to provést úplnou registraci. Vzhledem k případným negativním důsledkům pro dotyčné osoby bude třeba při posuzování dopadů opatření narušujícího důstojnost osoby splnit přísnější požadavky, pokud jde o otázky nezbytnosti a přiměřenosti a rovněž možnost jednotlivce uplatnit své právo na ochranu údajů, aby bylo toto opatření považováno za přípustné. Musí být zavedena vhodná opatření na ochranu proti rizikům stigmatizace nebo diskriminace těchto osob z důvodu jejich věku či jejich neschopnosti provést registraci.

Pokud jde o zavedení obecné právní povinnosti týkající se shromažďování biometrických identifikátorů u těchto skupin, zejména u malých dětí a starších osob při hraničních kontrolách za účelem identifikace, pracovní skupina zastává názor, že *„pro zachování důstojnosti osoby a zabezpečení důvěryhodnosti prováděných úkonů by získávání a zpracování otisků prstů mělo být u dětí a starších osob věkově omezeno a toto věkové omezení by mělo odpovídat věkovým omezením stanoveným u jiných biometrických databází EU (zejména systému Eurodac)“*[10].

Každopádně by měla být zavedena zvláštní ochranná opatření (např. vhodné náhradní postupy), aby bylo zajištěno respektování lidské důstojnosti a základních svobod každé fyzické osoby, která není schopna provést úspěšně proces registrace, a tím zamezit tomu, aby se tito jedinci stali obětí nedokonalého technického systému[11].

3.8. Citlivé údaje

Některé biometrické údaje lze považovat za citlivé ve smyslu článku 8 směrnice 95/46/ES, zejména údaje odhalující rasový nebo etnický původ či údaje týkající se zdraví. Údaje o DNA určité osoby například často obsahují zdravotní údaje nebo mohou odhalit rasový či etnický původ. V tomto případě jsou údaje o DNA citlivými údaji a kromě obecných zásad ochrany údajů stanovených ve směrnici je nutno použít zvláštní ochranná opatření uvedená v článku 8. Za účelem posouzení citlivosti údajů zpracovávaných biometrickým systémem je nutno vzít v úvahu rovněž kontext, v jakém jsou údaje zpracovávány[12].

3.9. Úloha vnitrostátních orgánů pro ochranu údajů

Vzhledem k rostoucí standardizaci biometrických technologií z důvodu interoperability se obecně uznává, že centrální uchovávání biometrických údajů zvyšuje riziko použití biometrických údajů jako klíče k propojení více databází (jež by mohlo vést k vytváření podrobných profilů jednotlivce) i zvláštní nebezpečí opětovného použití těchto údajů k neslučitelným účelům, zejména v případě neoprávněného přístupu.

Pracovní skupina doporučuje, aby systémy, které biometrické údaje používají jako klíč k propojení více databází, vyžadovaly dodatečná ochranná opatření, jelikož tento druh zpracovávání pravděpodobně představuje zvláštní rizika z hlediska práv a svobod subjektů údajů (článek 20 směrnice 95/46/ES). K zajištění vhodných ochranných opatření, zejména

---

[10] WP 134 – stanovisko č. 3/2007 o návrhu nařízení Evropského parlamentu a Rady, kterým se mění Společná konzulární instrukce k vízům pro diplomatické mise a konzulární úřady v souvislosti se začleněním biometrických prvků, včetně ustanovení o organizaci přijímání a zpracování žádostí o víza (KOM(2006) 269 v konečném znění).

[11] Viz WP 134 – stanovisko č. 3/2007, s. 8.

[12] Viz WP 29, poradní dokument o zvláštních kategoriích údajů („citlivé údaje“), Ref. Ares (2011)444105 – 20.4.2011.

k snížení rizik pro subjekty údajů, by správce měl před zavedením těchto opatření konzultovat příslušný vnitrostátní orgán pro ochranu údajů.

4. Nový vývoj a technologické trendy, nové scénáře

4.1. Úvod

Biometrické technologie dlouhou dobu používaly především státní orgány, nyní se však situace postoupně posunuje ke stavu, kdy při používání těchto technologií a vývoji nových produktů hrají hlavní úlohu komerční organizace.

Jednou z hlavních hybných sil tohoto vývoje je skutečnost, že technologie jsou natolik vyspělé, že biometrické systémy, které náležitě fungovaly pouze za kontrolovaných podmínek, jsou zdokonaleny a nyní jsou vhodné pro rozsáhlé používání v řadě různých prostředí. V tomto smyslu biometrické údaje v některých případech nahrazují či zdokonalují tradiční metody identifikace, zejména metody založené na několika faktorech identifikace, které jsou zapotřebí pro důkladné systémy autentizace. Biometrické technologie se používají stále více rovněž v aplikacích, které mohou osoby identifikovat snadno a rychle za cenu nižší míry přesnosti.

Používání biometrických technologií se postupně rozšiřuje z původní oblasti používání k identifikaci a autentizaci pro účely analýzy chování, dohledu a předcházení podvodům.

Pokrok v oblasti počítačových technologií a sítí vede taktéž k nárůstu toho, co se považuje za biometrii druhé generace, která je založena buď pouze na behaviorálních a psychologických rysech, nebo na kombinaci tohoto pojetí s jinými tradičními systémy, což vytváří multimodální systémy. K používání biometrie se nakonec postupně přechází při rozvoji inteligentního prostředí a všudypřítomné výpočetní techniky.

4.2. Nové trendy v oblasti biometrických technologií

Existuje řada biometrických technologií, které lze považovat za vyspělé technologie s řadou použití při vymáhání práva, v elektronické veřejné správě a v obchodních systémech. Neúplný seznam zahrnuje otisky prstů, geometrii ruky, snímek duhovky a některé druhy rozpoznávání obličeje. Objevují se rovněž biometrické technologie k analýze tělesných znaků. Zatímco některé z nich jsou nové, některé tradiční biometrické technologie získávají nový impulz vyplývající z nových kapacit v oblasti zpracování.

Typickými prvky těchto nových systémů je používání tělesných znaků umožňující kategorizaci/identifikaci jednotlivců a shromažďování těchto znaků na dálku. Shromážděné údaje se používají k vytváření profilů, dálkovému dohledu či k ještě složitějším úkolům, jako je inteligentní prostředí.

To je možné díky vývoji snímačů umožňujících shromažďování nových fyziologických vlastností a rovněž novým způsobům zpracovávání tradičních biometrických údajů.

Je třeba zmínit rovněž používání tzv. „soft“ biometrie, která se vyznačuje používáním velmi běžných znaků, jež nejsou vhodné k jednoznačnému rozpoznání nebo identifikaci jednotlivce, umožňují však zlepšit výkonnost jiných identifikačních systémů.

Dalším důležitým prvkem nových biometrických systémů je možnost shromažďovat údaje z určité vzdálenosti nebo v pohybu, aniž by byla nutná spolupráce nebo činnost ze strany

jednotlivce. Ačkoliv se dosud nejedná o zcela rozvinutou technologii, v této oblasti se vynakládá obrovské úsilí, zejména pro účely vymáhání práva.

Rychle se rozvíjí používání multimodálních systémů používajících různé biometrické údaje současně nebo několik hodnot/jednotek téhož biometrického údaje, které lze upravit za účelem optimalizace bezpečnosti/pohodlí biometrických systémů. To může snížit míru chybného přijetí, zlepšit výsledky systému rozpoznávání nebo usnadnit shromažďování údajů větší skupiny obyvatelstva, a to vyvážením neuniverzálnosti jednoho zdroje biometrických údajů jeho spojením s jinými zdroji.

Biometrické systémy používají stále častěji subjekty z veřejného i soukromého sektoru; ve veřejném sektoru se biometrické údaje používají pravidelně pro účely vymáhání práva; používání biometrických údajů se rychle zvyšuje ve finančním a bankovním sektoru a v elektronickém zdravotnictví, jakož i v jiných odvětvích, jako je školství, maloobchod a telekomunikace. Tento vývoj bude poháněn novými znaky odvozenými ze sbližování/spojování stávajících technologií. Příkladem je používání kamerových systémů, které umožňují shromažďování a analýzu biometrických údajů i znaků chování lidí.

Výše uvedené skutečnosti lze pokládat rovněž za změnu v zaměření, kdy se biometrické systémy rozvíjejí z nástrojů identifikace k účelům „soft“ rozpoznávání, jinými slovy od identifikace k zjišťování chování či zvláštních potřeb osob. To otevírá dveře použitím, která se velmi odlišují od rozsáhlých bezpečnostních aplikací: prospěch z větší interakce mezi člověkem a strojem umožňující více než jen identifikaci či kategorizaci jednotlivce bude mít osobní bezpečnost, hraní her a maloobchod.

4.3. Dopad na soukromí a ochranu údajů

Od samého počátku zavádění se uznávalo, že biometrické systémy mohou vyvolávat velké obavy v řadě oblastí, včetně soukromí a ochrany údajů, což jistě ovlivnilo jejich společenské přijetí a podnítilo diskusi o zákonnosti a omezení jejich používání a o ochranných opatřeních a zárukách, které jsou zapotřebí k zmírnění zjištěných rizik.

Tradiční odpor vůči biometrickým systémům byl a dosud je spojen s ochranou práv jednotlivce. Avšak i nové systémy a rozvoj stávajících systémů vyvolávají řadu obav. K nim patří možnost skrytého shromažďování, uchovávání a zpracovávání údajů, jakož i shromažďování materiálů s velmi citlivými informacemi, které mohou narušovat nejintimnější prostor jednotlivce.

Od doby, kdy se biometrické technologie a systémy začaly používat, představovalo vážnou obavu využití k jiným účelům; ačkoliv se jedná o známé riziko, jemuž je v tradičních biometrických technologiích věnována pozornost, je nesporně zřejmé, že vyšší technický potenciál nových počítačových systémů zvyšuje riziko toho, že údaje budou použity v rozporu se svým původním účelem.

Skryté techniky umožňují identifikaci jednotlivců bez jejich vědomí, což má za následek vážné ohrožení soukromí a postupnou ztrátu kontroly nad osobními údaji. To má vážné důsledky pro schopnost jednotlivců udělit svobodný souhlas nebo jednoduše získat informace o zpracovávání. Tyto systémy mohou mimoto tajně shromažďovat informace o emocionálním stavu nebo tělesných znacích a poskytovat zdravotní údaje, což vede k nepřiměřenému zpracovávání údajů a rovněž zpracovávání citlivých údajů ve smyslu článku 8 směrnice 95/46/ES.

Vzhledem ke skutečnosti, že biometrické technologie nemohou zajistit úplnou přesnost, existuje vždy riziko vyplývající z nesprávné identifikace. Tyto falešně pozitivní výsledky mají za následek rozhodnutí, která se dotýkají práv jednotlivce. Krádež identity na základě použití zfalšovaných nebo odcizených zdrojů biometrických údajů může vést k vážným škodám. Na rozdíl od jiných identifikačních systémů nelze jednotlivci poskytnout novou identifikaci pouze z důvodu jejího narušení.

Je třeba poukázat na vytváření profilů v rámci přijímání automatizovaných rozhodnutí nebo na předvídání chování či preferencí v určité situaci. Některé biometrické údaje mohou odhalovat fyzické údaje o jednotlivci. Tyto údaje lze použít k zaměření a vytváření profilů, může to však skončit rovněž diskriminací, stigmatizací nebo nechtěnou konfrontací s neočekávanými/nepožadovanými informacemi.

4.4. Odkaz na zvláštní biometrické systémy a technologie

4.4.1. Struktura žil a kombinované použití

Na rozpoznávání struktury žil jsou založeny dvě hlavní používané technologie: rozpoznávání žil na dlani a rozpoznávání žil na prstech, obě techniky se nyní široce využívají, zejména v Japonsku.

Z technického hlediska závisí rozpoznávání struktury žil na šabloně struktury žil zachycené infračervenou kamerou při osvětlení prstu nebo ruky blízkým infračerveným světlem. Pořízený snímek se zpracovává za účelem zobrazení charakteristických znaků struktury žil, přičemž výsledkem je zpracovaný snímek cévní soustavy. Hlavní výhodou této technologie je skutečnost, že jednotlivec nezanechává stopu svého biometrického znaku[13], jelikož není nutné „dotknout“ se čtečky. V současnosti je problematické shromažďovat biometrické údaje bez souhlasu subjektu údajů. Tuto techniku lze použít rovněž k zjištění toho, zda je subjekt prověřovaný systémem naživu či nikoli, a to analýzou toku krve.

Rozpoznávání struktury žil lze použít pro aplikace logického přístupu a k fyzickému přístupu do určitých prostor. Výrobci nabízejí rovněž možnost zabudování snímače do jiných produktů, zejména pro bankovní účely.

Rizika z hlediska ochrany údajů, která jsou spojená s používáním systémů rozpoznávání struktury žil, lze popsat následovně:

- Přesnost: Úroveň výkonnosti systému rozpoznávání žil je vysoká, jelikož tato technologie se považuje za schůdnou alternativu otisků prstů. Rozpoznávání struktury žil zajišťuje rovněž nízkou „míru nezdařených zařazení“ (Failure to Enrol Rate – FER), jelikož není ovlivněno poškozením prstu nebo ruky. Tyto technologie nebyly dosud vyzkoušeny/použity u velmi vysokého počtu obyvatel (v Japonsku je šablona porovnávána se šablonou uloženou v inteligentní kartě). V určitých případech může být tato technologie nepříznivě ovlivněna klimatickými podmínkami, které mají vliv na cévní soustavu (teplo, tlak atd.).

[13] Někteří autoři tvrdí, že technologie spojené s rozpoznáváním struktury žil mohou odhalit nemoci jako vysoký krevní tlak nebo onemocnění cévní soustavy.

- Dopad: Dopad systémů rozpoznávání struktury žil na ochranu údajů je omezený, jelikož biometrické údaje nelze shromažďovat snadno a používání struktury žil je v současnosti omezeno na aplikace v soukromém sektoru.

- Souhlas a transparentnost: Jelikož údaje o struktuře žil lze získat pouze pomocí blízkého infračerveného světla a kamer, lze mít za to, že osoba je vždy informována o zpracovávání a přiložením prstu nebo ruky k čtečce udělila svůj souhlas. Stejně jako u každého jiného biometrického systému je však nutno tento předpoklad v určitých zvláštních případech omezit, například v případě, je-li dotyčná osoba zaměstnancem správce údajů.

- Další účel nebo účely zpracování: V současnosti představují údaje o struktuře žil omezená rizika, pokud jde o jejich použití k dalším účelům. Toto riziko se může zvýšit, jestliže se tento druh zpracování používá obecně a je-li snazší zfalšování.

- Spojitelnost: Údaje o struktuře žil neposkytují informace, které lze spojovat s jinými údaji, s výjimkou údajů o struktuře žil z jiného zpracování.

- Sledování / vytváření profilů: Riziko sledování / vytváření profilů pomocí údajů o struktuře žil je omezené, dokud není tento druh biometrických údajů široce používán, například v centrální databázi pro platební karty.

- Zpracovávání citlivých údajů: Jediným citlivým údajem, který by bylo možno získat z údajů o struktuře žil, je zdravotní stav, tato záležitost však nebyla dosud oficiálně posouzena.

- Zrušitelnost: Zdá se, že údaje o struktuře žil jsou v čase velmi stálé, toto tvrzení je však nutno potvrdit pokusy (systémy rozpoznávání struktury žil jsou příliš nové, než aby poskytovaly potvrzené výsledky). Mělo by se proto mít za to, že údaje o struktuře žil nejsou zrušitelné.

- Ochrana proti falšování: Falšování údajů o struktuře žil nebylo dosud rozsáhle přezkoumáno, nedávný průzkum však ukázal, že je možné oklamat čtečku struktury žil na dlani[14]. Hlavním problémem při falšování údajů o struktuře žil je získání vzorku biometrických údajů.

4.4.2. Otisky prstů a kombinované použití

Rozpoznávání otisků prstů patří k nejstarším, nejvíce prostudovaným a nejrozsáhleji používaným biometrickým systémům. Identifikace pomocí otisků prstů se pro účely vymáhání práva používá více než 100 let, a to při ověřování totožnosti i identifikaci. Je založena na skutečnosti, že každý jednotlivec má jedinečné otisky prstů vykazující zvláštní znaky, jež lze změřit, aby bylo možno rozhodnout, zda otisk prstů odpovídá zaregistrovanému vzorku.

Registrace vyžaduje fyzickou přítomnost jednotlivce a podle očekávaného použití i vyškoleného personálu, aby byla zajištěna náležitá kvalita údajů. Pořízení otisků prstů není triviální úkol. V tomto smyslu bude přesnost srovnání záviset na kvalitě snímku ve vztahu k zobrazovací technice. Techniky se mohou lišit od pořízení otisku jednoho nebo dvou prstů

[14] Viz: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf

po všech deset prstů, a to plochého otisku nebo váleného otisku. V závislosti na systému lze otisky prstů použít k ověření totožnosti (1:1) nebo k identifikaci a porovnání se stopami (1: n). Jak však prokázaly některé studie, určitou část obyvatelstva nelze z různých důvodů zaregistrovat, což představuje problém, který vyžaduje existenci vhodných náhradních postupů, zejména v případě velkých systémů, aby se zamezilo tomu, že jednotlivci jsou zbaveni něčeho, na co mají nárok.

Ačkoli se v zásadě nejedná o metodu příliš narušující soukromí, může být jako taková vnímána, jelikož kvůli svému běžnému používání pro účely vymáhání práva je spojena s negativní představou osoby považované za podezřelou.

Otisky prstů vykazují různé znaky, které lze použít k ověření totožnosti / identifikaci, ačkoliv dosud je nejčastěji používanou technikou analýza markantů. Vývoj nových technik (např. skenerů s vysokým rozlišením) však umožní používání dalších znaků. K dalšímu rozvoji technik dochází rovněž s ohledem na možnost identifikace, což umožňuje používání velkých databází pro účely identifikace.

V tomto smyslu jsou nejvyspělejšími systémy tzv. automatizované systémy identifikace otisků prstů (AFIS) používané pro účely vymáhání práva, které lze využívat k výměně údajů a vyhledávání v různých úložištích v zahraničí. Výměna údajů však čelí problémům spojeným s různými lokalitami, formáty a úrovněmi kvality.

K příkladům systémů AFIS na úrovni EU patří systém Eurodac a Vízový informační systém, které budou podle předpokladů největšími databázemi na světě vzhledem k tomu, že v těchto systémech bude uloženo přibližně 70 milionů otisků prstů. Ve svých předchozích stanoviscích se pracovní skupina zabývala řadou otázek týkajících se používání velkých databází vzhledem k nutnosti zajistit přiměřenost. Zejména je třeba řešit problémy se spolehlivostí v souvislosti s falešně pozitivními a falešně negativními výsledky, účinnou kontrolu přístupu do těchto databází a problémy spojené s používáním otisků prstů dětí a starších lidí.

V biometrických systémech založených na otiscích prstů jsou běžně používány šablony, které jsou obvykle poskytovateli systémů považovány za způsob ochrany jednotlivců. V závislosti na systému / algoritmu používaném k vytvoření šablony však existují možná rizika související s možností spojovat šablony s jinými databázemi otisků prstů za účelem identifikace jednotlivců.

Důležitou otázkou je rovněž možnost oklamání systémů rozpoznávání otisků prstů pomocí umělých prstů nebo otisků prstů pořízených z umělého materiálu, což umožňuje krádež identity. K snížení zranitelnosti těchto systémů existují různé přístupy, jako je detekce živého prstu, systémy založené na rozpoznávání více prstů a rovněž používání odpovídajícího lidského dohledu při registraci a identifikaci / ověřování totožnosti.

Rizika z hlediska ochrany údajů, která jsou spojená s používáním otisků prstů, lze stručně popsat takto:

- Přesnost: Ačkoli otisky prstů zajišťují vysokou míru přesnosti, toto může být zpochybněno kvůli omezením spojeným s informacemi (nízká kvalita údajů nebo nejednotné pořizování otisků) nebo reprezentativností (zvolené znaky nebo kvalita algoritmů výběru). To může vést k chybnému odmítnutí nebo chybné shodě.

- Dopad: Nevratnost procesu může omezit možnost uplatňování práv jednotlivce nebo zvrácení rozhodnutí přijatých na základě chybné identifikace. Spoléhání se na přesnost otisků prstů může znamenat, že případné chyby lze hůře napravit, což vede

k dalekosáhlým důsledkům pro jednotlivce. To je nutno vzít v úvahu při posuzování přiměřenosti zpracování ve vztahu k určitému rozhodnutí, jež má být přijato na základě otisků prstů. Je třeba rovněž zmínit, že nedostatečná bezpečnostní opatření mohou vést ke krádeži identity, jež může mít na jednotlivce závažný dopad.

- Spojitelnost: Otisky prstů mohou být zneužity, jelikož tyto údaje lze spojit s jinými databázemi. Tato možnost propojování s jinými databázemi může vést k použití, které není slučitelné s původními účely. K snížení tohoto rizika lze použít určité techniky, například konvertibilní biometrické systémy nebo kódování biometrických údajů.

- Zpracovávání citlivých údajů: Podle některých studií mohou snímky otisků prstů poskytnout informace o etnickém původu jednotlivce[15].

- Další účel nebo účely zpracování: Centrální uložení údajů, zejména ve velkých databázích, znamená rizika spojená s bezpečností údajů, spojitelností a využitím k jiným účelům. V případě neexistence ochranných opatření to umožňuje použití otisků prstů k jiným účelům, než byl původní důvod zpracování.

- Souhlas a transparentnost: Souhlas představuje při používání otisků prstů k jiným účelům než pro účely vymáhání práva hlavní problém. Otisky prstů lze snadno zkopírovat z latentních otisků a dokonce fotografií bez vědomí jednotlivce. K dalším záležitostem týkajícím se souhlasu patří otázky spojené se získáním souhlasu dítěte a úlohou rodičů v tomto ohledu (např. používání otisků prstů ve školách) a rovněž s platností souhlasu s poskytnutím otisků prstů v rámci pracovního poměru.

- Zrušitelnost: Otisky prstů jsou v čase velmi stálé a měly by se považovat za nezrušitelné. Šablonu otisku prstu lze zrušit za určitých podmínek.

- Ochrana proti falšování: Otisky prstů lze získat snadno kvůli mnoha otiskům prstů, které za sebou jedinec zanechává. U mnoha systémů a snímačů lze mimoto použít falešné otisky prstů, zejména v případě, že tyto systémy neobsahují zvláštní ochranu proti falšování. Úspěch útoku závisí do značné míry na druhu snímače (optický, kapacitní atd.) a materiálu, který útočník použije.

Příklad:
Nemocnice používá otisky prstů uložené v centrální databázi k autentizaci pacientů na oddělení radioterapie s cílem zajistit, aby byla příslušnému pacientovi poskytnuta správná léčba. Otisky prstů se upřednostňují před strukturou žil, jelikož léčba poškozuje cévní soustavu. Centrální databáze se mimoto používá z toho důvodu, že stav pacientů (věk, patologie) znamená vysoké riziko ztráty průkazů, což by znemožnilo přístup k léčbě. V tomto případě se zdá, že používání otisků prstů je vhodným řešením.

4.4.3. Rozpoznávání obličeje a kombinované použití

Obličej se stejně jako otisky prstů rozsáhle využívá jako zdroj biometrických údajů řadu let. V poslední době lze z obličeje určit nejen totožnost, nýbrž rovněž fyziologické a psychologické rysy jako etnický původ, emoce a tělesnou i duševní pohodu. Schopnost získat tento objem údajů ze snímku a skutečnost, že fotografii lze pořídit z určité vzdálenosti

[15] http://www.handresearch.com/news/fingerprints-world-map-whorls-loops-arches.htm a http://www.crime-scene-investigator.net/fingerprintpatterns.html

bez vědomí subjektu údajů, naznačuje úroveň problémů spojených s ochranou údajů, které mohou vyplývat z těchto technologií.

Rozpoznávání tváře jako prostředek identifikace a ověření totožnosti nezůstalo bez povšimnutí ze strany donucovacích orgánů, ostatních orgánů veřejné správy nebo soukromých organizací. Fotografie se mnoho let objevují v cestovních pasech, řidičských průkazech, průkazech totožnosti a policejních záznamech. Není neobvyklé, že je fotografie vytištěna na kartě pro kontrolu přístupu či jiné legitimaci organizace. Tyto snímky jsou obvykle pořizovány při kontrolovaném osvětlení a jsou omezeny na čelní pohled nebo pohled z profilu. Používání takového kontrolovaného souboru snímků vedlo přirozeně k zahájení automatického zpracovávání a rozpoznávání jednotlivců. Tato možnost byla od té doby zdokonalena a v současnosti technologie umožňuje identifikaci ze snímků pořízených pomocí různých kamer, z různých úhlů a za různých světelných podmínek. Rovněž na internetu je veřejně přístupný obrovský objem snímků, například snímky přenesené na sociální sítě či jiné veřejně přístupné galerie. Tato rizika nejsou omezena na tradiční snímky, jelikož rozpoznávání obličeje bylo úspěšně zabudováno do pořizování videosnímků v reálném čase. V případě rozšíření stávajícího systému o nové funkce v oblasti zpracování (např. rozpoznávání obličeje v kamerových systémech) musí správci údajů poznat, že toto může změnit stanovený účel nebo účely původního systému, a musí znovu posoudit dopady této změny na soukromí.

Rizika z hlediska ochrany údajů, která jsou spojená s používáním systémů rozpoznávání obličeje, lze popsat takto:

- Přesnost: Nelze-li zaručit kvalitu snímků, existuje nebezpečí, že bude ohrožena přesnost. Není-li zachycena tvář (je zakryta vlasy nebo pokrývkou hlavy), je zřejmé, že porovnání nebo kategorizaci nelze provést bez vysoké míry chyb. Při rozpoznávání obličeje jsou nadále velkým problémem se značným dopadem na přesnost změny postoje a osvětlení.

- Dopad: Příslušný dopad konkrétního systému rozpoznávání obličeje na ochranu údajů bude záviset na jeho účelu a konkrétní situaci. Systém kategorizace k načítání demografických údajů účastníků určité atrakce bez funkce zaznamenávání bude mít jiný dopad na ochranu údajů než systém používaný donucovacími orgány ke skrytému dohledu za účelem identifikace potenciálních výtržníků.

- Souhlas a transparentnost: Riziko z hlediska ochrany údajů, které se u mnoha jiných druhů zpracovávání biometrických údajů nevyskytuje, představuje skutečnost, že snímky lze pořizovat a zpracovávat z mnoha zorných úhlů, v různých podmínkách okolí a bez vědomí subjektu údajů. Ve stanovisku č. 15/2011 k definici souhlasu zdůrazňuje pracovní skupina skutečnost, že aby mohl být právním základem zpracování souhlas, musí být „informovaný“. Pokud si subjekt údajů není vědom zpracovávání snímků za účelem rozpoznávání obličeje, nemůže tomu tak být. I když je subjekt údajů informován o přítomnosti kamery, nemusí existovat viditelné stopy pro rozlišování mezi kamerovým systémem s přímým přenosem nebo záznamovým kamerovým systémem a objektivem pořizujícím snímky pro systém rozpoznávání obličeje.

- Další účel nebo účely zpracování: Jakmile jsou digitální snímky pořízeny, ať už legálně nebo nezákonně, lze je snadno sdílet nebo kopírovat za účelem zpracovávání v jiných systémech, než jsou systémy, pro něž byly původně určeny. To je zřejmé

v oblasti sociálních médií, kde uživatelé nahrávají své osobní fotografie, aby je sdíleli s rodinou, přáteli nebo kolegy. Jakmile se snímky nacházejí na platformě sociálních médií, jsou k dispozici pro opětovné použití samotnou platformou pro řadu účelů, z nichž některé mohou být do platformy zavedeny až poté, co byl snímek pořízen a/nebo nahrán.

- Spojitelnost: Velká řada internetových služeb umožňuje uživatelům nahrát snímek k vytvoření spojení s profilem uživatele. Rozpoznávání obličeje lze použít k vytváření spojení mezi profily různých internetových služeb (prostřednictvím profilové fotografie), avšak rovněž mezi světem on-line a off-line. Není vyloučena možnost pořídit fotografii určité osoby na ulici a v reálném čase určit její totožnost prohledáváním těchto veřejných profilových fotografií. Rovněž služby třetí strany mohou prohledávat profilové fotografie a jiné snímky, které jsou veřejně přístupné, za účelem vytváření obrovských souborů snímků s cílem spojit tyto snímky s reálnou identitou.

- Sledování / vytváření profilů: Identifikační systém lze použít i v případě, že skutečná identita jednotlivce není známá. Systém rozpoznávání obličeje v nákupním středisku nebo podobném veřejném prostoru lze použít ke sledování tras a zvyků jednotlivých nakupujících. Snahou může být účinné řízení front nebo umístění výrobků s cílem zlepšit zkušenosti zákazníků. S možností sledovat nebo lokalizovat konkrétního jednotlivce je však spojena možnost vytváření profilů a poskytování cílené reklamy či jiných zvláštních služeb.

- Zpracovávání citlivých údajů: Jak bylo uvedeno výše, zpracování biometrických údajů může být využito k zjištění citlivých údajů, zejména údajů odvozených z viditelných znaků, jako je rasa, etnická skupina či případně zdravotní stav.

- Zrušitelnost: Jednotlivec může vzhled svého obličeje snadno změnit (vousy, brýle, pokrývka hlavy atd.), což může postačovat k oklamání systémů rozpoznávání obličeje, zejména pokud fungují v nekontrolovaném prostředí. Hlavní rysy obličeje jednotlivce se však v čase nemění a systémy mohou rozpoznávání zlepšit shromažďováním a spojováním různých známých „tváří“ jednotlivce.

- Ochrana proti falšování: Mnoho systémů rozpoznávání obličeje lze snadno oklamat, výrobci se však snaží zlepšit ochranu proti falšování pomocí technik, jako je 3D zobrazení nebo videozáznamy. Většina základních systémů používaných ve veřejných aplikacích však tento druh ochrany nezahrnuje.

Příklad:
Krajním imaginárním příkladem je systém dohledu nové generace využívající videokamery, který je nainstalován v nákupním středisku a který dovede rozpoznávat osoby, automaticky sleduje pohyb, rozlišuje výrazy obličeje, například úsměv nebo zlost. Systém by mohl rozpoznávat pravidelné zákazníky přijíždějící na parkoviště a směrovat je na upřednostňovaná parkovací místa. Jakmile zákazníci vstoupí do nákupního střediska, mohl by systém identifikovat oděv, aby jim navrhl, které obchody mají navštívit, a to v závislosti na dostupné nabídce obchodů, předchozí historii nakupování nebo předem stanoveném souboru ukazatelů. Bylo by rovněž možné zařídit přizpůsobenou reklamu ve výlohách nebo automatické odepření

vstupu do obchodů, restaurací či jiných prostor. Bylo by možno identifikovat potenciální zloděje aut a sledovat je dříve, než se dotknou určitého automobilu. V případě potřeby by mohly dálkově ovládané bezpilotní letouny s kamerami a jinými snímači sledovat podezřelé osoby, dokud není podezření vyvráceno nebo potvrzeno. Bylo by možné odhalit předměty skryté v oděvu (nože nebo ukradené věci). Tato technologie je založena nejen na nových biometrických systémech, ale spojuje a zpracovává i informace, které jsou již k dispozici, s jinými údaji ze široké škály různých systémů.

Podobná aplikace byla navržena v projektu INDECT (inteligentní informační systém s podporou sledování, vyhledávání a rozpoznávání pro bezpečnost občanů v městském prostředí), který spojuje technologie za účelem boje proti možným teroristickým útokům a trestným činům dříve, než k nim dojde. Pracovní skupina důrazně doporučuje, aby takové používání biometrických údajů vyžadovalo náležitý právní základ a přísné uvážení nezbytnosti a přiměřenosti těchto opatření.

4.4.4. Rozpoznávání hlasu a kombinované použití

Kromě používání rozpoznávání hlasu jako biometrického údaje pro účely identifikace patří k relativně běžnému použití určení zvláštních znaků v hlase ke kategorizaci mluvčího. Příkladem je analýza odpovědí jednotlivce během telefonního hovoru k určení přízvuku a vad řeči za účelem zjištění možných případů podvodu.

Reference zveřejněné výrobci udávají, že díky zavedení této technologie se společnostem poskytujícím finanční služby podařilo zvýšit počet odhalených podvodů a mohou rychleji vyřizovat skutečné požadavky.

Pokud se tato technologie používá v systému kategorizace, liší se rizika z hlediska ochrany údajů mírně od rizik biometrického identifikačního systému v tom, že by neměla existovat fáze registrace a nemělo by být nutné dlouhodobé uchovávání biometrické šablony. Je-li však telefonní rozhovor nahráván, jak tomu obvykle je u finančních institucí, musí být zavedeny vhodné kontroly, aby byla zajištěna bezpečnost těchto údajů.

- Přesnost: Jedno riziko takovéhoto systému z hlediska ochrany údajů spočívá v míře detekce, zejména počtu falešně pozitivních a falešně negativních výsledků, tj. kolik lidí bylo chybně identifikováno jako podvodníci nebo kolik podvodných požadavků nebylo zjištěno. Ačkoliv u systému kategorizace lze tolerovat vyšší míru chyb než u systému ověřování totožnosti či identifikace, musí být zavedeny vhodné postupy pro včasné řešení případů, které mohou být nesprávně zařazeny.

- Souhlas a transparentnost: U těchto technologií lze použít přístup zajišťující ochranu soukromí, jako je snaha zajistit, aby byly hovory prověřovány za účelem posouzení vhodnosti a aby byly subjekty údajů informovány o přijatém postupu. V jedné případové studii se mělo za to, že jednotlivci nejsou vhodní pro účely průzkumu, pokud jejich prvním jazykem nebyla angličtina nebo pokud měli poruchu sluchu či zhoršenou schopnost uvažování nebo neměli přístup k telefonu. Uchazeči mohli odmítnout zúčastnit se hovoru a poskytnout informace tradičním způsobem, aniž by však byly znevýhodněny subjekty údajů, které nechtěly nebo se nemohly zúčastnit takovéhoto systému.

- Další účel nebo účely zpracování: Ačkoliv většina těchto technologií bude při zavedení vyžadovat zvláštní změny infrastruktury, vzhledem ke skutečnosti, že veřejný a soukromý sektor konsoliduje své IT infrastruktury za účelem zabudování

technologií jako *Voice over IP*, může být zabudovávání technologií rozpoznávání hlasu snazší bez patřičného přihlédnutí k povinnostem správce týkajícím se ochrany údajů.

- Zrušitelnost: I v případě, že jednotlivec umí svůj hlas úmyslně změnit, charakteristika hlasu je poměrně stálá a může být účinná při jedinečné identifikaci jednotlivce, zejména v případě, není-li jednotlivec informován (a nemá proto sklon hlas měnit).

- Ochrana proti falšování: K oklamání systémů rozpoznávání hlasu lze použít nahrané hlasy. K technikám ochrany proti falšování patří otázky a odpovědi v určitém kontextu (dotaz na datum nebo zopakování řídce se vyskytujících slov).

4.4.5. DNA

Zdokonalení přístrojů používaných k sekvenování a porovnávání DNA a dostupnost zařízení pro analýzu DNA za přiměřené ceny vede k tomu, že je nutné znovu uvážit některé předpoklady uvedené v předchozím dokumentu o biometrických údajích (WP 80).

Jednou z hlavních změn v technologiích profilování DNA je zkrácení doby potřebné pro provedení sekvenování a porovnávání DNA. Neustálé pokroky, jichž v průběhu let dosáhl akademický výzkum a vývojáři biotechnologií, zkrátily dobu potřebnou pro vytvoření profilu DNA ze dnů na hodiny a dokonce zlomky hodiny.

Hlavním problémem trhu s internetovými službami založenými na DNA je ohrožení práva jednotlivců na ochranu údajů, zejména v případě, že služba vyžaduje předávání biometrických vzorků a biometrických údajů mezi různými zeměmi (včetně zemí mimo EU) a více zpracovatelů údajů a při zpracovávání genetických nebo zdravotních údajů neexistují vhodná ochranná opatření.

Je velmi pravděpodobné, že v blízké budoucnosti bude pomocí přenosných přístrojů možné provádět profilování DNA a porovnávání vzorků v reálném čase (nebo téměř v reálném čase), což bude představovat výchozí bod pro rozvoj biometrických systémů identifikace/autentizace na základě DNA s vyšší úrovní přesnosti v porovnání s autentizací pomocí otisků prstů, rozpoznávání hlasů a rozpoznávání obličeje.

Zdokonalování profilování DNA je zapříčiněno rovněž rostoucím zájem vlád, soudců a donucovacích orgánů o používání biotechnologií při vyšetřování trestných činů. Kvůli spolehlivosti srovnání DNA a skutečnosti, že vzorky DNA lze získat bez vědomí subjektu údajů, řada členských států postupem času vytvořila centrální databáze profilů DNA odsouzených osob a vzorků nalezených na místě spáchání trestného činu, nebo zahájila iniciativy k vytvoření takovýchto databází.

V květnu 2005 podepsalo sedm členských států dohodu známou jako „Prümská smlouva“ o posílení spolupráce v oblasti vyšetřování trestných činů a soudnictví prostřednictvím výměny informací. Smlouva zavádí nové základy spolupráce, jelikož signatářům uděluje určitá práva na přístup do vnitrostátních databází DNA v rámci represivních opatření (stíhání trestných činů), k údajům o otiscích prstů, osobním údajům a jiným informacím a rovněž k údajům o registraci vozidla. Od té doby se k této smlouvě připojily další členské státy a základní prvky smlouvy byly zahrnuty do rozhodnutí Rady 2008/615/SVV.

Na základě tohoto právního rámce řada členských států EU má nebo brzy bude mít funkční vnitrostátní databázi profilů DNA odsouzených osob a důkazů z místa spáchání trestného činu, což vyvolává určité obavy ohledně tohoto zvláštního zpracovávání údajů.

Jedním z hlavních problémů spojených s vytvářením databází DNA je skutečnost, že genetické údaje získané ze vzorků DNA (lokusů) mohou odhalit (nikoli okamžitě ve fázi sběru) informace související se zdravotním stavem, predispozicí k určitým onemocněním nebo etnickým původem. Z tohoto důvodu vyvolává vytváření databází DNA značné riziko z hlediska lidské důstojnosti a základních práv. Toto riziko bylo posouzeno v usnesení Rady 2009/C 296/01. Existují zvláštní předpisy o omezení analýzy DNA na ty úseky chromozómů, jež neosahují žádnou genovou expresi, a to pomocí zvláštního souboru markerů DNA, o nichž není známo, že by obsahovaly informace o konkrétních dědičných znacích (to je známo rovněž jako tzv. „ESS" – evropský standardní soubor).

Možnost, že některý ze získaných markerů obsažených ve vnitrostátní databázi DNA může v budoucnu odhalit určité dědičné znaky či jiné citlivé informace, však vyžaduje, aby byla vývoji v oblasti biologie věnována trvalá pozornost s tím, že v tomto politováníhodném případě by měly být některé z informací v databázi neprodleně vymazány. Jelikož databáze DNA shromažďují profily odsouzených osob, měla by být statistická analýza údajů přísně omezena s cílem zabránit vytváření profilů podle pohlaví nebo rasového původu.

Co se týká databází DNA pro účely policie a trestního soudnictví, Evropský soud pro lidská práva rozhodl, že je nutno jasně rozlišovat mezi zpracováváním osobních údajů a genetickými profily podezřelých osob a osob usvědčených ze spáchání trestného činu[16].

Existuje rovněž potenciální riziko použití analýzy DNA k identifikaci rodinných příslušníků nebo příbuzných, kteří mají nějakou spojitost s nevyřešeným trestným činem či odsouzenými osobami, jelikož profily DNA lze v databázi vyhledávat pomocí dílčích souborů markerů nebo zástupných znaků. Tato funkce nastoluje otázku důsledků v souvislosti s informacemi získanými při vyhledávání rodinných příslušníků.

Je nutno rovněž zmínit, že existují zvláštní rizika spojená s používáním souborů údajů o genomech v rámci výzkumu. Pracovní skupina se domnívá, že by přístup ke vzorkům a údajům měl být důsledně omezen na výzkumné pracovníky a měl by být povolen pouze za účelem výzkumu; mimoto je nutné objasnit, za jakých podmínek budou zjištění a výsledky výzkumu sděleny jednotlivcům (s přihlédnutím rovněž k jejich právu nevědět) nebo zahrnuty do zdravotnických záznamů.

Rizika z hlediska ochrany údajů, která jsou spojená s používáním DNA jako biometrického údaje, lze popsat takto:

- Přesnost: Ačkoliv DNA zajišťuje vysokou míru přesnosti, je nutno vzít v úvahu skutečnost, že to závisí na počtu analyzovaných markerů (lokusů). Testovací systémy by měly zajistit co nejvyšší míru přesnosti.

- Dopad: Používání DNA lze považovat za mimořádně narušující soukromí jednotlivce. Genetické údaje mohou odhalit citlivé informace. Statistickou analýzu údajů lze použít rovněž k vytváření profilů a to může mít diskriminační dopady na dotčené osoby.

- Další účel nebo účely zpracování: Nové technologie nyní umožňují výměnu většího množství údajů. Z tohoto důvodu musí být jasné, kdo může mít přístup k databázi DNA. Vyhledávání rodinných příslušníků nebo zaměření se na určitou rasu lze

[16] Evropský soud pro lidská práva, rozsudek ze dne 4.12.2008, S. a Marper v. Spojené království (žaloby č. 30562/04 a 30566/04), zejména bod 125.

považovat za novou technologii, která zpochybňuje původní účel zpracování v databázích DNA, jež jsou dostupné v současnosti.

- Souhlas a transparentnost: V současnosti jsou nabízeny služby týkající se provedení analýzy DNA z biologických vzorků zaslaných poštou (např. sliny), jejichž výsledky jsou poskytovány prostřednictvím internetu. Nedostatečné kontroly identity by mohly jednotlivcům nebo subjektům umožnit, aby poskytli vzorky jiných fyzických osob a získali tak citlivé osobní údaje o jiných lidech.

- Spojitelnost: Vzhledem k množství a rozmanitosti informací, které lze získat ze sekvenování DNA, skýtá DNA vysokou možnost zneužití, jelikož získané údaje lze snadno spojovat s jinými databázemi, což umožňuje vytváření profilů jednotlivců. Vyhledávání rodinných příslušníků umožňuje vytváření spojení s příbuznými osobami.

- Zpracovávání citlivých údajů: DNA může poskytnut informace o zdravotním stavu, predispozicích k určitým onemocněním nebo etnickém původu jednotlivce. Při výběru příslušných lokusů je proto nanejvýš důležité použití zásady minimalizace údajů. Údaje o DNA lze z mnoha vzorků získávat delší dobu, proto se doporučuje zajistit, aby byl přístup k vzorkům důsledně omezen na oprávněné uživatele a pouze pro povolená použití.

- Zrušitelnost: DNA nelze zrušit.

- Ochrana proti falšování: DNA lze velmi obtížně zfalšovat, v mnoha případech však není těžké získat vzorky DNA určité osoby (např. vlasy) bez jejího vědomí.

4.4.6. Biometrie podpisu

Biometrii podpisu lze považovat za příklad nového použití tradičních biometrických technologií. Biometrií podpisu se rozumí biometrické techniky založené na behaviorálních rysech, které měří chování určité osoby vyjádřené dynamikou vlastnoručního podpisu. Zatímco tradiční rozpoznávání podpisu závisí na analýze statických nebo geometrických znaků vizuální podoby podpisu (to, jak podpis vypadá), biometrie podpisu se místo toho vztahuje na analýzu dynamických znaků podpisu (jak byl podpis proveden), proto se na tyto techniky často odkazuje jako na „dynamický podpis“.

K typickým dynamickým znakům měřeným systémem pro biometrii podpisu (např. digitalizačním tabletem) patří intenzita tlaku, úhel psaní, rychlost a zrychlení pera, formování písmen, sklon písma a jiné jedinečné dynamické znaky. Tyto znaky se mezi jednotlivými dodavateli velmi liší, pokud jde a použití a význam, a obvykle jsou získávány pomocí přístrojů citlivých na dotyk. Některá zařízení pro rozpoznávání podpisu mohou provádět ověření pomocí kombinované analýzy statistických znaků (vizuální podoba) i dynamických znaků podpisu (tlak, úhel, rychlost atd.).

Rizika z hlediska ochrany údajů, která jsou spojená s používáním biometrie podpisu, lze popsat takto:

- Přesnost: Lidé se nemusí podepisovat vždy stejně, takže se během registrace a rovněž při ověřování totožnosti mohou setkat s problémy.

- Dopad: Biometrické údaje založené na behaviorálních rysech, jako je podpis, nemusí být v čase jedinečné a subjekt údajů je může měnit. Změny podpisu mohou mít často

rovněž fyziologickou příčinu a mohou vylučovat úspěšné ověření, což vyvolává potřebu alternativních postupů k ověření totožnosti jednotlivců.

- Ochrana před falšováním: Zatímco grafickou podobu tradičního podpisu může zkušená osoba snadno napodobit a padělat, při použití fotokopie nebo programového vybavení pro počítačovou grafiku je dynamický podpis bezpečnější, jelikož proces ověřování kontroluje rovněž dynamické znaky, které jsou složité a jsou specifické pro rukopis dotyčné osoby.

5. Obecné pokyny, doporučení pro odvětví a technická a organizační opatření

Zavedení biometrického systému spočívá ve spolupráci řady subjektů:

- výrobci: navrhují a testují biometrické snímače a stanoví výkonnost biometrických technologií;
- integrátoři: navrhují konečný produkt, který se bude prodávat zákazníkům: vybírají biometrickou technologii a částečně stanoví účely systému (volbou zákazníků, na něž se zaměří);
- prodejci: prodávají konečný produkt zákazníkům; obvykle zákazníky informují o výkonnosti, rizicích a případně právním rámci;
- instalátoři: instalují produkt v prostorách zákazníka;
- zákazníci: rozhodují o koupi biometrického systému: stanoví účel a prostředky zpracování, a jsou proto správci údajů;
- subjekty údajů: poskytují biometrické údaje používané systémem.

Některé subjekty plní jednu či více výše popsaných úloh. Každá úloha odpovídá za zajištění takového používání biometrických systémů, které zaručuje ochranu soukromí: instalátor nesmí například zavést bezpečnostní funkci, kterou nestanovil integrátor.

5.1. Obecné zásady

Co se týká biometrických údajů, prvořadým zájmem by měla být bezpečnost, jelikož biometrické údaje jsou nezrušitelné: narušení bezpečnosti biometrických údajů proto ohrožuje další bezpečné používání biometrických údajů jako identifikátoru a právo dotčených osob na ochranu údajů, jelikož ty nemají možnost zmírnit dopady tohoto narušení.

Rizika se zvyšují s počtem aplikací používajících tyto údaje (zejména riziko narušení bezpečnosti a využití k jiným účelům). Čím více biometrických údajů se používá, tím je pravděpodobnější jejich zcizení.

Pracovní skupina uznává stávající tendenci umožňovat dálkový přístup k biometrickým systémům, například rozhraní poskytovaná na internetu. Tato tendence vyvolává nové bezpečnostní problémy, z nichž mnohé jsou odvětví IT dobře známy. Zavádění takového systému by mělo zahrnovat účast odpovídajícího technického bezpečnostního personálu z odvětví IT již v počáteční fázi navrhování.

Při zpracovávání biometrických údajů pracovní skupina doporučuje vysokou úroveň technické ochrany s využitím nejnovějších technických možností. V tomto ohledu doporučuje pracovní skupina níže uvedené odvětvové normy pro ochranu systémů, v nichž se zpracovávají biometrické údaje.

5.2. Ochrana soukromí již od návrhu

Ochrana soukromí již od návrhu je koncepce aktivního zabudování ochrany soukromí do samotné technologie.

Co se týká biometrických systémů, ochrana soukromí již od návrhu se týká celého hodnotového řetězce biometrických systémů:

- výrobci by měli zásady ochrany soukromí již od návrhu uplatňovat při navrhování nových technologií a snímačů: to může zahrnovat automatický výmaz prvotních údajů po vytvoření šablony nebo používání kódování při uchovávání biometrických údajů (ať už v centrální databázi nebo na inteligentní kartě). Výrobci by se měli soustředit rovněž na rozvoj biometrických technologií, které zajišťují ochranu soukromí;
- integrátoři a prodejci by měli zásady ochrany soukromí již od návrhu uplatňovat při definování konečného produktu, který se bude prodávat, a to volbou technologií zajišťujících ochranu soukromí a připojením bezpečnostních opatření ke konečnému produktu, například decentralizované databáze;
- zákazníci (potenciální správci údajů) by měli zásady ochrany soukromí již od návrhu uplatňovat tehdy, když požadují určitý biometrický systém nebo stanoví technické parametry systému. V tomto případě by výrobci a integrátoři měli ve svém produktu umožnit určitou míru flexibility, aby bylo možno dodržet zásady přiměřenosti, omezení účelu, minimalizace údajů a bezpečnosti.

Tyto zásady již byly do některých biometrických zařízení úspěšně zavedeny: někteří výrobci zabudovali zvláštní kódovací funkce čteček biometrických údajů a spínače zamezující vytažení a manipulaci s cílem zabránit neoprávněnému přístupu k biometrickým údajům.

Pracovní skupina doporučuje, aby byly biometrické systémy navrhovány v souladu s formálním „životním cyklem vývoje“, který zahrnuje tyto kroky:

1. specifikaci požadavků na základě analýzy rizik a/nebo zvláštního posouzení dopadů na soukromí;
2. popis a odůvodnění toho, jak návrh splňuje požadavky;
3. validaci pomocí funkčních a bezpečnostních zkoušek;
4. ověření shody konečného návrhu s regulačním rámcem.

Pracovní skupina podporuje zavedení systémů certifikace, které by mohly zajistit uplatňování zásady ochrany soukromí již od návrhu a posílit informování správců údajů o rizicích z hlediska ochrany údajů, která jsou spojena s biometrickými systémy.

5.3. Rámec pro posuzování dopadů na soukromí

5.3.1. Obecné zásady

Posuzování dopadů na soukromí je proces, v jehož rámci určitý subjekt hodnotí rizika spojená se zpracováváním osobních údajů a stanoví dodatečná opatření, která mají tato rizika snížit. V případě technologie RFID pracovní skupina například stanovila, že subjekt, který stanoví použití, odpovídá za provedení posouzení dopadů na soukromí. Tímto subjektem může být správce údajů nebo poskytovatel, který navrhuje aplikaci RFID.

Vzhledem k zvláštním rizikům spojeným s používáním biometrických údajů pracovní skupina doporučuje, aby subjekt, který stanoví účel a možnosti zařízení, provedl posouzení dopadů na soukromí jako nedílnou součást fáze navrhování systémů používajících tento druh údajů. Tímto subjektem může být výrobce, integrátor nebo konečný zákazník.

Posouzení dopadů na soukromí by mělo vzít v úvahu:

- povahu shromažďovaných údajů,
- účel shromažďovaných údajů,
- přesnost systému, přičemž se předpokládá, že ze shody/neshody určitého biometrického prvku mohou pro jednotlivce vyplývat důležitá rozhodnutí,
- právní základ a dodržování právních předpisů; je zapotřebí souhlas?,
- přístup k zařízení a interní a externí sdílení informací v rámci organizace správce údajů, což bude znamenat bezpečnostní metody a postupy k ochraně osobních údajů před neoprávněným přístupem,
- opatření méně narušující soukromí, která již byla přijata. Existuje alternativa biometrického zařízení (např. žádost o předložení průkazu totožnosti)?,
- rozhodnutí přijatá s ohledem na dobu uchovávání a výmaz údajů. Jaká je příslušná lhůta? Jsou všechny údaje získány pro stejné období? Existuje mechanismus automatického rozhodování a vhodný náhradní postup?,
- práva subjektu údajů.

Posouzení dopadů na soukromí by se nemělo zaměřovat pouze na zjištění rizik, nýbrž by mělo zajistit rovněž přiměřená opatření k ochraně údajů a to, aby správce údajů navrhl vhodná řešení k zmírnění rizik z hlediska ochrany údajů, která byla určena v předchozím oddíle.

Poté, co výrobce nebo integrátor provedl posouzení dopadů na soukromí, může zavedení biometrického systému vyžadovat rovněž dodatečné posouzení s cílem zohlednit zvláštnosti správce údajů. Je-li například biometrický systém začleněn do informačního systému zákazníka, měl by zákazník provést dodatečné posouzení dopadů na soukromí, které zohledňuje jeho vlastní bezpečnostní opatření a postupy v oblasti IT.

5.3.2. Zvláštnosti biometrických údajů

Biometrické údaje vyžadují zvláštní pozornost, jelikož pomocí jedinečných behaviorálních nebo fyziologických rysů jednoznačně identifikují jednotlivce.

Z tohoto důvodu by posouzení dopadů na soukromí mělo usilovat o vyhodnocení toho, jak lze prostřednictvím analyzovaného systému zamezit níže uvedeným třem rizikům, nebo je významně omezit.

Prvním rizikem je zneužití identity, zejména v případě identifikace a autentizace. Biometrické zařízení by nemělo být oklamáno falešným pokusem a mělo by zajistit, aby osoba, která se pokouší provést porovnání, byla skutečně osobou, která je zaregistrována v systému. Tato hrozba se jeví jako méně významná u biometrických údajů, které nelze získat bez vědomí subjektu údajů, jako je struktura žil[17]. U zařízení pro rozpoznávání otisků prstů nebo obličeje to však představuje velký problém. Otisky prstů jsou zanechávány všude po pouhém dotyku určitého předmětu. Obličej může být zachycen na fotografii, aniž by si toho byla dotyčná osoba vědoma.

Druhým rizikem je změna účelu, a to buď ze strany samotného správce údajů, nebo třetí osoby, včetně donucovacích orgánů. Tato běžná hrozba pro osobní údaje je v případě používání biometrických údajů zcela zásadní. Výrobci by měli přijmout veškerá bezpečnostní

[17] I když lze obtížně předvídat, jaké útoky na technologii k rozpoznávání struktury žil budou možné v budoucnu, pokud se bude tato technologie používat šířeji.

opatření, aby zamezili nepatřičnému použití údajů, a zajistit, aby údaje, které již nejsou zapotřebí pro účely zpracování, byly neprodleně vymazány.

Stejně jako u ostatních údajů nesmí být legitimně zpracovávané nebo uchovávané biometrické údaje nebo zdroje biometrických údajů správcem zpracovávány nebo zaregistrovány pro nový či jiný účel, ledaže pro toto nové zpracování údajů existuje nový legitimní důvod.

Třetím rizikem je narušení bezpečnosti údajů, které v souvislosti s biometrickými údaji vyžaduje zvláštní opatření v závislosti na druhu údajů, které byly narušeny. Pokud se používá systém vytvářející biometrické údaje na základě algoritmu, který přeměňuje biometrickou šablonu na určitý kód, a jsou-li zcizeny nebo narušeny biometrické údaje nebo algoritmus, je nutno je nahradit. Jestliže narušení bezpečnosti údajů zahrnuje ztrátu přímo identifikovaných biometrických údajů, které jsou velmi blízko zdroji biometrických údajů, jako jsou snímky obličeje nebo otisky prstů, musí být dotyčná osoba podrobně informována, aby se mohla hájit v případě možného budoucího incidentu, kdy tyto narušené biometrické údaje mohou být použity proti ní jako důkaz.

5.4. Technická a organizační opatření

Zpracovávání biometrických údajů vyžaduje kvůli jejich povaze zvláštní technická a organizační opatření, jakož i bezpečnostní opatření, která zabrání nepříznivým dopadům na subjekt údajů v případě narušení bezpečnosti údajů – zejména kvůli riziku protiprávního jednání, které má za následek neoprávněnou „rekonstrukci“ biometrických prvků z referenční šablony, jejich propojení s různými databázemi, jejich další „použití“ bez vědomí subjektů údajů k účelům neslučitelným s původními účely a/nebo možnosti, že by některé biometrické údaje mohly být použity k odhalení informací o rasovém původu nebo zdravotním stavu subjektů údajů.

5.4.1. Technická opatření

- *Používání biometrických šablon*

Biometrické údaje by měly být pokud možno uchovávány jako biometrické šablony.

Šablona by měla být získána způsobem, který je specifický pro daný biometrický systém, a neměli by ji používat jiní správci podobných systémů, aby bylo zajištěno, že určitá osoba může být identifikována jen v těch biometrických systémech, které mají právní základ pro tento úkon.

- *Uchovávání v osobním přístroji oproti centrálnímu uchovávání*

Je-li povoleno zpracovávání biometrických údajů, upřednostňuje se vyhnout se centrálnímu uchovávání osobních biometrických údajů.

Zejména v případě ověřování totožnosti považuje pracovní skupina za vhodné, aby byly biometrické systémy založeny na čtení biometrických údajů uložených jako kódované šablony na médiích, která mají v držení výhradně příslušné subjekty údajů (např. inteligentní karty nebo podobná zařízení). Jejich biometrické prvky lze se šablonou nebo šablonami uloženými na kartě a/nebo v zařízení porovnat prostřednictvím běžných postupů srovnání, které jsou zavedeny přímo na dotyčné kartě a/nebo v zařízení, přičemž by se mělo obecně a pokud možno zamezit vytvoření databáze obsahující biometrické údaje. Je-li karta a/nebo zařízení ztraceno či založeno, existují omezená rizika zneužití biometrických údajů, které jsou v nich obsaženy. K snížení rizika krádeže identity by v těchto zařízeních měly být uchovávány omezené identifikační údaje týkající se subjektu údajů.

Pro zvláštní účely a v případě objektivní potřeby však lze centrální databázi obsahující biometrické údaje a/nebo šablony považovat za přípustnou. Použitý biometrický systém a zvolená bezpečnostní opatření by měla zmíněná rizika omezovat a zajistit, aby nebylo možné opětovné použití dotyčných biometrických údajů pro další účely, nebo aby bylo alespoň vysledovatelné. Měly by se používat mechanismy založené na šifrovacích technologiích, aby se zamezilo neoprávněnému čtení, kopírování, změně nebo odstranění biometrických údajů.

Pokud jsou biometrické údaje uloženy v zařízení, které fyzicky kontroluje subjekt údajů, měl by se u čtečky používat zvláštní kódovací klíč jako účinná záruka ochrany těchto údajů před neoprávněným přístupem. Tyto decentralizované systémy mimoto zajišťují lepší ochranu biometrických údajů již od návrhu, jelikož subjekt údajů má nad svými biometrickými údaji neustále fyzickou kontrolu a neexistuje žádný bod, na nějž by se bylo možno zaměřit nebo jej využít.

Pracovní skupina rovněž zdůrazňuje, že myšlenka centrální databáze zahrnuje širokou škálu technických řešení od uchovávání ve čtečce po databázi na síti.

- *Obnovitelnost a zrušitelnost*

Jelikož se zdroj biometrických údajů nemůže změnit, biometrické systémy, jejichž účelem je zajistit spojení s určitou identitou, musí být navrženy tak, aby proces registrace a zpracovávání biometrických údajů umožňoval, že z téhož zdroje lze získat více nezávislých biometrických šablon, aby je bylo možné v případě narušení bezpečnosti údajů nebo technologického vývoje nahradit.

Biometrické systémy by měly být navrženy tak, aby umožňovaly zrušení spojení s určitou identitou, a to za účelem obnovení nebo trvalého výmazu, například v případě odvolání souhlasu[18].

- *Zakódovaná forma*

Pokud jde o otázku bezpečnosti, je nutno přijmout odpovídající opatření k ochraně údajů uchovávaných a zpracovávaných biometrickým systémem: biometrické údaje musí být vždy uloženy v zakódované formě. Musí být stanoven rámec pro správu klíčů, aby bylo zajištěno, že dekódovací klíče jsou přístupné pouze na základě potřeby vědět.

Vzhledem k rozšířenému používání veřejných a soukromých databází obsahujících biometrické údaje a rostoucí interoperabilitě jednotlivých systémů používajících biometrické údaje by se mělo upřednostňovat používání zvláštních technologií nebo formátů údajů, které znemožňují propojování databází biometrických údajů a nekontrolované sdělování údajů.

[18] Například technologie TURBINE, která má chránit biometrickou šablonu pomocí kryptografické transformace údaje o otisku prstu na nevratný klíč, který umožní porovnání podle jednotlivých bitů. Transformované biometrické údaje nelze vrátit na biometrické vzorky a původní šablony. K zvýšení důvěry uživatelů bude tento klíč zrušitelný, tj. k vydávání biometrických identit lze vygenerovat nový nezávislý klíč. Viz rovněž: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-02-01_FP7_EN.pdf

- *Ochrana před falšováním*

K zachování spolehlivosti biometrického systému a zabránění zneužití identity musí výrobce zavést systémy, jež mají zjišťovat, zda jsou biometrické údaje pravé a spojené s fyzickou osobou. Pokud jde o rozpoznávání obličeje, zásadní může být zjištění, zda je tvář skutečná a zda se nejedná například o fotografii upevněnou na hlavě podvodníka.

- *Kódování a dekódování pomocí biometrických údajů*

Kódování pomocí biometrických údajů je technika, která jako součást kódovacího a dekódovacího algoritmu používá biometrické znaky. V tomto případě se jako klíč pro kódování identifikátoru potřebného pro službu obvykle používá výtah z biometrických údajů.

Tento systém má mnoho výhod[19]. V případě tohoto systému nedochází k uchovávání identifikátoru nebo biometrických údajů: uložen je pouze výsledek identifikátoru zakódovaného pomocí biometrických údajů. Osobní údaje jsou mimoto zrušitelné, jelikož je možné vytvořit jiný identifikátor, který lze rovněž chránit kódováním pomocí biometrických údajů. Tento systém je bezpečnější a jeho používání je pro osoby snazší: řeší problém související s pamatováním dlouhých a složitých hesel.

Překonání problému spojeného s šifrováním však není snadné, jelikož kódování a dekódování není tolerantní k jakýmkoli změnám klíče, zatímco biometrie poskytuje různé znaky, což může vést ke změnám získaného klíče. Systém musí být proto schopen vygenerovat stejný klíč z mírně odlišných biometrických údajů, aniž by se zvýšila míra chybného přijetí.

Pracovní skupina souhlasí s tím, že technologie kódování pomocí biometrických údajů představuje užitečnou oblast pro výzkum a stala se dostatečně vyspělou pro širší politické uvážení, vývoj prototypu a zvážení aplikací.

- *Mechanismy automatického výmazu údajů*

Aby se zabránilo tomu, že biometrické údaje jsou uchovávány déle, než je nutné pro účely, pro které byly shromažďovány nebo následně zpracovávány, je nutno zavést vhodné mechanismy automatického výmazu údajů rovněž v případě, že období uchovávání lze legitimně prodloužit, což zajišťuje včasný výmaz osobních údajů, které již nejsou pro fungování biometrického systému nutné.

V případě použití integrovaného uložení ve čtečce mohou výrobci zavést rovněž uchovávání biometrických šablon v energeticky závislé paměti, což zaručuje, že údaje budou vymazány, jakmile bude čtečka odpojena ze sítě. Je-li čtečka prodána nebo odinstalována, nezůstává tudíž žádná databáze biometrických údajů. K automatickému výmazu údajů v případě, že se někdo pokusí čtečku zcizit, lze použít rovněž spínače zamezující vytažení.

- *Velké databáze biometrických údajů a databáze „se slabou vazbou“*

Některé země používají velké databáze biometrických údajů, a to především ke dvěma účelům: poskytování pomoci při vyšetřování trestných činů a zabezpečení vydávání dokladů totožnosti (cestovní pasy, průkazy totožnosti, řidičské průkazy). Databáze používané k vyšetřování trestných činů obvykle shromažďují informace o pachatelích trestných činů a podezřelých osobách a musí být navrženy tak, aby identifikovaly určitou osobu pomocí biometrických údajů. Naopak databáze používané v boji proti zneužití identity obsahují biometrické údaje veškerého obyvatelstva a měly by se používat pouze k autentizaci osoby

[19] http://www.ipc.on.ca/images/resources/bio-encryp.pdf

(například v případě, že určitá osoba ztratí své doklady nebo zničila zabezpečený čip cestovního pasu, na němž jsou uloženy biometrické údaje).

Pokud se centrální databáze používá za účelem boje proti zneužití identity, pracovní skupina se domnívá, že je nutno zavést technická opatření, aby se zamezilo změně účelu. Za prvé, zásada minimalizace údajů vyžaduje, aby byly shromažďovány pouze údaje potřebné k autentizaci osoby. Usuzuje se například, že k autentizaci určité osoby je dostatečně přesné srovnání otisků dvou prstů.

Správci údajů mohou používat rovněž databáze se „slabou vazbou", kde identita osoby není spojena s jedním souborem biometrických údajů, nýbrž se skupinou souborů biometrických údajů. Návrh databáze by měl zaručit autentizaci osoby s velmi vysokou pravděpodobností (např. 99,9 %, což dostatečně odrazuje podvodníky) a zajistit, aby databázi nebylo možno použít k identifikaci (jelikož jeden soubor biometrických údajů odpovídá vysokému počtu osob).

Pracovní skupina podporuje používání takových systémů v případě, že se velké databáze biometrických údajů používají k boji proti zneužití identity.

Příklad: Technická opatření u systému autentizace
Zdroj biometrických údajů je jedinečný a je potenciálně celoživotně spojený se subjektem údajů. Pokud se používá jako základ pro systémy autentizace, je třeba mít na paměti, že nemůže být změněn, zatímco v případě běžných technologií autentizace, které obvykle vyžadují „znalost nebo vlastnictví" přístupových údajů (např. identifikační číslo uživatele, heslo), je možná změna těchto přístupových údajů. Systémy používající biometrickou autentizaci proto musí zavést zvláštní ochranná opatření s cílem chránit spojení mezi biometrickými údaji a jinými údaji o identitě:
– Údaje šablony by neměly být uchovávány centrálně, jelikož bezpečnost uchovávání biometrických údajů má zásadní význam pro celkovou bezpečnost biometrického systému. Mělo by se upřednostnit distribuované uložení (např. na inteligentní kartě). V tomto případě má subjekt údajů u sebe zdroj údajů i šablonu.
– Uchovávání a předávání biometrických údajů je nutno chránit pomocí vhodných šifrovacích technologií před zachycením, neoprávněným sdělením a změnou.
– Některé druhy biometrických údajů nejsou tajné (např. obličej) a v případě narušení bezpečnosti, sdělení nebo zneužití údajů je nelze zablokovat ani změnit. V důsledku toho by autentizace měla být spojena s jinými přístupovými údaji, které lze zablokovat nebo změnit.

5.4.2. Organizační opatření

K zaručení ochrany údajů je nutno naplánovat a provést organizační opatření. Správce údajů musí například stanovit jednoznačný postup, pokud jde o to, kdo má přístup k údajům v systému, je-li přístup částečný, či nikoli a z jakých důvodů. Všechny úkony bude nutno sledovat.

Pracovní skupina podotýká, že tyto úkoly lze zadat externím poskytovatelům služeb, včetně v případě žádostí o vízum (články 13 a 43 nařízení (ES) č. 810/2009 ze dne 13. července 2009 o kodexu Společenství o vízech), a toto řešení je stále oblíbenější kvůli častějšímu využívání cloudových úložišť.

V tomto případě musí správce údajů stanovit podrobnou politiku týkající se způsobů kontroly dodavatelů, jako jsou neočekávané kontroly, a požadovat záruky, pokud jde o zaměstnance, postup týkající se práv jednotlivce atd.

V Bruselu dne 27. dubna 2012

Za pracovní skupinu
předseda
Jacob KOHNSTAMM