

Zádrhele biometrického podpisu

LENKA HANKOVÁ

Ať chceme nebo ne, technologie využívající biometrické údaje se staly výrazným prvkem současného světa a našly si svoje místo v řadě odvětví. Má to však různá úskalí.



Biometrii by bylo možné velmi zjednodušeně charakterizovat jako automatizovaný způsob měření, zaznamenávání a rozpoznávání určitých jedinečných vlastností osob sloužících k identifikaci, potažmo ověření totožnosti (autentizaci) takové osoby. Může jít jak o fyzické vlastnosti (rysy tváře, podoba otisku prstu či dlaně, sítnice apod.), tak o vlastnosti chování osoby (např. způsob podepisování, hlasu, chůze).

Jedním ze způsobů využití biometrie je i tzv. dynamický biometrický podpis. Při podepisování na signpadu toto zařízení snímá a zaznamenává nejen samotný obraz (tvar) vlastnoručního podpisu, ale také jeho rychlost, zdvih,

Computerworld s využitím Dall-E

Dynamický biometrický podpis (DBP) není v českém právním řádu přímo definován ani regulován, což je bohužel kámen úrazu.

načasování, tlak, směr či další charakteristiky. Všechna tato data jsou pak zjednodušeně řečeno zašifrována a v podobě „balíčku“ uložena společně s podpisem.

Tento technologický proces je přitom třeba odlišit od pořízení pouhého grafického obrazu podpisu bez uvedených vlastností a stejně tak od elektronického podpisu, který je doprovázen biometrickou autentizací (ověřením totožnosti) a následnou autorizací (udělení oprávnění k nějakému jednání). Jako typický příklad v tomto směru můžeme uvést zadání příkazu k úhradě v elektronickém bankovníctví, kdy se ověří totožnost jednatelova užítím otisku prstu a potvrdí zadání příkazu.

Data na zlatém podnose

Dynamický biometrický podpis (DBP) není v českém právním řádu přímo definován ani regulován, což je bohužel kámen úrazu. Lze jej nicméně zařadit mezi tzv. elektronické podpisy. Ty jsou obecně právně vymezeny v evropském nařízení eIDAS (nařízení EU č. 910/2014) ve třech kategoriích jako tzv. prostý, zaručený a kvalifikovaný podpis.

Odborníci se přitom nemohou shodnout, zda DBP lze považovat za prostý elektronický podpis (spadal by tak do stejného „pytle“ jako obyčejné zaškrtnutí checkboxu nebo obrázek podpisu), nebo je již na úrovni zaručeného elektronického podpisu (tedy podpisu založeného na určitém certifikátu, který však není vydán oficiální certifikační autoritou). Z důkazního hlediska je i přesto DBP poměrně výjimečný.

Na rozdíl od vlastnoručního podpisu, kdy znalci z oboru písomoznalství musejí složité podpisy zkoumat a porovnávat, u DBP dostanou data o charakteristických vlastnostech podpisu téměř na „zlatém podnose“ v jednom balíčku. Objevují se tedy názory, že lze DBP považovat za podpis rovnocenný vlastnoručnímu. Bohužel však toto konstatování v právním řádu chybí.

Rozšířenějšímu použití DBP vystavil pomyslnou stopku také Úřad pro ochranu osobních údajů (ÚOOÚ). Ten považuje údaje o vlastnostech podpisu u DBP za tzv. biometrické osobní údaje ve smyslu čl. 4 odst. 14 nařízení GDPR (nařízení EU č. 2016/679), které jsou definovány jako „osobní údaje vyplývající z konkrétního technického zpracování, týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje“. Ty jsou přitom řazeny mezi vysoce chráněnou zvláštní kategorii (citlivých) osobních údajů.

V rozporu s GDPR

V roce 2019 Úřad pro ochranu osobních údajů (ÚOOÚ) vydal diskutabilní rozhodnutí (č. j. ÚOOÚ-10138/18-8 ze dne 21. 3. 2019), ve kterém shledal použití biometrického podpisu u elektronické úvěrové dokumentace mezi finanční institucí a jejím klientem v rozporu s GDPR.

Bylo konstatováno, že „pro účely uzavření a uchování smluvní dokumentace není nezbytné využívat dynamický biometrický podpis, neboť v případě podpisu dokumentů v listinné podobě není také vyžadován a jako dostatečný je pro stanovené účely prostý obraz podpisu klienta na dematerializované smluvní dokumentaci, který je srovnatelný s podpisem na smluvní dokumentaci v listinné podobě.“ Podle názoru ÚOOÚ tak byla porušena zásada „minimalizace“ osobních údajů, která ve zkratce znamená, že pokud příslušné osobní údaje vysloveně nepotřebují pro daný účel (v tomto případě pro podpis smlouvy), nesmím je vůbec mít.

ÚOOÚ uvedl, že jsou-li biometrické údaje zpracovávány za účelem jedinečné identifikace fyzické osoby, jde právě o zpracování zvláštní kategorie osobních údajů podle čl. 9 odst. 1 GDPR. Podle

Zavedení dynamického biometrického podpisu do praxe bude vyžadovat důkladnější zamyšlení a nebude možné jej zavést pro běžné podepisování, kde by stačil jednoduchý podpis na papíře nebo obrázek na signpadu.

Computerworld s využitím Dall-E

tohoto ustanovení je zakázáno takové údaje zpracovávat s výjimkou stanovených případů. Jedním z nich je sice podle čl. 9 odst. 2 písm. a) GDPR udělení výslovného souhlasu subjektu údajů s takovým zpracováním, čímž sice finanční instituce disponovala, ale v tomto případě to pro ÚOOÚ nebylo rozhodné.

Kritika odborníků

Citované rozhodnutí se stalo záhy terčem kritiky řady odborníků, kteří namítali, že údaje o charakteristice podpisu nemohou být biometrickými údaji ve smyslu GDPR, neboť tyto údaje nejsou zpracovávány za účelem jedinečné identifikace podepisujícího (ten je již předtím identifikován řadou jiných údajů), ale pouze pro účely podepsání dokumentu. Pro další identifikaci již pak správcem (tedy finanční institucí) nejsou používány, maximálně v případě sporu u soudu pro účely vytvoření znaleckého posudku na pravost podpisu. Odborníci taktéž zpochybnili názor ÚOOÚ o porušení zásady minimalizace v tom smyslu, že právě skutečnost, kdy biometrický podpis není nutnou a povinnou podmínkou pro dané jednání (naopak může subjekt využít klasický podpis na listině), je

výrazem svobody subjektu při udělení souhlasu.

Shora uvedené rozhodnutí ÚOOÚ, které nebylo dosud překonáno ani nijak dále rozvedeno, ještě zcela neznamená, že by DBP nebylo možné používat vůbec. Jeho zavedení v praxi však bude vyžadovat důkladnější zamyšlení a nebude možné jej zavést pro běžné podepisování, kde by stačil jednoduchý podpis na papíře nebo obrázek na signpadu. Nadto půjde o náročný proces i po stránce bezpečnostní a dokumentační.

Možná je potom už skutečně praktičtější zvolit jiné alternativy digitálního podepisování, které se mezitím vytvořily. V závěru pak může být výsledek stejný v podobě platného právního jednání, kdy přitom fyzické osoby nemusejí rozdávat své biometrické údaje na potkání každému. Pomalu, ale jistě si s příchodem eIDAS totiž razí cestu českými soudy i prostý elektronický podpis, byť ale ani ten nemá u některých právních jednání na různých ustláno a ne vždy vyhoví formalistickým požadavkům zákona, resp. soudců na písemnost právního jednání. Ale to už je zase jiný příběh. ■

Autorka je advokátka, Rōdl & Partner, advokáti

