Eva Kostrecová

Potreba ochrany osobných údajov z právneho hľadiska

Anotácia: Elektronická podpora každodenných činností ľudí na celom svete si z dôvodu ich identifikácie vyžaduje nahrávať, spracúvať a udržiavať osobné dáta v databázach rôznych štátnych i súkromných inštitúcií. Obchodné, bankové, poisťovacie a iné operácie sú realizované prostredníctvom informačno-komunikačných prostriedkov, ktoré sú lokalizované v rôznych krajinách, odlišných od miesta bydliska, pôsobiska, či pobytu aktérov operácie. Jednoducho povedané, informatika nepozná hranice štátov, preto vzniká potreba legislatívne chrániť súkromie jednotlivca. Príspevok predstavuje legislatívne rámce prijaté v tejto oblasti Radou Európy, inštitúciami EÚ, ale aj Nemecka, Švajčiarska, Francúzska a Slovenskej republiky. Súčasne približuje všeobecné IT pravidlá využívané pri ochrane údajov.

Kľúčové slová: Anonymizácia, dohovory, inštitúcie EÚ, vládne inštitúcie a orgány Francúzska/Nemecka/Švajčiarska, ochrana osobných údajov, pseudonymizácia, Rada Európy, smernice, zákony.

1. *Požiadavky na ochranu a právny vývoj prijatý Radou Európy*

Dohovor Rady Európy o ochrane osobných údajov (STE n° 108)[1] z 28. januára 1981 bol prvým medzinárodne právne záväzným nástrojom v oblasti ochrany údajov, ktorý bol otvorený na pristúpenie aj pre nečlenské štáty Rady Európy. Podľa dohovoru musia zmluvné strany prijať potrebné opatrenia vo vnútroštátnom práve a aplikovať v nich také princípy, aby na ich území bolo zabezpečené dodržiavanie základných práv ľudského jedinca vo vzťahu k spracúvaniu a ochrane osobných údajov. Stanovuje aj konkrétne zásady, v zmysle ktorých môžu byť osobné údaje zhromažďované a používané iba na vopred presne definovaný účel. Musia byť presné, primerané uvedenému cieľu a ukladané iba na čas potrebný na realizáciu tohto cieľa.

Článok 1 dohovoru ustanovuje, že: „Cieľom dohovoru je zabezpečiť, aby na území každej zmluvnej strany, ktorá dohovor podpísala, boli pri automatizovanom spracúvaní osobných údajov u každej fyzickej osoby, bez ohľadu na jej národnosť alebo trvalý pobyt, rešpektované jej základné práva a slobody, najmä jej právo na súkromie.“[2]

Dohovor tiež stanovuje právo každej fyzickej osobe na prístup k svojim údajom, ako aj možnosť ich opravy a vyžaduje špeciálnu ochranu citlivých údajov (napr. formou pseudonymizácie), najmä údajov o náboženskej a politickej príslušnosti a medicínskych a genetických dát.

Dodatkový protokol k Dohovoru n° 108 o dozorných orgánoch a cezhraničnom toku údajov (STE n° 181)[3], ktorý bol podpísaný 8. novembra 2001 v Štrasburgu, vyžaduje, aby členské štáty zriadili dozorné orgány, ktoré by vykonávali svoje kontrolné aktivity úplne nezávisle a boli účinným ochranným nástrojom fyzických osôb pri spracúvaní osobných údajov. S rozvojom internetu a elektronických aktivít obyvateľov našej planéty rastie aj výmena osobných údajov cez hranice štátov. Z tohto dôvodu je nevyhnutné prostredníctvom dozorných orgánov zabezpečiť účinnú ochranu ľudských práv a základných slobôd pre každého občana planéty, najmä jeho práva na ochranu súkromia vo vzťahu k takýmto výmenám osobných údajov.

---

[1] http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm

[2] 28/01/1981 Convention pour la protection des données à caractère personnel (STE n° 108), http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm

[3] 08/11/2001 Autorités de contrôle et flux transfrontalier des données (STE n°181), http://conventions.coe.int/Treaty/FR/Treaties/Html/181.htm

2. *Požiadavky na ochranu a právny vývoj v Európskej únii*

Európska únia prijatím dokumentu „Zmeny k Dohovoru STE n° 108 z 15. októbra 1999 (o pristúpení Európskych spoločenstiev k dohovoru)“ vyjadrila svoju vôľu posilniť nielen spoluprácu s Radou Európy, ale súčasne prispieť k posilneniu požiadaviek širokého medzinárodného fóra v oblasti ochrany údajov voči tretím krajinám. Podľa pôvodného textu dohovoru mohli k nemu pristúpiť aj nečlenské štáty Rady Európy, a preto vznikla nevyhnutná potreba a iniciatíva krajín združených v Európskej únii vypracovať zmeny umožňujúce pristúpenie Európskych spoločenstiev k dohovoru. Tieto zmeny boli 15. júna 1999 schválené Výborom ministrov Rady Európy a následne prijaté EÚ.

V súlade s dohovorom Rady Európy prijala v októbri 1995 Európska únia Smernicu Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (95/46/CE)[4], ktorá stanovuje, že spracovanie osobných údajov je prípustné len vtedy, ak je nevyhnutné a potrebné pre konkrétne definované ciele. Táto smernica tiež uvádza, že právo na súkromie a sebaurčenie je chránené najlepším spôsobom vtedy, ak nie sú osobné údaje, pokiaľ je to možné, vôbec zbierané a ukladané. Čo sa týka uplatňovania tejto zásady, Európska komisia podporuje rozvoj a implementáciu metód na zlepšenie ochrany dát, a to najmä v oblasti elektronického obchodovania, možností anonymného prístupu do komunikačných sietí a anonymných spôsobov platieb.[5]

Smernica 95/46/CE predstavuje v oblasti ochrany osobných údajov referenčný legislatívny rámec na európskej úrovni, ktorého cieľom je dosiahnutie rovnováhy medzi vysokou úrovňou ochrany súkromia a voľným pohybom osobných údajov v rámci Európskej únie. Na dosiahnutie tohto cieľa smernica stanovuje prísne limity na zber a využívanie osobných údajov a požaduje vytvorenie nezávislého národného orgánu zodpovedného za ochranu týchto údajov v každom členskom štáte EÚ. K dnešnému dňu už všetky členské štáty transponovali ustanovenia tejto smernice do svojej legislatívy.

Opatrenia prijaté v rámci Európskej únie sú však naďalej nepostačujúce voči súčasným elektronicky šíreným hrozbám, ktoré predstavujú nevyžiadané reklamy a správy (spaming), rôzne vírusy, červy a iné druhy nežiaducich kódov (malware), odcudzovanie a mystifikácia identity (phishing, pharming), odpočúvanie a odchytávanie tokov dát prenášaných po počítačových sieťach (snifing, spoofing), nezákonné šírenie chránených autorských diel (warezing), ale aj „nabúravanie sa“ do počítačov (hacking) a krádež dát alebo zničenie ochrán (cracking). Inštitúcie Európskej únie preto pokračujú vo vedení dialógu o ochrane osobných údajov a v spolupráci s tretími krajinami aj v boji proti týmto hrozbám a proti trestnej činnosti s nimi spojenej.

Cieľom Smernice Európskeho parlamentu a Rady o spracúvaní osobných údajov a ochrane súkromného života v sektore elektronických komunikácií (2002/58/CE)[6] je harmonizácia legislatívnych ustanovení členských štátov potrebných pre zabezpečenie rovnakej úrovne ochrany základných ľudských práv a slobôd, a najmä práva na súkromie, pri spracúvaní osobných údajov v sektore elektronických komunikácií, ako aj voľný pohyb týchto údajov a komunikačných zariadení a služieb v Európskej únii.

3. *Požiadavky na ochranu a právny vývoj v Nemecku*

Nemecký federálny ústavný súd uznal právo na anonymitu občanov Nemecka už v roku 1983 v rozhodnutí o sčítaní ľudu. V tomto rozhodnutí sa v súlade so stanoviskom

[4] Smernica 95/46/CE Európskeho parlamentu a Rady z 24. októbra 1995, publikovaná v JO n° L 281, str. 31
[5] Oznámenie Komisie o elektronickom obchode, COM (97) 157, http://www.cordis.lu/esprit/src/ecomcom.htm
[6] Smernica 2002/58/CU Európskeho parlamentu a Rady z 12. júla 2002, publikovaná v JO n° L 201, str. 37

Ústavného súdu hovorí: „Pre ochranu práva na informačné sebaurčenie, a to najmä vo fáze zberu dát, je nutné dodržiavať zásady účinnej anonymizácie už od prvopočiatku vzniku dát a urobiť nevyhnutné kroky, aby sa zabránilo strate anonymity“.[7]

Rada pre výskum, technologický rozvoj a inovácie[8], ktorá pracuje pod záštitou spolkovej kancelárky a spolkového ministra pre vzdelávanie, vedu, výskum a technológie, vo svojej správe o ochrane údajov konštatuje: „V systémoch, v ktorých sú spracovávané alebo prostredníctvom komunikačných sietí prenášané údaje o ľudských jedincoch, by mala byť venovaná prioritná pozornosť zachovaniu maximálneho stupňa anonymity týchto jedincov.“ Podobné znenia sú uvedené aj v publikáciách Bundestagu a Bundesratu pojednávajúcich o téme "Nemecko smerujúce k informačnej spoločnosti"[9].

V prípade zákonov prijatých v oblasti médií je aj právo na anonymitu už dávno považované za aspekt základného práva ľudského jedinca. Zásada nevytvárania neanonymných dát je tiež zakotvená v zákone o ochrane údajov v telekomunikačných službách (Teledienstdatenschutzgesetz), ktorý je súčasťou zákona o službách spracovania a prenosu informácií, ako aj v Dohode spolkových krajín o mediálnych službách (Mediendienste-Staatsvertrag). Na základe týchto právnych predpisov musia dať poskytovatelia telekomunikačných a mediálnych služieb možnosť svojim zákazníkom používať a uhrádzať služby buď pod úplnou anonymitou, alebo pomocou pseudonymizácie, za predpokladu, že je to možné z technického hľadiska.[10]

4. *Požiadavky na ochranu a právny vývoj vo Švajčiarsku*

Článok 13 Federálnej ústavy a ustanovenia zákona č. 235.1 Švajčiarskej konfederácie o ochrane údajov (LPD) z 19. 6. 1992 ustanovujú, že každá osoba má právo na ochranu svojho súkromného a rodinného života, svojej korešpondencie a spojení, ktoré realizuje prostredníctvom pošty a telekomunikácií, ako aj na ochranu proti nezákonnému použitiu údajov, ktoré patria do sféry jej súkromia. Osobné údaje musia byť spracúvané úplne spoľahlivým spôsobom a nesmú byť ani predávané, ani poskytnuté tretím stranám.

„Osobné údaje musia byť chránené proti akémukoľvek neoprávnenému spracúvaniu vhodnými organizačnými a technickými opatreniami.“[11]

Pravidlá tejto ochrany sú detailnejšie rozpracované vo vykonávacom predpise RS 235.11 k zákonu LPD.[12] Aj ďalšie zákony obsahujú početné ustanovenia o ochrane osobnosti v rôznych špecifických oblastiach. Napríklad články 28 a nasledujúce Švajčiarskeho občianskeho zákonníka (CC)[13] ustanovujú opravné prostriedky použiteľné v prípade porušenia súkromia.

Federálne orgány a inštitúcie úzko spolupracujú so všetkými spracovateľmi dát prostredníctvom monitoringu a pravidelných auditov, aby boli databázy s osobnými údajmi čo možno najlepšie chránené proti útokom zvonku, stratám, zneužitiu a falšovaniu. Súčasne tieto dáta používajú na tvorbu anonymizovaných štatistík a prehľadov na účely hodnotenia

---

[7] (BVerfGE 65, 1-49 Volkszählung), www.bundesverfassungsgericht.de

[8] Rat für Forschung, Technologie und Innovation

[9] Entschließung zu der Empfehlung an den Europäischen Rat „Europa und die globale Informationsgesellschaft“ und zu der Mitteilung der Kommission „Europas Weg in die Informationsgesellschaft: Ein Aktionsplan“, Bundesrat, publication 776/96, 10.10.1996, Bonn

[10] Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IuKDG), Deutscher Bundesrat, Publication 420/97, 13.06.97, Bonn

[11] Art. 7 Sécurité des données, Loi fédérale sur la protection des données (LPD)

[12] Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD)

[13] Code civil suisse (CC)

hospodárskych, demografických, sociálnych a iných ukazovateľov v rámci Švajčiarskej konfederácie.

Federálny zákon zo 6. októbra 2000 o monitorovaní poštových zásielok a telekomunikačných spojení (LSCPT)[14] ukladá zákonnú povinnosť uchovávať údaje o spojení počas najmenej 6 mesiacov. Ustanovenia tohto zákona však nedovoľujú prístup k osobným údajom bez špeciálneho špecificky vymenovaného dôvodu a jeho schválenia príslušným kompetentným orgánom. Už počas nahrávania elektronickej formy osobných dát sú tieto záznamy ukladané do separátnej databázy, z ktorej neexistuje žiadna spojitosť ani prepojenie so súbormi obsahujúcimi každodenne monitorované dáta o telekomunikačných spojeniach a poštových zásielkach.

Od 23. apríla 2001 môže zverejňovať Švajčiarsky Federálny súd na internete všetky jeho rozsudky v plnom znení. Vo všeobecnosti tak robí, čo znamená, že zverejňuje mená zástupcov oboch strán a v niektorých prípadoch aj samotných strán súdneho sporu. Pred akýmkoľvek zverejnením však najprv pristupuje k individuálnemu posúdeniu prípadov, ktoré mu boli pridelené, a zváži najmä záujmy zúčastnených strán. V závislosti od zhodnotenia situácie nemusí byť rozsudok publikovaný vôbec, alebo môže byť publikovaný len čiastočne. Vo väčšine prípadov sú mená zúčastnených strán pred zverejnením odstránené. V obmedzenom počte prípadov, ak tomu nebráni žiadny rozhodujúci súkromný záujem, sú naopak publikované aj mená zúčastnených strán.

V praxi však existuje povinnosť zverejňovať súdne rozhodnutia, pričom je potrebné brať do úvahy ustanovenia zákona o ochrane údajov, ktoré povoľujú zverejňovanie údajov prístupných širokej verejnosti. Z toho vyplýva, že uvedená prax federálneho súdu, t. j. individuálne posúdenie otázky zverejňovania rozsudkov a vážení záujmov zúčastnených strán, je v súlade s ochranou dát. Ak sa dotknutá osoba domnieva, že zverejnenie jej mena v súvislosti s publikáciou rozsudku federálneho súdu môže spôsobiť ujmu na jej osobnosti alebo súkromí, môže sa obrátiť priamo na federálny súd s popisom škôd, ktoré môže utrpieť a požiadať ho, aby publikoval rozsudok výhradne v anonymizovanej forme. Či federálny súd vyhovie tejto žiadosti, alebo odôvodní prevažujúci verejný záujem na neanonymizovanom zverejnení, je posudzované pri každom prípade individuálne.

5. *Požiadavky na ochranu a právny vývoj vo Francúzsku*

Z legislatívneho hľadiska začal vo Francúzsku boj proti nezákonnému zberu, ukladaniu a spracúvaniu osobných údajov už prijatím zákona o počítačoch, súboroch a právach[15] zo 6. januára 1978, ktorým bol súčasne zriadený aj orgán zodpovedný za zabezpečenie ochrany osobných údajov a súkromia – Commission nationale de l´informatique et des libertés (CNIL) – Národná komisia pre informatiku a práva. Od prvého prijatia tohto zákona už prišlo k jeho desiatim úpravám, ktoré modifikovali nielen početné ustanovenia pôvodného zákona, ale aj jeho názov. K poslednej úprave prišlo prijatím zákona n° 2009-526 z 12. mája 2009. K najvýznamnejším úpravám pôvodného znenia však pristúpili francúzske kompetentné orgány 6. augusta 2004, keď bol prijatý zákon n° 2004-801 o ochrane fyzických osôb pri spracúvaní osobných údajov.

Poslaním Národnej komisie pre informatiku a práva je kontrola rešpektovania ustanovení zákonov pri prevádzkovaní počítačových programov a databáz na území Francúzska, ukladanie sankcií, zostavovanie noriem a predkladanie nových návrhov

[14] RS 780.1 Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT)

[15] Loi 78-17 relative à l´informatique, aux fichiers et aux libertés du 6 janvier 1978, http://www.cnil.fr

legislatívnych a regulačných opatrení vláde, ktorých cieľom je prispôsobiť ochranu osobných dát a súkromia vývoju informačno-komunikačných technológií.

V zmysle článku 1 zákona 78-17 musí byť výpočtová technika službou dostupnou pre každého občana, pričom rozvoj tejto služby a spôsoby elektronickej komunikácie musia byť predmetom medzinárodnej spolupráce. Základným predpokladom zostáva fakt, že spracovanie osobných údajov nesmie spôsobiť žiadnu ujmu na ľudských právach, na ľudskej identite ani na súkromí a osobných a verejných právach ktoréhokoľvek ľudského jedinca.

Pod osobným údajom sa v zmysle článku 2 tohto zákona rozumie: „každá informácia týkajúca sa identifikovanej fyzickej osoby alebo osoby, ktorú je možné priamo alebo nepriamo identifikovať, na základe identifikačného čísla alebo na základe jedného alebo viacerých prvkov, ktoré sú jej vlastné.“[16]

Rovnako zákon v ustanoveniach článku 8 zakazuje „zhromažďovať alebo spracúvať osobné údaje, ktoré priamo alebo nepriamo ukazujú na rasový alebo etnický pôvod ľudského jedinca, na jeho politické názory, filozofickú alebo náboženskú príslušnosť, príslušnosť k odborovým zväzom alebo iným združeniam osôb, alebo ktoré sa týkajú jeho zdravia alebo sexuálneho života.“

Zákon 78-17 zohľadňuje aj možnosť režimu „opt-in“, t. j. každá dotknutá osoba môže dať svoj výslovný súhlas vopred k spracúvaniu svojich neanonymizovaných alebo nepseudonymizovaných osobných údajov, avšak s výnimkou prípadov, pre ktoré je zákaz vymenovaný v ustanoveniach zákona.

V kapitole XII, článku 68 zákon ustanovuje, že spracovateľ osobných údajov môže prenášať tieto údaje do štátu, ktorý nie je členským štátom Európskej únie iba vtedy, ak tento štát poskytuje primeranú úroveň ochrany súkromia a základných práv a slobôd jednotlivcov pri spracúvaní, ukladaní a zaobchádzaní s týmito údajmi.

6. *Požiadavky na ochranu a právny vývoj na Slovensku*

Zákon č. 428/2002 Z. z. o ochrane osobných údajov v informačných systémoch[17] ustanovuje nielen ochranu základných práv a slobôd fyzických osôb pri spracúvaní ich osobných údajov, ale aj práva a povinnosti týchto fyzických osôb pri poskytovaní osobných údajov do informačných systémov. Súčasne upravuje práva, povinnosti a zodpovednosť právnických a fyzických osôb, ktoré sa zúčastňujú na spracúvaní osobných údajov a práva a povinnosti prevádzkovateľov informačných systémov, prostredníctvom ktorých sa realizuje zber, prenos a spracovanie osobných údajov.

V § 3 a § 4 sú definované základné pojmy. Osobnými údajmi sa na účely tohto zákona rozumejú údaje týkajúce sa určitej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe identifikačného čísla alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu. Pod anonymizovaným údajom sa rozumie osobný údaj upravený do takej formy, v ktorej ho nemožno priradiť dotknutej osobe, ktorej sa týka.

V § 5 sa definuje, že vykonávať spracúvanie osobných údajov môže iba prevádzkovateľ a sprostredkovateľ. Prevádzkovateľ musí zabezpečiť, aby sa nespracúvali osobné údaje, ktoré sú svojím rozsahom a obsahom nezlučiteľné s daným účelom spracúvania alebo sú časovo alebo vecne neaktuálne vo vzťahu k účelu spracúvania.

Podľa § 7 ods. 1 spracúvanie osobných údajov sa smie vykonávať iba so súhlasom dotknutej osoby. Tento súhlas sa nevyžaduje, ak to ustanovuje osobitný zákon.

---

[16] Article 2 de la Loi 78-17 relative à l´informatique, aux fichiers et aux libertés du 6 janvier 1978

[17] Zákon č. 428/2002 Z. z. z 3.7.2002 o ochrane osobných údajov

Podľa § 8 je zakázané spracúvať osobitné kategórie osobných údajov, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženskú vieru alebo svetonázor, členstvo v odboroch a údaje týkajúce sa zdravia alebo pohlavného života a odsúdenia.

V zmysle uvedených skutočností je možné konštatovať, že právny vývoj na Slovensku v oblasti ochrany osobných údajov je plne v súlade s príslušným právnym vývojom Európskej únie.

7. *Všeobecné pravidlá o ochrane osobných údajov v informačných systémoch*

Ak sa pozrieme na tradičné systémy určené na spracovanie informácií v celej ich komplexnosti, nájdeme v nich niekoľko nasledujúcich klasických parciálnych procesov, pri ktorých sú vytvárané, uložené a spracúvané osobné údaje identifikujúce užívateľa:

- **Autorizácia** – predstavuje udelenie povolenia prístupu k dátam a transakciám spracúvania dát v informačnom systéme
- **Identifikácia a autentizácia** – overenie identity používateľa a potvrdenie jeho oprávnení používať informačný systém
- **Kontrola prístupu** – overenie oprávnení prístupu používateľa k informačnému systému vzhľadom na požadovanú aktivitu alebo službu
- **Monitorovanie** – zoznam aktivít a prihlasovacích transakcií používateľa
- **Fakturácia** – spoplatnenie poskytnutých a použitých služieb používateľovi.

Hlavnými dôvodmi, pre ktoré je nevyhnutné poznať osobné údaje zákazníka používajúceho informačný systém, sú výhradne vyššie uvedené procesy. Skutočná identita používateľa nie je vôbec potrebná pre fungovanie informačného systému.[18]

Z tohto dôvodu je vhodné už pri návrhu informačného systému overiť, tak globálne, ako aj na úrovni každého procesu, či je absolútne nevyhnutné disponovať skutočnými osobnými údajmi jednotlivých používateľov, alebo či v navrhovanom systéme môže byť využívaná anonymizácia alebo použitie pseudonymov.

8. *Anonymizácia*

Anonymizácia je založená na modifikácii osobných údajov takým spôsobom, aby údaje vzťahujúce sa na osobné alebo majetkové pomery nemohli byť dané do korelácie s určitou alebo určiteľnou fyzickou osobou.

Samotný proces anonymizácie a jeho efektívnosť závisí od rôznych faktorov. Určujúcimi prvkami sú načasovanie momentu anonymizácie, jej nevratnosť, ochrana prostriedkov, prostredníctvom ktorých sú osobné dáta ukrývané a maskované, a vylúčenie možnosti prepojenia rôznych transakcií vykonávaných s dátami tou istou osobou. Aj konkrétny obsah zaznamenávaných alebo spracúvaných údajov (napr.: výška mzdy, pracovné zaradenie a pod.) má vplyv na výber a kvalitu metódy anonymizácie. Ak medzi spracúvanými údajmi figurujú údaje, ktoré narušajú anonymitu, tieto musia byť zoskupené s ostatnými. Ak takáto modifikácia nie je možná, či už z technických dôvodov, alebo dôvodov súvisiacich s obsahom dát, nemôže byť dosiahnutá anonymita dát.

---

[18] H. van ROSSUM, H. GARDERNIERS, J. BORKING a kol. „Privacy-enhancing Technologies, The path to anonymity“, Diel I a II, Achtergrondstudies en Verkenningen 5b, Registratiekamer, The Netherlands & Information and Privacy Commissioner/Ontario, Kanada, august 1995

Cieľom techník zvyšujúcich ochranu dát je zabezpečenie nahrávania údajov tak, aby už od samotného začiatku elektronického vkladania dát do informačných systémov boli používané postupy na vymazanie identifikačných prvkov osôb, ktoré poskytli údaje, alebo ihneď, ako je to možné, sa pristúpilo k ich anonymizácii.

Príkladom oblastí, kde je najčastejšie využívaná anonymizácia dát, je oblasť štatistických spracúvaní, oblasť výskumov a sondáží, ale aj používanie anonymných telefónnych kariet, anonymných platobných kariet využívaných napríklad pri doprave osôb a pod.

9. *Pseudonymizácia*

Pseudonymizácia je založená na modifikácii osobných údajov a maskovaní identít prostredníctvom kryptovacieho algoritmu takým spôsobom, aby nebolo možné informácie týkajúce sa osobných alebo majetkových pomerov dať do korelácie s určitou alebo určiteľnou fyzickou osobou bez poznania alebo použitia tohto kryptovacieho algoritmu.

Cieľom tejto metódy je taký stav kódovania dát, pri ktorom nie je možné nájsť a obnoviť koreláciu s príslušnou osobou, s výnimkou prípadu nevyhnutnej potreby tejto korelácie, avšak iba pri dodržaní vopred stanovených podmienok. Pseudonymizácia sa môže uskutočniť vysledovateľným spôsobom pomocou zoznamov súladu identít a ich pseudonymov alebo pomocou dvojsmerných kryptografických algoritmov na pseudonymizáciu. Identity sa môžu zamaskovať aj spôsobom neumožňujúcim opätovnú identifikáciu, napríklad jednosmernou kryptografiou, pri ktorej sa vo všeobecnosti vytvárajú anonymizované údaje. Dvojsmerné kryptografické algoritmy by mali byť využívané najmä vtedy, ak nie je možné použiť iba anonymizáciu.[19]

Samotný proces pseudonymizácie a jeho efektívnosť závisí od rovnakých faktorov ako proces anonymizácie, a to od načasovania momentu pseudonymizácie, jej nevratnosti, od ochrany prostriedkov, prostredníctvom ktorých sú osobné dáta ukrývané a maskované, a vylúčenia možnosti prepojenia rôznych transakcií vykonávaných s dátami tou istou osobou.

Pseudonymy by mali byť náhodné a nepredvídateľné. Počet možných pseudonymov by mal byť taký veľký, aby sa ten istý pseudonym nikdy nevybral náhodne dvakrát. Ak sa vyžaduje vysoký stupeň bezpečnosti, súbor potenciálnych pseudonymov musí byť minimálne rovný počtu hodnôt bezpečných kryptografických hašovacích funkcií.[20]

Anonymizácia je pre väčšinu prípadov potreby ochrany osobných údajov vhodnejšia ako pseudonymizácia. Pseudonym je vhodné používať vtedy, ak sa predpokladá, že by mohlo prísť k potrebe obnoviť identifikáciu osoby, avšak prepojenie medzi pseudonymom a osobnými údajmi je možné zrealizovať výhradne dotknutou osobou, prostredníctvom zoznamov identít a príslušných pseudonymov, alebo prostredníctvom jednosmernej kryptovacej funkcie s unikátnymi tajnými parametrami predstavujúcimi kódovací kľúč.

Literatúra

http://www.disclaimer.admin.ch/informations_juridiques.html
http://www.edoeb.admin.ch/dokumentation/00612/00653/00661/index.html?lang=fr#sprungmarke1_11
http://www.coe.int
http://www.ladocumentationfrancaise.fr/dossiers/internet-monde/donnees-personnelles.shtml

[19] BORKING, John Der Identity Protector; Datenschutz und Datensicherheit 11/96, Verlag vieweg, Wiesbaden, 1997, str. 654-658

[20] GRIMM, R., ZANGENEH, K. Cybermoney im Internet. Gesellschaft für Mathematik und Datenverarbeitung, Institut für Telekooperationstechnik. Darmstadt, január 1996

http://www.cnil.fr

[1] 28/01/1981 Convention pour la protection des données à caractère personnel (STE n° 108)
[2] 15/10/1999 Amendements à la Convention 108 (adhésion des Communautés Européennes)
[3] 08/11/2001 Autorités de contrôle et flux transfrontalier de données (STE n° 181)
[4] Loi 78-17 relative à l´informatique, aux fichiers et aux libertés du 6 janvier 1978
[5] Code civil suisse
[6] Zákon č. 428/2002 Z. z. z 3.7.2002 o ochrane osobných údajov

Key words: Anonymization, conventions, European Union institutions, governmental institutions and authorities of France/Germany/Switzerland, protection of personal data, pseudonymization, Council of Europe, directives, laws

Summary

Electronic support of people daily activities throughout the world requires, because of their identification, to record, process and maintain personal data in the databases of various governmental and private institutions. Business, banking, insurance and other operations are conducted through information and communication resources which are located in various countries, different from the place of residence, realm or stay of operations actors. Simply put, informatics knows no national boundaries, therefore there is need for legislation to protect individuals´privacy. This contribution presents the legislative frameworks adopted in this area by the Council of Europe, EU institutions, but also by relevant institutions of Germany, Switzerland, France and Slovak Republic. At the same time it closes to the gemńeral IT rules used in data protection.

RNDr. Eva Kostrecová, PhD.
Fakulta Elektrotechniky a informatiky
STÚ v Bratislave
Katedra aplikovanej informatiky a výpočtovej techniky
e-mail : eva.kostrecova@stuba.sk

Recenzent : doc. JUDr. Vladimír Zoubek, CSc.