

ZAUPNI PODATKI V DOKUMENTARNEM IN ARHIVSKEM GRADIVU

Tomaž Lavrič*

UDK: 930.25:349

Tomaž Lavrič: Zaupni podatki v dokumentarnem in arhivskem gradivu. Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja. Zbornik referatov z dopolnilnega izobraževanja, Maribor 7/2008, str. 41-51.

Izvirnik v slovenščini, izvleček v slovenščini in angleščini, povzetek v angleščini.

Prispevek obravnava zaupnosti, s katerimi se srečujemo pri dnevnem poslovanju in nastajajo v okviru dokumentarnega gradiva. Gradivo, ki je označeno kot zaupno, je potrebno zavarovati pred dostopom oseb, ki do njega niso upravičene. Vse gradivo pa postane v javnih arhivih po izteku časa dostopno tudi ostali zainteresirani javnosti.

UDC: 930.25:349

Tomaž Lavrič: Classified Information in Records Management and Archives. Technical and Field Related Problems of Traditional and Electronic Archiving. Conference Proceedings, Maribor 7/2008, pp. 41-51.

Original in Slovenian, abstract in Slovenian and English, summary in English.

This article discusses a set of classified information we can find on a daily basis within records management. All the documents, when marked as classified, must be secured against non-authorized individuals. The public is allowed to access records in all public archive institutions, when time of their secrecy expires.

Ključne besede: zaupnost, dokumentarno gradivo, arhiv, dostop, zavarovanje, upravičenost.

1. UVOD

Z zaupnimi informacijami in podatki se pri delu srečujemo občasno. Predvsem jih srečamo takrat, kadar opravljamo kakšne naloge za organizacijo, v kateri delamo, in jih ta opredeli kot zaupne. Zaupne informacije ali podatke moramo varovati na poseben način zato, da se z morebitnim razkritjem ali zlorabo ne bi povzročile škodljive posledice organizaciji, posredno pa tudi zaposlenim in delovnim procesom.

Normativno urejanje varovanja zaupnih podatkov (v praksi poznamo zaupne podatke kot skrivnosti in tajnosti) je relativno novo. Izoblikovalo se je predvsem na vojaškem področju. Varovanje zaupnosti je razcvet doživelo ob vzpostavljanju bipolarnega sveta v šestdesetih letih prejšnjega stoletja, pomembni koraki pa so bili storjeni z vključevanjem novih srednjevzhodnoevropskih držav v evrointegracije pred nekaj leti. Ne smemo pozabiti tudi na globalizacijo, ki je vzpostavila pogoje tržne konkurence in s tem vzpodbudila organizacije, da še bolj ščitijo pomembnejše podatke pri svojem poslovanju.

Zaupni podatki se pojavljajo v pisnih virih in v ustnem komuniciranju. Z vidika arhivistike je toliko bolj pomemben pisni vir, ki ohranja kulturno vrednost skozi daljše časovno obdobje. Pomen zaupnih podatkov v dokumentarnem in arhivskem

* Mag. Tomaž Lavrič, višji svetovalec, Davčna uprava Republike Slovenije, Šmartinska cesta 55, 1000 Ljubljana, Slovenija.

gradivu kaže na to, da vse stvari, dogodki, vsebine niso prosto dostopne različnim zainteresiranim skupinam ali posameznikom, ampak velja načelo, da se smejo s pomembnimi informacijami in podatki, kadar so kot taki označeni, seznaniti samo upravičeni ter pooblaščenim posameznikom. To pa je bistvo varovanja zaupnosti.

2. DOKUMENTARNO GRADIVO ZAUPNE NARAVE

Slovenska zakonodaja regulira s skrivnostmi in tajnostmi, varovanje informacij in podatkov,¹ ki so tako pomembni, da bi z njihovim razkritjem lahko škodovali delovanju in izvajanju nalog državnih organov, organizacij ali celo interesom Republike Slovenije. Namesto skrivnosti² in tajnosti³ uporabljam v nadaljevanju tega prispevka primernejši izraz - zaupnosti. Z zaupnostjo lahko razumemo omejevanje pravice dostopa do pridobivanja občutljivih informacij in podatkov s strani neupravičenih oseb oziroma zmožnost sprejemanja in ohranjanja pridobljenih zaupanih informacij ali podatkov, ki so namenjeni samo določenim posameznikom. Poznamo naslednje vrste zaupnosti:

- **tajne podatke** (urejene v zakonu o tajnih podatkih, v nadaljevanju: ZTP),
- **davčno tajnost** (urejeno v zakonu o davčnem postopku),
- **osebne podatke** (urejene v zakonu o varstvu osebnih podatkov),
- **poklicno skrivnost** (urejeno v zakonu o zasebnem varovanju, zakonu o javnih uslužbencih in v drugih predpisih),
- **uradno tajnost** (urejeno v zakonu o industrijski lastnini, v predpisih ministrstva za obrambo, ministrstva za notranje zadeve, ministrstva za zunanje zadeve ter v drugih predpisih),
- **vojaško tajnost** (urejeno v različnih neusklajenih predpisih organov javne uprave),
- **državno tajnost** (urejeno v zakonu o slovenski varnostno-obveščevalni agenciji in v drugih predpisih),
- **bančno tajnost** (urejeno v bančnem kodeksu Združenja bank Slovenije, zakonu o bančništvu in v drugih predpisih),
- **poslovno skrivnost** (urejeno v zakonu o gospodarskih družbah, v zakonu o bankah in hranilnicah in v drugih predpisih),
- **poslovno tajnost** (urejeno v zakonu o detektivski dejavnosti),
- **industrijsko skrivnost** (urejeno v notranjih predpisih gospodarskih družb),

¹ Podatek je dejstvo ali ideja (pojema, misel) v formalizirani obliki, primeren za komuniciranje, ki o določeni stvari kaj pove ali se nanj nanaša, informacija pa vsebuje pomen, ki ga da človek podatkom v danih okoliščinah, gre za vednost o določeni stvari.

² Skrivnost je nekaj nerazumljivega, nerazložljivega, nikoli odkritega in predstavlja misterij.

³ Kot pravi Anžič (1997, str. 156), je beseda tajnost prevzeta iz drugih slovanskih jezikov. Upoštevati velja, da se je raba izraza tajnost v slovenskih predpisih povečala pod vplivom jugoslovanske zakonodaje, kjer se je uporabljal izraz "tajna", pojem tajnosti pa se v slovenski državi pogosto enači s pojmom skrivnosti. Tudi SSKJ ločuje oba izraza, vendar v delu, ki je bistven za delo državne uprave, dovoljuje enakopravno rabo obeh in ne daje prednosti enemu ali drugemu.

- **zdravniško skrivnost** (urejeno v notranjih predpisih zdravstvenih organizacij) in druge zaupnosti.

Vse te zaupnosti nastajajo pri rednem delu upravnih organov v širšem smislu, kamor štejemo poleg državne uprave še samoupravne lokalne skupnosti, nosilce javnih pooblastil ter nenazadnje gospodarske družbe in organizacije.

Vsak posamezni predpis vrste zaupnosti ureja način označevanja dokumentov in medijev (naj gre za zemljevide, fotografije, slikovne in zvočne zapise na kasetah, CD-jih, DVD-jih in drugih elektronskih medijih). S predpisanim označevanjem zaupnih informacij in podatkov lahko zagotavljamo pravilno obvladovanje (upravljanje) in hrambo prejetega dokumentarnega gradiva. Vsak dokument, ki ga prejme glavna pisarna, sprejemnica ali vložišče, lahko namreč uslužbenec takoj razvrsti med navadno - redno pošto, in posebno pošto, ki je ponavadi zaupne narave. Ker je obravnava zaupnih podatkov omejena na vodstvene in vodilne uslužbenice, je evidentiranje in dostava takih pošilk prednostna. Torej pravilnost označevanja zaupnosti kakršnegakoli medija bistveno zmanjša možnosti zlorab ali razkritij podatkov s prebiranjem vsebine, ki je namenjena samo pooblaščenim osebam.⁴

Dodati je potrebno, da vse zaupnosti nimajo urejenega načina in postopkov varovanja podatkov v zakonih in podzakonskih aktih. Sem lahko štejemo primer osebnih podatkov, poklicne skrivnosti, poslovne tajnosti, poslovne skrivnosti ipd. Pri poslovni skrivnosti, kot jo ureja zakon o gospodarskih družbah, velja, da sprejme notranji akt o zavarovanju osebnih in zaupnih podatkov direktor ali upravni odbor. V notranjem predpisu navede način in postopke (logično-tehnične ukrepe) zavarovanja zaupnih podatkov. S takim dokumentom se ponavadi seznanijo le poslovodni uslužbenci in zaposleni v tej organizaciji. Drugi takega predpisa ne poznajo, zato je v teh primerih potrebno pridobiti notranji akt organizacije, v katerem so predpisani načini in postopki varovanja, ki omogočajo prejemniku zaupnih pisanj enakovrstno hrambo gradiva, kot ga je predvidel tisti, ki ga je označil za zaupnega v gospodarski družbi.

Poleg formalnega označevanja je pri zaupnih gradivih pomembna še dostava in prevzem take pošte. Pravilna navedba naslova na ovojnici in dostava pošte naslovniku onemogočata možnost zlorabe in nepravilnega vročanja. Taka ovojnica se ne odpira, ampak se pripne k dokumentu ter po pisarniški odredbi shrani v zbirki dokumentarnega gradiva. V izrednih primerih ima lahko ovojnica pomembno dokazno vrednost pravilnosti oziroma nepravilnosti naslavljanja in vročanja, ob pravilnem in pravočasnem prejemu pa tudi zmanjša morebitno gospodarsko ali drugo škodo ali pridobi določeno korist organizaciji. Zaupno gradivo se obravnava pred obdelovanjem splošnega "navadnega" gradiva, zaradi tega ima posledično tudi strožji pogoj varovanja in hrambe.

Gradivo, ki prispe v organ in je označeno z oznako zaupnosti, se evidentira po notranjih predpisih, saj so vrste zaupnosti različne po vsebini (obstajajo predpisi, ki v celoti regulirajo upravljanje dokumentarnega gradiva), pri evidentiranju pa se zahteva le splošen vpis atributov, ki v zbirki prejete ali odposlane pošte ne prikazuje zaupnih podatkov iz prejetega gradiva.

⁴ V primeru tajnih podatkov so to osebe, ki imajo dovoljenje za dostop do tajnih podatkov določene stopnje: ZAUPTNO, TAJNO ali STROGO TAJNO.

3. ZAUPNI PODATKI MED DOKUMENTARNIM IN ARHIVSKIM GRADIVOM

Temeljno načelo varovanja zaupnih podatkov je ravno zagotavljanje njihove nedostopnosti osebam, ki do njih niso upravičene ali pooblaščne. Predpisi, ki urejajo npr. tajne podatke, pogojujejo osebam dostop do takih podatkov s potrebo po védenju (t. i. "need to know" načelo), ki izhaja iz njihovega dela. Posamezniki se z zaupnim gradivom lahko srečamo kot uslužbenci, ki prenašamo gradivo (kurirji, tajnice, študenti) ali osebe, ki se v zadnji fazi ukvarjajo z arhiviranjem gradiva (arhivarji). Sem štejemo tudi osebe, ki se z zaupnim javnim arhivskim gradivom po izteku roka nedostopnosti srečajo kot raziskovalci, zgodovinarji in take dokumente pregledujejo. Za vse te osebe velja načelo, da varujejo informacije in podatke, do katerih so prišle pri opravljanju svojega dela. To vrsto zaupnosti imenujemo poklicna skrivnost oziroma poklicna molčečnost. Zaveza k varovanju tako pridobljenih podatkov se vzpostavi na podlagi potrditve odgovornosti posameznika s podpisom na listini (izjava o seznanitvi s predpisi in zavezo o varovanju pridobljenih podatkov). Ta zaveza velja za posameznika nedoločno dolgo.

Gradivo, ki vsebuje zaupne podatke, se skozi faze obdelave in na koncu v hrambi ustrezno evidentira. Lahko je vpisano v posebno - ločeno zbirko prejetega gradiva (ročna ali elektronska zbirka) z zaznamkom uporabnika takega gradiva, v kolikor se tak dokument še obdeluje, lahko pa je že odloženo v priročnem arhivskem prostoru ali v arhivskem skladišču.

Pristojni uslužbenci javne uprave so tako s področnimi zakoni kot tudi z Uredbo o upravnem poslovanju zavezani varovanju zaupnosti podatkov, kadar jih kot take označijo stranke, ponudniki in drugi poslovni subjekti. Njihova odgovornost glede na določeno časovno obdobje je, da za gradivo zaupne narave, ko se prenaša iz zbirke (nerešenih zadev, tekoče ali stalne zbirke) ali prenese pristojnemu arhivu oziroma uniči, kadar ni arhivsko, in je bila stopnja tajnosti znižana (lahko tudi na stopnjo nič), poskrbi za predajo pravilnih in popolnih napotkov strokovnim službam, kako ravnati s takim dokumentarnim gradivom, naj si bo v klasični ali elektronski obliki. Kot sem v prejšnjem razdelku že navedel, je pravilno naslavljanje pošiljk zelo pomembno. Poleg tega je pomembna tudi pravilna pisarniška odredba glede hranjenja dokumentacije po izteku rokov hranjenja (kot so opredeljeni npr. v načrtu klasifikacijskih znakov). Odgovornosti uslužbenca od predaje gradiva strokovnim službam (glavna pisarna, arhivar) znotraj istega organa ni mogoče prenesti, v kolikor odredba in predaja nista bili navedeni in izvedeni pravilno. Na koncu obdobja hrambe nekega gradiva, se s temi dokumenti namreč sreča arhivar, ki vsebinsko ni nikdar reševal zadeve zaupne vsebine, zaupnosti pa s časom poteka dogodkov oz. veljavnosti ali zaradi sprememb predpisov niso bile znižane ali anulirane. To povzroči dodatne obremenitve in napore glede finančnih sredstev za opremljanje arhivskih prostorov ali skladišč s tehničnim varovanjem, izdelavo načrta hrambe, načrta varovanja itd.

Primer takega reševanja problematike dokumentarnega gradiva, ki se hrani v redni stalni zbirki organa in kasneje ob prevzemu v pristojnem arhivu, so tajni podatki, kot jih ureja ZTP. Zakonodaja v prehodnih in končnih določbah namreč določa, da se tajnim podatkom, ki jim je bila stopnja tajnosti določena po prejšnjih predpisih in so v zbirki nerešenih zadev, spremeni oznaka stopnje tajnosti najpozneje do določenega zakonskega roka. Ne glede na ta rok oznak stopenj tajnosti ni potrebno spreminjati tajnim podatkom v elektronski ali drugi nepapirni obliki, ki se hranijo v tekoči ali stalni zbirki dokumentarnega gradiva. Tem tajnim podatkom se

oznako stopnje tajnosti spremeni ob njihovi ponovni uporabi ali posredovanju drugemu uporabniku.

Ne glede na hrambo gradiva v eni izmed zbirk so pooblašcene osebe, ki razpolagajo s tajnimi podatki, dolžne pregledati stopnje tajnosti enkrat letno pri oznaki STROGO TAJNO in na vsaka tri leta pri INTERNO, ZAUPNO, TAJNO ter oceniti obstoj potrebe po njihovi zaupnosti. Odgovornost posameznika, ki ravna z zaupnimi podatki, je torej tisti varnostni element, ki omogoča redno preverjanje in pravilno hrambo gradiva v organu. Ne smemo pozabiti na predajo zaupne dokumentacije pristojnim arhivom. Arhivska znanost se je v zadnjih 20 letih izredno razvila, še posebej ob novih oblikah hrambe gradiva v elektronski obliki.

Komisijo, ki jo imenuje predstojnik, sestavljajo ponavadi uslužbenci glavnih pisarn in strokovni uslužbenci, ki rešujejo zadeve iz nekega vsebinskega področja. Tu je vloga pooblaščenih oseb, ki so ali še ravnajo z zaupnim gradivom, izredno pomembna, saj lahko konkretno vplivajo na pregledovanje starejših zaupnih vsebin v dokumentih, potrjujejo veljavnost in ocenjujejo morebitno škodljivost ob razkritjih. Hkrati so te osebe dovolj verodostojne, da vsebino gradiva, ki ga pregledujejo, zaradi pridobljenih varnostnih dovoljenj in preverjanj ohranijo le zase. Manjše, kot je število oseb, ki pregleduje zaupne vsebine, manj je možnosti zlorab in razkritij. Drugo pomembno dejstvo je, da lahko te osebe s primopredajo zaupne vsebine določajo način in pogoje varovanja, ki velja za različne vrste in stopnje zaupnosti.

Pravilno označevanje in organizacija prevoza v okviru internih kurirskih služb zmanjšujeta možnost odtujitev in povečujeta pravilnost primopredaj, saj se npr. zunanje prevozne selitvene službe ponavadi ne zavedajo pomembnosti vsebin, ki jih prenašajo drugim naslovnikom, pristojnim arhivom, ali pa odvažajo v uničenje.⁵

Odgovornost varovanja zaupnih informacij in podatkov velja poleg zaposlenih tudi za vse tiste osebe, ki imajo posebno dovoljenje za dostop do zaupnih podatkov, s pridobljenimi informacijami pa ne smejo ravnati na način, ki bi utegnil povzročiti morebitno razkritje, zlorabo oziroma celo izdajo. Zaupne podatke so dolžne varovati tudi osebe,⁶ ki so imele kot druge osebe v postopku priznано pravico udeležbe zaradi varstva svojih pravnih koristi. Ker je pravna korist na zakonu oprta na osebno korist, mora informacije ali podatke, s katerimi se je seznanila stranka, na podlagi načela zaupnosti ohraniti zase. Enako velja tudi, kadar se uveljavlja poslovni in življenjski interes. Sicer bi v nasprotnem primeru veljalo, da mora zaposleni zaupne podatke varovati, stranka pa bi jih lahko zlorabljalala in razglašala tretjim, neupravičenim osebam.

To možnost omogočajo na primer 82. člen Zakona o splošnem upravnem postopku, 68. člen Zakona o varstvu dokumentarnega in arhivskega gradiva in arhivih in 22. člen Uredbe o upravnem poslovanju. Ti predpisi, z nekaterimi izjemami, omogočajo osebam, ki nastopajo kot stranke v postopkih in izkažejo svoj pravni

⁵ Tu poznamo primer, da so v novembru leta 2007 izgubili datoteko s podatki 25 milijonov Britancev, na katerih so bila imena, naslovi, rojstni podatki ter številke bančnih in zavarovalnih računov. Uradnik centra za zdravstveno zavarovanje v Newcastlu naj bi zbirni pisarni v London poslal po neustaljenih postopkih paket podatkov na elektronskem mediju, ki pa se je med potjo izgubil.

⁶ Osebe, ki nastopajo v postopku, so lahko: stranke, stranski udeleženci,časni zastopniki, skupni predstavniki, pooblaščenci, zakoniti zastopniki, strokovni pomočniki, svetovalci, pravni nasledniki, skrbniki, tuji državljani, priče, izvedenci, tolmači, dediči, garant, predstavniki banke, zavarovalnice, osebe, udeležene na javni dražbi itd. Posebna izjema velja tudi za druge uradne osebe, inšpektorje, računske revizorje, izvajalce strokovnega nadzora, državne tožilce, pravobranilce, policiste, odvetnike, duhovnike, ki morajo take podatke že po svoji službeni dolžnosti varovati kot poklicno tajnost.

interes za udeležbo v postopkih, pravico do vpogleda v svoje dokumente zadeve, ki je nastal pri nekem organu.⁷ Za te osebe in za vse druge osebe, ki glede na zakonske možnosti verjetno izkažejo, da imajo od tega pravno korist, velja, da lahko z vpogledom pregledujejo, izpisujejo, prepisujejo ali kopirajo gradivo, ki se nanaša le na njih. Pri tem so vse osebe, ki se jim omogoči vpogled, dolžne varovati podatke kot zaupne.

Izjemo stopnje varovanja dokumentarnega gradiva tako v klasični papirni kot v elektronski obliki iz informatiziranih evidenc, kadar se z njimi seznanijo stranke, ki imajo pravico do vpogleda, predstavljajo podatki in zapisi v dokumentih, ki vsebujejo tajne podatke in so bili uporabljeni kot podlaga za odločitve v postopku. S to določbo so vse v opombi naštetе osebe lahko seznanjene s tajnimi podatki tudi do stopnje STROGO TAJNO po ZTP, kar je sicer v nasprotju s postopki, načinom in upravičenostjo dostopa do tajnih podatkov po ZTP, pa vendar so zainteresirane osebe tako pridobljene podatke vsekakor dolžne ohraniti kot zaupne samo zase, ne glede na stopnjo tajnosti, v katero so imele vpogled. To odgovornost varovanja zaupnosti lahko posameznik potrdi s podpisom izjave v organu, kjer je dobil vpogled v gradivo, vendar k podpisu po obstoječi zakonodaji ni povsod obvezan.

4. HRAMBA IN ZAVAROVANJE (VAROVANJE) PODATKOV

S hrambo zagotavljamo dolgodobno varovanje gradiva ne glede na obliko ali medij, v katerem se ta nahaja. Kot ugotavlja Dobernik (2007, str. 39) v svojem prispevku z naslovom: "Mikrofilmanje kot del sistema trajnega shranjevanja podatkov," prihaja gradivo v arhive še vedno večinoma na papirju, ostali nosilci pa so zastopani v manjši meri. Kot pravi, je vedno več digitalnih zapisov kot duplikatov papirnega gradiva, vendar so prisotni tudi že kot izvorni zapis. Vse več pa je tudi različnih baz podatkov, ki se vzdržujejo samo v digitalni obliki.

Pri hrambi in zavarovanju gradiva je potrebno poleg materialnega varstva dokumentarnega in arhivskega gradiva upoštevati še vrsto drugih dejavnikov, ki potencialno škodujejo gradivu, ki je v hrambi. Gre za materialno tehnične vidike zavarovanja gradiva v smislu:

- opreme (kovinski arhivski regali, aluminijaste lestve, gasilni aparati, merilniki vlage, temperature, tlaka, protipožarno in protivlomno varovanje ...),
- prostorskega in lokacijskega načrtovanja arhivskih prostorov in skladišč,
- izdelave načrta hrambe dokumentarnega gradiva in izvajanja varnostnih ukrepov iz načrta,
- ureditve dostopa - dviga ter vračila gradiva iz arhivske zbirke,
- ločevanja elektronskih nosilcev zapisa od klasičnih,
- zagotavljanja funkcionalnosti in operativnosti informacijskotehničnih naprav za branje podatkov,
- ločevanja zaupnega gradiva od drugega pisanja ali gradiv in še bi lahko naštevali.

⁷ Izjema je 17. člen Zakona o Slovenski obveščevalno-varnostni agenciji, ki posamezniku ne omogoča pravice do vpogleda v zbirko osebnih podatkov, na katerega se podatki nanašajo.

Tu bi se navezal predvsem na zadnjo alineo, ki sporoča, da je potrebno zaupne podatke (skrivnosti in tajnosti) pri hrambi obravnavati specifično, strožje. Tako Uredba o upravnem poslovanju v 191. členu kot Uredba o varstvu dokumentarnega in arhivskega gradiva v 42. členu določata, da se dokumentarno gradivo, ki vsebuje tajne podatke po ZTP⁸ v skladu s posebnimi predpisi hrani ločeno,⁹ za hrambo pa se uporabljajo določbe predpisov o varovanju tajnih podatkov.

Uredba o varovanju tajnih podatkov v 31. členu določa, da se dokumenti, ki vsebujejo tajne podatke po ZTP, arhivirajo v skladu s predpisi, ki urejajo arhivsko dejavnost, 65. člen Uredbe o varstvu dokumentarnega in arhivskega gradiva pa za arhivsko gradivo pravi, da je kompletna celota, če vsebuje celotno arhivsko gradivo, nastalo pri javnopравни osebi v določenem časovnem obdobju. V 28. členu uredbe je še zapisano, da Arhiv RS dokumentacijo registracije ponudnikov opreme in storitev za hrambo v digitalni obliki, če je v skladu s predpisi označena kot tajna ali zaupna, varuje v skladu s predpisi, na podlagi katerih ji je bila določena tajnost oziroma zaupnost.

Tu lahko povzamemo, da se mora zaupno gradivo poleg samega obravnavanja v postopku nastajanja tudi po predaji pristojnemu arhivu obravnavati ločeno in varovano po predpisanih postopkih. Podobno velja tudi za primere poslovne skrivnosti, ki velja v gospodarskih družbah. Tu je dolžan arhiv upoštevati notranji akt o zavarovanju zaupnih podatkov in način varovanja, kot ga je opredelila gospodarska družba v svojem aktu.

Ločena hramba gradiva prinaša koristi in slabosti. Med prednosti bi lahko šteli hitrejšo najdbo dokumentacije v zbirki, celovito varovanje pomembnih in občutljivih podatkov ter informacij, razvrščanje po stopnjah tajnosti in vrstah ali celo kategorijah zaupnosti. Slabosti pa predstavlja predvsem finančni vložek v zagotavljanje tehničnih pogojev varovanja, omejen (kontroliran) dostop do podatkov drugih uporabnikov, administriranje dostopov in vpogledov v dokumentacijo in še bi lahko naštevali.

Ločena hramba in strožja obravnava takih podatkov zagotavlja trajnost zapisanih vsebin, ki so pomembne za posameznika in skupnost ter omogočajo celovito zavarovanje podatkov pred nepooblaščenimi osebami.

Razkritje zaupne informacije ali podatka se kot škodljivo in s tem kaznivo izkaže takrat, ko se posreduje osebi, ki do nje ni upravičena niti pooblaščen. Ohranjanje zaupnosti pomeni tudi to (*lat. in camera charitatis*), da vse kar nastane, ostane znotraj štirih sten oz. med štirimi očmi. Pri delu se namreč pogosto zgodi, da se s kakšnim zaupnim podatkom (osebne ali uradne narave) srečajo tako naključni sodelavci, ki mimogrede pokukajo na sosednjo mizo, ko pridejo na sestanek, stranke pri okencih, ki čakajo na obdelavo podatkov pri uslužbencu in imajo vpogled na listine na njegovi mizi, ali pa v dnevnikih pogovorih med uslužbenci, uslužbenci in strankami, ali celo doma v pogovoru s partnerjem. Visoko stopnjo zanesljivosti varovanja zaupnih podatkov glede na sprejete notranje varnostne predpise se lahko zagotavlja le v organizacijah z majhnim številom uslužbencev, kontinuirano upravljavsko strukturo, predpisanimi postopki dela in procesov in kjer poteka

⁸ Deloma velja smiselno tudi za ostale zaupnosti, npr. poslovno skrivnost, davčno tajnost, bančno tajnost.

⁹ Tako, da je zavarovana njihova tajnost.

poslovanje brez obiskovalcev ali drugih zunanjih strank. Za varovanje zaupnosti smo seveda v prvi vrsti odgovorni sami.¹⁰

5. TRAJNOST ZAUPNIH PODATKOV V ARHIVSKEM GRADIVU

Zaupni državni dokumenti podležejo strožjim pravilom varovanja kot osebni podatki. Če bi bili vsi osebni podatki v evidencah, na obrazcih, plastičnih karticah in drugod označeni z stopnjo zaupnosti, bi povzročili gromozansko administriranje in zakrivanje ter s tem zlorabljanje teh podatkov. Zato so celoviteje (sistemske) varovani državni zaupni podatki, manj pa osebni podatki posameznika, razen seveda nekaterih najbolj občutljivejših osebnih podatkov. Izjeme veljajo tudi pri dostopu do takih podatkov. Medtem ko velja, da mora biti pri tajnih podatkih oseba, ki jih želi vpogledati, varnostno preverjena in mora ustrezati določenim pogojem, se z osebnimi podatki lahko seznanijo več drugih oseb, od receptorjev, varnostnikov, policistov, uradnikov, zdravnikov, odvetnikov, psihologov itd. Za vse te osebe se zahteva, da morajo podatke, s katerimi so se seznanili, varovati kot *poklicno skrivnost*. Gre torej za poklicno varovanje informacij in podatkov, ki so jih izvedeli v okviru svojega dela.

Tu izpostavljam področje trajanja zaupnosti osebnih in tajnih podatkov. Za osebne podatke iz javnih zbirk velja, da so dostopni javnosti, če posameznik tega ni prepovedal, v 10 letih po smrti ali v 75 letih od nastanka, tajni (poslovne, davčne in druge skrivnosti) pa po 40 letih od nastanka in po predaji pristojnemu arhivu.

Kot pravi Žontar (1984, str. 14), zavzema zgodovina poglavitno mesto med znanostmi, ki preučujejo preteklost. Naloga zgodovine je, da se ukvarja z razvojem človekove preteklosti z vseh zornih kotov in v vseh časovnih obdobjih. Znanstvene raziskave so pomemben segment proučevanja preteklih zgodovinskih dogodkov, zato nobena javna informacija ne more biti trajno omejena in nedosegljiva javnosti.

Sem lahko štejemo tudi eno izmed ustavnih pravic, in sicer pravico posameznika, da dobi informacijo javnega značaja, za katero ima v zakonu utemeljen pravni interes. Kot pravi Bohinc (2001, str. 5), predstavlja javnost dela državnih organov ter transparentnost njihovih odločitev in ukrepov temeljno sestavino sodobnih demokratičnih družbenih ureditev. Podobno meni tudi Rovšek (2001, str. 35-36): "Javnost dela državnih organov, odprtost in preglednost (transparentnost) njihovega dela, v povezavi z možnostjo dostopa do podatkov in informacij javnega značaja, so značilnost sodobne demokratične in pravne države. Z ustreznim obveščanjem, odprtostjo in možnostjo nadzora se krepi zaupanje državljanov v delo državnih organov in javne uprave v širšem pomenu.

Če je delovanje teh organov zaprto, je veliko več možnosti za nepravilnosti, zlorabe oblasti in različne oblike korupcije." Tu dodajam, da smisel varovanja zaupnih informacij, ki to niso (zaradi namenskega prikrivanja sicer javnih informacij ali neusposobljenosti javnih uslužbencev pri označevanju zaupnih podatkov), ni v prid preglednemu in javnemu delovanju organov javne uprave.¹¹

¹⁰ *Stoodstotnega sistema, ki bi bil zanesljiv proti razkritjem ali zlorabam podatkov, ni. To smo le mi, posamezniki, ki se enkrat srečujemo z zaupnostmi kot uporabniki, drugič pa kot upravljavci zbirk takih podatkov.*

¹¹ *Dostop do informacij javnega značaja se nanaša le na organe javne uprave, podrobneje glej Zakon o dostopu do informacij javnega značaja.*

Velik korak na področju dostopa do zaupnih podatkov so do sedaj opravili že varuh človekovih pravic, inšpektor za varstvo osebnih podatkov in pooblaščenec za dostop do informacij javnega značaja. Predvsem v zadnjem času je mogoče opaziti večje premike v luči zagotavljanja varstva človekovih pravic in temeljnih svoboščin glede na določila ustave in zakona, s strani informacijskega pooblaščenca, ki na javno izpostavljene primere tudi medijsko reagira, najsi gre za poseg v osebne podatke ali pa za *skrivnosti ter tajnosti*.

Kot sem že navedel, vsem zaupnostim, opredeljenim v slovenski zakonodaji, rok zaupnosti nekoč poteče.

V kolikor zaupnost (skrivnost in tajnost v javni upravi) ni preklicana, postane taka dokumentacija dostopna šele po 40 letih od njenega nastanka oziroma po 75 letih od nastanka v primeru osebnih podatkov. Ta rok lahko glede na določila Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih Vlada RS na obrazložen zahtevek arhivske komisije podaljša, če obstaja interes, lahko pa ga tudi skrajša, če obstaja močnejši javni interes (test javnega interesa).

V nadaljevanju predstavljam izrezke iz nekaterih medijev o odprtju zaupnih arhivov v pomembnih institucijah.

Arhivi Pija XI. dostopni javnosti

Vpogled v vatikanski odnos do nacizma

Svet, 1. julij 2006 14:27
Vatikan - RTV SLO

Vatikan bo za javnost odprl arhive z vsemi dokumenti iz obdobja pontifikata papeža Pija XI. med letoma 1922 in 1939.

Dokumenti, ki bodo na vpogled, bodo omogočili lažje razumevanje odnosa Pija XI. in Vatikana do naraščajočega nacizma v Evropi v tistem obdobju, podali pa bodo tudi nove informacije o stališču Katoliške cerkve do španske državljanske vojne leta 1939. Prav tako bodo javno dostopne diplomatske listine iz skrivnih arhivov tistega obdobja in papeževa neobjavljena enciklika "Humani Generis Unitatis", v kateri je obsodil rasizem in nacionalizem v Nemčiji.

Zgodovinarji so pozvali Vatikan, naj odpre arhive za javnost, da bo bolj poznana vloga Katoliške cerkve med drugo svetovno vojno in po njej. Vendar pa arhivi iz obdobja Pija XII., ki je bil obtožen, da ni želel pomagati Judom in da je vedel za nacistični genocid med drugo svetovno vojno, kljub mnogim prošnjam ostajajo zaprti za javnost.

Vatikanski arhivi hranijo odloke in enciklike vseh papežev ter vso diplomatsko korespondenco.

Pošlji | Natisni | Komentari (0)

Ocena novice: ★★★★★ Vaša ocena: ★★★★★
0 ocene od 0 glasov Ocenite to novico!



Dokumenti posameznih papežev so v javnost prihajali v različnih intervalih, večina arhivske zbirke pa je bila za javnost odprta v 19. stoletju. Foto: EPA

Odprtje Vatikanskih arhivov

Nacistični arhivi na ogled javnosti

BERLIN – V sredo so po več kot 60 letih za javnost odprli tajne arhive o nacističnih taboriščih, ki osvetljujejo usodo 17,5 milijona žrtev nacizma širom po Evropi. Arhive so lahko odprli, šele ko je vseh enajst držav članic odbora, ki jih upravlja – ZDA, Izrael, Poljska, Britanija, Belgija, Luksemburg, Nizozemska, Italija, Grčija, Francija in Nemčija –, ratificiralo sporazum iz leta 2006, ki omogoča javni dostop do 47 milijonov dokumentov. Doslej so imeli dovoljenje za vpogled v arhive le najožji družinski člani žrtev nacističnega režima. Po besedah direktorja arhivov Reta Meistra bodo dokumenti zgodovinarjem med drugim omogočili preučevanje gibanja zapornikov, izpopolnjevanje podatkov o zaprtih v nacističnih taboriščih in podatkov o prisilnih delavcih. Kljub velikemu zanimanju za arhive pa marsikateri zgodovinar misli, da ni pričakovati dramatičnih novih odkritij o nacističnem režimu. **STA**

Članek v časniku *Delo* z dne 29. 11. 2007:
Odprtje nacističnih arhivov

Odkritje v arhivih Stasija

Licenca za ubijanje

Stasijevi agenti so imeli ukaz, da morajo streljati na ubežnike, tudi če so med njimi ženske in otroci

BERLIN – Tik pred današnjo 46. obletnico postavitve berlinskega zidu je v širšo nemško javnost prvič prišel dokument, ki naj bi dokazoval, da so vojaki, ki so varovali mejo Nemške demokratične republike, imeli ukaz, da morajo streljati na bežeče ljudi. Odkrila ga je magdeburška podružnica državnega urada, ki skrbi za Stasijeve arhive. Dokumentu pripisujejo posebno težo, ker so nekdanji vzhodnonemški vodilni kadri zanikali obstoj ukaza s takšno vsebino.

OD NAŠEGA DOPISNIKA

Najdeni ukaz, izdan leta 1973, so našli v arhivu posebne enote Stasija. Njeni pripadniki so bili sicer v enakih uniformah kakor običajni graničarji, Stasi pa jim je ukazal takojšnje streljanje na dezerteerje, ki so se odločili za pobeg na Zahod. »Ne omahujte pri streljanju, tudi če preboj meje poteka z ženskami in otroki, kar so izdajalci že večkrat izkoriščali,« se je glasilo navodilo agentom. Strogi ukrep naj bi bil posledica tega, da so čez mejo v Zvezno republiko Nemčijo zbežali številni vojaki ljudske armade, samo v obdobju 1971-74 jih je bilo 144.

Za direktorja spominskega centra žrtev Stasija v berlinskem Hohenschönhausen Hubertusa Knaba je odkriti ukaz kot licenca za ubijanje. Ukazovanje, da morajo streljati tudi na ženske in otroke, bi bilo po njegovem mnenju lahko obravnavano kot napeljevanje k umoru, z zadevo bi se moralo ukvarjati tožilstvo in ugotoviti, kdo je izdal takšen ukaz, zlasti zato, ker je od 91.000 uslužbencev Stasija pravzaprav le eden končal v ječi.

Vodja urada za Stasijeve arhive Marianne Birthler je opozorila, da obdelave početja razvpite vzhodnonemške tajne službe še zdaleč ni konec. Najdeni dokument da kaže na veliko brutalnost, samo s temeljitimi raziskavami pa se lahko spoprimejo z lažmi in legendami. Ker je bil enak dokument že pred desetimi leti objavljen v neki znanstveni publikaciji, kritiki očitajo Birthlerjevi, da poskuša s takšnimi senzacionalističnimi odkritji zagotoviti nadaljevanje dela svojega urada, ki mu grozi zaprtje.

Najdeni ukaz se razlikuje od drugih doslej odkritih po tem, da je v njem neposredno navedeno, da morajo vojaki brezpogojno streljati na ubežnike. V drugih so opozorilni strelji in uporaba orožja omenjeni kot zadnje sredstvo. Že ob postavitvi berlinskega zidu pa je partijski vrh zahteval njegovo varovanje tudi s strelji na begunce. Ne meji z Zahodno Nemčijo je bilo po podatkih različnih raziskav ustreljenih do 780 ljudi, eno od združenj žrtev pa navaja številko 1300. Pri poskusu bega čez berlinski zid je umrlo več kot 130 ljudi.

PETER ŽERJAVIČ

Članek v časniku *Delo* z dne 13. 8. 2007:
Odkritje v arhivih Stasija

6. ZAKLJUČEK

Dokumentarno gradivo ima veliko kulturno in zgodovinsko vrednost za proučevanje razvoja nekega naroda. Spoštovanje gradiva v materializirani obliki (papir) in v vsebinski (zapisano besedilo) sta temelj informacij in podatkov, ki jih je potrebno zavarovati in hraniti.

Pri tem seveda ne smemo pozabiti na vsebine, ki so pomembnejše od ostalih vsebin in jih varujemo strožje kot bi jih sicer. Pravilno varstvo dokumentarnega gradiva zagotavlja ohranjanje vrednosti zapisanih informacij, najsi bodo splošne ali pa zaupne narave.

LITERATURA

- ANŽIČ, Andrej. *Varnostni sistem Republike Slovenije*, Zbirka učbeniki. ČZ Uradni list RS, Ljubljana, 1997.
- BOHINC, Rado. *Uvodni nagovor*. V: *Javna predstavitev mnenj o predlogu Zakona o tajnih podatkih*, Ministrstvo za notranje zadeve ter Visoka policijsko-varnostna šola, Ljubljana, 2001.
- DOBERNIK, Marjan. *Mikrofilmanje kot del sistema trajnega shranjevanja podatkov*. V: *Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja*. Pokrajinski arhiv Maribor, Maribor, 2007.
- ROVŠEK, Jernej. *Dostopnost informacij javnega značaja in dopustnost omejitev z vidika ustave in varstva človekovih pravic*. V: *Javna predstavitev mnenj o predlogu Zakona o tajnih podatkih*, Ministrstvo za notranje zadeve ter Visoka policijsko-varnostna šola, Ljubljana, 2001.
- ŽONTAR, Jože. *Arhivistika*. *Dopisna delavska univerza UNIVERZUM*, Ljubljana, 1984.
- *Revija Mag*, 28. 11. 2007, str. 82.
- *Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/2007)*.
- *Zakon o dostopu do informacij javnega značaja (Uradni list RS, št. 51/2006)*.
- *Zakon o gospodarskih družbah (Uradni list RS, št. 42/2006 s spremembami)*.
- *Zakon o Slovenski obveščevalno - varnostni agenciji (Uradni list RS, št. 23/1999 s spremembami)*.
- *Zakon o tajnih podatkih (Uradni list RS, št. 50/2006 s spremembami)*.
- *Zakon o varstvu dokumentarnega in arhivskega gradiva in arhivih (Uradni list RS, št. 30/2006)*.
- *Uredba o varstvu dokumentarnega in arhivskega gradiva (Uradni list RS, št. 86/2006)*.
- *Uredba o varovanju tajnih podatkov (Uradni list RS, št. 74/2005)*.
- *Uredba o upravnem poslovanju (Uradni list RS, št. 20/2005 s spremembami in dopolnitvami)*.
- *Sklep o določitvi pogojev za varnostno tehnično opremo, ki se sme vgrajevati v varnostna območja (Uradni list RS, št. 94/2006)*.
- *Bančni kodeks Združenja bank Slovenije*. http://www.zbs-giz.si/slo/akti/bancni_kodeks/05-varovanje_bancne_tajnosti.htm.
- http://www.rtvsllo.si/modload.php?&c_mod=rnews&op=sections&func=read&c_menu=2&c_id=120181.

SUMMARY

CLASSIFIED INFORMATION IN RECORDS MANAGEMENT AND ARCHIVES

Record management has a great cultural and historical value for exploring the evolution of a nation. The respect for records in their materialized form (paper) and their content (written text) is the foundation of information and data, which must be protected and preserved for many years. We must not forget more important contents, which are protected more than the others. The correct conservation and protection of records ensures long lasting value of written information, regardless of their general or classified nature.