Revija za kriminalistiko in kriminologijo / Ljubljana 52 / 2001 / 1, s. 3-10

Javnost ali tajnost državnih podatkov*

Janez Pečar**

Arcanis rebus defesse silenter habemus
O skrivnostih je treba molčati.

Upravljanje s tajnimi podatki je posebno nadzorstveno vprašanje tudi zato, ker država omejuje samo sebe predvsem pri porazdeljevanju informacij in ne toliko pri njihovem proizvajanju. Zaradi spoštovanja človekovih pravic in državljanskih svoboščin pa si mora zastavljati tudi ovire in razne obveznosti. Zato predpisuje postopke za zbiranje podatkov, kategorizira zbirke in omejuje njihovo uporabo. Z digitalno revolucijo pa se v informacijski družbi nakazujejo številna vprašanja, ki izhajajo iz moči države pri kopičenju in obvladovanju informacij. Zato se nam zastavljajo vprašanja: kdo sploh sme proizvajati tajne podatke, zakaj ter v kakšnem obsegu glede na naravo zaupnosti; kakšne stopnje diskretnosti dovoljevati pri dosegljivosti podatkov; komu naj služijo tajni podatki; kaj je s transparentnostjo države; kakšna naj bo ustreznost ljudi za upravljanje tajnih podatkov; koliko onemogočati, da državne informacije postanejo tajne in s tem preprečiti dominacijo in manipulacijo ljudi in njihovih skupin; kako urediti debirokratizacijo dostopnosti podatkov brez zapletene juridizacije, in ne nazadnje, kakšna je korist tajnih informacij v primerjavi s stroški upravljanja, če je relativizirana s produkcijo tajnosti.

Ključne besede: država, tajnost, zasebnost, transparentnost, informatizacija, skrivnostnenje, normativizacija, varnostno preverjanje oseb

UDK: 65.012.8:343.322.2

Sestavek skuša obravnavati konfliktnost med skrivanjem državnih tajnih podatkov in pričakovano ter zaželeno prozornostjo države. To je zamotan pojav, močno podoben pravici do obveščenosti ob hkratni pravici do zasebnosti. Ali spopadanju med pravicami in dolžnostmi, ko imajo prednost predvsem pravice in ne dolžnosti (npr. zahteva po varstvu pravic bolnikov, varstvo pravic otrok itd.), ko dostikrat ni jasno, kaj je kaj za koga na eni ali drugi strani prava in ko nastajajo položaji, da ima prav tisti, ki do tega ni upravičen. Ob upravljanju s tajnimi podatki, ki jih ustvarja država gre pri tem še za teoretiziranje in intelektualiziranje polja med ustvarjanjem tajnosti in razkrivanjem ali panoptizacijo (državnih) podatkov, še posebej, ker je pred nami digitalna revolucija.

A. OBVLADOVANJE INFORMACIJ – TEMELJNA NALOGA DRŽAVE

1. Država – nadzorstvo – informacije

Nobena država s svojim pravom in mehanizmi nadzorovanja ter varovanja pred nevarnostmi in ogrožanjem ni neodvisna od politike in oblasti. Vsaka oblast je že od nekdaj v človeški zgodovini nekomu pripadala. Za oblast se že od nekdaj neusmiljeno borijo, in ko jo že imajo, bi jo na vsak način radi obdržali. In prav zato je prenekatero razmišljanje o neodvisnosti, samostojnosti, strankarsko-politični nevpetosti in neprizadetosti in ob popolni avtonomnosti posameznih mehanizmov države – neredko popolna iluzija. Res pa je, da so **posamezni državni mehanizmi različno odvisni od vsakodnevne politike**. Zato imajo razlage o zakonitosti, pravičnosti in enakosti lahko povsem različen pomen. Če pa pri tem upoštevamo še različne stopnje »nadzorstvene ali nadzorovalne« (obvladovalne) svobode, ki jo dopuščajo določenim okoliščinam ustrezni pravni režimi, kake izredne razmere ali upoštevanje posameznih globalnih nevarnosti (npr. konvencija ZN proti mednarodnemu organiziranemu kriminalu – Palermo 12.-15. december 2000), kako prevratno obdobje itd., potem se navadno **dogaja, da namen začenja posvečevati sredstva** in da država, predvsem pa njeni nadzorstveni mehanizmi, vedno nekomu služi(jo). To pa je tisti, ki ima moč, da nadzorstvo sploh ima, da ga ustvarja in postavlja, po svoje oblikuje (v zadnjem času celo prilagojeno zahtevam Evropske Unije), omejuje s predpisovanjem postopkov in mu daje tudi legalnost in legitimnost. Zato se le redko dogaja, da hodita oblast in nadzorstvo vsak svojo pot. Vsaka oblast se najprej potrudi, da ima državo z nadzorstvom po svoji meri, ki bo varovalo njene razredno-politične interese. Ti pa so že od nekdaj odvisni od narave oblasti. To velja tudi za sleherno demokratično družbo, ki vzbuja zaupanje, čeprav ugotavljajo, da demokratična ureditev še zdaleč ni najboljše, kar je mogoče doseči, toda boljšega sistema še nimamo.

Nadzorstvo je s svojo dejavnostjo v vsaki družbi razvejan, danes visoko specializiran, številen in zlasti družbi odtujen mehanizem, ki deluje (kot aparat) po pravu in se vpleta v odkrivanje, dokumentiranje, procesiranje, kaznovanje in ocenjevanje individualnih in družbenih pojavov, kakorkoli nevarnih

* Prispevek za javno predstavitev mnenj o predlogu Zakona o tajnih podatkih, 6. 3. 2001.

** Janez Pečar, univ.dipl. pravnik, doktor znanosti, redni profesor za kriminologijo, Rozmanova 2, 1000 Ljubljana.

za družbenopolitično ureditev. H konvencionalnim kontrolizmom se danes, zaradi novih potreb in zahtev, pridružujejo novi in tudi družbene reakcije zoper kriminal in odklonskost se spreminjajo. Zaradi humanitarnih teženj pa se celo pogledi na kaznovanje sprevračajo pod težo stroškov in koristi v alternativna nadomestila omejevanja človekove svobode. V ta okvir gotovo ne sodi podaljšanje zaporne kazni na trideset let, kar smo pri nas po nepotrebnem sprejeli pod tujimi vplivi, ki nedvomno motijo naš pogled na politiko upravljanja s kriminalom in odklonskostjo. Toda prav to **kaže na nove silnice od zunaj**, ki jih upoštevamo (s tem pa omejujemo lastno samostojnost), in dokazuje oviranje avtonomnosti (majhne) države.

Kakršnakoli nadzorstvena **oblast** pa na področjih svojih dejavnosti, po uradni dolžnosti ali mimo nje, **ustvarja neskončno količino podatkov o ljudeh, pojavih, dogodkih in procesih** in jih zapisuje, dokumentira, arhivira in analizira, sporoča drugim, ali skriva in zagotavlja tajnost. Hkrati tudi vdira v zasebnost, ki je večinoma samo »svoboda, dovoljena od drugih« (Caliman 2000: 390) in jo operacionalizira za preiskovanje, procesiranje, kaznovanje, za terapevtske in druge namene, iz katerih pogosto izhajajo temeljni pogledi na številne dejavnosti sodobne represije, izražene z legitimnostjo kaznovanja, kontrolnim pravom in kompjuteriziranim človeštvom. Zato načeloma tudi kompjuterizacija informacij o ravnanju z ljudmi in obvladovanju njihove zasebnosti služi interesu (kontrolne) oblasti pri zagotavljanju javnega reda in miru, pri čemer imajo največji pomen različne policijske vloge in storitve (celo pri produkciji tajnosti – za naš namen).

2. Zasebnost in državni interesi – transparentnost

Že od nekdaj velja, da je zasebnost določena, predvsem zaželena stopnja osamljenosti (ne označuje jo družinska, skupinska, družbena ali kakšna druga izločenost), ki je za posameznika še posebno pomembna, kadar si to sam želi. S tem naj bi bilo zagotovljeno, da si vsak sam išče in izbira stike z drugimi in jih tudi po svojih izhodiščih vzpostavlja ali omejuje. (Šelih, A. 1977: 202) Zato ima tudi **pravico do varstva tako zasebnosti kot osebnosti**, ki imata različne razsežnosti. Navajajo tri sestavine zasebnosti: zasebnost v prostoru, zasebnost osebnosti ter informacijsko zasebnost (Čebulj J. v Zupančič B.: Ustavno-kazensko procesno pravo 2000: 396). Posamezniku ogrožajo pravice do zasebnosti drugi posamezniki in druge skupine – tako formalno kot neformalno. Predvsem pa mu grozi nevarnost od države. To dokazujejo številni mednarodni akti, deklaracije in konvencije, ter ne nazadnje, skoraj povsod po svetu dejavni varuhi človekovih pravic, kar je gotovo najpomembnejša **državna ustanova za varovanje ljudi pred državno agresivnostjo**.

Včasih se mora posameznik odrekati zasebnosti zaradi nekih državnih interesov in dovoljevati vdiranje vanjo zaradi posegov, ki so večinoma urejeni s pravom. Večina teh možnosti pa je podvržena tudi inštančnemu nadzoru, tako da je vmešavanje javne oblasti podrejeno ustavnemu pojmovanju zasebnosti. Zato je **zasebnost ustavno varovana vrednota**, in poseganje vanjo je dovoljeno le v izjemnih primerih in predvsem takrat, kadar posameznik ali skupine ljudi s svojim vedenjem in ravnanjem ustvarjajo situacije, v katerih so ogroženi družbeni ali državni interesi in ko nastajajo možnosti oškodovanja različnih subjektov, katerih delovanje varuje država kot najbolj pomembna družbena organizacija.

Sodobna država pa zlasti pred koncem drugega tisočletja nenehno ustanavlja, širi in poglablja najrazličnejše mehanizme za varovanje lastnih interesov. Ti mehanizmi so večinoma nadzorstveni in dosti manj varnostni, četudi večini nadzorstvenih mehanizmov ne moremo odrekati varnostnih storitev. Zato sleherni posameznik večinoma vstopa v razmerja z družbenimi ali državnimi nadzorstveninimi mehanizmi, ki na podlagi državne regulative uresničujejo, kot pravimo v nadzorstvoslovju, tako »net widening« kot nadzorstveni »net deepening«.

Posamezniki in cele skupine ljudi so v družbeni skupnosti zato čedalje bolj podrejeni različnim nadzorovalnim tehnikam, različnim normalizacijam in socializacijam, celo terapevtskim obravnavanjem ter interakcijam različnega poseganja v zasebnost. V zadnjem desetletju pa se tovrstne dejavnosti celo privatizirajo in komercializirajo ali pa potekajo kot samoorganiziranje in samopomaganje v prostovoljnih, karitativnih, samaritanskih ali pa verskih skupinah. S tem pa nastajajo čedalje večje **možnosti za poseganje v človekovo zasebnost in svobodo,** kar je marsikomu neprijetno, nadležno, nesprejemljivo, nezaželeno in je marsikdaj sploh nedopustno.

Toda zaradi odklonskega vedenja ali samo zaradi suma nanj, mora vsakdo v pravni državi, v vladavini prava, ob pravni varnosti in ob splošnem zaupanju v pravo, računati z ukrepi ustreznih »kontrolizmov«, včasih celo »ante delictum« in ne samo »post delictum«, ko je posledica že tu. Kajti država mora delovati »po uradni dolžnosti«, ko to izzovejo indici, ki kažejo na nevarnost. Človeško **življenje je torej neprestano omejevanje in prilagajanje drugim** pa tudi državnim regulacijam, pri čemer nihče ne more pričakovati, da bo smel početi, kar bi se mu zljubilo, in pri čemer sme prav tako računati, da mu bodo, vključno z državo, pomagali drugi, kadar bo ogrožen. In ker moramo pri tem nenehno upoštevati ne le pravice, ampak tudi omejitve, se je treba zavedati možnosti poseganja v posameznikovo zasebnost, osebnost, svobodo in pravice.

Svet postaja v marsičem, prav zaradi zasebnosti, svoboščin in prava čedalje bolj omejevan. In več ko je omejitev, več je ogrožanja, in več ko je ogrožanja, več kontrolizmov se ustvarja. Prihajamo v položaj, ko prav določeni kontrolni mehanizmi nadzorujejo druge kontrolizme. S tem pa se zdavnaj preko-

računje staro vprašanje Rimljanov »Quis custodiet (ipsos) custodes«, ker večino nadzorovalcev spet nadzorujejo druga nadzorstva. Zato prihaja do novih moralnoetičnih dilem, ki jih sprožajo konflikti in interesi med zasebnostjo in varstvom interesov oz. razmerja med posameznikom in državo (in njenimi kontrolizmi) oz. transkontrolizmi in panopticizmi, in ko se **ustvarja množica podatkov o človeškem vedenju in ravnanju** ter o njegovi prosojnosti.

Človeška »prozornost« pa je tista okoliščina, ki jo sleherna država želi kar najbolj **udejaniti zaradi lastne učinkovitosti**, z množico strokovnjakov in raznimi tehnikami, testi, načini in sredstvi vdiranja v zasebnost, in uravnavati ljudi v željeni smeri zaradi nekih višjih ciljev ali za čisto preprosto normaliziranje in nadzorovanje. Toda obe strani varujeta vsaka svojo zasebnost in diskretnost in se hkrati upirata transparentnosti – tako posameznik kot njegova država.

3. Ustvarjanje podatkov, namen in razvrščanje

Mehanizmi družbenega nadzorovanja ustvarjajo neskončne količine informacij, ki služijo različnim namenom, predvsem pa nadzorovalnim, preiskovalnim in kaznovalnim, usmerjevalnim, reaktivnim in proaktivnim in sploh operativnim, strateškim, preventivnim in ne nazadnje tudi raziskovalnim. Dokumentirane so različne človeške posebnosti: fizične, fiziološke, psihične, ekonomske, kulturne, socialne, vedenjske in druge, med katerimi je dosti takih, ki bi jih marsikdo **najraje obdržal zase, ker sodijo v skrivnosti,** ki jih nerad odkriva drugim. Pomenijo osebne značilnosti, katerih uporabnost je lahko v izbranih situacijah za posameznika usodna. Zato ni odveč poudariti, da se nekateri nadzorstveni mehanizmi za prav določene namene naravnost trudijo pridobivati podatke, s katerimi vodijo določene osebke v smereh, v katerih ga potrebujejo in izrabljajo diskretnost podatkov za pridobivanje nadmoči. Zaradi takih podatkov se mora posameznik dostikrat odločati med dvema zloma. Tega se že od nekdaj zavedajo vse obveščevalne, preiskovalne in podobne službe tega sveta.

Baze podatkov omogočajo vdiranje v zasebnost, dopuščajo manipuliranje z ljudmi, infiltriranje v skupine in izvajanje dominacije nad njimi; pospešujejo nadzorovanje, zagotavljajo obvladljivost razmer in poleg vsega naravnost vabijo k uporabi za druge namene, ki so daleč od tistih, zaradi katerih se posamezne zbirke sploh oblikujejo. In to na podlagi prava, zakonskih in podzakonskih aktov, s katerimi se določajo: vrsta zbirk, stopnje zaupnosti, ukrepi in postopki za varovanje, pravice in varstvo pravic registrirancev, tja do nadzora različnih vrst. Zbirke se poleg operativnih namenov uporabljajo še za različne preglede, analize, strategije in politike, kot so lokalne, sistemske, globalne itd. Zbirke večinoma uporabljajo avtorizirani dejavniki za svoje potrebe, se okoriščajo z različnim podatkovnimi bazami, tako da ustvarjajo »prosojnost« posameznih področij, pojavov in procesov, ljudi in skupin, ki za to največkrat sploh ne vedo, kljub pravici do vpogleda in normativizaciji zagotavljanja domnevnega varstva. Toda, kaj se v resnici dogaja in kaj se sploh skriva za tem – to največkrat sploh ni znano, ker je **država** dovolj vešča delovati nejavno in prikrito, saj **ima** v ta namen **dovolj visoko specializiranih ljudi, ki morajo varovati** (državne) **tajnosti.** In tisto, kar se ne ve, nikogar ne boli, ne glede na to, ali je bilo kaj uporabljeno v skladu z načelom sorazmernosti ali ne, in ne glede na to, ali je bilo z manjšim zlom vendarle odpravljeno večje.

Zbiranje podatkov o ljudeh **je** bilo že od nekdaj **namenjeno discipliranju,** normaliziranju, razvrščanju, spreminjanju in kaznovanju. Klasificiranje pa je v stoletju, ki smo ga zapustili, predvsem s kompjuterizacijo doseglo nesluten razmah in postalo pomembna dejavnost v nadzorstvenih disciplinah. Klasificiranje in kategoriziranje je danes nepogrešljivo pomagalo v strokah, ki se kakorkoli ukvarjajo s kriminaliteto, odklonskostjo in drugimi asocialnimi pojavi ne glede na kontrolizme, ki jih obravnavajo. Kajti formalno nadzorstvo si že od nekdaj veliko obeta od dovršenega razvrščanja ljudi, kar mu omogoča uspešnejše, racionalnejše, hitrejše, cenejše in bolj usklajeno delovanje. Zato ugotavljajo, da je »moč klasificiranja najčistejša usedlina profesionalizma» (Cohen S.: Visions of Social Control, 1985: 196), čeprav ni malo kritik, ki opozarjajo na klasifikacijsko nepodjetnost, na psihozo klasificiranja, na pretiranost tipoloških pričakovanj itd.

Tudi nekatere baze podatkov vzbujajo dvome v pravno neoporečnost, v zanesljivost njihovih upravljalcev, zadržanost glede ustreznih pristojnosti, nezaupanje v neodvisnost zbiranja podatkov za določene namene itd. Nasploh pa je **državljan nemočen in sam pred državo,** ki ga s svojim centralnimi ali lokalnimi in celo zasebnimi bankami podatkov dela prosojnega in ga bodisi individualizira bodisi generalizira, odvisno za kaj sploh gre bodisi v splošnih bodisi v posebnih okoliščinah. To pa so tiste, v katerih se podatki uporabljajo za predkazenski ali kazenski postopek, za kriminalno prognozo, za rehabilitacijo, za resocializacijo, za odmero kazni ali za različne obveščevalne ali protiobveščevalne, varnostne in druge namene. Zato formalno-državno nadzorstvo z vsemi svojimi mehanizmi sploh ne more več brez bank podatkov, raznih tipologij, razvrščanja in klasificiranja, **vključno z določanjem** narave oz. **stopnje tajnosti.** Ta se morda iz »usedline profesionalizma«, kot pravi znameniti nadzorstvoslovec Cohen, spreminja v »korenine birokratizma«, ki tipizira človekovo osebnost po pomenskosti razvrščanja, ne pa po vsebini, delovanju in rezultatih človekovega vedenja in ravnanja.

4. Normativizacija informatizacije

Z razvojem odnosov med ljudmi in v tem okviru zlasti v razmerjih med državljani in državo, ali natančeneje, med državnimi kontrolnimi organi in njihovimi klienti, je slej ko

prej moralo priti do tega, da so **začeli urejati pravice in dolžnosti obeh strani** tudi pri evidentiranju, registriranju, arhiviranju in ohranjevanju podatkov, tja do dostopnosti oz. javnosti vsaj določenega dela nadzorstvene informatizacije. Četudi ostaja del podatkovnih baz posameznih kontrolnih mehanizmov vendarle pod določenim embargom, vendarle prihaja do opaznejše transparentnosti države na splošno, kontrolizmov pa še posebej. To se seveda ni zgodilo čez noč, poteči so morala stoletja, da se država polagoma odpira družbeni skupnosti, ne nazadnje tudi pod vplivi političnih gibanj za človekove pravice in državljanske svoboščine, ki jih podpirajo svetovne in mednarodne organizacije. Počasi pride do tega, da se zlasti kontrolnim in preiskovalnim mehanizmom **začno omejevati nezakoniti načini pridobivanj informacij,** ki pomenijo vdiranje v zasebnost, čeprav se tudi to dopušča v izjemnih primerih, ki jih določa državno pravo – od ustavnega navzdol.

Zato se v okviru državnega delovanja na področju njene lastne informatizacije srečujemo z več možnostmi ne le omejevanja pri pridobivanju podatkov, ampak tudi pri upravljanju informacij. Tako se danes sodobna država v informacijski (in delniški, borzni, kapitalistični itd.) družbi omejuje in hkrati nadzoruje pri zbiranju, evidentiranju in registriranju, razpolaganju in objavljanju svojih podatkov.

Ker pa državno nadzorstvo sestavljajo različni podsistemi, je **ureditev obvladovanja podatkov dokaj obsežna in razvejana.** Vsaka človeška dejavnost je namreč že od nekdaj močno nadzorovana in to na različne načine – celo z multikontrolizmi (formalno in neformalno). Do regulacije varstva podatkov ali ureditve kontrolne informatizacije pa prihaja dokaj pozno in to predvsem iz naslednjih razlogov: zaradi količine podatkov, ki jih zbira in upravlja država; zaradi možnega ogrožanja človekovih in državljanskih svoboščin – to se povečuje z vedno bolj uspešnim obvladovanjem posameznikove zasebnosti in zaradi zmogljivosti uporabe podatkov s pomočjo sodobne informacijske tehnologije ter hitrejšega prenosa informacij z enega dela sveta v druge.

Danes je **delovanje številnih državnih nadzorstvenih organov podprto** z računalništvom, informatiko, opazovalno, zasledovalno in preiskovalno tehnologijo, različnimi taktičnimi in metodičnimi sredstvi, posameznimi strategijami, ob sodelovanju raznih znanosti in izsledkov, nastalih sicer za popolnoma drug namen, vendar uporabnih za vdiranje v posameznikovo osebnost in njegovo obvladovanje in ogrožanje človekovih organizacij. Zato lahko danes državno nadzorstvo prodira v vse pore človekovega življenja tako, da ob poznavanju preteklosti lahko trdimo, da je sedanje nadzorovano življenje kupljeno za ceno človekove svobode na načine, s katerimi je obvladovana civilizacija.

Zato pa je nujno potrebna regulacija varstva osebnih in drugih podatkov. V središče naše pozornosti gotovo prihajajo vsi nadzorstveni podsistemi, ki se med seboj povezujejo za skupno obravnavanje odklonskosti in kriminala, poboljševanje vedenja in varovanje družbene skupnosti pred kakršnimkoli ogrožanjem. Vsak izmed njih ima svoja sredstva in norme, ki veljajo samo zanj, čeprav so vezani tudi na splošne predpise, ki jih zavezujejo že zato, ker so njihovi končni cilji – identični. Ker pa državni nadzorstveni mehanizmi niso samo zaradi oblasti, marveč tudi zaradi ljudi, se nam **država tudi pri kontrolni informatizaciji začne ponujati v dveh vlogah hkrati: v obremenjevalni in zaščitniški.** Na eni strani zbira o nas podatke, za katere največkrat menimo, da bi bilo najbolje, če jih ne bi bilo, ker so nam predvsem v škodo. Po drugi strani pa nas ščiti celo pred samo seboj s tem, da omejuje sebe pred agresivno, razbrzdano in nenadzorovano uporabo informatizacije. To je gotovo ambivalentnost ali contradictio in adiecto ter nas spominja na hipokrizijo, ki jo je redko videti tako jasno pri drugih sistemih. **Toda regulacija varstva** osebnih podatkov, določanje zaupnosti podatkov, varovanje podatkov in sploh uporaba državnih in drugih tajnosti, varovanje informatorjev ter infiltracijskih operacij, prestrezanje digitaliziranih informacij, predpisovanje varnostnih ukrepov, varstvo podatkov pred odnašanjem na tuje, varovanje informacijske zasebnosti, pravica vpogleda, svoboda informacij, zakonitost in pristojnost informacij, urejenost različnih okoliščin in pogojev za razraščanje informacij, izmenjava podatkov in kontrola in celo (de)centralizacija ob morebitnem zadrževanju in združevanju informacij, trajanje informacij tja do različnih konvencij, deklaracij in sporazumov, **kažejo na vso zapletenost pojava.** Toda, ali je lahko drugače?

5. Telekomunikacijska tehnologija v nadzorstveni informatizaciji

Preskrbljenost mehanizmov formalnega nadzorstva z ustreznimi podatki je najpomembnejša okoliščina za uspešnost njihovega delovanja. Avtomatizacija prenekaterih dejavnosti in opravil omogoča dosegati boljše rezultate kot v preteklosti, vsaj pričakovati je tako, kljub splošnemu nezadovoljstvu z državnimi organi in pri nas še posebej s sodstvom. Toda telekomunikacije, digitalizacija, kibernetizacija in podobno, so danes ključni problemi intelektualizacije, pogosto dokaj preprostih dejavnosti, ki se **morajo meriti z vitalnostjo kriminalnega podzemlja.** Ta se kaže predvsem z intelektualizacijo mednarodnega organiziranega kriminala, gospodarske odklonskosti (s pranjem denarja, nevidno kriminaliteto, kakorkoli povezano z delovnim mestom), ekološkim ogrožanjem in strukturalno deviantnostjo močnih in elit v katerikoli družbi. Ti delujejo s protiinformatizacijo, tehničnimi, taktičnimi in strateškimi sredstvi ter metodami, ki jih ne omejujejo nobeni moralni in pravni zadržki. Kajti njihova osrednja motivacija je izključno samo – dobiček.

To pa pomeni, da sta obe strani (država in kriminalne organizacije) nenehno v spopadu, pri čemer državo »poganja pravo« s poklicnim etosom nadzorovalcev, medtem ko krimi-

nalni svet navdihuje z ničemer ovirana želja po dobičku, za katero veljajo morda samo tista pravila, s katerimi se vzdržuje delovanje kriminalne organizacije. **Nobena** od obeh plati ni **brez telekomunikacij in lastne informatizacije,** čeprav še tako primitivne. Toda razloček je v tem, da se sleherna država, tudi s pravom, omejuje v svobodi informiranja in izkoriščanja marsičesa, kar bi ji lahko pomagalo k uspešnosti. Zato gre prav na tem področju za čedalje večjo »neenakost v rabi orožja«, ki bo mehanizme formalnega nadzorstva vedno bolj ovirala, kot mu telekomunikacijska tehnologija pomaga. To je gotovo spet ena od modernih hipokrizij, ki se kažejo v neprilagodljivem uporabljanju načela, da morda vendarle velja z majšim zlom odpravljati večje. Toda, kdo naj vnaprej presoja, kaj bo kaj?

»Informacija je sama po sebi značilnost oblasti« (Burkinshau v Zupančič et al. s. 424). Vendar, **informacije niso samo v posesti državne oblasti.** S telekomunikacijami v digitalni dobi jih je čedalje več na drugi strani zakona, to je na tisti, ki se oblasti upira in kot mednarodni organizirani kriminal postaja država v državi. S to državo v državi pa se ni vedno mogoče spoprijemati v rokavicah, hkrati ko pravna država pri svoji dejavnosti ne sme posnemati tiste, ki ni »prava država«.

Informacijska družba prihodnosti naj bi bila načeloma **odprta družba,** v njej naj bi bilo sleherniku dostopno vladno odločanje in navsezadnje tudi omogočen vpogled v državne podatke, k čemur se deloma približujemo tudi pri nas – sicer s številnimi omejitvami. Že globalni telematični koncepti, gostota in intenzivnost informacij za nadzorstveno dejavnost, kiberprostor nasploh in prizadevanje za varnost v njem, kultura elektronske svobode, digitalizacija prihodnosti, avtomatizirano obdelovanje podatkov z videonadzorovanjem in elektronskim prisluškovanjem, zunanjim in notranjim opazovanjem, vključno z avtomatizirano vizualizacijo, in različne druge informacijske tehnike ustvarjajo **pomisleke tako o svobodi informiranja** (transparentizacija) kot o blokadah in **zadržkih, ki te svobode ne dopuščajo** (klandestinizacija). In potem se res postavi vprašanje, »za kakšno vrsto informacije gre, in če jaz ne vem, ali je kdo upravičen, da ve namesto mene in do kakšnega obsega je ta upravičen, da (iz)ve?« (Burkinshau v Zupančič, prav tam, s. 242).

S tem v zvezi pa ne gre samo za (državne) upravljalce podatkov, ampak tudi za vdiralce v banke podatkov in za izkoriščanje informacij in telekomunikacij za nezakonite in povsem kriminalne namene. Poznavalci menijo, da bo prestrezanje digitalnih podatkov čedalje lažje, kljub morebitnemu šifriranju in raznim možnostim prikrivanja, pri čemer nikoli ne bo zagotovljena pričakovana mobilizacija prava z ustrezno previdnostjo in protiukrepi. Sodobna telekomunikacijska tehnologija skoraj vsakemu omogoča dostop do različnih podatkov na nezakonit način. S tem pa se hkrati začenja tudi boj zoper nezakonito prestrezanje komunikacij, elektronski vandalizem in terorizem, telekomunikacijsko piratstvo in druge možnosti ogrožanja zbirk podatkov in vdiranje v zaupnost informacij.

Zato gre za dvoje nevarnosti: neustrezno upravljanje državnih in nedržavnih (zaupnih) informacij in za onemogočanje nepooblaščenega vstopanja vanje, bodisi za državne bodisi za povsem nedržavne interese in namene.

B. »VARNOSTNO PREVERJANJE OSEB« V DRŽAVNEM UPRAVLJANJU TAJNIH PODATKOV

S splošnimi nadzorstvenimi pogledi na kontrolne telekomunikacije in državno varovanje podatkov velja obravnavati tudi nekatere dejavnosti in opravila, ki zadevajo to varovanje. Kajti pravne regulacije na področju telekomunikacijske in informacijske odklonskosti odpirajo veliko vprašanj, ki jim velja pozornost tudi pri obravnavanju tajnosti. Pri tem ne gre samo za državno zlorabljanje, marveč tudi za nove oblike kriminala, poleg doslej znanih – z angleškimi izrazi – tapping, bugging, tracking, spying, hacking, scanning (Grabosky Smith 1998) itd.

Z upravljanjem tajnih podatkov se povezuje med drugim tudi »varnostno preverjanje oseb«, urejeno že s 36. členom Zakona o policiji (Ur. list 2040 – 49/98, z dne 3.7.1998). V tem členu je določeno, kakšna dejavnost je to, za kaj se ustanavlja, kdo so subjekti preverjanja, koga se varuje itd. Ključno pri tem je »ugotavljanje morebitnih varnostnih zadržkov« za delo, ki ga kdo opravlja pri nekom in za nekoga. Seveda, kolikor se ta dejavnost povezuje s tajnostjo podatkov.

1. Proizvajanje tajnosti

Tajnost je že od nekdaj vse, kar je treba skrivati pred drugimi, da ne bi uporabili zoper tistega, ki bi rad ohranjal skrivnost predvsem zase in za tiste, ki jim povsem zaupa. Že pri Rimljanih je veljalo načelo: »Cela secreta, loquere pauca« (Skrivaj tajnost, govori malo). Pri celotni problematiki obravnavanja tajnosti je vedno **več ukrepanja pri upravljanju s tajnimi podatki,** potem ko že na kakšenkoli način obstajajo, **kot pa previdnosti pred njihovim ustvarjanjem.** O čuvanju skrivnosti je vedno dosti pravil, neprimerljivo manj pa se govori o njihovi proizvodnji. Če ustvarjanja državnih (in drugih) skrivnosti ne bi bilo toliko, bi imeli dosti manj opraviti z njihovim varovanjem. In če je varovanje dokaj urejeno, se ustvarjanje pretežno prepušča diskrecionarnemu in selektivnemu administriranju, sicer določenega kroga oseb, ki delujejo na ohlapno določenih področjih. Pri tem pa so za varnostno preverjanje povsem izvzete osebe, ki tajnosti sploh proizvajajo.

Določanje tajnosti se prepušča odločanju po prostem preudarku ali diskreciji. Prosta presoja pa pomeni, da so v okviru določenega in pravno urejenega delovanja dopustne in možne osebne in od posameznikove volje odvisne, dogodku primerne odločitve o tem (Cohen, A. 1966: 110) (za tale naš namen), ali je nek podatek skrivnost in za kakšno skrivnost gre in še kaj zraven.

Večina pravnih ureditev omejuje diskrecijo in selekcijo pri odločanju – če je le mogoče. Vendar je pri tem pogosto zelo težko predvideti vse mogoče skupne in skladne lastnosti in jih normirati za praktično rabo. Hkrati ko je spet problematično prepuščati ustvarjanje tajnosti nedoločenemu številu nenehno menjajočih se ljudi z različnim dojemanjem družbene resničnosti, da se ad hoc odločajo o nečem in prilagajajo svoja merila številnim okoliščinam ustvarjanja tajnosti po lastnih izhodiščih.

Zato se prav tako **pojavlja potreba po regulaciji ustvarjanja tajnosti,** morda tudi zato, da bi se izognili razraščanju pravil o njihovem varovanju.

2. Različnost tajnosti

Različnost tajnosti in odločanje zanje večinoma temelji na teži in stopnji možne sumničavosti. **Sum je za nadzorovanje najpomembnejša okoliščina,** ki narekuje ustrezno odzivanje na pričakovane posledice, ki jih je treba preprečiti, še preden nastanejo. Torej je tajnost in upravljanje s tajnostmi večinoma **preventivno delovanje sui generis.** Zato se v proizvodnji tajnosti že od vsega začetka določajo ne le stopnje, ampak tudi postopki, kako ravnati z njimi in kakšne lastnosti morajo imeti upravljalci s tajnostmi vnaprej določenih vrst.

To ima nedvomno **več posledic.** Prva je gotova v selekciji določanja stopenj, ki temelje na ravni »zaupnosti«, ki jih spet določajo selektivno in diskrecionarno, kljub morebitnim posledicam pri kasnejšem varovanju. Tajnost in njene stopnje ustvarjajo določene ali pooblaščene osebe, ki navadno, kot večina praktičnih nadzorovalcev, nikoli niso psihofizično in varnostno preverjene. Zato se lahko marsikaj dogaja, kar ne bi bilo treba, in je tudi vprašanje različnosti tajnosti mogoče problematizirati, kot npr., kaj vpliva na odločitev, da nekaj ogroža »obstoj ali vitalne interese«, »hudo oškoduje varnost« ali »škoduje varnosti« ali pomeni možno »škodo delovanju državnih organov« Republike Slovenije.

Take splošne določbe spet dopuščajo široko prosto presojo in odločanje, ki je lahko že samo **zaradi izredne širine – škodljivo.**

3. Upravljanje tajnih podatkov

Sodobna država zelo spoštuje, zlasti s svojimi nadzorstvenimi, obveščevalnimi, preiskovalnimi in varnostnimi mehanizmi – kljub demokratizaciji družb, kjer delujejo – načelo: »Secretum est inter duos tantum« (Skrivnost je samo med dvema). Zato **omejuje število ljudi, ki so upravičeni vedeti, kar je drugim nedostopno.** In če že skrivnosti ne zadevajo zgolj varstva države, njenih interesov in varnosti sploh, pa so nekateri v posameznih položajih zavezani k molčečnosti zaradi preiskovalnih, varnostnih in prenekaterih zasebnih interesov. Zato je občutljivost za določanje tajnih podatkov najbolj očitna pri mehanizmih, ki jim je skrivnostnost – osrednja lastnost pri opravljaju svoje dejavnosti. Sicer pa je nasploh znano izhodišče, da so najboljši in najbolj sposobni tisti kontrolizmi države – o katerih nič ne vemo. Seveda se za »tajinstvenostjo« neredko skriva še kaj drugega, kot bi pričakovali, o čemer nam zgodovina človeške družbe ponuja nešteto podatkov, zgodb, konfliktov in predvsem nezakonitosti. Nekateri mehanizmi države pa so **zaradi tajne dejavnosti tudi slabo nadzorljivi.** Prav »nenadzorljivost« je danes ena izmed tistih ugank, ki terjajo rešitve o tem, kako nadzorovati tajne in podobne službe in kako regulirati ravnovesje med njihovo prozornostjo in skrivnostnenjem. Sodobnost je danes čedalje bolj občutljiva za neprosojnost državnih dejavnosti, ki se vzdržujejo z davki in ki tajno vdirajo v našo zasebnost za državno rabo.

Zato prihaja upravljanje tajnosti od časa do časa vendarle v središče zanimanja ne samo kar zadeva prosojnost regulacij, ampak tudi drugače, za politično, publicistično, državljansko in podobno rabo. Hkrati pa se s tem v zvezi odpira **vprašanje, ali je koristno vzdrževati** velike količine (državnih) tajnih podatkov, ob razraščanju zasebnih zbirk podatkov (zasebnovarnostne dejavnosti, zasebni detektivi, zasebne obveščevalne dejavnosti, informatizacija političnih strank itd.) in stroškov države, ki nastajajo z njihovim upravljanjem. O tem sorazmerju nihče ne ve veliko. Podatki o problematiki se navadno ne razkrivajo, ker noben državni organ, ki upravlja podatke, ne objavlja izdatkov z zbirkami in ne razgrinja razmerja med stroški in koristmi (cost/benefit). Kakšna pa sploh je korist od tega, da imamo »tajne podatke«? Ali je ta cost/ benefit sploh izračunljiv? Zasebnik bi nam verjetno lažje odgovoril, kaj se mu splača s tem početi, ali je to sploh dobičkanosno? Država se za ta vprašanja ne zmeni. Mi pa smo sploh srečni, da imamo svojo državo.

4. Pristajanje na varnostno preverjanje

»Varnostno preverjanje oseb« je samo segment celokupne problematike tajnosti državnih podatkov in se odpira zaradi ljudi, ki si največkrat šele prizadevajo za dostop do skrivnosti, s katerimi se bodo srečevali pri svojem delu. To pomeni, da si morajo **pridobiti »potrdilo«,** da ni varnostnih zadržkov za delo, ki ga bodo opravljali, in **odvrniti sume** o svoji varnostni neoporečnosti. Šele to omogoča, da se zaposlijo na delovnih mestih, ki jih »prežemajo skrivnosti« različnih vrst. Pri tem pa naj bi najprej (razen izjemoma) sami pristali bodisi na **enostavno** bodisi na **razširjeno varnostno preverjanje,** s katerima ugotavljajo, ali obstajajo varnostni zadržki ali ne.

S soglasjem prizadetega za njegovo preverjanje si želijo tovrstne ureditve ohraniti čiste roke, kar jim velja priznati v dobro. Kajti vsaka država lahko to opravlja brez soglasja, kar

res največkrat počenja brez naše vednosti. Vemo namreč, da se večina sumov o storitvi kakšne nepravilnosti preverja brez soglasja ali pa šele na kasnejšo pisno odločitev pristojnega državnega organa. Tu pa se upošteva pravilo: »Pravijo, da je skrivno storjeno tisto, kar se napravi brez vednosti tistega, ki ga zadeva« (Clam fieri dicitur illud quod fit ignorante eo ad quem res pertinebat – Farinacius). Za »varnostno preverjanje oseb« pa naj bi bila odpravljena skrivnostnost preverjanja. Najbrž se res ne spodobi, da bi še preverjanje ljudi za upravljanje s tajnimi podatki – »klandestinizirali«. In če kdo izmed možnih preverjancev ne da pisne privolitve z navedbo podatkov, ki posegajo v zasebnost s prenekaterimi vprašanji (o zadolženosti in finančnih obveznostih, o odvisnostih in zasvojenostih, o stikih s tujimi varnostnimi obveščevalnimi službami itd.) potem se že naprej odreka delovnemu mestu, katerega varnost se na ta način preverja. Vsakdo mora torej sam in vnaprej avtorizirati svobodo ugotavljanja svoje transparentnosti.

Če naj bi bilo v demokratični družbi kaj pomembno bi lahko bilo naprej to, da bi tudi vsi tisti, ki jih ne zadevajo določbe, ki urejajo varnostno preverjanje, vsaj pred nastopom državnih fukcij izročali nakakšne izjave (o svoji varnostni neoporečnosti), ne da bi jih varnostno preverjali. V nekaterih postsocialističnih družbah so državne funkcionarje res izpraševali npr. ali so sodelovali z obveščevalnimi ali podobnimi službami v bivšem režimu. Pri nas pa naj bi bili pod **udarom strogosti varovanja tajnost predvsem nižji ešaloni upravljalcev** in ne državni funkcionarji kot da med njimi nikoli ni bilo nobenih vohunov. Ali vohune ob transparentnosti naše države od zunaj sploh še kdo potrebuje? Ali predlagana ureditev ne pomeni politične »subordinacije« našega formalnega nadzorstva že vnaprej?

5. Razlikovanje v upravljanju tajnosti – dajanje prednosti

Razločevanje državnih podatkov se kaže v urejenosti posameznih stopenj (državna tajnost, stroga tajnost, tajno in interno), v preverjanju ljudi za primernost ravnanja s posameznimi stopnjami, v enostavnem in razširjenjem preverjanju, po trajanju dostopnosti podatkov, skupaj z začasnostjo upravljanja s podatki najnižje stopnje in še čem.

S **tovrstnim razlikovanjem tajnosti se razločujejo tudi ljudje,** toda ne po kvalifikacijah, potrebnih za stroko, marveč po nekih povsem drugih – to je »varnostnih« izhodiščih, ki ostajajo formalnopravno povsem neurejena in spet prepuščena nekim docela personaliziranim in ad hoc izbranim načelom. Pri tem ni nobenega pravnega avtomatizma, ampak **spet prosta presoja** o tem, komu je lahko »dovoljen dostop do tajnih podatkov«. V tem je gotovo videti »moč eksekutivcev«, ki po nekih »sumih« odločajo, kaj je treba upoštevati pri ugotavljanju primernosti ali neprimernosti upravljanja s tajnimi podatki določenih stopenj in kako omejevati dostopnost, da ne bi prišlo do nepooblaščenega posredovanja tretjim osebam. O tem seveda odločajo predvsem tisti, ki so nasploh pooblaščeni za ustvarjanje tajnih podatkov (ki pa se jih večinoma varnostno sploh ne preverja).

Dostop do tajnih podatkov se torej omejuje na ozek krog ljudi, ki se jim daje moč za razpolaganje s podatki, kar je povsem sprejemljivo in verjetno ni pričakovati drugega. To v državnih nadzorstvenih službah (kjerkoli po svetu) nujno pelje ne le v razlikovanje med ljudmi zaposlenimi v nekem organu, ampak tudi, da se jim daje **prednost zaradi opravljanja dejavnosti,** za katere so pooblaščeni oz. h katerimi so prepuščeni na podlagi varnostnega preverjanja (na katerega so prej pristali – ker bi se sicer odrekli zaposlitvi na prav določenih, verjetno najbolj »vročih« delovnih mestih).

Ta previdnost pa je dosti ohlapnejša, ko gre za »premeščanje« tajnih podatkov »organizacijam, gospodarskim družbam in drugim subjektom«, s katerimi naj bi se sklepale pogodbe o tajnih podatkih, ki jih dobijo »samo, če je to nujno potrebno za izvršitev nalog državnega organa«. S tem pa se lahko odpira »velika luknja« in to brez »cedila«, s čimer popušča državna previdnost v korist dvomljive »transparentizacije« tajnosti. **Seveda spet po prostem preudarku oz. diskrecionarno.**

C. SKLEP

Udeležba Slovenije v najrazličnejših mednarodnih povezavah, harmonizacija našega prava z evropskim, ugotavljanje naših sposobnosti od tujih strokovnjakov (celo za slovensko vojsko) in druge oblike mednarodnega sodelovanja, satelitsko nadzorovanje, privatizacija države, mednarodno poizvedovanje in nadzorovanje (projekt Ešelon) itd. **zmanjšujejo pomembnost varovanja tajnih podatkov** do te mere, da se moramo vprašati, kaj sploh lahko še ostane tajnost, ki »ogroža obstoj ali vitalne interese Slovenije«. Prav to je verjetno največja hipokrizija pri upravljanju in sankcioniranju varstva tajnosti. Tu gre za »curljanje« podatkov skozi špranje, medtem ko nam dragocen informacijski kapital uhaja skozi glavna vrata. Že samo zato se ustanavljanje nekega »Urada za nadzor nad tajnimi podatki» kaže v naših razmerah kot megalomanija in neutemeljeno širjenje državne uprave ter ustvarjanje novih stroškov. Dosti več bi morali storiti za primerno tako **družbeno kot individualno varnostno kulturo,** da ne bomo priče »odtekanja« in »curljanja« najrazličnejših informacij iz državnih organov – od parlamenta navzdol. S tem pa seveda ni rečeno, da ne potrebujemo nobene regulacije o upravljanju državnih podatkov in enotnih pogledov nanje – od ustvarjanja do njihovega minevanja.

Osrednje vprašanje, kolikor sploh potrebujemo zakonodajni akt o tematiki, je omejevanje diskrecije in to od proizvajanja tajnih podatkov do njihovega upravljanja ter zoževanja števila ljudi, ki tajnost sploh določajo in z njo kakorkoli

manipulirajo. In prav s tem v zvezi bi se že sam »akt« lahko imenoval tudi drugače. Predlog v naslovu predvsem poudarja ravnanje s tajnimi podatki in ne njihovo nastajanje. Oboje pa bi moralo postati **uravnoteženo.** Še posebej, ker ostaja zasebno upravljanje »skrivnih« podatkov zunaj vsake regulacije. Toda negativne posledice se vedno pokažejo pri nepooblaščenem (nezakonitem – kolikor ne kaznivem) izročanju informacij in zato je razumeti skrb za nezaželeno tveganje hrambe »tajnih podatkov« z dokajšnjim številom ljudi. Že zato je odkrivanje vohunstva neproduktivno in zapleteno, pri čemer je tudi raba represije povsem neučinkovita. Toda ta represivnost se odraža tudi z zasnovo predloga, ki je zelo podroben in hkrati pooblašča vlado še za tri podzakonske akte.

Regulacija upravljanja s tajnostmi ne načenja državne zlorabe informacij za ogrožanje zasebnosti. To, kar nam ponuja, vzbuja vprašanje: koliko zasebnosti sploh imamo, pred kom jo skrivati in zakaj, kaj početi z njo, kako jo varovati itd. Pri tem gre za specifično nacionalno zakonodajo, ki z vstopom v Evropsko Unijo lahko kasni ali pa je prezgodnja v svoji evropeizaciji, ki ima polno neznank. Zaradi tega je **tematika tajnosti, zaupnosti, skrivnosti itd. izjemno zanimiva tudi za javnost** in ne samo za državno upravljanje informacij in varstvo informacijske zasebnosti. Še posebej, ker ostaja zasebno upravljanje skrivnih podatkov zunaj vsake regulacije. Toda ključni namen je vendarle onemogočanje ali celo odpravljanje infiltracijskih operacij v državne tajnosti – vsaj formalno. Največja količina tajnosti pa danes prihaja v tuje roke povsem neformalno – ker smo (ali bomo) informacijska družba.

Sestavek končan 28.12.2000

LITERATURA:

1. Caliman, C. (2000). La gestion de l'information policère dans la loi du 7 décembre 1998 et les principes relatifs à la protection de la vie privée. **Revue de droit pénal et de criminologie.** 2: s. 389-426.
2. Cohen, A. (1966). **Deviance and Control.** Englewood. Prentice Hall.
3. Cohen, S. (1985). **Visions of Social Control.** Cambridge, Polity Press.
4. Foucault, M. (1984). **Nadzorovanje in kaznovanje.** Ljubljana, Delavska enotnost.
5. Grabosky/Smith. (1998). **Crime in the Digital Age**-Controlling Telecomunications and Cyberspace Illegalities. New Yersey, Federation Press.
6. Pečar, J. (1988). **Formalno nadzorstvo.** Ljubljana, Uradni list SRS, Delavska enotnost.
7. Šelih, A. (1977). **Kazenskopravno varstvo pravice do zasebnosti.** Raziskava Inštituta za kriminologijo, štev. 48
8. Zupančič, B. (2000). **Ustavno kazensko procesno pravo.** Ljubljana, Založba Pasadena.

Public or secret nature of state information

Janez Pečar, L.L.D., Professor of Criminology, Rozmanova 2, 1000 Ljubljana, Slovenia

Management of secret data represents a special question of control/, because a state imposes on itself restrictions concerned more with the distribution of information than its production. Since a state must observe human rights and civil liberties, it must cope with certain obstacles and obligations. For this reason, it provides the most diverse procedures, makes a categorisation of its collections and restricts their use. Digital revolution in the information society has triggered many questions, arising from the state's power to accumulate and control information.

The questions that are the focus of attention are the following: who in genera is entitled to produce secret data, why, and to what extent with regard to the nature of confidentiality; what degree of discretion is allowed in attainability of data; whom are secret data supposed to serve; what about the transparency of the state; what people are appropriate to manage secret data; how to prevent state information from becoming secret and thus to prevent the domination and manipulation of people and groups; how to regulate the debureaucratisation of availability of data without complicated legal procedures, and last, but not least, what is the benefit of secret information in comparison with its management costs and relative to the production of secrecy.

Key words: state, secrecy, privacy, tranparency, use of information technology, production of secret information, establishing norms, checking of persons for security purposes

UDC 65.012.8 : 343.322.2