UDK — 007 + 347.77

др Ловро Штурм,
редовни професор Правног факултета у Љубљани

ПРАВНИ АСПЕКТИ ЗАШТИТЕ ПОДАТАКА У САВРЕМЕНИМ ИНФОРМАЦИОНИМ СИСТЕМИМА

1. ОПИС ПРОБЛЕМА

Проблеми заштите података настали су услед све већег коришћења савремене рачунарске технологије на најразличитијим подручјима човекове делатности, а посебно у јавној управи.

У прво време рачунари су се користили за аутоматску обраду рутинских послова у јавној управи (нпр. при разрезивању пореза, за израчунавање личних доходака итд.), па се такав развој оцењивао као користан са гледишта рационализације и модернизације управне делатности. Међутим, већ је замисао о „банкама података", а нарочито када су оне почеле да се стварају у појединим подручјима јавне управе, створила извесно осећање нелагодности код грађана оних држава које су међу првима почеле употребљавати рачунаре у наведене сврхе. То осећање нелагодности настајало је, с једне стране, услед недовољног познавања нове технологије, а, с друге стране, због спознаје да се појединац, услед великог обиља података који се воде у „банкама података", обрађује као бројка и на тај начин се деперсонализује, што може да означава дехуманизацију међуљудских односа у друштву.

Ипак, проблеми су се показали у правом светлу са планирањем, а нарочито са увођењем и деловањем модерних информационих система у јавној управи код којих се врши интегрисана обрада података. Наиме, показало се да суштински значај аутоматске обраде података помоћу модерне информацијске технологије није само у брзини извођења рачунских и других логичких операција већ, пре свега, у могућности интегрисане обраде међусобно повезаних појединачних елементарних података који настају из веома различитих извора а тако агреговане информације могу се на захтев добити за само неколико секунди. При данашњем стању развоја савремене технологије и организације информационих система могуће је да се овакви системи међусобно повезују унутар тако великих подручја, као што су јавна управа, привреда и наука.

За интегрисану обраду података може се рећи да представља значајан циљ савремених информационих система у јавној управи. Њеном реализацијом, техничка рационализација у јавној управи дос-

тиже свој врхунски домет. С једне стране, омогућено је стварање потпуне базе података уз минимум напора, будући да све податке о лицима која треба да буду предмет обраде можемо захватити, сместити у меморију и чувати, а такође и брисати, практично једанпут, то јест, једним поступком. С друге стране, на тај начин достиже се оптимализација рачунарске обраде и информацијских токова, будући да се прикупљени подаци веома често обрађују и зависно од могућности, приступачни су све већем броју корисника(1).

Такође је значајно истаћи да савремена периферна опрема рачунара омогућује успостављање такозваног „двосмерног информационог система". „Двосмерним информационим системом" називамо систем код кога је, и поред удаљености од извора информација, могуће добити одговор за мање од 24 часа. На тај начин терминал рачунара се је изједначио са до сада познатим двосмерним системима — уређајима, као што су телефон и телепринтер. Сви други информациони системи, као што су, на пример, часопис, телевизија, радио, пошта или класични off-line рачунар су, дакле, једносмерни системи(2).

Из изложеног се може установити да се, у вези са настанком и повезивањем информационих система у јавној управи, ствари не могу посматрати тако као да су у питању само проблеми техничке или организационе природе. Не сме се, дакле, изгубити из вида околност да савремена информацијска технологија и на њој заснован централизован, јединствен и високо специјализован информациони систем могу да у себи крију потенцијалну опасност да их злоупотреби неки отуђени центар друштвене моћи.

Изванредан значај наведених проблема и њихов могућ непосредан утицај на сферу интимног живота људи и њихов лични интегритет узрок су повећаном интересовању и бављењу овим питањима угледних научника у области правних наука и законодавних тела у многим државама.

Дубље проучавање проблема, који произлазе из стања савремене информацијске технологије и њене примене на подручју јавне управе, указује на потребу прецизнијег одређивања појмова који се односе на „заштиту података". Пажљивом анализом могуће је установити да израз „заштита података" садржи два суштински различита појма, који се такође међусобно допуњавају. Један аспект „заштите података" односи се на физичко „осигурање података", док се други односи на посебну „заштиту личних података"(3).

Изразом „осигурање података" желе се означити све превентивне мере техничке и организационе природе које се проводе да би се спречило уништење, губљење, фалсификовање или злоупотреба података у електронским рачунарским центрима. Таквим мерама заштићује се сам рачунарски систем за аутоматску обраду података, програми и подаци

(1) Wilhelm Steinmüller, *Datenschutz als Teilaspekt gesellschaftlicher Informationskontrolle*" у зборнику „Detenschutz und Datensicherung", Karlsruhe 1975, с. 49.

(2) Hans-Peter Gassmann: *Probleme bei internationalen Datenflüssen und Gemeinsamkeiten des Datenschutzes in Europa* у зборнику „Datenschutz und Datensicherung", Köln 1976, с. 13.

(3) Израз „осигурање података" употребљава се као синоним за „data security" (енгл.), „sécurite des donnés" (франц.) и „Datensicherung" (нем.); заштита личних података" означава појмове као што су: „privacy" (енгл.), „protection des données privées" (франц.) и „Datenschutz" (нем.).

у њиховом физичком стању и начину организовања, и то против штетног деловања спољних чинилаца, као што су виша сила (катастрофа), грешке и злоупотребе. Према томе, објекти осигурања су рачунарски систем и прикупљени и у меморију смештени подаци са њиховом обрадом(4).

Разлози за осигурање података су следећи:

а) настанак великих „банака података" које на једном месту удружују индивидуалне податке;

б) употреба мултипрограмирања и time-sharinga, што омогућује да рачунарски систем истовремено користи велики број корисника;

в) даљинска обрада података, која омогућује двосмерни ток информација преко терминалног прикључка који се налази у просторијама корисника.

Изразом „заштита личних података" означава се старање да се, у процесу захватања, смештања у меморију и чувања као и коришћења података који се налазе у „банкама података" у информационим системима а односе се на статус и личне односе појединаца, спрече могуће злоупотребе прикупљених података или њихових комбинација односно агрегација од стране других физичких лица или организација или неовлашћених органа или организација. „Лични подаци", који се заштићују, индивидуални су подаци о личним или стварним односима одређеног физичког лица или лица које је могуће одредити. Заштита личних података обезбеђује се правним средствима, а по потреби и организационим и техничким заштитним мерама. Заштита личних података обухвата како директну заштиту физичких лица, тако и њихову заштиту од недозвољене обраде података који се односе на појединце(5).

Разлози због којих је потребна заштита личних података су следећи:

а) настанак великих „банака података", како је то већ наведено као разлог за осигурање података;

б) интегрисана обрада података у јавној управи у оквиру информационих система о становништву, о организацијама, о простору и о финансијским подацима;

в) мултидимензионално повезивање датотека које се налазе код различитих, до сада институционално распоређених органа у јавној управи.

„Заштиту личних података" појмовно треба доследно разликовати од „осигурања података". Како је већ наведено, код „осигурања података" ради се о разним мерама које се проводе да би било обезбеђено неометано функционисање рачунарског система у интересу његових корисника. Израз „осигурање података", који се одомаћио у свим језицима, може да обмане, мада се суштински ради о осигурању самог рачунарског система.

Бројне мере које се проводе у циљу осигурања података могу бити веома значајне и за заштиту личних података. Међутим, треба узети у обзир и ситуације када интереси корисника рачунарског сис-

(4) Види *Datenschutz in der Komunalverwaltung*", KGSt Bericht № 21/1976, Köln, s. 5.
(5) Види претходно цитирано дело.

тема (нпр. пореских органа) и субјеката заштите личних података (нпр. пореских обвезника) могу бити дивергентни, што захтева довођење у склад оваквих могућих сукоба интереса.

Треба такође указати на околност да није могуће обезбедити потпуно осигурање података, будући да је сваки рачунарски систем рањив(6).

Институт „заштите личних података" је, за разлику од института „осигурања података", инструменат правне природе којим треба да буду заштићене уставом гарантоване слободе појединаца у њиховим односима са органима државне власти и другим носиоцима друштвене или економске моћи(7).

2. ПОКУШАЈИ ПРАВНОГ УРЕЂИВАЊА ЗАШТИТЕ ПОЈЕДИНАЦА

Поред облика заштите личних података о којима ће касније бити говора, правна регулатива у новије време уводи и посебан орган парламента. Поред судског и других врста надзора над радом органа управе, функција посебног органа парламента је да штити права држављана односно да обезбеђује да државни органи поштују начело законитости(8).

У Шведској, где је такав орган најпре установљен, као и у другим скандинавским државама, постоји индивидуални орган који се назива „омбудсман". У Великој Британији од 1967. године тај орган назива се „комесар парламента за питања управе", у Квебеку носи назив „заштитник држављана" а у Француској од 1973. године „медиатор"(9). Институт „омбудсмана" и сличних органа не замењује судски надзор над радом органа управе, али озбиљно утиче на побољшање рада органа управе и непосредним и неформалним поступцима доприноси заштити права појединаца.

Идеје, које су дошле до изражаја код установљења института „омбудсмана" и њему сличних органа, надахнуле су и креаторе законодавних решења који су седамдесетих година приступили правном уређивању питања заштите личних података. Иако први законски нацрти и парламентарне расправе потичу још из шездесетих година, први закон угледао је светлост дана тек 1970. године у држави Хесен, федералној јединици Савезне Републике Немачке. Тај закон увео је нов индивидуални државни орган — „пуномоћника за заштиту личних података" и дао му одговарајућа овлашћења(10).

Први национални закон који уређује питања заштите личних података био је усвојен у Шведској 1973. године(11), а годину дана касније донет је и у САД(12). Исте године, то јест 1974., Генерални секре-

(6) G. Löchner, W. Steinmüller: *Datenschutz und Datensicherung*", *Karlsruhe* 1975, с. 92.

(7) Види претходно цитирано дело, с. 2.

(8) Види Драгаш Денковић,*Медиатор — Le Mediateur* (француски омбудсман)", „Вестник Института за јавно управо", 18 (1982), 1—2, с. 15.

(9) Види претходно цитирано дело, с. 16.

(10) „Закон о заштити личних података" (Datenschutzgesetz) државе Хесен, донет 7. октобра 1970. године.

(11) „Datalag", донет 11. маја 1973. године, новелиран 1. јула 1982. године.

(12) „Privacy Act", донет 31. децембра 1974. године.

тар Уједињених народа припремио је исцрпан извештај за економски и социјални савет УН о овој проблематици под насловом „Људска права и научни и технолошки развој — Употреба електронике која може да утиче на лична права и ограничења која би, због такве употребе, требало увести у демократском друштву"(13).

Поред других међународних организација које су се бавиле овим проблемима, треба нарочито поменути Европски савет, који је о томе усвојио две резолуције 1973. и 1974. године и конвенцију 1980. године(14) и Организацију за економску сарадњу и развој (OECD), која је 1980. године завршила своје студијске анализе из седамдесетих година издавањем *Смерница о заштити сфере приватног живота и о преносу личних података преко државних граница*(15).

У другој половини седамдесетих и почетком осамдесетих година, националне законе о заштити података усвојило је више држава. Према стању на дан 31. XII 1983. године, може се утврдити да овакве законе има 12 европских држава, САД, Канада, Израел и Јапан, а да су у приближно истом броју држава припремљени нацрти закона(16).

3. УЛОГА МЕЂУНАРОДНИХ ОРГАНИЗАЦИЈА У ПРАВНОМ РЕГУЛИСАЊУ ЗАШТИТЕ ПОДАТАКА

Користећи сазнања до којих је дошла правна доктрина која је иначе посветила велику пажњу проблему заштите података и ово подручје брижљиво обрадила, међународне организације су дале суштински најзначајнији допринос у обликовању општих међународних стандарда употребљивих за национална законодавства.

Треба истаћи да се правна доктрина из разумљивих разлога, слично као и препоруке међународних организација и поједина национална законодавства, првенствено бави правним регулисањем заштите личних података док подручје осигурања података разматра као секундарно. Присутно је сазнање да је осигурање података као подручје регулисања мање компликовано у поређењу са заштитом личних података. Правно, ово је могуће решити прописивањем обавезних техничких стандарда које би припремили технички извршиоци независни од произвођача рачунарских система и програмске опреме. Већ усвојене и правно санкционисане техничке стандарде, који обезбеђују колико је то могуће висок степен осигурања података, треба пратити с обзиром на брз развој информацијске технологије и прилагођавати их развојним трендовима, па их са овог разлога повремено обнављати. Из наве-

(13) „Human rights and scientific and technological developments — Uses of electronics which may affect the rights of the person and the limits which should be placed on such uses in a democratic society", Report of the Secretary — General, E/CN. 4/1142, 31. I 1974., 112 p.

(14) Резолуција из 1973. године односи се на сектор међудржавних односа, а резолуција из 1974. године на државни и уопште јавни сектор. Конвенција је била усвојена у Страсбуру 22. септембра 1980., а за потпис је била припремљена 28. јануара 1981. са оригиналним насловом: *Convention for the protection of individual with regard to automatic processing of personal data — Convention pour la protection des personnes a l'égard du traitement automatisé des données a caractère personnel.*

(15) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (23 rd September 1980), OECD, 1981, Paris.

(16) Види Борут Јустин: *Извештај о OECD симпозијуму, Међународни пренос података — Transborder Data Flow, Лондон, 30. XI—2. XII 1983.* Информацијски центар Љубљана, 12. XII 1983.

дених разлога, у даљем тексту ограничићемо се на проблеме заштите личних података, што значи да нећемо разматрати питања осигурања података нити посебна питања која настају у вези са преносом података преко државних граница.

Од докумената међународних организација најпре се треба зауставити на већ поменутом извештају генералног секретара Уједињених народа о људским правима и научном и технолошком развоју из 1974. године (у даљем тексту: Извештај УН), у коме се у закључку првог дела, под тачком 320., указује на могуће полазне ставове за правно уређивање питања заштите права појединаца пред претњама које могу настати током коришћења рачунаром потпомогнутих информационих система који садрже личне податке(17).

Извештај УН најпре препоручује државама које још немају законе, који се односе на заштиту личних података, да их што пре донесу и то како за државни, тако и за недржавни сектор. Законодавство би, по могућству, требало да обухвати све врсте података (статистичке, истраживачке, управне и обавештајне).

Извештај УН даље набраја минималне материјалне стандарде које треба поштовати приликом припремања националног законодавства. Као прво, треба прикупљати само оне личне податке и информације, који су неопходно потребни с обзиром на циљеве због којих се успоставља одређени информациони систем. Следећа група препоручених стандарда утврђује право појединца да буде обавештен о томе да се о његовој личности прикупљају подаци као и да се тражи његов пристанак пре него што се информација забележи и стави у меморију. Изузеци од напред наведеног начела су дозвољени у случајевима који се односе на националну безбедност, примену начела законитости и у казнено-судском поступку, као и у случају да закон изрично одређује да нотификација и пристанак појединца нису потребни због специфичне намене прикупљања информација. Међутим, и за такве изузетне случајеве такође су предвиђене посебне заштитне мере, које су утврђене у претходном извештају Генералног секретара УН из 1973. године, који је био посвећен правима појединаца на заштиту сфере приватног живота у светлу техничког напретка(18).

Следећи међународни документ новијег датума, који заслужује посебну пажњу и који је доказао своју вредност, већ су поменуте смернице OECD из 1980. године(19). Смернице OECD, које су биле објављене у облику препорука Савета OECD, плод су вишегодишњег рада међународне групе експерата којој је председавао аустралијски судија M. D. Kirby. Савет OECD је, наиме, препоручио државама-чланицама (међу њима је такође Југославија која има статус придруженог члана) да у национална законодавства уграде начела која се односе на питања заштите личних података и слобода појединаца.

Смернице OECD су кратке и сажете. У уводном поглављу оне разматрају општа начела, дају дефиниције коришћених појмова и об-

(17) Види дело наведено под (13), с. 110.

(18) *Human rights and scientific and technological developmets — Respect for the privacy of individuals and the integrity and souvereignty of nations in the light of advances in recording and other technics,* Report of the Secretary—General E/CN. 4/1116, 23. I 1973., параграф 117.

(19) Види дело наведено под (15).

јашњавају њихов циљ. Веома је важан појам „лични податак", који смернице определују као било какву информацију која се односи на одређеног појединца или појединца кога је могуће одредити (субјекат информационог система), и то начелно, без обзира на употребљену технологију. У том смислу, смернице OECD се односе такође на конвенционално вођене, а не само на рачунаром потпомогнуте информационе системе; међутим, могу да се односе само на ове последње.

Према томе, „лични подаци" су подаци о физичким лицима који се воде у унутрашње-државном и у сектору међународних односа а који, због њихове природе или контекста у коме су употребљени, представљају опасност за приватни живот и слободе појединаца. Као „личне" сматрамо све оне податке у информацији, која нам се преноси, који непосредно (нпр. помоћу личног матичног броја) или посредно (нпр. помоћу адресе) указују на одређено физичко лице.

Следећа кључна дефиниција односи се на појам „надзорник података". Смернице OECD овим изразом означавају орган који је, с обзиром на интерно државно законодавство, надлежан да одлучује о садржини и коришћењу личних података, без обзира на то да ли тај орган сам прикупља, чува, обрађује и посредује такве податке или то ради неко други по његовом овлашћењу. Следствено томе, „надзорник података" је такође онај субјекат који је одговоран за све активности и поступке у вези са обрадом личних података.

Смернице OECD такође предвиђају изузетне случајеве у којима се не примењују, али се такви случајеви поименце наводе. То су подручја националног суверенитета, националне безбедности и јавног реда. Међутим, оне истовремено постављају два општа критерија који треба да буду водич приликом ограничавања опште важности препоручених норми. То су следећи критерији: изузеци треба да буду што је могуће више рестриктивни и треба да буду обнародовани јавности (нпр. путем објаве у државном службеном гласилу). Сматраће се да су услови другог критерија испуњени, ако је на уопштен начин познато постојање одређених збирки података, чак и ако су из разумљивих разлога детаљи о појединачним подацима означени као поверљиви и због тога се сматрају тајним. Што се тиче ширине изузетака, важи уопштено начело да треба да буду ограничени само на оне случајеве који су потребни у демократском друштву.

У другом поглављу, које је са садржајне стране кључно, смернице OECD у седам чланова обрађују основна начела у циљу њиховог коришћења у националним законодавствима. То су следећа начела: начело увођења ограничења приликом прикупљања личних података; начело релевантности и квалитета прикупљених података; начело ограниченог коришћења прикупљених података; начело старања о осигурању података; начело отворености информација; начело учешћа субјеката информационог система и начело одговорности.

Побројана начела су међусобно тесно повезана; њихова међузависност је толика да се из практичних разлога морају посматрати као целовити скуп начела.

Прво начело има у виду ограничења која се, по правилу, уводе приликом прикупљања података који се, због начина њихове обраде, природе података, контекста у оквиру кога се искоришћавају или из

других разлога, сматрају нарочито осетљивим за појединце. Ово начело такође садржи одређене захтеве у погледу метода захватања података. Наиме, подаци морају да буду прибављени на законит и поштен (fair) начин, а ако је то могуће, и са знањем и пристанком лица на које се подаци односе.

Начело релевантности и квалитета података одређује да подаци треба да се прикупљају у складу са постављеним циљевима због којих је прикупљање података утврђено, као и да подаци у односу на њихову веродостојност не смеју да буду сумњиви ни у ком моменту, што значи да увек морају да буду потпуни, тачни и ажурни. Утврђивање циљева прикупљања података може да се посматра и као посебно начело; овим се поставља захтев да циљ или циљеве прикупљања података треба унапред утврдити, а најкасније пре почетка захватања односно записивања података, као и да претходно треба да на несумњив начин буде утврђено, како ће се прикупљени подаци користити. Ако се циљ или циљеви прикупљања података касније промене или допуне, утврђивање нових циљева мора да се обави по истој формално одређеној процедури. Ако подаци више не могу да служе циљу или циљевима ради којих су прикупљени, препоручљиво је да буду уништени или претворени у анонимни облик.

Начело ограниченог коришћења прикупљених података разматра могућа одступања од претходно наведеног начела, то јест, коришћење података супротно утврђеном циљу или циљевима, укључујући и обнародовање података. Смернице OECD познају два изузетка од правила, да се лични подаци не смеју употребљавати у друге намене од оне која је утврђена приликом њиховог захватања односно записивања. Одступања су допуштена, ако је добијена сагласност субјекта чији су подаци у питању, или ако постоји посебна законска одредба која то на изричит начин дозвољава.

Начело старања о осигурању података одређује да се лични подаци морају обавезно осигурати, то јест, морају се предузети прикладне заштитне мере да би се спречили такви покушаји и штетне активности, као што су неовлашћен приступ, уништење, искоришћавање, мењање или обнародовање података. Ово начело произлази из сазнања да проблеми осигурања података и заштите личних података нису идентични, мада су мере које се предузимају за осигурање података корисно допунско средство за спречавање могућег обнародовања или недозвољеног коришћења података. Као што је познато, мере које се предузимају за осигурање података могу бити физичке, организационе и информацијске. Посебно треба истаћи да у организационе мере спада такође обавеза особља да се стара о веродостојности података.

Начело отворености информација представља услов за остваривање начела учешћа субјеката информационог система. Ово начело прокламује отвореност и могућност сазнавања какви се информациони системи и базе података са личним подацима воде, ко их надзире и користи. Информације о свим овим питањима треба да буду доступне без великог губитка времена, претходног знања, путовања и томе слично, и без већих трошкова.

Начело учешћа субјеката информационог система практично обезбеђује право појединца да има приступ подацима који се на њега од-

носе као и да има право приговора. Правна доктрина и политичка пракса гледају на ово начело као на кључно и најзначајније за обезбеђење заштите сфере приватног живота помоћу заштите личних података; међутим, ово начело није апсолутно што значи да се у изузетним случајевима, о којима је било говора, не би могло примењивати.

Смернице ово начело одређују на јасан и разумљив начин. Свако треба да има право да од надзорника података или од неког другог добије одговор да ли се у систему налазе подаци који се на њега односе или то није случај. Уколико је одговор позитиван, појединац има право да те податке добије у разумном времену, уз прихватљиве трошкове, на прикладан начин и у облику који му је лако разумљив. Ако његови захтеви буду одбијени, мора да буде обавештен о разлозима одбијања и мора да му буде дата могућност приговора због одбијања захтева. Појединац такође мора имати могућност улагања приговора, уколико презентирани подаци нису његови и, ако приговор буде усвојен, нетачни подаци морају да буду избрисани, поправљени, допуњени или измењени. Право приговора треба иначе тумачити екстензивно; оно укључује не само право приговора који се даје надзорнику података, него и коришћење других правних средстава (притужба, тужба, управни спор) у складу са интерним законодавством појединих држава која регулишу питања поступака и могућих правних средстава.

Начело одговорности утврђује да је надзорник података одговоран за остваривање напред наведених начела у свакодневној пракси и да мора спроводити све проведбене мере које то омогућују и обезбеђују.

Од осталих питања која разматрају смернице OECD, треба још поменути одредбе које имају за циљ уграђивање наведених начела у интерна законодавства појединих држава. Уградња начела препуштена је државама, при чему треба узети у обзир постојеће традиције, разлике у правним системима и достигнути степен развоја. Одредбе препоручују државама да у том циљу донесу одговарајуће правне акте, да обезбеде потребна средства за заштиту права појединаца, да предвиде одговарајуће санкције и захтеве за накнаду штете и да спречавају дискриминацију према субјектима информационих система. За нас је такође од интереса посебна одредба којом се подстиче настанак и развој аутономних и самоуправних норми о разматраним питањима.

Из досадашњег кратког приказа активности међународних организација, које су биле усмерене на уједначавање ставова у вези са правним регулисањем заштите података, може се закључити да су оне дале значајне и непосредно употребљиве предлоге; у даљем тексту биће размотрено како су ти предлози били уграђени у важећа законодавства различитих држава.

4. УПОРЕДНИ ПРЕГЛЕД ЗАКОНОДАВСТАВА ПОЈЕДИНИХ ДРЖАВА

У циљу упоређивања националних законодавстава о заштити личних података, најпре ће бити анализирани основни ставови и општа начела, а касније заштитне мере.

Подручје заштите личних података, по правилу, уређује се законима; код федералних држава, поред савезних, постоје и закони федералних јединица (СР Немачка, САД, Аустрија, Швајцарска итд.). Као посебну занимљивост треба навести околност да две државе, то јест, Португалија и Шпанија, вероватно због лоших искустава из блиске прошлости тих земаља, посвећују овим питањима толику пажњу да их уређују на изричит начин уставима, тако да заштита личних података постаје предмет регулативе највишег правног акта односно Устава(20).

Из закона који су узети у обзир за потребе овог прилога(21), видљиво је да су на различите начине уређена питања „важности закона" и „субјеката чија права закон штити" (титулари права); ова питања спадају иначе у круг основних законских ставова.

У вези са питањем „важности закона" треба истаћи да већина држава истим законом уређује подручје прикупљања, обраде и заштите личних података како за државне тако и за приватне (недржавне) организације. Неке државе (Данска, Норвешка) имају посебне законе за државни односно приватни сектор. Међутим, Канада и САД својим законима уређују напред наведена питања само за државни сектор.

Канада и САД такође одступају од других држава при одређивању круга „субјеката чија се права штите" законом; као субјекте права на заштиту оне одређују само своје држављане и странце који имају легално стално пребивалиште, док друге државе у том погледу не познају ограничења и у круг субјеката права на заштиту укључују сва физичка лица која живе на њиховим територијама. Неке државе (Аустрија, Данска, Луксембург и Норвешка) још више проширују круг субјеката права на заштиту и у њега, поред појединаца, укључују такође и приватне корпорације.

Разноликост у законодавствима је видљива такође код одређивања објеката правног регулисања. Тако, док у већини држава закони важе како за рачунаром потпомогнуте тако и за конвенционално вођене информационе системе, у неким државама важе само за рачунаром потпомогнуте информационе системе (Аустрија, Шведска, Луксембург), а у неким само за оне конвенционално вођене информационе системе који се могу повезати са рачунаром или који садрже за појединце посебно осетљиве податке.

---

(20) Португалски устав обезбеђује својим држављанима право приступа свим подацима који се на њих односе а налазе се у збиркама података; они даље имају право да буду обавештени о начину коришћења тих података, а признаје им се и право да захтевају се појединн подаци, по потреби, поправе и обнове. Види члан 35. Устава Португалије из 1976. године.

Шпански устав садржи одредбу којом се захтева да коришћење информатике треба да гарантује поштовање личности и сфере приватног живота држављана, као и потпуно обезбеђивање њиховог права у овој области. Види члан 18. Устава Шпаније из 1978. године.

(21) Упоредна анализа била је извршена на основу оригинала закона који уређују питања заштите личних података у Шведској („Datalag" усвојен дана 11. маја 1973., новелиран 1. јула 1982), СР Немачкој („Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung" од 27. јануара 1977), Француској („Loi relatif à l'informatique et aux libertées" од 6. јануара 1978), Данској („Lov om private registre" од 8. јуна 1978. и „Lov om offentlige myrdigheders registre" од 8. јуна 1978), Исланду („Act № 63/1981" respecting Systematic Recording of Personal Data), САД („Privacy Act" од 31. децембра 1974), Канади („Human rights Act) Loi canadienne sur les droits de la personne" из 1976. године који је ступио на снагу 2. јуна 1977) Аустрији („Bundesdatenschutzgesetz" од 1. октобра 1978), Израелу („Protection of Privacy Law", 5741—1981) и приказа садржине правних аката донетих у Белгији, Норвешкој, Луксембургу, Новом Зеланду, Холандији, Швајцарској, Шпанији и Португалији, Data Protection Developments Reported, „Newsletter", IBI, № 29/1979, с. 18 и сл.

Законодавна решења су уједначена код одређивања обима заштите личних података и утврђивања активности које су везане за обраду података, које се у свим државама узимају у најширем смислу. Појам „обрада података" обухвата све степене обраде, односно у тај појам укључује се прикупљање података и сви начини њиховог захватања (записивања), затим сама обрада и прерада прикупљених података и њихово уношење у збирке података и, најзад, посредовање и уопште сви облици ширења (дисеминације) системом обухваћених података.

У уводним одредбама законодавци су у свим законима посветили велику пажњу дефинисању основних појмова који су релевантни за примењивање и извршавање закона. Тако су нарочито брижљиво и недвосмислено одређени појмови, као што су „лични подаци", „регистри", „регистратори", „надзорници", „збирке података и слични појмови, чиме су покушали да дају допринос што је могуће прецизнијим и у правно-техничком погледу непротивуречним правним решењима.

Све државе познају изузетке од начела опште важности закона о заштити личних података о чему је било говора у Извештају УН. Овакви изузеци могу се утврдити само посебним законом.

Заштитне мере иначе бројне и веома сличне у законима различитих држава, могу се поделити у две категорије: превентивне мере и разне санкције. Смисао превентивних мера је да спрече разна могућа угрожавања човековог приватног живота и његових слобода као и кршење одговарајућих прописа којима су та питања уређена. Казненоправне и материјалноправне санкције утврђују разне аспекте одговорности за извршену противправну радњу или догађај. Санкције у извесном смислу такође делују превентивно, будући да само њихово постојање, а посебно ако су довољно оштре и добро познате, спречава могуће незаконите радње.

Важну заштитну меру представља и установљење посебног органа за заштиту личних података и слобода људи. Овакве органе познају све државе, мада су они различити по саставу и по добијеним овлашћењима. У неким државама ти органи су индивидуални; у Канади, то је „комесар за заштиту сфере приватног живота" а у СР Немачкој назива се „савезни пуномоћник за заштиту личних података", има мандат од пет година и именује га лично председник државе. Занимљиво је да постоји старосни услов, најмање 35 година, за избор наведеног савезног пуномоћника(22). Поред савезног пуномоћника, који је надлежан за случајеве кршења савезних закона, немачко законодавство познаје и „државне пуномоћнике за заштиту личних података"који су надлежни за предузимање мера у складу са одговарајућим законодавством поједине федералне јединице — државе у СР Немачкој. Иначе, државни пуномоћници имају традицију, будући да је државни пуномоћник у држави Хесен био први такав државни орган у свету.

У другим државама већином налазимо колегијалне органе. Они се различито називају, на пример, „комисија за заштиту личних података" (Аустрија), „уред за заштиту сфере приватног живота" (Белгија), „инспекција за заштиту података" (Шведска), „национална комисија за информатику и слободе" (Француска), „рачунарски одбор" (Исланд).

(22) Члан 17. закона СР Немачке наведеног под (21).

Значајно је истаћи да се за председника колегијалног органа, као и за индивидуални орган, захтева поред познавања проблема и правна наобразба највишег степена.

Органи за заштиту података имају бројна значајна овлашћења. На њихов захтев, лица која воде информациони систем дужна су да им омогуће одговарајући увид, ако надзор над информационим системом спада у законом утврђену надлежност органа за заштиту података. Ови се органи старају о извршавању закона и објављују годишње извештаје јавног карактера о стању и проблемима на подручју заштите личних података. Код њих морају да буду регистровани сви регистри, датотеке и информациони системи који се односе на физичка лица. У већини држава ови органи су такође надлежни за издавање посебних дозвола (лиценци) без којих би прикупљање личних података и вођење одговарајућих регистара било незаконито.

Законима су такође предвиђене посебне формалности за вођење информационих система и изричите обавезе овлашћених носилаца регистара личних података. Те обавезе су у националним законима готово истоветно утврђене. Тако, национални закони постављају захтеве да подаци у регистрима морају да имају посебна својства, а нарочито да су веродостојни и прецизни, да се редовно ажурирају и да су примерени и у складу са утврђеном наменом прикупљања података.

Сви закони предвиђају такође увођење мера за осигурање података и обавезу лица, која раде са регистрима и евиденцијама, да сазнања до којих су дошли о појединцима чувају као службену тајну. Већина закона такође садржи захтеве да подаци морају да буду прибављени законитим средствима и на допуштен (fair) начин, да искоришћавање података мора да буде временски ограничено и да овлашћена лица треба да воде обавезне записнике или пословне дневнике о посредовању личних података и информација трећим лицима. Прикупљати се могу само такви лични подаци, чије је прикупљање предвиђено законом или прописом донетим на основу законског овлашћења.

Секундарно искоришћавање регистара, односно коришћење у друге намене (нпр. за статистичке намене или за научна истраживања), мора да буде ограничено и да се обавља под условом да буде искључена могућност идентификације појединаца. Подаци о постојању разних регистара, о њиховом саставу и структури, као и каталози података морају да буду објављени у годишњем извештају заштитног органа или у службеним гласилима.

У групу превентивних заштитних мера спадају и права појединаца која извиру из начела учешћа субјеката информационог система са личним подацима који су предмет заштите. У свим размотреним законима појединцу је дато право да буде обавештен о записивању податка који се на њега односи и о улагању таквог податка у датотеке, регистре и томе слично. Сви закони признају право појединцу да буде у потпуности обавештен о садржини свих информација и података који се на њега односе. Од овог начела закони познају изузетак само када су у питању забелешке о здравственом стању: појединац нема директног приступа таквим подацима али може да захтева да их добије његов лекар. Најзад, у националним законодавствима је свима признато

право приговора на записане податке са захтевом да се, према потреби, евентуално поправе или избришу.

Систем заштитних мера правне природе заокружују казненоправне и цивилноправне санкције. Казненоправне санкције познају сви закони и оне обухватају сразмерно високе новчане казне и казне затвора за прекршиоце важећих закона о заштити личних података. Цивилноправне санкције обезбеђују оштећеном материјалну накнаду за насталу штету, с тим што се у штету убраја како стварна тако и морална штета. Поред осталих мера, ове санкције такође ефикасно доприносе обезбеђењу вишег степена правне заштите личних података.

LITERATURA

1. „Datenschutz und Datensicherung", зборник, Karlsruhe 1975.
2. Денковић Драгаш, *Медиатор — Le Mediateur (француски омбудсман)*, „Вестник Института за јавно управоjj, 18 (1982), 1—2.
3. „Datenschutz und Detensicherung", зборник Köln 1976.
4. *„Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"* OECD, Paris 1981.
5. „Human Rights and Scientific and Technological Developments", Reports of the Secretary — General, E/CN 4/1142, 31. I 1974. и E/CN. 4/1116, 23. I 1973.
6. Justin Borut, *Poročilo o ECD simpoziju, Mednarodni pretok podatkov — Transborder Data Flow, London*, 30. XI — 2. XII 1983, Informacijski centar Ljubljana, 12. XII 1983.
7. „Datenschutzgesetz", (Hessen) 7. X 1970.
8. „Datalag", (Шведска) 11. V 1973 и 1. VII 1982.
9. „Privacy Act" (САД) 31. XII 1974.
10. „Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung" (СР Немачка) 27. I 1977.
11. „Loi relatif à l'informatique et aux libertées" (Француска) 6. I 1978.
12. „Lov om private registre" (Данска) 8. VI 1978.
13. „Act № 63/1981", respecting Systematic Recording of Personal Data (Исланд).
14. „Human Rights Act" (Канада) из 1976 (важи од 2. VI 1977).
15. „Bundesdatenschutzgesetz" (Аустрија) 1. V 1978.
16. „Protection of Privacy Law, 5741—1981" (Израел).
17. „Data Protection Developments Reported", „Newsletter", IBI, № 29/1979.
18. „Datenschutz in der Komunalverwaltung", KGSt Bericht № 21/1976, Köln.

Dr. Lovro Šturm,
Professor of the Faculty of Law in Ljubljana

LEGAL ASPECTS OF PROTECTION OF DATA IN CONTEMPORARY INFORMATION SYSTEMS

Summary

The protection of data has two different aspects, namely the one relating to the protection of personal data, and the other relating to physical ensuring of data. In the first case what is needed are the legal measures, while in the second case the organisational ones, alqthoug, quite frequently there is a need for a combination thereof. The institute of the protection of personal data has been created together with the development

of the information technology, namely with creation of the information systems aided by the computers in the sphere of public administration with the integrated processing of data. The protection of personal data in fact means the protection of individual rights and freedoms of man in a computerized society.

Beginning with the sixties of the present century, the legal doctrine has seriously and carefully elaborated the issues of protection of personal data, while the international organisations had contributed to the creation of generally usable standards, which were subsequently used by national legislatures within some thrity countries. The rights of individuals have been determined to be informed on data related to them, as well as on the way of utilisation of recorded data, which includes the possibility of submitting objection, as well as request, concerning eventual changing, addition or erasing or data, namely concerning their use in accordance to the established purpose. Also established are the agencies which effect control in concordance to the statutory powers, and the corresponding penal and property law sanctions against the perpetrators, including the case of emergence of damaging events.

Dr Lovro Šturm,
professeur à la Faculté de droit à Ljubljana

LES ASPECTS JURIDIQUES DE LA SAUVEGARDE DES DONNES DANS LES SYSTEMES INFORMATIQUES CONTEMPORAINS

Résumé

La sauvegarde des données contient deux aspects: le premier se rapporte à la sauvegarde des données personnelles et le deuxième à l'assurance physique des données; le premier aspect nécessite les mesures juridiques et le duxième les mesures techniques et organisationnelles, bien que des mesures combinées soient également utiles. L'institut de la »sauvegarde des données personnelles« est crée parallèlement au développement de la technologie de l'information, c'est-a-dire, avec la mise et place des systèmes d'information informatisés dans l'administration publique impliquant le traîtement des données intégré. La sauvegarde des données personnelles resprésente, en réalité, la sauvegarde des droits et des libertés de la personne au sein de la société informatisée.

Depuis les années soixantes, la doctrine jurisprudencielle examine sérieusement et soignesement les questions de la sauvegarde des données personnelles tandis que les organisations internationales contribuent à l'élaboration des standards d'application générale, contenus actuellement dans les législations nationales d'une trentaine de pays. On a défini les droits de la personne d'être informée sur les données qui les concernent et sur les moyens de leur utilisation ainsi que le droit de soumettre des requêtes ou d'opposer des exceptions pour changer, compléter ou effacer certaines données ou pour les utiliser en conformité avec leur fin établie. On a, en outre, mis sur place des organes de contrôle au terme des dispositions législatives, ainsi que des sanctions pénales et matérielles, contre les personnes ayant commis des actions illicites ou bien dans le cas où les dommages seraient causés.