

др Стеван Лилић,  
доцент Правној факултету у Београду  
Душан Врањанац

## ЗАКОНОДАВСТВО О ЗАШТИТИ ПОДАТАКА УПОРЕДНО—ПРАВНИ ОСВРТ

1. *Пројиси* о заштити личних података грађана, односно о праву приватности, први пут се јављају почетком седамдесетих година, да би касније број прописа знатно порастао. Данас је у свету на снази двадесетак законских прописа који регулишу ову материју. По правилу, ова област се регулише посебним законима, односно, уколико је држава федералног типа, и посебним законима федералних јединица (нпр., у СР Немачкој, САД, Канади итд.). У неким земљама које су недавно донеле нове уставе, ова питања су регулисана непосредно и уставима тих земаља (нпр. Шпанија, Португал). Према расположивим подацима, то су:

(а) Закон о подацима — Шведска (Datalag, 11. V 1973 — новелиран 1. VII 1980); (б) Закон о заштити података — Велика Британија (Data Protection Act — United Kingdom, 12. VII 1984), односно Закон о надзору података — Велика Британија (Data Surveillance Act 1969, United Kingdom — ван снаге); (в) Закон о информатици, евиденцијама и слободама — Француска (Loi No. 78 — 17 du 6. Janvier 1978 relatif à l'informatique, aux fichiers et aux libertés); (г) Закон о заштити од злоупотреба личних података при обради података — СР Немачка (Gesetz zum Schutz vor Missbrauch Personenbezogener Daten bei der Datenverarbeitung, 27. I 1977), и, посебно, Закон о заштити података савезне државе Хесе (Hessenisches Datenschutzgesetz, 11. XI 1986), односно ранији Закон о заштити података Хесеа (Datenschutzgesetz, für das Land Hessen, 12. X 1970 — ван снаге); (д) Савезни закон о заштити података — Аустрија (Bundesdatenschutzgesetz, 1. X 1978); (е) Закон о јавним евиденцијама и Закон о приватним евиденцијама Данска (Lov om offentlige myrdigheders registre — 8. VI 1978; Lov om private registre — 8. VI 1978); (е) Закон број 63 (који се односи на систематску евиденцију личних података) — Исланд (Act N<sup>o</sup>. 63/1981); (ж) Закон о приватности — САД (Privacy Act, 31. XII 1974); (з) Закон о приватности — Канада (1982), односно, Закон о људским правима (Federal Privacy Act — An Act to Enact the Access To Information Act and the Privacy Act, С.П. 1982; Human Rights Act/Loi Canadienne sur les Droits de la Personne, 31. XII 1976); (и) Закон број 65 (који се односи на заштиту података у јавном сектору — канадске државе Квебек (Québec Law 65, 1. X 1982); (ј) Закон о заштити приватности — Израел (Protection of Privacy Law — Israel, 5741/1981) и др. Поред наведених посебних закона, одговарајући закони о заштити података постоје, или се припремају, још и у Белгији, Норвешкој, Луксембургу, Новом Зеланду, Холандији, Швајцарској, Шпанији и Португалу. У нашој земљи ова материја није посебно регулисана, мада су неки аспекти дотакнути Законом о основама друштвеног система информисања и о информационом систему Федерације („Службени лист СФРЈ“, 68/81) — као и предлогом за измене и допуне овог закона (1987).

### II

1. Сумарна компаративно-правна анализа појединих законских аката показује, поред одређених општих начела од којих се полази, и одређене специфичности, односно, поједи-

на другачија решења у регулисању појединих питања у зависности од појединих земаља, односно, правних система<sup>(1)</sup>.

(а) У погледу регулисања „*примене закона*“, у већини земаља је заштита података регулисана јединствено, као, у погледу вођења службених, тако и у погледу вођења неслужбених евиденција (нпр., Данска, Норвешка). Са друге стране, поједине државе ову материју регулишу само у односу на вођење службених евиденција (нпр., САД, Канада). Међутим, све земље познају изузетке у погледу важења закона, с тим што та одступања морају бити предвиђена посебним законима, односно, за њих мора постојати посебан правни основ.

(б) Слична је ситуација и у односу на регулисање „*субјектна заштита*“, тј. лица чија се права штите. Закони о заштити података појединих држава не уводе ограничења у погледу субјекта заштите, односно, предвиђају примену ових аката на сва лица са своје територије. Неке од ових земаља то право чак и проширују, тако да законодавна регулатива не обухвата само појединце, већ и (приватне) корпорације (нпр., Аустрија, Данска, Норвешка). Са друге стране, поједине државе ово право релативно ограничавају, тако да се односи само на своје држављане, односно, на странце који имају стално пребивалиште на њиховој територији (нпр., САД, Канада).

(в) Одређене разлике могу да се уоче у погледу одређивања „*објекта заштите*“. У већини земаља законске одредбе односе се како на (службене, односно, неслужбене) евиденције које се воде конвенционалним — „мануелним“ методима (картотеке, регистри итд.), тако и на евиденције које се воде уз помоћ савремене компјутерске технологије, тј. аутоматски. У неким земаљама, пак, ове законске одредбе се односе само на заштиту података у компјутеризованим информационом системима (нпр., Аустрија, Шведска).

(г) Сви закони, по правилу, посвећују посебну пажњу детаљном и прецизном *дефинисању* кључних категорија, као што су, рецимо, „лични подаци“, „субјект података“, „евиденција“, „компјутерски центар“ итд. Ове околности јасно указују на тенденцију прецизне позитивно-правне регулације ове области, као и намеру да се у највећој могућој мери избегну разне нејасноће правно-техничког карактера, посебно у погледу тумачења ових категорија.

(д) Закони који регулишу ову материју предвиђају и одговарајућа *средства и мере правне заштите*. У ширем смислу, као посебна превентивна заштитна мера подразумева се и право лица да буде обавештено о томе да ли се о њему прикупљају, обрађују и користе одређени лични подаци, као и право да у потпуности буде обавештен о свим подацима који се односе на њега. У том смислу, у свим законима се предвиђа могућност коришћења одговарајућих правних средстава — захтева, приговора, жалби и других ради брисања, корекције, односно, ажурирања података. Правна средства заштите подразумевају и прописивање одговарајућих кривично-правних, односно, грађанско-правних санкција. Кривично-правне санкције су, по правилу, новчане, а прописују се и одговарајуће казне затвора. Грађанско-правне санкције, уз различите модалитете, уведене су да би се одштетило лице у случајевима када му је услед незаконитог или неправилног располагања личним подацима нанета материјална или морална штета<sup>(2)</sup>.

2. Као општа карактеристика (уз поједине изузетке — нпр., САД) специфичног законодавства о заштити података, свакако је и образовање *посебних органа* којима је поверено старање о заштити личних података. Ови се органи, међутим, разликују како по саставу, тако и по обиму и ширини овлашћења. Међутим, иако надлежности и овлашћења органа за заштиту података варирају од земље до земље, њихова овлашћења су, по правилу, бројна и веома значајна.

(1) David Flaherty, „Privacy and Data Protection“ — An International Bibliography, London, 1984; Ловро Штурм, *Правни аспекти заштите података у савременим информационом системима*, „Анали Правног факултета у Београду“, бр. 6, 1986; В. Чок, С. Лилић, Д. Врањанец, *Пројекат: „Заштита личних података у компјутеризованим информационом системима — Компјутерско-правна анализа*, Институт за упоредно право, Београд, 1987; Стеван Лилић: *Data Protection and New Technologies In Public Administration*, European Center For Research and Documentation In Social Sciences, 1987 и др.

(2) Ловро Штурм, *Правни аспекти заштите података у савременим информационом системима* „Анали Правног факултета у Београду“, бр. 6, 1986, стр. 652.

(а) У појединим земљама орган за заштиту података је образован као *инокосни* (индивидуални) орган, а различито се назива. Тако је, на пример, индивидуални орган за заштиту података одређен као „комесар за заштиту приватности“ (Канада), односно, „повереник за заштиту личних података“ (СР Немачка), „регистар за заштиту података“ (Велика Британија) итд. У савезним (федералним) државама, рецимо у СР Немачкој, поред „савезног повереника за заштиту података“, постоје још и одговарајући „земаљски повереници за заштиту података“ у појединим савезним земљама. Иначе, установа повереника у СР Немачкој има доста дугу „традицију“, с обзиром да је као орган за заштиту података први пут и уведена, управо у савезној држави Хесе.

(б) За разлику од тога, друге земље које су образовале посебан орган за заштиту личних података, установиле су га у *колегијалном* облику. И ови, колегијални органи којима је поверена заштита личних података, разликују се, како по називима и структури, тако и по надлежностима и овлашћењима. Тако је на пример, овај колегијалан орган образован као Комисија за заштиту личних података (Аустрија), Уред за заштиту приватности (Белгија), Комисија за заштиту података (Шведска), Национална комисија за информатику и слободе — тзв. CNIL (Француска), Рачунарски одбор (Исланд). За руководиоца, односно, председника ових колегијалних органа (као и за инокосни орган), по правилу се тражи одговарајућа стручна, пре свега, правна квалификација, као и познавање проблематике права и слобода грађана, односно заштите података.

3. Сви закони садрже одредбе на основу којих се прописује да се лични подаци могу прикупљати само на начин који је одређен *законом*, тј. на законит и правилан начин. Поред тога, коришћење личних података временски је ограничено, у смислу да се могу прикупљати само они лични подаци за које је законом предвиђено да се могу прикупљати. Коришћење података из евиденције у друге сврхе — рецимо, ради статистичких или научних истраживања — могуће је само под условом да се лични подаци „претворе у анонимни облик“, тј. да на основу њих није могуће идентификовати конкретну особу.

### III

Селективне илустрације ради, дајемо краћи приказ закона појединих земаља, пре свега европских (Шведске, Велике Британије, Француске, и савезних закона СР Немачке и Аустрије) уз мотивацију да упознавање са њима, макар и у сумарном облику, може бити од користи — не само за увид у стања појединих земаља у овој области, већ и при позитивно-правном регулисању закона код нас.

(а) *Шведска*<sup>(3)</sup>. Шведски закон о подацима (1973) први је национални закон једне државе који регулише ову област (не рачунајући Закон о заштити података савезне државе Хесе). Закон првенствено штити приватност до чије повреде може да дође у процесу аутоматизоване обраде података. Закон има шест делова који обухватају 26 параграфа.

Први део Закона чине *Уводне одредбе* где се дефинишу лични подаци и још неки други основни појмови.

Други део садржи одредбе о издавању одобрења за оснивање и вођење регистра личних података. Тако је за оснивање и вођење регистра потребно претходно одобрење Комисије за надзор података. Ово правило се не односи на регистре који су установљени одлуком Краља или Парламента. Међутим, и у овом случају је потребно прибавити мишљење Комисије.

Трећи део Закона регулише обавезе субјеката који се баве обрадом података, као и права оних лица на које се подаци односе. Одредбе овог дела се првенствено односе на тачност података и њихову доступност.

Четврти део Закона је посвећен Комисији за надзор података, чији је основни задатак да контролише да аутоматска обрада података не доведе до неоснованог и неоправданог мешања у област приватности појединца. Надзор се врши тако да се у што већој мери ос-

(3) Datalag, 11. V 1973, новелиран 1. VII 1982. Коришћен је немачки превод према: J. Schücan, *Datenbanken und Persönlichkeitsschutz*, Zürich, 1977.

твари циљ заштите, а да се истовремено не отежа рад субјеката који обрађују податке, односно да не дође до несразмерних трошкова. У сврху обављања надзора, Комисија располаже и одговарајућим овлашћењима. Представник Комисије може да уђе у просторије у којима се обрада врши и у које су смештени компјутерски уређаји и датотеке. Комисија има право увида у сва документа везана за обраду података. Поред тога, овлашћена је да исклучи уређаје (компјутере) из употребе уколико ошени да је то потребно.

Пети део Закона се односи на казнене мере и накнаду штете, а шести регулише прелазне одредбе.

(б) *Велика Британија*<sup>(4)</sup>. Пошто је Велика Британија прихватила Европску конвенцију за заштиту појединаца у односу на аутоматску обраду личних података (1981), у овој земљи су, у току 1982. године, почеле припреме за израду законодавне регулативе. У том смислу, било је нужно донети посебне прописе ради њене инкорпорације ове Конвенције у домаће законодавство.

Закон о заштити података Велике Британије (1984), између осталог, предвиђа образовање Регистара за заштиту података, тј. посебног „матичара за вођење матичне евиденције о заштити података“ кога именује Круна и који практично не зависи од владе. Регистрар је орган за заштиту података који има овлашћења слична овлашћењима „повереника парламента“, односно, „омбудсмана“. Регистрар региструје све кориснике компјутеризованих информационих система за обраду личних података, како у јавном, тако и у приватном сектору. У процедуралном смислу, овај се Закон определио за становиште поједностављеног поступка, тј. „поступка регистрације“ (по тзв. систему пријаве), наспрот релативно сложене процедуре издавања дозвола (по тзв. систему одобрења) — на којем становишту стоји законодавство, на пример, у Шведској или Француској<sup>(5)</sup>. Увођењем Регистрара, као независног тела, овај закон, у ствари, напушта традицију common-law система и попрама јавно-правна обележја. Разлози за ово се свode на економске интересе Велике Британије да не буде искључена из уносног европског тржишта електронске обраде података<sup>(6)</sup>.

Закон о заштити података Велике Британије представља сложену структуралну и садржинску законодавну целину. По својој структури, обухвата Закон у ужем смислу („Act“) и још четири додатка („Schedules“). Овај Закон регулише „употребу информација добијених аутоматском обрадом које се односе на појединца, као и на обављање делатности које се односе на такве информације“. Закон има пет делова и 43 параграфа, подељених у већи број подсекција и тачака.

Први део Закона — *Уводне одредбе* садржи три параграфа који се односе на одређивања значења основних израза, начела заштите података, као и Регистрара за заштиту података, односно Суда за заштиту података. Тако, „податак“ означава чињенице које су евидентирани у облику у коме могу бити обрађене уређајима који раде аутоматски на основу инструкција датих у ту сврху; „лични податак“ означава податке о чињеницама које се односе на живот појединца који се на основу њих може идентификовати; „субјект података“ означава појединца на кога се лични податак односи; „корисник податка“ означава лице које располаже податком; „компјутерски центар“ пружа другим лицима услуге у односу на податке; „обрада“ података се односи на мењање, проширење, брисање или реорганизацију података или коришћење информација добијених на основу података, а у случају личних података, односи се на ове операције када су везане за субјекта података; „саопштавање“ података подразумева саопштавање информација добијених на основу података. У циљу примене Закона образује се и посебан матичар — Регистрар за заштиту података кога именује Њено Величанство указом, као и посебан арбитражни Суд за заштиту података.

Други део Закона — *Регистрација и надзор над корисницима података и компјутерских центара* обухвата посебне одељке о регистрацији, надзору и правним средствима. Ре-

(4) Data Protection Act — United Kingdom, 12. VII 1984.

(5) David Flaherty, *Privacy and Data Protection* — An International Bibliography, Лондон, 1984, стр. XIX.

(6) Види R. C. Austin, *The Data Protection Act 1984 — Public Law Implications*, Public Law, Winter 1984, стр. 619.

гистрар води евиденцију (регистар) корисника података који располажу подацима, као лица која воде компјутерске центре којим се пружају услуге у односу на личне податке. У регистар ће се евидентирати сваки захтев за регистрацију. Не може се располагати личним подацима колико није извршена регистрација корисника података, односно, корисника података који води компјутерски центар. Регистрар ће најдошњи у року од шест месеци од пријема захтева за регистрацију, писмено обавестити подносиоца захтева да ли му је захтев прихваћен или одбијен, а у случају да одбије захтев за регистрацију, навешће разлоге и обавестити подносиоца о правним средствима која му стоје на располагању.

Трећи део Закона — *Права субјеката података* односи се на питања у вези са правима субјеката података, могућностима накнаде штете, исправљањем грешака и брисањем података, као и на питања у односу на надлежност и поступак. Свако лице има право да га информише сваки корисник података да ли подаци којим располаже укључују и његове податке.

Четврти део закона — *Изузеци*, регулише питања у вези с изузецима од примене одредбе овог Закона. У том смислу, Закон посебно и детаљно предвиђа изузетке који се одnose на одређене, посебно назначене и регулисане области, као што су државна безбедност; кривичне и пореске ствари; здравствено и социјално осигурање; финансијске услуге; судијски имунитет и право тајности заступника; платни спискови и рачуни; породични и други разлози; испитне оцене итд.

Пети део Закона — *Опште одредбе*, регулише поједина питања везана за општа права и овлашћења Регистрара, сарадњу Велике Британије и осталих земаља потписница Европске конвенције, обављање услуга, обрађивање података са иностраним елементом, овлашћење за доношење подзаконских аката и др. Тако, Регистрар може разматрати сваку представку која се односи на питање повреде начела заштите података или одредаба овог Закона.

Уз Закон су донета и четири посебна *Додатка*: I — Начела заштите података; II — Регистрар за заштиту података и Суд за заштиту података; III — Поступак по правним средствима; IV — Право увида и инспекцијска овлашћења.

в) *Француска*<sup>(7)</sup>. Француски закон којим је регулисана област заштите података 1978. године и носи назив Закон о информатици, евиденцијама и слободама. Међутим, обично се спомиње у скраћеном облику, било као Закон о информатици и слободама, или још краће, као Закон о информатици. Овим Законом, између осталог, формирана је и Национална комисија за информатику и слободе, тзв. CNIL. Комисија је колегијални орган од седамнаест чланова. Специфичност и оригиналност њене структуре чини околност да се у њеном саставу, поред високих државних, односно, административних функционера (свега три члана непосредно именује извршна власт), налазе и представници парламента као и представници других политичких и друштвених структура. Члановима комисије мандат траје пет година. У досадашња четири мандатна периода Комисијом су председавале угледне личности правног и јавног живота — први председник комисије био је председник Касацног суда, други — сенатор, трећи — ранији председник Рачунског суда, док је садашњи председник, бивши директор угледног дневника „Le Monde“. Како би остварила поверене јој задатке, Комисији су дата значајна овлашћења, како регулативног, тако и контролног карактера<sup>(8)</sup>. Комисија има саветодавна овлашћења, која се могу односити на различита питања. Тако, CNIL даје објашњења вршиоцима обраде о начинима олакшавања примене права приступа; помаже код одређивања употребе изборних евиденција; указује институцијама на испитивање мњења како поступати с осетљивим подацима; саветује о примени мера безбедности; проучава односе управе великих градова са становништвом; ангажова-

(7) Loi No. 78 — 17 du 6 Janvier 1978 Relative à L'informatique, aux Fichiers et aux Libertés. („Journal officiel“ du 7 Janvier 1978 et rectificatif au J. O. du 25 Janvier 1978).

(8) Стварањем ове Комисије проширен је круг тзв. независних административних тела — којег, поред CNIL-а, чине још и Медијатор („омбудсман“), Високи уред за аудио-визуелну комуникацију, Национална комисија за комуникацију и слободе, Комисија за приступ подацима у службеним евиденцијама, Национална комисија за транспарентност и плурализам штампе итд. Види: Herbert Maisl *Etat de la Legislation Française et Tendances de la Jurisprudence Relatives à la Protection des données Personnelles*, „Revue Internationale de Droit Comparé“. N° 3, 1987, стр. 562.

на је на успостављању стандарда у вези са коришћењем личних података у области здравства итд. Комисија има и широка контролна овлашћења у односу на администрацију. У том погледу, овлашћена је да врши контролу у односу на државне органе, локалне заједнице, јавне установе, као и у односу на приватна лица којима је поверено вршење јавне службе. Различити су облици вршења ове контроле — од доношења одлука у претходном поступку и непосредног увида на лицу места, до разматрања представки у вези са тешкоћама у остваривању права приступа.

За овај Закон се може рећи да је општи и потпун закон који регулише примену информатике у свим областима. У стварности, међутим, ово се своди на оне области у којим је у протеклом периоду интервенисала Комисија — између осталог — здравство, финансије, радни односи, локална управа, унутрашњи послови, полиција, порези, правосуђе, наука, телекомуникације, итд.

Закон има 48 чланова структурисаних у седам поглавља.

У првом поглављу Закона — *Принципи и дефиниције*, поред осталог, истиче се да информатика мора бити у служби сваког грађана. Њен развој мора да се креће у оквирима међународне сарадње. Њеном применом не сме да се вређају људско достојанство, људска права, приватни живот, као ни личне, односно јавне слободе. Свако лице има право да са зна и да оспори податке, као и сврху вођења аутоматске обраде, уколико му се наноси штета.

Друго поглавље закона — *Национална комисија за информатiku и слободе*, регулише статус и овлашћења Комисије, којој се поверава спровођење одредаба овог Закона. Она је, пре свега, задужена да информише заинтересована лица о правима и обавезама, као и да контролише примену информатике у обради личних података. Комисија је „независно административно тело“, сачињава је 17 чланова именованих на пет година — својство члана комисије неспојиво је, између осталог, са чланством у влади или вршењем јавних функција, као и са учешћем у раду фирми за израду материјала и пружање услуга у области информатике и телекомуникације. У вршењу својих овлашћења, чланови Националне комисије за информатiku и слободе „не подлежу упутствима ниједне власти“.

Треће поглавље Закона — *Претходни поступак у вези с аутоматском обрадом личних података*, регулише поступак који се спроводи у циљу да се обрада личних података у службеним и неслужбеним евиденцијама врши у складу са одредбама овог Закона.

Четврто поглавље Закона — *Прикупљање, репродуковање и чување личних података*, утврђује да је забрањено прикупљање података преваром, односно неправилним или недопуштеним поступцима. Није допуштено чување личних података у меморијама информационих система, осим уз изричиту сагласност заинтересованог лица, који се непосредно или посредно односе на расно порекло, односно, политичка, филозофска и верска уверења, као и припадност појединим удружењима. Међутим, верске, филозофске, политичке и синдикалне организације могу водити аутоматизоване евиденције података о својим члановима — није дозвољено вршење било ког облика надзора над њима. Због јавних интереса се могу, декретом Државног савета предвидети изузеци у примени ове одредбе.

Пето поглавље Закона — *Остваривање права приступа*, утврђује да свако лице има право да се обрати служби, односно, органима који су овлашћени да врше обраду личних података у циљу утврђивања да ли се обрађују подаци који се на њега односе, тј. има право да о томе буде обавештено. Јасно формулисано обавештење мора бити у складу са садржајем евиденција које се воде. Уколико постоје сумња и нејасноће у овом погледу, заинтересовано лице може да се обрати надлежном судији ради предузимања мера у циљу отклањања нетачности и непотпуности и може да захтева исправку, употпуњавање, појашњење, допуњавање или брисање података који су нетачни, непотпуни, погрешни или застарели, односно, оних података чије прикупљање, коришћење, саопштавање и чување није допуштено.

Шесто поглавље Закона — *обухвата Казнене одредбе*, а седмо — *Остале одредбе*. Влада може, на предлог Комисије, одлучити да се поједине одредбе овога Закона примењују и на неаутоматизовану, односно, механографски вођену евиденцију.

(г) *СР Немачка*<sup>(9)</sup>. Савезни закон о заштити података од злоупотребе СР Немачке (1977), у ствари, не регулише непосредно заштиту података, већ интересе који могу бити угрожени злоупотребом ових података. Закон даје општа начела која се односе на заштиту личних података и ствара правни и појмовни оквир за остале прописе који регулише ову материју — Закон се примењује увек када неко питање није регулисано посебним прописима. Овај Закон има шест делова и обухвата 47 параграфа.

Први део Закона обухвата *Опште одредбе*, и има шест параграфа који се односе на примену Закона, одређивање значења основних појмова, допуштеност обраде података, права лица на која се подаци односе, тајност података и техничке и организационе мере у вези вршења обраде. Обрада података је допуштена само у случају када је то овим Законом, односно другим прописом, допуштено, односно када постоји сагласност лица о коме се подаци обрађују.

Други део Закона регулише обраду података од стране државних органа и јавних служби. Овај део Закона посебно регулише питање прикупљања и мењања података, пренос (трансфер) података, исправљање, блокирање и брисање података. Параграфи 17 — 21. Закона се односе на Савезног повереника за заштиту података, кога именује Председник Републике на предлог Савезне владе. Његова улога је првенствено саветодавне природе, мада је, с обзиром на ауторитет личности које обављају ову функцију, његов стварни утицај на остваривање законитости у овој области велики. У вршењу своје функције Повереник је независан од владе, и везан је само законом. Правни надзор над његовим радом врши савезна влада (тј. министар за унутрашње послове). Повереник контролише примену одредаба овог Закона, као и других прописа о заштити података — у том циљу може да предлаже мере за побољшање заштите и да се обрати влади и министрима.

Трећи део Закона се односи на обраду података од стране недржавних субјеката — физичких и правних лица, друштава и других приватних организација које, ради остваривања својих циљева, врше обраду личних података. Овај део садржи одредбе о обради података недржавних субјеката и сличан је, уз одговарајуће специфичности, одредбама Другог дела Закона које регулишу одраду података од стране државних органа.

Четврти део Закона садржи одредбе о обради података коју врше овлашћени субјекти за потребе других корисника. Пети део Закона садржи казнене одредбе, а шести прелазне и завршне одредбе.

(д) *Аустрија*<sup>(10)</sup>. Савезни закон о заштити података Аустрије (1978) регулише заштиту личних података полазећи од одређења да свако има право на тајност података који се на њега односе, посебно уколико су везани за заштиту личног и породичног живота. Закон штити не само податке лица чији је идентитет познат, већ и оних која се могу са вероватноћом идентификовати. По својој структури у погледу основних одређења, Закон се не разликује много од осталих европских закона који регулишу ову област.

Овај Закон је подељен на седам делова: *Опште одредбе*, *Обрада података у јавном домену*, *Обрада података у приватном домену*, *Међународни пренос података*, *Комисија за заштиту података*, *Савет за заштиту података* и *Казнене одредбе и Прелазне и завршне одредбе*.

Посебно обележје овог Закона, за разлику од већине других земаља, јесте да надзор над заштитом података врше два колегијална органа — Комисија за заштиту података и Савет за заштиту података. Комисију чине четири члана које, на предлог савезне владе, именује Председник Републике. Она ради самостално и не могу јој се давати упутства или налози — Комисија предузима мере ради остваривања заштите података и спроводи поступак заштите лица на које се подаци односе. За разлику од Комисије, Савет за заштиту података је надлежан да путем надзора над применом Закона штити првенствено јавни интерес. Савет сачињавају одговарајући представници најважнијих политичких странака, радничких удружења, федералних јединица, општина и градова, као и један представник кога именује Савезни канцелар.

(9) Gesetz zum Schutz vor Missbrauch Personenbezogener Daten bei der Datenverarbeitung, 27. I 1977.

(10) Bundesdatenschutzgesetz, I. X 1978.