

Реалност улоге, значаја и будућности права у заштити личне приватности, као једног од основних људских права

СВЕТ, ОКРУЖЕЊЕ, СРБИЈА

(кратак осврт)

ЦИЉ:

Циљ овог кратког осврта јесте покушај сажетог давања одговора на више суштинских питања непосредно везаних за заштиту приватности личности (личне приватности) у свету, а посебно у Србији. Нагласак је стављен на упознавање са основним карактеристикама система правних (и сродних) правила којима се лична приватност штити. Та питања се односе на:

- Домашај правне заштите у светлу убрзаног развоја и масовне примене нових технологија (електронских комуникација пре свега); једноставније говорећи - каква правила и до које мере могу да заштите приватност личности?

- Способност савремених система правних прописа (националних и међународних, међу којима првенствено ЕУ) у прилагођавању променама на пољу технологије, тј. 1) како и зашто прописи из ове области морају бити посебног квалитета; 2) о каквом квалитету је реч; колико је тај квалитет остварен на нивоу ЕУ; колико у Србији; 3) да ли постоји јединствена међународна пракса у тој области; постоји ли јединствена пракса на територији ЕУ; 4) да ли су иста решења и стандарди у домену заштите приватности могући и целисходни у земљама на различитом степену развијености технолошких и безбедносних система; једноставније речено - када се српски законодавац позива на искуства Европе и међународне заједнице, на шта он, уствари, мисли?

- Оправданост високог степена заштите приватности, односно података о личности; тј. како недостаци у таквој заштити могу директно да угрозе појединца; о каквим је недостацима у заштити заправо реч; једноставније - зашто тренутно стање у области права, политике, економије и друштва уопште чини ризичним увођење нових технологија за прикупљање и обраду података о грађанима Србије, на начин и брзином која се најављује.

ПРИСТУП:

Упуштање у расправу о правној материји, посебно из овако осетљиве области, уз присутно временско ограничење, тј. ограничење у погледу количине текста, носи са собом ризик извесне недоречености. Зато ће наша аргументација морати да буде кратка и, надамо се, довољно јасна.

Пошли смо од схватања правног система као остваривог, ефикасног, устројавајућег механизма колективног понашања и живота. Дакле, квалитет правних норми (система) овде је посматран првенствено у светлу мотива за њихово узакоњење (дакле - шта штите, чему служе, коме служе) и практичне вредности (односно успеха у остваривању прокламованог циља).

Посебан нагласак је стављен на одударања у поимању граница, средстава и начина заштите приватности личности између институција ЕУ, посебно Европског суда за људска права, са једне стране, и правних система појединих земаља чланица са друге.

За стављање система заштите приватности ЕУ у центар пажње определили смо се првенствено зато што је упоредно испитивање показало да ЕУ до сада има највише успеха у развијању ове врсте заштите.

РАЗЛОГ:

Ово разматрање подстакнуто је постојећом праксом заштите приватности, односно података о личности у Србији, то јест променама које се у тој области најављују. Постојећу праксу и најављене промене сматрамо недовољно јасно мотивисаним, системски и фактички неодрживим (под условом да заштита приватности, као једно од основних људских права, и даље представља кључни интерес), посебно због изостанка прикладног обавештавања шире јавности о могућим, како корисним, тако и штетним, последицама.

Процене и претпоставке које у том погледу износимо темеље се на нашем тумачењу досадашњих законских промена и пратећих збивања на пољу заштите приватности; не сматрамо да је то тумачење и једино могуће.

Конкретније говорећи, подстакнути смо најавом увођење јединственог електронског документа (о чему се са правне тачке гледишта може говорити само начелно, јер конкретан текст још није предложен) и актом Владе под називом: Стратегија о заштити података о личности, од 16. августа 2010. год.

НАПОМЕНА:

Овај текст представља саставни део целине, која обухвата и текстове (излагања) осталих учесника трибине *Електронски документи-слобода или логор?*, Београд, 18.11.2010. Зато поједина питања, првенствено детаљи који се односе на природу, улогу и примену предметних технологија, нису обрађена на овом месту.

Једнообразност и усклађеност прописа о заштити приватности личности у међународним и оквирима ЕУ

Документ који обухватно илуструје односе и развојне тенденције у области заштите података о личности јесте коначни извештај Европске комисије од 20. јула 2007. (*Comparison of Privacy and Trust Policies in the Area of Electronic Communication* - у наставку Коначни извештај).

На основу овог извештаја, поред осталог, закључујемо да позивање на "међународне правне стандарде", што је омиљен манир домаћег законодавца¹ представља неутемељену и више-мање произвољну формулацију. Наиме, не постоје две државе у којима би питање ове врсте приватности било уређено на јединствен начин. Таква униформност, тј. усклађеност, није постигнута ни на нивоу ЕУ, иако институције Уније, посебно "Радна група за заштиту података о личности, по члану 29" и Европски суд за људска права здушно раде на остварењу тог циља.

Можда позивање на "европско" или "међународно" искуство² и не би представљало паушалну формулацију када би домаћи законодавац поступао у складу са закључцима, препорукама, директивама и одлукама релевантних наднационалних институција ЕУ. Међутим, он то не чини или чини парцијално и недоследно.

¹ На пр. Закон о телекомуникацијама (Сл. гласник РС 44-24.4.2003.), чл. 1

² Погледати Образложење Предлога Закона о заштити података о личности (ИИ) од 23.11.2008.

Правна заштита не подразумева само добар нормативни текст

Подаци из Коначног извештаја упућују нас да степен заштите приватности посматрамо као производ више чинилаца: са једне стране ту су позитивни (тренутно важећи) правни прописи, затим обавезе и права из различитих уговора (на пр. са провајдерима интернет услуга, телефоније и сл.) ка чијој се све већој стандардизацији тежи, затим поштовање безбедносно-технолошких стандарда (на пр. ИСО/ИЕЦ 27001), потом други фактори (као на пр. деловање удружења потрошача, организација за означавање нелојалних и необезбеђених учесника на тржишту посредством интернета, организација за превенцију крађе идентитета, као што је Privacy Rights Cleaning House у Америци и сл.), а ту су, коначно, и капацитети за спровођење прописа (домен извршне власти), где су од кључне важности политичка воља, техничко-технолошка оспособљеност, али, првенствено - јасно, обухватно, обједињено и свима разумљиво законодавство, са којим је јавност детаљно упозната. Искуства из САД упозоравају на штетне последице компликованих и недовољно јасних регулаторних формулација. Један од заговорника права потрошача, кога су представници Европске комисије интервјуисали за сврхе састављања Коначног извештаја, указује да компликована правила "уствари служе ономе ко их доноси као средство за избегавање евентуалне одговорности" у случају повреде личне приватности.

Да ли прописи домаћег законодавства задовољавају основне критеријуме за ефикасну заштиту приватности грађана?

"Коначни извештај" надаље утврђује да прецизност, усмереност на конкретна питања (на супрот општем и начелном прокламовању) и узајамна усклађеност (кохерентност) правних и сродних норми стоји у директној сразмери са висином степена успеха заштите података о личности.

Да ли тренутно постојећи правни оквир у Србији задовољава тај критеријум?

Не, почев још од Закона о заштити података о личности, од 23.11.2008. У образложењу Предлога овог закона наведено је и следеће: " Овим законом је детаљно уређена заштита података о личности..."

На произвољност ове оцене указано је у једном од првих докумената који су анализирали Предлог Закона о заштити података о личности. Реч је о "Критичком осврту" Центра за проучавање и употребу савремених технологија Српске православне цркве (који је и даље доступан на интернету)³.

³ Наводимо део Осврта, ради упоређења са недостацима у постојећој регулативи на коју нас (тек сада!) упозорава влада у својој Стратегији (поменуто горе, у уводу): **Шта предложени закон уопште не регулише, насупрот упоредном законодавству (поједини примери)**

Оно што предложени закон уопште нема, јесу посебне одредбе везана за обраду података у литерарне и уметничке сврхе. Дословним тумачењем члана 6. предлога могли бисмо закључити да би таква обрада била противзаконита. Ово представља крупан пропуст, који је несхватљив уколико је Предлагач заиста имао увид у законска решења из ЕУ. Са друге стране, упадљива је несразмера у исцрпности којом члан 33. британског закона регулише обраду у историјске, статистичке и научно-истраживачке сврхе (члан 6. Предлога), чиме је могућност накнадног тумачења сведена на најмању меру, а заштита таквих архивираних података није препуштена неком накнадном пропису. Британски закон такође на више места посебно регулише питање времена на које се одређени подаци могу задржавати, што Предлог решава само у начелу (ако уопште).

Акти које повереник доноси и спроводи према руковоацу такође се посебно одређују, што са нашим Предлогом није случај, а требало би. У члану 42. британски закон омогућава заинтересованом лицу директан захтев поверенику ради оцене рада руковоаца, док је у нашем Предлогу то могуће једино путем жалбе. Као трећи степен установљен је Трибунал за заштиту података (који обухвата представнике различитих органа и група заинтересованих лица, као што су синдикати, удружења...), коме је такође могуће поднети жалбу под прописаним условима, и против решења повереника (по одредбама нашег Предлога на то се може реаговати једино у управном спору).

Британски законодавац се не задовољава подразумевањем правних стандарда, већ их што прецизније одређује. Док у Предлогу у чл. 15 имамо квалификатив „савесно поступање“ без објашњења, у британском имамо одређење да тај квалификатив, у смислу конкретних правила у коме се на њега позива значи : „ такво поступање у обради података о личности за које повереник процени да је пожељно у погледу интереса лица на које се подаци односе и других, и подразумева (мада се тиме не исцрпљује) поступање у складу са одредбама овог закона“ (“good practice” means such practice in the processing of personal data as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, and includes (but is not limited to) compliance with the requirements of this Act). Тиме што је утврђивање тог стандарда, у крајњем, јасно одређено стављањем у надлежност поверенику, отклоњена је опасност од накнадних тумачења и обезбеђен прикладан степен правне сигурности. Насупрот томе, Предлог карактерише више подразумевање, него недвосмисленост.

Истраживањем, Центар је дошао до сазнања да је у погледу заштите података о личности британски закон (Data Protection Act) дао најбоље резултате. Само летимичано упоређење текстова српског и британског закона довољно је за непобитан закључак да ни о каквом детаљном уређивању код нас не може бити ни речи.

Тек данас влада у својој Стратегији за заштиту података о личности, од 16.8.2010. говори оно на шта је СПЦ у поменутом Критичком осврту (и не само СПЦ) упозоравала још 2008. Штавише, у Стратегији се наводи да надлежни државни органи до дана данашњег нису чак ни утврдили који прописи уопште уређују материју заштите података, нити су их анализирали, нити су их ускладили са подзаконским актима⁴, већ да то "тек треба урадити". Овде ћемо ставити нагласак на термин "подзаконска регулатива". Под тим термином могу да се подразумевају различите уредбе, одлуке и слично - дакле, не акти законодавног тела, не измене и допуне закона! А још више погађа чињеница да су ради прецизирања таког непотпуног закона, за све ово време донета свега три подзаконска акта.

На основу тумачења упоредно-правне праксе у поменутом у Коначном извештају Европске комисије може се закључити да регулативу из ове области у Србији можемо оправдано назвати расцепканом (фрагментарном), што је, како поменути Коначни извештај показује, супротстављено ефикасној заштити приватности. Чак и када бисмо фрагментарност као квалификацију довели у питање, једна карактеристика стоји ван сваког спорења - непотпуност заштите приватности личности у Србији, о чему сведочи и сам текст Стратегије владе.

Аплауз влади на списку ствари које би тек требало урадити (Стратегија заштите података о личности) ипак мора бити уздржан, јер би макар и оквирно узимање у обзир поменутог "Критичког осврта", или барем законских решења из других земаља Европе, на која се у њему указује, било довољно да се предупредите исти они недостаци на које влада тек сад упућује, правећи од тога правно-технички спектакл.

Но, то и није за чуђење, будући да је у самом образложењу Предлога Закона, његово доношење по хитној процедури, било означено као краткорочни приоритет, посебно мотивисан обећаним "стављањем на белу Шенген листу".⁵ У одсуству детаљнијег упознавања шире јавности (обухватне јавне расправе),

Предлог закона такође није узео у обзир специфичности одређених врста података и руковалаца. Тако Предлог нема детаљне одредбе везане за однос према синдикатима и подацима којим они оперишу, према подацима који се размењују у оквиру међународне сарадње (што ипак представља област коју је нужно законски уредити, а не само одредити), према подацима које послодавци, односно управа предузећа прикупља од запослених, односно располагању и размени истих, посебно ако је реч о предузећима која размењују информације са иностранством или имају седиште у иностранству или су део холдинга (за чију је злоупотребу у британском закон предвиђена одговорност и у случају грубог нехата!), подацима који се обрађују у маркетиншке сврхе, потом према подацима који се прикупљају ради утврђивања кредитне способности, подацима који се прикупљају од деце и малолетних лица (у Предлогу само начелно регулисано чл. 10.), постављењем и статусом судија и носилаца јавне власти (у Предлогу само начелно), оцена којима се вреднује академски успех и професионална способност (што је посебно битно регулисати с обзиром на рокове и начин обраде у појединим случајевима), података везаних за професионалну тајну, за поступак регрутације и друге податке о личности којима оперишу оружане снаге, полиција итд. Нарочито треба нагласити потребу јасног законског регулисања обраде података везаних за процес усвајање, односно пријема у хранитељску породицу. О свему овоме Data Protection Act садржи посебне одредбе, као и оне којима се врши усаглашавање са постојећом предметном регулативом. Предлог такође не садржи решења везана за евентуални сукоб закона са важећим прописима у нужном периоду усклађивања, нити о начину и периодици усклађивања са другим прописима – све то је препуштено накнадном регулисању, а да му нису дати ни оквири. Пропуштено је и да се одреде детаљи преласка са ручно вођене на аутоматизовану обраду одређених података (ако државна власт уопште у томе намерава да поступа плански) како би се могли предупредити потенцијални проблеми. Предлог закона такође не регулише посебно ни начин достављања обавештења и одлука повереника, што британски чини чланом 65. Ово је од значаја јер је на основу тих одлука руковалац бива обавезан и на одређено поступање према заинтересованом лицу, чији интерес (да дамо очигледан пример), често може да буде условљен роковима и сл. Предлог закона се не бави посебно ни питањем прављења резерви података (back-up) као мери обезбеђења, што би требало законски регулисати због специфичних безбедносних ризика, посебно опасности да одређени подаци буду уништени, односно задржани дуже или другачије од онога што закон прописује. У вези са надзором, Предлогом нису утврђени детаљи везани за акте надзорних органа (повереник и његова овлашћена лица), што би требало учинити због специфичности предмета. Исто тако нигде у Предлогу није прописана обавеза руковоца да у случају оспорености или измене податка обавести кориснике података о таквој измени.

⁴ ...Због тога је потребно утврдити који закони и други прописи уређују материју заштите података о личности и извршити анализу њихове усклађености са Законом о заштити података о личности и подзаконским актима донетим на основу тог закона.

Постоје, такође, веома важне области у којима још увек нису донети одговарајући прописи којима се уређује питање обраде података о личности које је веома заступљено у тим областима, као што су нпр. маркетинг, видео надзор, употреба биометријских података и др...

⁵ Предлог Закона, исто

озбиљност недостатака овог Закона прошла је, практично, незапажено. Идентична ствар поновила се у случају усвајања другог закона који темељно задире у приватност грађана: Закона о електронским комуникацијама од 29.6.2010. А управо такво необавештавање грађана горепоменути Извештај Европске комисије означава као фундаментални недостатак у заштити приватности, посебно у друштвима у развоју (примери Индије и Малезије представљају за нас прилично добар модел за поређење, уз напомену да се технолошки и информатички развијају приметно брже од Србије).

Степен обавештености јавности о потреби за заштитом личне приватности, начинима, технологији, правним механизмима и институцијама које им стоје располагању, темељни је показатељ ефикасног остваривања ове врсте заштите. Према подацима Еуробарометра 2003 око 60% становника ЕУ било је заинтересовано и махом упућено у значај заштите личне приватности, а у Јапану невероватних 80%. Каква је ситуација по том питању у нашој земљи можемо само да нагађамо. А без тих података свако даље нормирање је мањкаво.

Дакле, до сада смо показали да се стандарди прецизности, целовитости, обухватности и прикладног упућивања јавности у актуелном домаћем законодавству не могу сматрати задовољавајуће оствареним.

Да ли се наше законодавство заиста темељи на прокламованим "европским вредностима"?

Испитајмо сада да ли се наш законодавац доследно у придржава европских вредности. Као пример узећемо већ поменуто спорење око права полиције и других служби безбедности (БИА, ВБА, ВОА) на несметан увид у податке о комуникацији грађана без одлуке суда ("податке о саобраћају"), сходно сопственој процени, што је омогућено Законом о електронским комуникацијама (и не само њим). Да подсетимо: "подаци о саобраћају" говоре ко је, када, са ким, колико дуго, на који начин, преко које опреме био у контакту, као и где је та опрема лоцирана. Ти подаци се ажурирају и чувају дванаест месеци (видети посебно чланове 128. и 129.). Наш законодавац сматра, упркос противљењима Повереника за информације од јавног значаја и заштиту података о личности, као и Заштитника грађана, да ти подаци не угрожавају приватност, јер се оваква присмотра не уплиће у сам садржај комуникације. Да ли тако мисли и Европа?

Погледајмо само један случај о ком је одлучивао Европски суд за људска права (а било их је далеко више⁶) - Копланд против Велике Британије (Copland vs. UK).

Линета Копланд била је лична секретарица директора једног колеџа. Због сумње да користи службени телефон и интернет за личне потребе, заменик директора контролисао је телефонске и интернет рачуне (листинге). Дакле, реч је била о "подацима о саобраћају".

Европски суд за људска права донео је одлуку којом се констатује да је Линети Копланд било угрожено основно људско право на приватност, прописано чланом 8. Конвенције о заштити основних људских права и слобода. Обратимо пажњу и на ово: период реченог надзора (дакле, "задржавања података" - по терминологији Закона о електронским комуникацијама) трајао је свега "неколико месеци", никако годину дана, као што је код нас случај. Притом, суд је у образложењу одлуке навео да на постојање повреде ни од каквог утицаја нису следеће чињенице, на које се позвала супарничка страна: 1) да је реч о службеним ресурсима (телефону, интернету, канцеларији...), 2) да је колеџ до телефонског рачуна дошао на редован, законит начин, 3) да задржани подаци нису ником обелодањени, па чак нису ни у једном поступку коришћени против оштећене.

⁶ Copland vs. UK, Klass vs. Germany, Amann vs. Switzerland, Leander vs. Sweden, Rotaru vs. Romania, Peck vs. UK, Perry, vs. UK

Из одлуке Европског суда за људска права (ЕСЉП) посебно би требало издвојити следеће детаље: да се члан 8. Конвенције о заштити основних људских права и слобода примењује и ако нема применљивог националног прописа, а и ако га има - такав пропис мора задовољити одговарајући стандард да би био примењен. Дакле, чак ни постојање прописа, ма како законито донешеног, није довољан основ за његову примену у случајевима угрожавања личне приватности.

"По ЕСЉП... услови под којима се врши надзор морају бити експлицитно наведени у закону, и морају бити сагласни "владавини права", што значи да "законски термини морају бити довољно јасни како би појединцу дали одговарајућу назнаку у погледу околности и услова под којима је дозвољено предузимање таквих мера."⁷ Будући да тада није постојао закон који би посебно регулисао надзор телефона и интернета од стране послодавца, то ни тај надзор није могао бити "законит", у време када је повређена приватност Линете Копланд.

Ако овако захтевну прецизност покушамо да применимо на поменуте домаће законе, видећемо да ју они ни најмање неиспуњавају. Већ је и истицање арбитражног одлучивања органа безбедности о увиду у податке о саобраћају, као и време задржавања тих података, довољно да поткрепи такав закључак. Погледајмо шта о томе даље кажу институције ЕУ.

Радна група за заштиту података, под званичним називом "Радна група по члану 29" (РГ29) у својој препоруци 3/99 и другим документима (од којих је већина побројана у Мишљењу 9/2004) чврсто стоји на становишту да подаци о саобраћају јесу подаци о личности, са чиме је сагласан и ЕСЉП, који их у горепоменутој одлуци назива очигледним (*prima facie*) подацима о личности. Штавише, у Препоруци 3/99 наводи се: "...Препорука РГ29 је да податке о саобраћају не би требало чувати искључиво у циљу спровођења закона, а да национални закони не би требало да утврђују обавезу задржавања података о саобраћају на период дужи од оног који је потребан да се наплати услуга..."

Дакле, примећујемо да ове стандарде наш законодавац није узимао у обзир - за њега подаци о саобраћају нису уопште подаци о личности, а задржавају се целих дванаест месеци.

Са друге стране, две чињенице би условно могле да "помире" овако недоречено, а тиме и ризично, законодавство, са прокламованом тежњом ка прикључењу ЕУ.

Наиме, на територији саме ЕУ, правна решења у овом домену нису усаглашена. На пр. Немачка и Француска нису се обазирале на смернице, закључке и притиске европских институција. То не угрожава интегритет ЕУ, јер надзор од стране органа извршне власти представља искључиво предмет националног суверенитета држава чланица. Међутим, потреба за усклађивањем прописа на целом подручју ЕУ у области заштите личне приватности, представља стратешки циљ који се убрзано реализује кроз поменуте институције (Радна група, Суд за људска права...), тако да критика на рачун нашег законодавца ипак остаје. Посебно ако (опет!) у обзир узмемо непрецизност (неразрађеност) и расцепканост домаће регулативе. Ево још једног примера који о томе упечатљиво говори: "одредбе закона о електронским комуникацијама које одређују приступ задржаним подацима, без увида у садржај, већ постоје у Закону о БИА, ВБА и ВОА"⁸.

⁷ цитат преузет из European Court of Human Rights Expands Privacy Protections: Copland v. United Kingdom, By Fred H. Cate August 6, 2007, Volume 11, Issue 21

⁸ Јован Стојић, шеф кабинета директора БИА

У вези са приметном фрагментацијом у домену заштите приватности личности ваљало би напоменути да искуства из САД потврђују да таква карактеристика директно утиче на повећање трошкова пословања⁹, јер за последицу има смањену правну сигурност (примена различитих прописа на средње случајеве) и по правилу компликоване административне процедуре, што додатно отвара врата корупцији. Исте последице производи и недовољно конкретизована регулатива, о чему смо већ говорили.

Колико је реална и озбиљна опасност коју производе недоречености у правним прописима?

Можда би се могло поставити и следеће питање: Да ли је противљење мерама какве садрже наши поменути закони мотивисано некаквим параноичним страхом? Или, можда, неоправданим неповерењем у државу? Било би добро да је тако. Али, искуства из земаља које су далеко и организационо и техничко-технолошки оспособљеније у овом смислу од наше, говоре другачије.

Наиме, становиште "Радне групе ЕУ о задржавању података" јесте да задржавање података у безбедносно-обавештајне сврхе представља велику опасност и да је "само избрисан податак безбедан податак". Зашто? Ево неких примера:

Хапшењима у Италији септембра 2006, откривена је завера неколицине официра војно-обавештајне службе, службеника италијанског телекома и лица различитог профила, која су у државне системе инсталирала недозвољене рачунарске програме, што је довело до прислушкивања и уцењивања више од пет хиљада лица из света политике, финансија, али и оних који нису јавне личности.

У Немачкој је 2006. године украдена база о личним подацима 17 милиона корисника услуга немачког телекома, која је обухватала адресе пребивалишта, датуме рођења, електронску пошту....

А сличне и опасније повреде приватности забележене су и у Мађарској, Грчкој, Словачкој, Бугарској, Литванији...¹⁰

Ко би требало да контролише оне који могу да контролишу све остале?

Речени пример из Италије доводи нас до још једног суштинског питања: ко, под којим условима, којим средствима и са каквим овлашћењима контролише оне који имају могућност да контролишу све остале? Ако је за то надлежна једино Канцеларија Савета за националну безбедност¹¹ и заштиту тајних података, а не Повереник, као независан орган¹², онда би наш правни систем још једном пао на европском испиту. Наиме, све Директиве ЕУ, почев од основне из области коју разматрамо, Директиве 95/46, инсистирају на независности надзора. Но, чак и да нема европских директива, да нема никаквих упоредних примера - начела владавине права, поштовања људских права и поделе власти требало би да на нас, при суочавању са оваквим, озбиљним питањима, делују отрежњујуће.

Заштита приватности личности у посебним областима

⁹ Final Report... одељак 10.1

¹⁰ В. WORKING GROUP ON DATA RETENTION: Position on the processing of traffic data for "security purposes".

¹¹ Стојић, исто

¹² Директива 95/46 инсистира на независном надзору (видети и Директиве 2002/58 - која се непосредно бави приватношћу у области електронских комуникација; 2004/24)

Приликом јавних разматрања заштите приватности од стране носилаца државне власти и других заинтересованих субјеката, потпуно је занемарен аспект заштите података о личности у специфичним областима, као што су трговина и пословање уопште. Подаци из упоредне праксе показују да на том плану постоје бројне опасности, али и (пословне, развојне) могућности. Један од случајева који у том смислу делује упозоравајуће већ смо поменули - крађа базе података о корисницима немачког телекома. Са друге стране примери из САД и Јужне Кореје, где већ одавно функционишу механизми јавног обележавања квалитета заштите приватности, сведоче да увођење ознака квалитета ове врсте, посебно када је реч о пословању путем интернета, може да представља битну конкурентску предност. Али, потребно је имати на уму да Европска Комисија у свом Коначном извештају од 20. јула 2007. долази до закључка, на основу упоредне праксе, да је за успешну примену кодекса понашања у пословању, односно успешно функционисање система заштите приватности путем ознака квалитета, неопходно имати утемељење или бар подстицај у предметном законодавству. То код нас, као што видимо, још увек није случај. Помињање ове области заштите неко би могао да сматра преурањеним, с обзиром на релативну развијеност нашег тржишта. Међутим, ако погледамо податке из већ поменуте Стратегије владе, видећемо да то није случај:

"...Око 350.000 субјеката јавног и приватног сектора баве се обрадом података о личности. Већина тих субјеката, има по неколико збирки или база података о личности и укупан број евиденција се процењује на преко милион. Ове евиденције обухватају евиденције државних органа, установа пензијског и здравственог осигурања, образовања, социјалне заштите, банкарског система, комуналних служби, удружења грађана, као и обраду података путем видео надзора на јавним местима, пословним и стамбеним објектима и др. За многе од тих обрада података не постоји изричит законски основ, односно сагласност лица или законом није уређена сврха и обим података који се обрађују, трајање и др, а у многим од ових случајева се ради о обради нарочито осетљивих података, као што су подаци о лечењу, социјалном статусу и др."

Пословање ма ког привредног субјекта неодвојиво је од банкарских трансакција. А, као што видимо, заштита података о њима још увек није одговарајуће регулисана.

Међутим, наведене информације изнете у Стратегији упозоравајуће су по више основа. Прво, ако бисмо следили горенаведену правну аргументацију Европског суда за људска права, надзирање, па и само задржавање набројаних врста података могло би да представља повреду приватности.

Друго, то отвара могућности за бројне злоупотребе (сетимо се горњег примера из Италије - материјал за уцену може се прибавити из података о здравственој заштити, чак и лакше него ли прислушкивањем телефона).

Питање стандарда применљиве технологије

Ова запажања доводе нас до следеће незаобилазне тачке: питање односа права и применљиве технологије. Под применљивом технологијом подразумевамо ону која задовољава одређене стандарде, прихватљиве са гледишта ваљано устројеног система прописа. О томе наш законодавац ништа посебно не говори. Претпоставимо да намерава да преузме правна решења ЕУ. Али, која решења када смо показали да на пољу заштите приватности између држава чланица постоје огромне разлике? Наш законодавац, стога, ту мора да буде до крајности прецизан. То за сада, видимо, није случај.

Потреба за прилагођавањем динамичи технолошког развоја

Са друге стране, поставља се питање како ће наше законодавство да нормира потребу за сталним прилагођавањем, с обзиром на промене које се све већом брзином одвијају на пољу савремене технологије? Примећујемо да је Влада то одредила као један од стратешких интереса (глава 3. Стратегије).

Међутим, предлог конкретног решења, био је присутан већ и у време доношења Закона о заштити података о личности 2008. у "Критичком осврту" СПЦ, који су као основ за амандмане преузели бројни посланици:

Не сме се из вида изгубити ни чињеница да је заштита података условљена променљивим околностима које диктира убрзан развој технологије. Предлог закона не предвиђа постојање никаквог тела састављеног од стручњака, које би обезбеђивало неопходну прилагодљивост таквим условима, што је предуслов ефикасности. Да ли ће се и то уређивати неким накнадним прописом? Па и у том случају би свакако такав институт требало уврстити у Закон, макар и оквирним, али јасним, одређењем. Формирање таквога тела, управо би требало да буде законска обавеза (а не само могућност) повереника, ради ваљаног испуњења обавеза регулисаних одредбама члана 44... (Надлежност), а посебно тачака од 10-13 (...10) прати примену мера за заштиту података и предлаже побољшање тих мера; 11) даје предлоге и препоруке за унапређење заштите података; 12) даје претходно мишљење да ли одређени начини обраде представља специфичан ризик за права и слободе грађанина; 13) прати уређење заштите података у другим земљама;...)"

Питање избора и извора технологије

Надаље, законом није регулисано питање избора, контроле и евентуалног санкционисања лица од кога се технологија за обраду података о личности набавља, односно које ју производи. Наше је мишљење да то не би требало препустити подзаконској регулативи, ако ни због чега другог, оно због изостанка јавне расправе, то јест обавештавања шире јавности на јасан начин, а у складу са одлукама и мишљењима горепомнутих институција ЕУ.

У вези са тим, поменућемо још једном, да наш законодавац не даје ваљане оквире за развој сродних система правила, као што су она којима се устројава добра пословна пракса. Наиме, давање личних података и њихова обрада могу се темељити и на уговору. Управо на том пољу правни механизми заштите приватности ЕУ, за које се и ми залажемо, а којима наше законодавство није доследно, доказују своју вредност. Коначни извештај Европске комисије бележи да се норме и стандарди правне заштите у овој области све чешће преузимају као саставни делови уговора, који регулишу пословне односе ван ЕУ. Тај тренд је посебно приметан у САД.

ЗАКЉУЧАК:

Упоредна пракса, а посебно инсистирање кључних институција ЕУ на сталном усавршавању правних прописа који се односе на заштиту приватности, указује да право представља темељни инструмент за остваривање такве заштите. То је и становиште Европске комисије.¹³ Али не било какво право, већ оно које задовољава одређене стандарде, о којима смо говорили у претходном тексту.

Решења која нуди правни систем Србије данас, те стандарде не испуњавају. Наша досадашња аргументација и сам текст Стратегије заштите података о личности, Владе РС од 16.8.2010. говоре томе у прилог.

У Коначном извештају Европска комисија истиче да постоје велике разлике у могућностима адекватне заштите личне приватности између земаља у развоју и развијених земаља. На примеру Индије јасно је показано да нерешена социјална и егзистенцијална питања великог дела становништва онемогућавају висок степен заштите, чак и поред обухватних правних решења и добре техничко-технолошке подлоге. Будући да је у Србији друштвена ситуација донекле слична, а обухватних правних решења и добре техничко-технолошке подлоге нема,¹⁴ свако даље експериментисање са новим технологијама кадрим да

¹³ у Коначном извештају

¹⁴ "...У вези са капацитетима, треба констатовати да у Републици Србији, специјализованих кадрова за заштиту података о личности готово да нема...", Стратегија заштите података о личности Владе РС

угрожавају личну приватност не би требало да буде ни предмет размишљања. Стога би, из разлога целисходности, требало одбацити идеју о увођењу било каквог јединственог електронског документа.

Тренутно стање у области права, политике, економије и друштва уопште чини ризичним увођење нових технологија за прикупљање и обраду података о грађанима Србије, а озбиљно доводи у питање сигурност и целисходност примене већ уведених (биометрије).

Такав закључак је оправдано и једноставно изводив већ након узимања у обзир примера из праксе институција ЕУ које смо поменули у горњем тексту. Додатну потврду дају нам и следеће чињенице везане за Србију данас: 1) висок степен корупције државних институција, 2) постојање монопола, 3) нефункционисање државне ревизије (по чему је Србија јединствена у Европи), 4) тајност финансирања политичких странака и 5) недодирљивост српских "тајкуна" што све, на обједињен и сажет начин, износи Верица Бараћ, Председник савета за борбу против корупције (Блиц, 15.8.2010.).

У вези са поменутиим, за процену ситуације у којој се као друштво тренутно налазимо, значајно је искуство Малезије. Наиме, представници Европске комисије уочили су¹⁵ да интереси и лобирање индустријалаца и даље представљају препреку обухватној заштити приватности.

За крај, подсетимо се и следећег:

У савременим условима управљање подацима јесте управљање људима. Појединац се у односу према држави (друштву уопште) све више одређује скуповима података. Тешко је пренагласити потребу за прецизним законским регулисањем заштите личне приватности, односно заштите података о личности. У Србији данас за то не постоје одговарајуће правно-системске претпоставке, нити одговарајући степен политичке воље, нити потребна упућеност, а тиме ни притисак јавности.

Доведени смо до тачке где је самоодбрана неопходна.

А нама су руке и даље спуштене, очи и даље затворене.

Александар Загорац, новембар 2010.

¹⁵ У Коначном извештају