Проф. др Предраг Димитријевић
Правни факултет у Нишу

UDK: 342.721:004738.5

ПРАВО ПРИВАТНОСТИ НА ИНТЕРНЕТУ[*]
(позитивноправни оквир)

Апстракт: *Интернет је глобална кибернетска информациона мрежа у којој учествују многи субјекти као корисници различитих информација. У том глобалном виртуелном интерактивном комуникацијском простору, размењују се различите информације па се поставља питање безбедности и интегритета тих података, аутентичност, односно идентитет корисника, као и потврда пријема и слања података. Подаци који се налазе у кибернетском простору могу бити угрожени од стране разних појединаца или правних лица, институција али и државних органа. Да би се ти подаци заштитили државе доносе разне законске и подзаконске акте којима се пружа заштита података али истовремено се легализује контрола података, односно ничим контролисано прикупљање и обрада података на Интернету од стране државних органа.*

Кључне речи: *Интернет, сајбер право, право приватности, подаци о личности.*

---

[*] Овај рад настао је као резултат истраживања у оквиру пројекта „Приступ правосуђу - инструменти за имплементацију европских стандарда у правни систем Републике Србије“, који реализује Правни факултет Универзитета у Нишу уз финансијску помоћ Министарства науке и заштите животне средине, на основу Уговора о реализацији пројекта из програма основних истраживања бр. 149043Д од 23. 2. 2006. године.

1. Cyberspace и право

Милиони људи широм света користе Интернет за прикупљање информација, разна истраживања, финансије и кореспонденцију а да при том и не помисле колико су правна питања повезана и саставни део електронске комуникације и трговине. Интернет као продукт нових информационих технологија сустински мења начин рада и комуницирања у свим областима зивота. Присиљени смо да нове информационе технологије користимо за успешније и квалитетније обављање послова. Интернет даје свакоме могућност да има свој wебсите, једнаку могућност на објављивање текста, свако може емитовати своју информацију, став или мишљење широм света, без потребе да предходно иде до издавача неког часописа и слично. С друге стране, многе владе реагују на информације са Интернета тако што контролишу и website и оне који приступају Интернету.

Интернет је мрежа компјутерских мрежа, коалиција свих светских мрежа (Internet Society).[1] Интернет је глобални електронски комуникациони систем међусобно повезаних рачунарских мрежа и уређаја, намењен размени свих врста информација у складу са Интернет стандардима**.** Интернет стандарди су документи који се односе на концепте, процедуре умрежавања, протоколе, интерфејсе и методе идентификације у оквиру Интернета.[2] Само име Интернет долази од појма међу мрежа ("inter-networking") где су више компјутерских мрежа повезане заједно. Преко Интернета се одвија бизнис арена, електронска пошта (e-mail), трансфер фајлова и чатовање (chat rooms), док се трговина и поуздани проток информација одвија посредсвом глобалне светске мреже (World Wide Web - www). Заједно они чине свет кибрернетског простора (world of cyberspace) где правна питања и проблеми почињу да енормно расту, а међу њима су приватност и безбедност.

Како Право реагује и одговара на нове технологије? Широко је распрострањена повреда ауторских права од стране оних који

[1] **G. R. Ferrera, S. D. Lichtestein, M. E. K. Reder, R. August, W. T. Schiano**, *Cyberlaw, Your Rights in Cyberspace*, Thomson Learning, Canada, 2001, web: http://www.thomsonrights.com

[2] Интернет стандарде, под називом *Реqуест Фор Цомментс* (RFC) доноси међународна организација *Internet Engineering Task Force* (IETF).

преузимају и копирају материјале са других wеbсајтова или нечијих књига, чланака и сл. и презентују их као своје без писмене дозволе носилаца ауторских права (аутора). Регулисање проблема заштите ауторских права и питања заштите приватности на Интернету представљају само неке од области које сајбер право регулише.

Сајбер простор карактерише брисње физичких, политичких и социјалних граница. Нове границе, једино могу бити домени који су дефинисани техничким карактеристикама. Назив домена (domain name system **- DNS**) који је уведен 1984, је глобално јединствена текстуална ознака која повезује скуп рачунара, уређаја и сервиса на Интернету у јединствену административно-техничку целину. Домени могу заузети место граница у кибернетском простору у традиционалном смислу. [3]

Свака држава покушава да законима и подзаконским актима регулише поначање на Интернету а који не може да се ограничи на државне границе. Националне владе не могу да обуздају могућности сајбер простора, баш због природе глобалне технологија. Кибернетским простором путују различите информације а при томе аутори тих различитих садржаја немају могућност контроле над употребом и ширењем својих дела на Интернету. Због невероватне лакоће којом се дигитални материјал може копирати и слати, закон би требало да заштити ауторе од таквог копирања писаног материјала, музике, графичких дела, софтвера. Међутим, постоји и мишљење да јавност треба да слободно располаже оваквим садржајима, на исти начин на који је традиционално располагала копијама књига, музике и осталих ауторских дела.

Корисницима Интернета[4] је, због његовог мултинационалног карактера, омогућено да избегну примену прописа који им не одговарају. Понекад, то значи тежњу ка попустљивијим прописима,

[3] Ипак, границе у сајбер простору су још увек повезане са стварним ефектима у физички ограниченом стварном простору. Зато је један од највећих теоријских изазова сајбер права да препозна, артикулише и опише обим и улогу ових простора. **Ана Марковић**, *Законска регулатива и Интернет* (http://e-trgovina.co.yu/pravo/zakonska_regulativa1.html, страница последњи пут посећена 08.12.2008.), Београд, 2008.

[4] *Корисник Интернета* је физичко или правно лице које користи Интернет услуге и/или остале услуге преноса података по основу закљученог уговора или на други предвиђени начин.

односно избегавање прописа; али уколико је то погодније, и тежњу ка стриктнијим прописима. Тачније, веб-сајт лако може бити смештен ван јурисдикције граница државе (нације) и тако не буде лимитиран њеним законима. Ово off-shore правосуђе са минимумом правних прописа може претворити Интернет у рај за коцкање и остале радње које су забрањене на другим местима.[5]

2. Закон о телекомуникацијама

Садржи бројне одредбе али издвојићемо оне које се тичу приватности и безбедности информација а оне су смештене у делу који прописује "остале обавезе јавних телекомуникационих оператора" (члан 54. и 55.). У том смислу, узећемо у обзир последњи став члана 54. по коме је Јавни телекомуникациони оператор дужан да надлежним државним органима омогући приступ и анализу података о саобраћају који се односе на појединачне кориснике и који се обрађују ради успостављања веза, а које иначе по закону јавни телекомуникациони оператор може у чувати и обрађивати само у обиму који је неопходан за испостављање рачуна кориснику и исте може доставити само пошиљаоцу и примаоцу порука.

Друго, (члан 55) Закон изричито забрањује све активности или коришћење уређаја којима се *угрожава* или *нарушава приватност и поверљивост порука* које се преносе телекомуникационим мрежама, осим када постоји *сагласност корисника*[6] или ако се ове активности врше у *складу са законом* или *судским налогом* издатим у складу са законом. При томе се не каже којим закон, јер то евидентно није ЗоТ. Такође, закон обавезује оператора да као део система, о сопственом трошку, оформи подсистеме, опрему и инсталације за *законом овлашћени електронски надзор* одређених телекомуникација.

[5] Питање је на који начин се доносе одлуке, у недостатку колективног интернационалног тела и да ли постоји простор за консензус између страна. Да ли ће појединачни, или колективни поступци потиснути националну и интернационалну регулативу?

[6] То је тзв. "обрада са пристанком" података. *Закон о заштити података о личности*, Службени лист 97/2008, члан 10. Пристанак се може опозвати, па је у том случају "обрада података" *недозвољена* после опозива пристанка (члан 11).

При томе, тзв. "техничке услове" за ове подсистеме, уређаје, опрему и инсталације дефинише Агенција (РАТЕЛ), у сарадњи са телекомуникационим операторима и *државним органима надлежним за непосредно спровођење електронског надзора*.

3. Технички услови за Интернет мреже

На основу *Закона о телекомуникацијама*[7] и *Статута Републичке агенције за телекомуникације*[8], Републичка агенција за Телекомуникације (РАТЕЛ),[9] донела је *Техничке услове за подсистеме, уређаје, опрему и инсталације интернет мреже* (11.07.2008. године). Овим се општим правним актом дефинишу технички услови за подсистеме, уређаје, опрему и инсталације за законом овлашћени надзор одређених телекомуникација које су јавни телекомуникациони оператори (мрежни оператори, пружаоци услуга и пружаоци приступа) дужни, да као део система оформе о сопственом трошку. Електронски надзор се врши за потребе надлежних државних органа. Да би се тај надзор могао да спроведе *јавни телекомуникациони оператори* се обавезују да:

- уредно воде и ажурирају све базе података свих закупљених линија и веза,
- омогуће директан приступ и увид у базе података,
- омогући директан увид у евиденције о сметњама на телекомуникационом уређајима[10] и прекидима телекомуникационог саобраћаја,
- да уклоне криптозаштиту пре достављања садржаја комуникације надлежном државном органу,

[7] "Службени гласник РС" бр. 44/03 и 36/06, члан 55. став 3.

[8] "Службени гласник РС" број 78/05, члан 18. тачка 7.

[9] **Дејан Шупут**, *Републичка агенција за телекомуникације*, Правни живот, бр. 10, Београд, 2008, стр. 807.

[10] Телекомуникациони подсистеми, уређаји, опрема и рачунарски системи смештају се у просторијама државног органа (овлашћеног) за електронски надзор и/или у посебним просторијама у оквиру телекомуникационих центара. Ове просторије обезбеђују и опремају јавни телекомуникациони оператори, по захтеву и техничким прописима надлежног државног органа.

- да на захтев надлежног државног органа достави податке о свим комуникационим средствима која су се појављивала на одређеној географској, физичкој или логичкој локацији у минималном периоду од последњих 48 часова, независно од постојања телекомуникационе активности.

Пружалац Интернет услуга је дужан да надлежним државним органима омогући:

- приступ ажурној бази података о претплатницима и *на захтев* доставља *експортовану базу података*.[11]

- приступ ажурној бази података о корисницима електронске поште,

- упознаје их о начину заштите података о корисницима,

- именује, уз сагласност државних органа особу за контакт и комуникацију са њима,

- у реалном времену потпуно аутономни пасивни мониторинг,

- интернет активности произвољног претплатника и преусмеравање долазног и одлазног саобраћаја ка аквизиционом центру надлежног државног органа,

- односно обезбеди хардвер и софтвер за пасивни мониторинг у реалном времену, сервиса електронске поште и преусмеравање садржаја поште ка аквизиционом центру надлежних државних органа.

- обезбеди хардвер и софтвер за мониторинг саобраћај између произвољног претплатника, преко пружаоца Интернет услуга, према трећем Интернет провајдеру.

- да не ствара техничких могућности којима би сви наведени подаци постали доступни трећој страни.

Хардвер и софтвер, који обезбеђује пружалац Интернет услуга, треба да омогуће: пасивни мониторинг Интернет активности у реалном времену; прикупљање и анализу статистике Интернет активности; пресретање електронске поште, придружених садржаја (attachment) и обраду Web mail-a; пресретање IP телефонског саобраћаја, факсимила и IP видео саобраћаја; пресретање IM (instant messenger) саобраћаја; пресретање саобраћаја на peer-to-peer

[11] База треба да садржи: личне податке из уговора са претплатником и врсту услуга, информацију о постојању заштите преноса података, начин приступа претплатника, максималну брзину преноса података и идентификационе адресе.

мрежама, конструкцију пресретнутог саобраћај до нивоа апликације и филтрирање по: корисничком имену или корисничком телефонском броју, адреси електронске поште, IP адреси и IM (instant messenger) идентификацији.

На основу изнете регулативе може се оправдано коонстатовати да под маском наводних "техничких услова за Интернет мреже" у Србији се уводи до сада незабележени масовни и ничим ограничени *надзор и архивирање* свих облика електронских комуникација за потребе службе безбедности. Мишљење је да чак ни у најгора времена није се правила оваква регулатива. Индикативно је и то да је агенција РАТЕЛ као независно регулаторно тело и доносилац овог нормативног акта, истом дала ретроактивно дејство, односно дејство пре објављивања јер у овом документу стоји да тзв. "технички услови" ступају на снагу наредног дана од дана доношења, а то значи пре формалног објављивања. На основу свега дошло је и до стављања ван снаге овог општег акта РАТЕЛ-а.

4. Правилник о Интернету

На основу *Закона о телекомуникацијама*[12] Републичка агенција за телекомуникације донела је *Правилник о условима за пружање интернет услуга и осталих услуга преноса података и садржају одобрења* (23.09.2008),[13] којим се утврђују технички услови за пружање Интернет услуга и осталих услуга преноса података (прописивање образаца, начин издавања и садржај одобрења и др.).

"Интернет услуге" су јавне телекомуникационе услуге преноса података које се реализују у складу са Интернет стандардима а за чије остваривање је неопходна употреба *јавних IP адреса*[14], осим

[12] "Службени гласник РС", бр. 44/03 и 36/06, члан 38. ст. 5, 6. и 9.

[13] Републичка агенције за телекомуникације (РАТЕЛ) је овим посебним општим актом (правилником) регулисала комерцијално пружање услуге преноса говора, радио и телевизијских програма у реалном времену. Даном ступања на снагу овог правилника престао је да важи *Правилник о условима за пружање Интернет услуга и садржају одобрења* („Службени гласник РС", број 60/06").

[14] *Јавна ИП адреса* је нумерички идентификатор, који једнозначно идентификује мрежу или приступну тачку у склопу Интернета, а за чије је додељивање

комерцијалних услуга преноса говора, радио и телевизијских програма у реалном времену.[15] За пружање Интернет услуга морају бити испуњени основни технички услови у складу са препорукама и стандардима међународних организација, а нарочито: IETF, ITU, ETSI, IEEE, CEN/CENELEC, ISO, IEC и општим актима Агенције.

Агенција издаје одобрење за пружање Интернет услуга лицу које је регистровано за телекомуникациону делатност, које је Агенцији поднело пријаву за регистрацију и које испуњава законом прописане услове.[16]

Ималац одобрења је дужан да у складу са својим техничким могућностима обезбеди Услуге свим заинтересованим корисницима, без било какве дискриминације (принцип једнакости и недискриминације).

Ималац одобрења је дужан да обезбеди поверљивост и безбедност својих услуга, података о корисницима својих услуга и забрањено му је да користи или пружа информације трећим лицима о садржају, чињеницама и условима преноса порука, изузев минимума који је неопходан за пружање услуга или у случајевима предвиђеним законом.

Ималац одобрења не може вршити било какве ограничења приступа услугама на основу националног, расног, верског, политичког, територијалног или било којег другог критеријума, који би могао довести до кршења људских права и основних слобода.

Ималац одобрења не сме успоставити монопол било ког облика, закључујући уговоре са другим пружаоцима телекомуникационих услуга.

Он је дужан да обезбеди уређаје, опрему и инсталације које ће у разумној мери гарантовати заштиту података претплатника и онемогућити злоупотребу од стране трећих лица.

Надлежни орган врши контролу недозвољеног садржаја. Уколико надлежни орган коначном одлуком наложи имаоцу одобрења, да

на светском нивоу надлежна организација Internet Assigned Numbers Authority (IANA).

[15] "Остале услуге" преноса података су јавне телекомуникационе услуге које се реализују помоћу уређаја за пренос података који су прикључени на јавну телекомуникациону мрежу, и за чије остваривање се не користе јавне ИП адресе.

[16] *Закон о телекомуникацијама*, "Службени гласник РС", бр. 44/03 и 36/06.

уклони садржај за који је установљено да је недопуштен, увредљив, штетан, или да крши заштићена ауторска права, ималац одобрења је дужан да без одлагања поступи према таквој одлуци.

Ималац одобрења за пружање Интернет услуга је обавезан да у границама својих техничких могућности кориснику омогући заштиту од нежељене електронске поште и/или штетних садржаја.

Он је дужан да уговором односно општим условима обавеже кориснике на забрану слања нежељене поште и штетних садржаја. У случајевима слања нежељене поште или штетних садржаја, повреде права интелектуалне својине, ималац одобрења је у обавези да упути писано упозорење кориснику. Уколико корисник настави са слањем нежељене поште, штетног садржаја или повреде права интелектуалне својине ималац одобрења може да престане са пружањем услуге том кориснику.

Агенција не сноси одговорност за настанак било какве материјалне или друге врсте штете нанете претплатнику односно кориснику, проузроковане коришћењем услуга имаоца одобрења (нпр. нежељена пошта - „spam", вируси, „phishing", и др).

5. Закон о заштити података о личности[17]

Овим законом се уређују услови за прикупљање и обраду података о личности[18], права лица и заштита права лица чији се подаци прикупљају и обрађују, ограничења заштите података о личности, поступак пред надлежним органом за заштиту података о личности, обезбеђење података, евиденција, изношење података и надзор над извршавањем закона.

[17] Службени лист 97/2008. Одредбе овог закона примењују се на сваку аутоматизовану обраду, као и на обраду садржану у збирци податка која се не води аутоматизовано.

[18] *Податак о личности* је свака информација која се односи на физичко лице, без обзира на облик у коме је изражена и на носач информације (папир, трака, филм, електронски медиј и сл), по чијем налогу, у чије име, односно за чији рачун је информација похрањена, датум настанка информације, место похрањивања информације, начин сазнавања информације (непосредно, путем слушања, гледања и сл, односно посредно, путем увида у документ у којем је информација садржана и сл), или без обзира на друго својство информације.

1. Заштита података о личности обезбеђује се сваком физичком лицу, без обзира на држављанство и пребивалиште, расу, године живота, пол, језик, вероисповест, политичко и друго уверење, националну припадност, социјално порекло и статус, имовинско стање, рођење, образовање, друштвени положај или друга лична својства. Послове заштите података о личности обавља *Повереник за информације од јавног значаја и заштиту података о личности*, као самосталан државни орган, независан у вршењу своје надлежности. Он је успостављен са циљем да, у вези са обрадом података о личности,[19] сваком физичком лицу обезбеди остваривање і заштиту права на приватност и осталих права и слобода.

Међутим, ***закон не примењује на обраду свих података.*** Одредбе овог закона не примењују се на обраду одређене групе података сем уколико "очигледно претежу супротни интереси лица". То су следеће групе података: подаци доступни свакоме (јавна гласилиа и публикације, архиве, музеји), породични и лични подаци који нису доступни трећим лицима, затим, подаци о члановима политичких странака и других облика удруживања, који се обрађују од тих организација, али док траје чланство, и података које је лице само објавило о себи, а оно је способно да се само стара о својим интересима.

Сви други подаци који се прикупљају и обрађују у друге сврхе могу да се обрађују искључиво у историјске, статистичке или научноистраживачке сврхе, ако не служе доношењу одлука или предузимању мера према одређеном лицу уз обезбеђивање одговарајућих мера заштите.[20]

---

[19] *Обрада података* је свака радња предузета у вези са подацима као што су: прикупљање, бележење, преписивање, умножавање, копирање, преношење, претраживање, разврставање, похрањивање, раздвајање, укрштање, обједињавање, уподобљавање, мењање, обезбеђивање, коришћење, стављање на увид, откривање, објављивање, ширење, снимање, организовање, чување, прилагођавање, откривање путем преноса или на други начин чињење доступним, прикривање, измештање и на други начин чињење недоступним, као и спровођење других радњи у вези са наведеним подацима, без обзира да ли се врши аутоматски, полуаутоматски или на други начин.

[20] Мере заштите података који се архивирају у искључиво историјске, статистичке или научноистраживачке сврхе уређују се посебним прописом.

2. Закон наводи изричито ситуације у којима *обрада података* (али не и прикупљање) није дозвољена, и то ако:

1) физичко лице није дало пристанак за обраду или се обрада врши без законског овлашћења;

2) се врши у сврху различиту од оне за коју је одређена, без обзира да ли се врши на основу пристанка или законског овлашћења;

3) сврха обраде није јасно одређена, ако је измењена, недозвољена или је већ остварена;

4) је лице на које се подаци односе, одређено или одредиво и након што се оствари сврха обраде;

5) је начин обраде недозвољен;

6) је податак који се обрађује непотребан или неподесан за остварење сврхе обраде;

7) су број или врста података који се обрађују несразмерни сврси обраде;

8) је податак неистинит и непотпун, односно када није заснован на веродостојном извору или је застарео.

Постоји изричита *забрана аутоматске обраде* одређене врсте података. Тако, одлука која производи правне последице или погоршава његов положај неког лица, не може бити искључиво заснована на подацима који се обрађују аутоматизовано и који служе оцени неког његовог својства (радне способности, поузданости, кредитне способности и сл), сем када је то законом изричито одређено, односно када се усваја захтев лица у вези са закључењем или испуњењем уговора, уз спровођење одговарајућих мера заштите. У том случају лице мора бити упознато са поступком аутоматизоване обраде и начином доношења одлуке.

Оно што је посебно интересантно је таксативно навођење ситуација када је обрада података допуштена *ex lege* иако нема пристанка, тзв "***обрада без пристанка***". Обрада без пристанка је дозвољена:

1) да би се остварили или заштитили животно важни интереси лица (живот, здравље и физички интегритет);

2) у циљу извршења законских обавеза или обавеза одређених актом донетим у складу са законом;

3) у другим (под) законским случајевима, ради остварења претежног оправданог интереса лица, руковаоца или корисника.

Обрада податке без пристанка лица од стране органа власти врши се ако је обрада неопходна у циљу остваривања интереса националне или јавне безбедности, одбране земље, спречавања, откривања, истраге и гоњења за кривична дела, економских, односно финансијских интереса државе, заштите здравља и морала, заштите права и слобода и другог јавног интереса, а у другим случајевима на основу писменог пристанка лица.

3. Закон прави разлику између "обраде" података и "прикупљања" података. У том смислу што каже да се подаци прикупљају од *лица на које се односе*,[21] од *органа управе* који су овлашћени за прикупљање и од *другог лица* ако:

1) је то предвиђено *уговором* закљученим са лицем на које се подаци односе;

2) је то прописано *законом* или другим прописом;

3) је то неопходно с обзиром на *природу посла*;

4) прикупљање података од самог лица захтева прекомерни утрошак времена и средстава;

5) се прикупљају подаци ради остварења или заштите животно важних интереса лица на које се односе, посебно живота, здравља и физичког интегритета.

Закон уводи посебну категорију података који се зову "***нарочито осетљиви подаци***" у коју спадају: подаци који се односе на националну припадност, расу, пол, језик, вероисповест, припадност политичкој странци, синдикално чланство, здравствено стање, примање социјалне помоћи, жртву насиља, осуду за кривично дело и сексуални живот. Ови подаци имају посебан законски режим прикупљања и обраде. Ови "нарочито осетљиви подаци" су посебно законом заштићени јер се могу обрађивати искључиво *на основу **слободно датог пристанка** лица*. Закон их посебно штити јер уводи

[21] Руковалац који податке прикупља од *лица на које се односе*, односно од *другог лица*, пре прикупљања, упознаће лице на које се подаци односе, односно друго лице о свом идентитету, сврси прикупљања и даље обраде, начину коришћења података, обавезности и правном основу, односно добровољности давања података и обраде и др. *Обавеза обавештавање о обради* не постоји када такво упознавање, с обзиром на околности случаја, није могуће или је очигледно непотребно, односно непримерено, а нарочито ако је лице на које се односе подаци, односно друго лице већ упознато са тиме или ако лице на које се подаци односе није доступно.

још један степен заштите када прописује да се законом може *забранити* обрада ових нарочито осетљивих података иако је и дат пристанак.[22]

Изузетно, подаци о политичкој припадности, здравственом стању и социјалној помоћи, могу се обрађивати и без пристанка лица, ако је то законом допуштено.

6. Уместо закључка

Ова сумарна анализа позитвноправних решења отвара бројна питања. Питање је, који су то државни органи надлежни да врше електронски надзор приватних података, који су то случајеви када закон допушта електронску контролу, како могу појединци заштитити своју приватност од е-надзора или мониторинга у "законом допуштеним систуацијама". У том контексту, да ли је закон о заштити приватности у Србији и подзаконска регулатива РАТЕЛА-а донета управо у супротном циљу да легализују административну контролу приватности. То је осетљиво питање граница државне контроле и права приватности у виртуелној стварности.

[22] Закон познаје институцију "опозива пристанка" за обраду нарочито осетљивих података, у ком случају, лице које је дало пристанак дужно је да руковаоцу накнади оправдане трошкове и штету, у складу са прописима о одговорности за штету, осим ако је друкчије одређено у изјави о пристанку.

LL.D. Full-time Professor Predrag Dimitrijević
Law Faculty of the University of Niš

RIGHT TO PRIVACY ON THE INTERNET

Summary

Internet is a global cybernetic information network in which many subjects participate as users of different information. In that global virtual communication space different information are exchanged and that creates a question of security and integrity of the data, authenticity, user's identity, as well as confirmation of receipt and sending of data. Data found in the cybernetic space can be endangered by various individuals or legal entities, institutions and government bodies. To protect the data, states make various laws and legislation that provides data protection, but at the same time they legalize control of data, and not controlled collection and processing of data on Internet by state authorities. The question is, which authorities can control private data, which are cases when the law allows electronic control, how individuals can protect their privacy from e-surveillance or monitoring in the "situations allowed by law". In particular, the question is whether the laws on the protection of privacy bring in the opposite order to legalize the administrative control of privacy. It is a sensitive issue of boundaries of state control and privacy in virtual reality.

Keywords*: Internet, cyber law, the right to privacy, personal data.*