

УДК 342.738:004.056(560)
004.738.5:351.083.8(560)

DOI: 10.5937/pr76-43696

Прегледни рад

*Даница Лазовић**

Институт друштвених наука, Београд

ПОЛИТИКА ПРАВА НА ПРИВАТНОСТ И ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ НА ИНТЕРНЕТУ: СТУДИЈА СЛУЧАЈА ТУРСКЕ

Сажетак

Право на приватност и право на заштиту података о личности постају једно од најзначајнијих питања у области владавине права и поштовања фундаменталних права и слобода. Развитак модерних технологија, а пре свега интернета је допринео увећању значаја ових права али и све већој пажњи коју им националне и међународне институције придају. Република Турска, као једна од најзначајнијих држава на међународном плану, по свом стратешком положају, економској, политичкој и војној моћи, доспела је у средиште интересовања медија, међународних и наднационалних организација попут Уједињених нација и Европске уније у контексту процене поштовања људских права и слобода. Политичке промене настале усвајањем уставних амандмана који су начелно препознали значај наведених права, супротно очекивањима, допринеле су њиховом већем кршењу и расту моћи извршне власти, при чему турски политички систем све више добија карактеристике хиперпрезидентијализма. Основна питања на које ће рад настојати да одговори односе се на расветљавање стварног значаја и садржаја ових права, постојаност турске легислативе у односној области и испитивање утицаја легислативе на стварно стање по питању њиховог

* d.lazovic96@gmail.com

поштовања. Будући да је Република Турска држава која претендује на чланство у Европској унији, биће неопходно размотрити и правно наслеђе Европске уније у овој области.

Кључне речи: приватност, заштита података о личности, Република Турска, легислатива, интернет

УВОД

Стање владавине права у области коришћења интернета и у контексту заштите података о личности и приватности постаје савремена и значајна академска тема у доба глобализације и растућег обима размене информација на друштвеним мрежама. У политичком и практичном смислу, недостатак владавине права у овим областима доприноси затварању државе и њених грађана према свету и онемогућава развој плурализма, демократије и транспарентности. Самим тим, оставља се простор властима да кроз контролу медија и интернета утичу на обликовање јавног мњења, проток и доступност информација. Питање цензуре интернета, злоупотребе личних података грађана и нарушавања њихове приватности од стране власти постаје важно питање у савременим друштвима, где се примећују све раширеније тенденције власти да посредством своје политичке моћи утичу на ограничавање слободног коришћења и приступа садржајима на интернету (Warf 2010, 123).

Поред тога, власти које настоје да ограниче фундаментална људска права и слободе, често коришћењем своје етаблиране политичке позиције онемогућавају висок степен приватности грађанима, контролишући њихове приватне податке и пратећи начин на који учествују у животу на мрежи. У том контексту, Република Турска није била изузетак оваквим тенденцијама. Иако су усвојени многи закони који се баве областима људских права и слобода, најпре у сајбер простору (*cyber space*), евидентан је раскорак између прокламованих законских правила и практичног стања, са изузетком оних одредби представљају неки вид озакоњења државног мешања у приватну сферу појединца и потпуно нарушавање заштите података о личности и права у овом домену.

Легислатива у области медија и интернета у Турској базира на се Закону бр. 5.651, усвојеном 2007. године. У периоду од 2007. до данас,

Турска је прошла кроз процес уставних промена, након референдума одржаног 2017. године, када је већина грађана подржала увођење хиперпредседничког система, који је омогућио веће концентрисање моћи у рукама председника. Закон је промењен амандманима 2014. године. Доношењем Закона бр. 7.253. из 2020. године, легислатива о интернету додатно је изменила правила игре, наметнула још оштрије санкције за кршење предвиђених одредби и онемогућила приступ многим страним сајтовима, чиме се стање владавине права у области слободе медија и изражавања драстично погоршало.

Чланом 4. Закона бр. 7.253, Управа за информационе и комуникационе технологије (*Bilgi Teknolojileri ve İletişim Kurumu*) као основно национално регулаторно и инспекцијско тело у области телекомуникација добила је улогу контролора над страним провајдерима. Страни провајдери су обавезани да оснују своја представништва у Турској, сачињена од турских држављана или резидената. Складно усвојеном закону, представништва страних провајдера у обавези су да подносе шестомесечне извештаје о раду, уклањају неподобне садржаје, прикупљају личне податке корисника у Турској, као и да плаћају административне и судске казне у случају кршења донетог закона (видети *Kanun 7253/2020*). Закон о заштити личних података (*Kişisel Verilerin Korunması Kanunu*) познатији као Закон бр. 6.698 усвојен је 2016. године, те поред споменутих Закона о интернету чини један од основних легислативних оквира који ће бити предмет анализе са циљем стварања комплетне слике о поштовању једног од круцијалних људских права у које спада и право на заштиту података о личности.

Овај истраживачки рад настоји да кроз анализу релевантне легислативе у области заштите права на приватност и права на заштиту података о личности одговори на питање да ли је постојање закона у односним областима позитивно или негативно допринело стварном поштовању тих права у пракси, као и да појасни могуће импликације које интернет заједно са другим модерним средствима комуникације производи у домену споменутих права.

РАЗВОЈ ПРАВА НА ПРИВАТНОСТ И ПРАВА НА ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ

Право на заштиту података о личности једно је од фундаменталних људских права о коме почиње да се говори и

пише још у античко доба, али се правни корени његовог схватања у савременој мисли најпре налазе у правним тековинама Сједињених америчких држава (САД), Организације Уједињених нација (ОУН) и Европске уније (ЕУ).

Право на заштиту приватности препознато је у есеју *Право на приватност* аутора Семјуела Варена (*Samuel Warren*) и Луиса Брендејса (*Louis Brandeis*). У есеју *Право на приватност*, аутори констатују да промене које се дешавају у свету морају бити праћене конституисањем и признавањем нових права, која настоје да омогуће правну заштиту појединаца у новонасталим околностима.

Између осталог, право на приватност појединца неопходно је утемељити у правном поретку и дати му универзални значај (*Warren and Brandeis 1890, 193–220*). У том контексту, право на приватност ране америчке јуриспруденције у том домену односи се на право да будемо остављени на миру (*right to be left alone*). Развој новинарства допринео је угрожавању приватности појединца због објављивања различитих мање или више истинитих тврдњи, као и слика појединаца. Све већа изложеност приватности појединца у јавности, путем медија као што су новине, допринела је угрожавању слобода појединца и права да буде остављен на миру (196). Доношење Универзалне декларације о људским правима 1948. године од стране тела као што су ОУН, представља велики корак у утемељивању основних слобода и права људи. Глобални значај Универзалне декларације о људским правима огледа се у чињеници да је усвојена у ОУН, телу које по свом саставу одликује изразита хетерогеност у религијском, културном, социјалном, политичком и економском смислу, што показује да је универзалност права и значај његове свеобухватне заштите препознат на глобалном нивоу без обзира на унутрашње разлике које неминовно постоје међу државама чланицама. Чланом 12. Декларације истиче се да: „Нико не сме бити изложен произвољном мешању у приватни живот, породицу, стан или преписку, нити нападима на част и углед” (Универзална декларација о људским правима 1948, чл. 12). Поред тога, истим чланом истиче се да је нужно обезбедити законску заштиту од таквих напада свим грађанима.

Тенденције уобличавања, дефинисања и промоције људских права и слобода потекле под окриљем УН, испраћене су и на европском континенту, најпре у правним оквирима ЕУ. Током 1950. године, усвојена је Европска конвенција о људским правима,

која је значајна због бројности и просторне разноврсности држава потписница Савета Европе (Council of Europe [COE], n.d.). Будући да је усвојена под окриљем Савета Европе, у чије чланство се укључују и друге европске државе, без обзира на то да ли су чланице ЕУ или не, Турска је као нечланица али претендент на чланство, такође потписница. Јемац поштовања односних права и слобода у овом случају јесте Европски суд за људска права са седиштем у Стразбуру, који делује на захтеве појединаца, држављана држава чланица Савета Европе, те оних које су потписале Европску конвенцију о људским правима. У том контексту, овај суд је значајан јер омогућава појединцу да добије правну заштиту онда када сматра да су његова права и слободе угрожени и када правну заштиту није било могуће добити у домаћој држави и њеним судовима (Европски суд за људска права [ЕСЈП] 2021, 7).

Шездесетих година XX века, Вилијам Прозер (*William Prosser*) објављује чланак под називом *Приватност*, у коме дефинише прекршаје против приватности појединца, подложним тужби починиоца који треба оштећеном да надокнади штету. Међу прекршајима против приватности појединца, аутор препознаје мешање у приватне послове, јавно откривање непријатних приватних информација, негативни или лажни публицитет као и присвајање нечијег имена или лика (Prosser 1960, 383–423). Растом и развојем технологија и изложености појединца и његове приватности у јавности, расла је потреба за дефинисањем садржаја права на приватност и проналажења законских темеља за кажњавање прекршаја против приватности. У књизи *Приватност и слобода* објављеној 1967. године Алан Вестин (*Alan Westin*) дефинише приватност као „захтев појединаца да одређују када, како и у којој мери ће информације о њима бити изношене” (Reynolds 1969, 7).

Деведесете године XX века обележила је експанзија нових информатичких технологија, повећаног и све бржег протока информација, као и бојазни како ће се технолошко-информатичке промене негативно одразити на права појединца у смислу заштите приватности и података о личности. Развоју права појединца на приватност и на заштиту података о личности у великој мери допринела је легислатива ЕУ, која је посебно значајна уколико се просторно у анализу укључе оне државе које су чланице или које то претендују да постану. Директива ЕУ о заштити појединца у

вези са обрадом личних података и о слободном протоку таквих података усвојена је 1995. године.

Повеља ЕУ о основним правима усвојена је 2007. године, а њен други део односи се на дефинисање слобода међу којима чл. 8 истиче и право на заштиту података о личности које се неминовно везује за појам људског достојанства. Члан 8. ст. 2., истиче да: „[...] подаци морају бити обрађени поштено за унапред одређену сврху и на основу информисаног пристанка особе или на неком другом легитимном основу уређеном законом. Свако има право да приступи прикупљеним подацима о својој личности и има право да затражи њихову исправку” (Charter of fundamental rights of the European Union 2007/C 303/01). Повеља је очигледно направила дистинкцију између два права – права на приватност и права на заштиту података о личности, што не искључује њихову међусобну повезаност и нераскидивост. Основна људска права, прокламована Повељом, инкорпорирана су и у уставне принципе на којима почива ЕУ. Неизоставни надзорник поштовања људских права и слобода, међу којима се убрајају и право на приватност и право на заштиту података о личности јесте Суд правде ЕУ, који је та права и слободе утемељио и настоји да буде гарант њиховог поштовања.

Европска унија је у наредним годинама наставила да промовише значај и неопходност поштовања права на заштиту података о личности и приватности уопште, те је 2012. године Европска комисија усвојила предлог детаљнијег одређивања правних оквира у домену заштите података о личности. Овај предлог суштински би омогућио грађанима ЕУ да поднесу захтев за брисање личних података из претраживача на интернету (Regulation 2012/0011, Art. 17). Предлог Европске комисије идејно је утемељен на европској регулативи из 1995. године, познатијој под називом *Право да се буде заборављен (Right to be forgotten)* (Directive 95/46/1995).

Због критика које су упућене оваквој формулацији права на заборав, најпре због питања остваривости концепта, у ЕУ је 2018. године на снагу ступила Општа регулатива о заштити података о личности (*General Data Protection Regulative – GDPR*). Општа регулатива значајна је и због свог просторног обима, јер је њено важење препознато не само у оквиру ЕУ, већ и у оквиру Европског економског простора у који спадају и државе нечланице попут Норвешке, Исланда и Лихтенштајна. Специфичност Опште регулативе односи се на нужност поштовања одредаба, чак и за

фирме чија се седишта налазе ван граница ЕУ, а послују у ЕУ и могу да се служе обрадом података о личности грађана ЕУ (Regulation 679/2016, Art.3).

ДЕФИНИСАЊЕ И ЗНАЧАЈ У САВРЕМЕНОМ СВЕТУ

Два права која су предмет истраживања веома су сродна и нераскидиво повезана. Оба термина су уско везана за физичка лица, односно за појединце. Нераскидива повезаност ова два концепта видљива је у немогућности да се посматрају одвојено или да се изолују на начин који би омогућио засебно разматрање испуњености односних права. Поједностављено гледано, то би значило да не постоји приватност без права на заштиту података о личности, нити да постоји право на заштиту података о личности без поштовања и уважавања права на приватност. Међусобна повезаност видљива је у судској пракси ЕУ, која иако препознаје оба права засебно, не прави суштинске и значајне дистинкције између њиховог дефинисања и примене. Када се анализирају ова два права у контексту судске праксе ЕУ, примећује се да су она виђена као „два различита али повезана система која осигуравају заштиту основних људских права” (Kokott and Sobotta 2013, 222–228). Како је већ познато, порекло оба права није скоријег времена, али се њихов значај увећавао и постајао све очигледнији током индустријских, комуникацијских и технолошких промена које су измениле животе држава и појединаца у свим постојећим сферама, па и у сфери права и владавине права. Да би било могуће закључити какав је значај ових права у модерном свету, неопходно је понудити њихове дефиниције, које ће допринети бољем разумевању садржаја и суштине.

Право на приватност се у европским оквирима, а складно Европској конвенцији о људским правима, везује за право на поштовање приватног и породичног живота. У оквиру овако дефинисаног права, у члану 8. се под поштовање приватног и породичног живота убраја и приватност преписке. Даље се истиче да власти могу да наруше ова права, али само под одређеним условима и у специфичним околностима које демократска друштва обавезују да свесно кршећи права и слободе појединаца заштите националну или јавну безбедност, спрече криминалне активности и неред, заштите здравље и морал грађана, али и економску добробит државе (Европска конвенција о људским правима, чл. 8). У том

смислу, право на приватност подразумева слободу од нежељеног уплитања власти у приватну сферу појединца, или сликовитије објашњено право да се буде остављен на миру. Са друге стране, Повеља о основним правима ЕУ, издваја право на заштиту података о личности као посебно право. По дефиницији Европске комисије, подаци о личности подразумевају: „[...] сваки податак који се односи на физичко лице које се може идентификовати или које је идентификовано” (European Commission [EC] 2019).

Значај ових права посебно је актуелан и видљив у савременом, глобализованом друштву, које је повезано путем различитих средстава комуникационих технологија попут интернета више него икада у историји човечанства. Иако је таква комуникација немерљиво допринела олакшавању преношења информација, мултимедијалних садржаја и порука међу људима независно од њихове географске удаљености, интернет као и друге савремене комуникационе технологије омогућиле су брзу размену података. Тај начин размене информација са собом је, поред олакшавања међусобне комуникације, донео многоструке ризике најпре у домену поштовања фундаменталних људских права у која свакако спадају и право на приватност и право на заштиту података о личности. Ризици који се јављају везани су за могућност искоришћавања личних података које појединци свесно или несвесно остављају на мрежи, а чија злоупотреба може значајно нарушити приватност и угрозити право на заштиту личних података. Поред злоупотреба које су могуће од стране других физичких лица, још опаснија је могућност системског кршења ових права, што значајно утиче на квалитет живота грађана, поштовање њихових основних права и слобода, свеопште стање владавине права и показује карактер режима који такво системско кршење права спроводе.

АНАЛИЗА ТУРСКЕ ЛЕГИСЛАТИВЕ

Усвајањем амандмана 2010. године, Устав Републике Турске, препознао је категорију права на приватност и права на заштиту података о личности. Члан 20. Устава наведена права сврстава у групу фундаменталних људских права које је начелно загарантовано свим грађанима (Constitution of the Republic of Turkey 2019, Art. 20). У наставку, чланом 22. Устава Републике Турске, гореспоменута права надовезују се на заштиту слободне комуникације, која у

доба експанзије интернета постаје све већи изазов у контексту поштовања људских права и приватности (Art. 22). Иако је отпочет процес препознавања значаја ових права, о чему сведочи Устав Републике Турске, конкретна легислатива која би се детаљније бавила заштитом података о личности није постојала све до 2016. године, када је усвојен Закон о заштити личних података (*Kişisel Verilerin Korunması Kanunu*) – Закон бр. 6.698.

До ступања на снагу Закона о заштити личних података, основни оквир за поступање на интернету био је Закон о интернету (бр. 5.651), који је амандманима из 2014. године значајно измењен, при чему су измене допринеле погоршању стања демократије, људских права и слободе. Измене су подразумевале допуштање интернет провајдерима да чувају податке о активности корисника до две године без њиховог пристанка и знања, те да по потреби и захтеву власти те податке могу учинити доступним (Letsch 2014). Амандманске измене потпомогле су јачање цензуре на интернету, најпре давањем овлашћења Директорату за телекомуникације и комуникације (*Telekomünikasyon İletişim Başkanlığı*) да уклања садржаје са интернет сајтова и блокира приступ популарним платформама попут Јутјуба (*Youtube*) (London Privacy International 2014, 6). Због оптужби за прислушкивање, надзор корисника и неовлашћено прикупљање и дељење података о личности, под притиском јавности, 2016. године угашен је Директорат за телекомуникације и комуникације.

У сфери заштите података о личности и права на приватност грађана, неизоставно је осврнути се на Закон о изменама и допунама Закона о државним обавештајним службама и националној обавештајној организацији – Закон бр. 6.532 из 2014. године. Одредбе овог закона омогућиле су „[...] обавештајним агенцијама прикупљање приватних података, докумената или информација о појединцима, без потребе судског налога [...]” (8). На тај начин, измене и допуне које су усвојене прошириле су капацитете државних обавештајних служби у контексту доступности и коришћења података о личности, чиме су права из ове области додатно угрожена. Тенденција проширивања моћи државних органа, нарочито извршне власти и обавештајних служби наишла је на бројне критике међународних невладиних организација које се баве људским правима. Америчка међународна невладина организација Чувар људских права (*Human rights watch*) оценила је да усвојени закон приморава правна лица и организације које немају статус правног лица на обавезу да достављају податке

о личности и приватне информације о грађанима, те је на тај начин поништава све друге законе из односне области који такво прикупљање информација и података настоје да ограниче и отежају. Ступање на снагу овог закона проблематично је и због тога што нарушава и подрива слободу медија, слободу изражавања и право на приступ информацијама од јавног значаја (Human Rights Watch [HRW] 2020).

Закон о заштити података о личности ступио је на снагу 2016. године, чиме је Турска добила закон који се директно бави правом на заштиту података о личности. Овај закон први је покушај Турске да легислативу у области заштите података о личности приближи стандардима ЕУ. Новине које су унете овим законом најпре се односе на оснивање Националног тела за заштиту података, које добија статус „[...] независног и регулаторног тела које има организациону и финансијску аутономију и јавноправни статус који му омогућава извршавање законом прописаних дужности” (Kişisel Verileri Koruma Kurumu [KVKK] n.d. 2019, 5).

Од доношења закона до 2018. године, овај орган имао је девет чланова, од којих је пет чланова бирала Скупштина, док је председник Републике и Веће министара имало право на избор по два члана. До промена је дошло 2018. године, када је измењен процентуални удео различитих грана власти у избору чланства. Утицај председника Републике на састав и избор чланства значајно је повећан одлуком да уместо дотадашња два члана, председник има право на избор четири члана, док је Веће министара потпуно изгубило право на избор чланова Националног тела за заштиту података.

Такође, приликом анализе турске легислативе у датој области неопходно је споменути и Закон бр. 7.253, тачније Закон о изменама и допунама Закона о регулацији емитовања на интернету и борби против злочина почињених таквим емитовањем (*İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi*) који је ступио на снагу 2020. године (Sahin 2022, 1). Будући да је претходни закон као учеснике у саобраћају на интернету дефинисао добављаче садржаја (*content provider*), добављаче услуга хостинга (*hosting provider*) и добављаче приступа (*access provider*), Законом бр. 7.253. уведена је и категорија страних добављача друштвеног умрежавања (*foreign social network providers*). Ова категорија односи се на оне добављаче који у Турској имају више од милион дневних приступа садржајима, а чија се седишта

налазе ван Турске. Новине у погледу страних добављача друштвеног умрежавања односе се на законску обавезу именовања представника у Турској, који ће бити турски држављани или правна лица са пребивалиштем у Турској, те ће редовно подносити извештаје о раду, уклањати неподобне садржаје на захтев корисника који сматрају да је њихова приватност угрожена. Поред тога, турски закон наметнуо је обавезу страним добављачима друштвеног умрежавања да складиште податке својих турских корисника у Турској, због чега је дошло до оправданих сумњи у истинску приврженост турских власти и законодаваца праву на заштиту података о личности и праву на приватност грађана (Özer 2020).

Тенденције нарастајућег хиперпрезиденцијализма најочигледније су практично испољене уставним променама у Турској, које су додатно подстакле процес свеобухватног погоршања стања владавине права у држави, те је такав политички развој догађаја довео до замагљивања принципа поделе власти, јачања извршне власти на уштрб судске и законодавне и тиме отворио пут Ердогановој ауторитарној власти. Будући да је јасна подела власти један од најзначајнијих ослонаца владавине права и поштовања људских права, закључује се да је оваква политичко-правна ситуација подстакла власт да усвајањем измена и допуна постојећег закона о интернету утиче на видљиво смањење нивоа слободе медија и изражавања, допринесе процесу озакоњавања цензуре на интернету и омогући државно прикупљање података о личности.

ПРАКТИЧНА ПРИМЕНА УСВОЈЕНЕ ЛЕГИСЛАТИВЕ

У периоду од усвајања уставних амандмана 2010. године до 2016. године, када је на снагу ступио Закон бр. 6.698, турска јавност прошла је кроз период различитих пракси које су несумњиво допринеле ограничавању људских права, појачаном надзору и цензури, што је омогућено постојећим законским оквирима и интензивирањем президенцијализма, који је након референдума из 2017. године почео да прераста у хиперпрезиденцијализам.

Једна од познатијих афера у области заштите права на приватност и права на заштиту података о личности на интернету везује се за ТТНЕТ (*Türk Telekom Net*), највећег интернет провајдера у Турској са преко седам милиона корисника. Овај интернет провајдер 2012. године је заједно са системом Форм (*Phorm*), који се бави

прикупљањем података о корисницима на основу њиховог понашања на интернету, угрозио приватност и злоупотребио личне податке корисника, те је кажњен од стране Управе за информационе и комуникационе технологије, главног националног регулаторног и инспекцијског тела у области телекомуникација (Akgül and Kırıldoğ 2015). Исте године, догодила се афера у области просвете, када је креирани мобилни портал за ученике и студенте искоришћен за прикупљање личних података који су касније продати мобилним оператерима у маркетиншке сврхе (London Privacy International 2014, 5).

Поред тога, проблем у сфери поштовања односних права у пракси евидентан је и у ограничењима која су у Турској наметнута у погледу енкрипције, тј. процеса кодирања/ шифровања којим се подаци корисника штите од нежељених активности и читања. Због коришћења хардвера и софтвера који омогућавају енкрипцију ради заштите података и њихове приватности, у Турској је дошло до хапшења бројних новинара и активиста. Политички званичници настојали су да такве хардверске и софтверске системе доводе у везу са милитантним и терористичким групама (Freedom House 2020).

Узимајући у обзир ограничења која су садржана како у турским законима, тако и у европским конвенцијама и повељама у овој сфери, очигледно је да су турске власти имплицирајући заштиту државне безбедности и борбу против тероризма, управо та ограничења искористиле у случају новинара, доказивајући основаност њиховог задржавања и хапшења позивањем на законска ограничења, која у датим случајевима допуштају властима да штитећи државну безбедност прекрше право на приватност и заштиту података о личности. Током 2015. године забележени су случајеви хапшења новинара Вајса (*Vice*) због коришћења енкрипцијског хардвера и софтвера (Duru Aydin, 2015).

Складиштење података корисника у Турској, наметнуто је као законска обавеза великим технолошким компанијама које су присутне у држави, на начин да се путем локализације података подаци о корисницима остављају на дохват руке властима, које их могу злоупотребити у случају да се ради о појединцима које сматрају политичким противницима или новинарима и активистима који настоје да објективно извештавају о друштвеним и политичким дешавањима у држави (Rodriguez and Temel 2020). На овакав развој праксе кршења и злоупотребе предметних права утицао је у великој

мери и покушај војног пуча 2016. године, када је законским уредбама (бр. 670, 671, 680) омогућено прикупљање личних података без било каквог претходног судског налога. Надлежност у прикупљању података дата је Управи за информационе и комуникационе технологије (Ünver 2018, 94–95).

ЗАКЉУЧАК

Права на приватност и заштиту података о личности представљају веома сродна права, те иако донекле различитог садржаја, њихова суштинска повезаност и нераскидивост не допушта да се разматра о испуњености једног права без освртања на испуњеност другог. Интензификацијом процеса глобализације, међународног умрежавања, експанзије комуникационих технологија попут интернета и друштвених мрежа, односна права постала су још осетљивија и подложнија злоупотребама, те је дошло до потребе да се још прецизније унесу у националне легислативе. Трендове је у том смислу пратила и Република Турска, која је у свом легислативном оквиру настојала да обухвати и регулише права грађана у контексту њихове приватности и заштите личних података на интернету. Иако су одређени помаци направљени, политичке промене које су довеле до јачања извршне власти на уштрб законодавне и судске, отвориле су простор за све веће упливе извршне власти у права и слободе грађана, што је значило да ни ова права неће бити изузета од нових трендова. Сходно томе, не може се рећи да Турска нема легислативни оквир у овом домену, већ да до проблема настаје приликом примене закона и раскорака између одређених законских одредби и стварног поступања према грађанима и њиховим правима у пракси. Пракса показује да Турска представља пример државе која системски крши право на приватност и право на заштиту података о личности својих грађана, на шта свакако указују и оцене Европске уније, као и неких међународних невладиних организација, које у својим извештајима опомињу да је стање владавине права у овој држави на незадовољавајућем нивоу, те да постоје стална кршења наведених права, које држава користи у сврхе надзора грађана, неовлашћеног прикупљања и објављивања података, позивајући се управо на законе који у одређеним ситуацијама, под велом заштите националне безбедности, политичког поретка или економске стабилности државе, омогућавају хиперпрезидентијалистичком

и ауторитарном режиму владајуће Странке правде и развоја да се обрачунава са својим политичким неистомишљеницима и да на тај начин осигура што дужи боравак на власти, не осврћући се на степен поштовања фундаменталних људских права и слобода грађана.

РЕФЕРЕНЦЕ

- Европски суд за људска права [ЕСЈП]. 2021. *Европска конвенција о људским правима*. Стразбур: Европски суд за људска права. Последњи приступ: 12. јануар 2023. https://www.echr.coe.int/Documents/Convention_SRP.pdf.
- Европски суд за људска права [ЕСЈП]. 2021. *ЕСЈП у 50. питања*. Стразбур: Европски суд за људска права. Последњи приступ: 12. јануар 2023. https://www.echr.coe.int/Documents/50Questions_SRP.pdf
- Akgül, Mustafa, and Melih Kırılıdoğ. 2015. "Internet Censorship in Turkey." *Internet Policy Review* 4 (2): 1–22. doi:10.14763/2015.2.366.
- Aydin, Deniz Duru. 2015. "Turkey v. Encryption: An Attack on Freedom of Expression." *Accessnow*. Last accessed: 17. November 2022. <https://www.accessnow.org/turkey-v-encryption-an-attack-on-freedom-of-expression/>
- Charter (EU) No. 2007/C 303/01 of the European Parliament, European Commission and Council on fundamental rights of the European Union., OJ C 303/1, 14.12.2007.
- Council of Europe [COE], n.d. "A Convention to protect your rights and liberties". *Council of Europe*. Last accessed: 19. January 2023. <https://www.coe.int/en/web/human-rights-convention>
- Directive (EU) No. 95/46/1995 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data., OJ L 281, 23.11.1995.
- European Commission [EC]. 2012. "Proposal for a Regulation of the European Parliament and of the Council on the Protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)". *European Commission*. Last accessed: 13. December 2022. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:en:PDF>

- European Commission [EC]. 2019. “What Is Personal Data?” *European Commission*. Last accessed: 1. December 2022 https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en.
- Freedom House [FH]. 2020. “Turkey: Freedom on the Net 2020 Country Report.” *Freedom House*. Last accessed: 29. October 2022. <https://freedomhouse.org/country/turkey/freedom-net/2020>.
- Human Rights Watch [HRW]. 2020. “Turkey: Spy Agency Law Opens Door to Abuse.” *Human Rights Watch*. Last accessed: 27. December 2022. <https://www.hrw.org/news/2014/04/29/turkey-spy-agency-law-opens-door-abuse>.
- Kanun No. 7253., “Resmi Gazete”, Sayı: 31202/2020. Last accessed: 7. December 2022. <https://www.resmigazete.gov.tr/eskiler/2020/07/20200731-1.htm>.
- Kişisel Verileri Koruma Kurumu. [KVKK]. 2019. “Data protection in Turkey”. *Kişisel Verileri Koruma Kurumu*. Last accessed: 14. December 2022. <https://www.kvkk.gov.tr/Icerik/5389/Data-Protection-in-Turkey>.
- Kokott, Juliane, and Christoph Sobotta. 2013. “The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECHR.” *International Data Privacy Law* 3 (4): 222–228. doi: 10.1093/idpl/ipt017.
- Letsch, Constanze. 2014. “Turkey Pushes through New Raft of ‘Draconian’ Internet Restrictions.” *The Guardian*. Last accessed: 16. December 2022. <https://www.theguardian.com/world/2014/feb/06/turkey-internet-law-censorship-democracy-threat-opposition>.
- London Privacy International [LPI]. 2014. “Report Universal Periodic Review – Stakeholder Report 21st Session, Turkey – The Right to Privacy in Turkey.” *London Privacy International*. Last accessed: 16. December 2022. <https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=1400&file=EnglishTranslation>.
- Özer, Yusuf Mansur. 2020. “Parliament Finally Amends Internet: New Social Media Regulations and Removal of Content.” *IR Global*. Last accessed: 18. January 2023. <https://www.irglobal.com/article/parliament-finally-amends-internet-law-new-social-media-regulations-and-removal-of-content/>.

- Prosser, William L. 1960. "Privacy." *California Law Review* 48 (3): 383–423. doi: 10.2307/3478805.
- Regulation (EU) No. 679/2016 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)., OJ L 119/1, 27.04.2016, p.32–33.
- Reynolds, Osborne Jr. 1969. "Privacy and Freedom. by Alan F. Westin." *Administrative Law Review* 22 (1):101–106. doi: 10.1093/sw/13.4.114-a.
- Rodriguez, Katitza, and Hilal Temel. 2020. "Turkey Doubles down on Violations of Digital Privacy and Free Expression." *Electronic Frontier Foundation*. Last accessed: 4. December 2022. <https://www.eff.org/deeplinks/2020/11/turkey-doubles-down-violations-digital-privacy-and-free-expression>.
- Şahin, Zeynep. 2022. "Evaluation of the Law No. 7253 on Amendment of the Law on the regulation of Broadcasts Made on Internet and Combating Crimes committed through These Broadcasts in the Context of Freedom of Expression and Personal Rights." *Euroasia Journal of Social Sciences & Humanities* 9 (2): 28–44. doi: 10.38064/eurssh.332.
- The Grand National Assembly of Turkey. 2019. "Constitution of the Republic of Türkiye." *The Grand National Assembly of Turkey*. Last accessed: 10. December 2022. https://www.anayasa.gov.tr/media/7258/anayasa_eng.pdf.
- United Nations Human Rights Office of the High Commissioner [OHCHR]. n.d. "Universal Declaration of Human Rights." *United Nations Human Rights Office of the High Commissioner*. Last accessed: 7. December 2022. https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/cnr.pdf.
- Ünver, Akin. 2018. "The Logic of Secrecy: Digital Surveillance in Turkey and Russia." *Turkish Policy Quarterly* 17 (2): 93–103. Last accessed: 11. November 2022. <http://turkishpolicy.com/article/923/the-logic-of-secrecy-digital-surveillance-in-turkey-and-russia>.
- Warf, Barney. 2010. "Geographies of Global Internet Censorship." *GeoJournal* 76 (1): 1–23. doi: 10.1007/s10708-010-9393-3.
- Warren, Samuel D. and Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4 (5): 193–220. doi: 10.2307/1321160.

Danica Lazović**Institute of Social Sciences, Belgrade*

PRIVACY POLICY AND PERSONAL DATA PROTECTION ON THE INTERNET: A CASE STUDY OF TURKEY

Resume

The right to privacy and the personal data protection are two highly intertwined rights. In the era of globalization, the ever more extensive and widespread use of communication technologies, the challenge of protecting these rights from abuse in non-democratic states arises. The analysis of the legislation of the Republic of Turkey shows that Turkish state has formally regulated the area of protection of the right to privacy and protection of personal data on the Internet, while practice shows many abuses and violations. The development of the Internet and other instruments of communication has enabled the authoritarian and undemocratic regime to collect personal data, use it for the purpose of dealing with political dissidents and consequently violate the general principles of the rule of law. The political changes that followed the referendum held in 2017. meaningfully contributed to the growth of the president's power. These constitutional changes resulted in a change in the share of power in the decision-making process regarding the selection of members of the National Data Protection Authority. In this sense, the Council of Ministers was completely squeezed out of the membership selection process, and the influence of the president was doubled. Referring to the existing legislation, the state, under the guise of protecting national interests and national security, violated discussed rights. The same excuse was used for the purpose of arresting political dissidents and unfit journalists, which generally led to a large reduction of the rule of law in this country. The main results and conclusions arising from this article refer to the

* d.lazovic96@gmail.com

recognition of the trend of general reduction and violation of mentioned rights, which is connected and explained by constitutional changes and implementation of the adopted legislation.

Keywords: right to privacy, protection of personal data, Republic of Turkey, legislation, internet

* Овај рад је примљен 30. јануара 2023. године, а прихваћен за штампу на састанку Редакције 8. маја 2023. године.