# Владавина закона на интернету и у ширем дигиталном свету

Сажетак и Комесарове препоруке

**Тематски документ**

COMMISSIONER FOR HUMAN RIGHTS
COMMISSAIRE AUX DROITS DE L'HOMME
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

# Владавина закона на интернету и у ширем дигиталном свету

**Тематски документ објавио Комесар за људска права Савета Европе**

Сажетак и Комесарове препоруке

Савет Европе

Комесар за људска права објављује тематске документе са циљем да допринесе дискусији и размишљању о значајним текућим питањима људских права. Многи од њих садрже и Комесарове препоруке за решавање препознатих питања. Мишљења изражена у овим експертским документима не морају да одражавају и Комесарове ставове.

Цели текст тематског документа на енглеском језику може се добити на адреси: commissioner@coe.int; електронска верзија је доступна и на: http://www.coe.int/web/commissioner/publications

Фотографија на насловној страници: © Shutterstock

Корице и прелом: Одељење за продукцију докумената и публикација (SPDP) Савета Европе



Штампано у Савету Европе

Захвалност:

Овај тематски документ је припремио професор Дауе Корф, гостујући истраживач, Универзитет Јејл (Пројекат о информационом друштву) и ванредни професор на Факултету Оксфорд Мартин, Универзитет Оксфорд, Уједињено Краљевство. Он и Комесар захваљују Џоу МекНамију из организације Европска дигитална права (EDRi) на изузетно корисним коментарима и додацима током припреме нацрта документа, нарочито у вези с приватизованом применом закона.

# Садржај

# Сажетак

Овај тематски документ разматра битно питање: како можемо обезбедити да се на интернету и у ширем дигиталном свету успостави и одржава владавина закона? У првом делу се описује распон активности на интернету, као и претње том окружењу; други део разматра све присутније принципе "управљања интернетом", те примећује посебну контролу коју над дигиталним светом имају Сједињене Америчке Државе (као и Уједињено Краљевство у Европи), што би заузврат могло да доведе до фрагментације интернета. Трећи део представља међународне стандарде владавине закона, као и неке проблеме у примени закона на ово ново окружење. Четврти део детаљније разматра кључна питања која произилазе из претходних делова – слободу изражавања, приватизовано примењивање закона, заштиту података, сајбер криминал и националну безбедност – те говори о тананој равнотежи коју траже.

Комесар Савета Европе за људска права је, на основу питања која поставља овај документ, формулисао неколико препорука и оне су дате након овог сажетка.

## Ново окружење за људске активности

Живимо у глобалном дигиталном окружењу које је створило нове начине вођења локалних, регионалних и глобалних активности, укључујући нове врсте политичког активизма, културне размене и остваривања људских права. Те активности нису виртуелне у смислу да "нису стварне". Штавише, оне су заправо суштински део животâ стварних грађана. Ограничења у приступу интернету и дигиталним медијима, те покушаји да се наше активности, односно наша електронска комуникација прате онлајн, мешају се у наша основна права на слободу изражавања и информација, слободу удруживања, приватност и приватни живот (а можда и друга права, као што су право на исказивање вероисповести и убеђења или право на праведно суђење).

Наравно да ново глобално дигитално окружење ствара и нови простор за незаконито деловање: за ширење говора мржње или дечије порнографије, за подстицање на насиље, кршење ауторских права ("пиратерија"), превару, крађу идентитета, прање новца и нападе на саму инфраструктуру електронских комуникација, кроз злоћудни софтвер, тзв. *malware* (попут *тројанаца* и *црва*) или нападе који *онемогућавају услугу*. Сајбер криминал и сајбер безбедност су постали питања од огромног значаја.

Ове претње су све више транснационалне, те постоји генерални интернационални консензус о потреби да се одговори на сајбер криминал, сајбер безбедност и тероризам, али знатно је нижи степен сагласности о специфичностима – или чак о томе шта представља претњу.

Истичу се четири питања. Прво, државно деловање са циљем борбе против сајбер криминала, претњī сајбер безбедности и претњī националној безбедности све више се преплиће; границе између таквих активности су помућене, а институције и агенције које се њима баве све више сарађују. Друго, државе сад координирају своје активности у свим овим аспектима. Треће, рад државних агенција за националну безбедност и обавештајни рад све више зависи од праћења активности појединаца и група у дигиталном окружењу. Четврто, уместо спровођења закона *ex post facto*, сада је нагласак на обавештајном раду и превенцији, а агенције за борбу против криминала користе технике – и технологије – које су раније биле само у домену тајних служби.

## Природа дигиталног окружења

### Опасни подаци

У доба "великих података" (када се подаци о нашим активностима размењују и/или користе у обједињеном облику) и "интернета разних ствари" (када све више физичких предмета – ствари – комуницира путем интернета), постаје тешко обезбедити истинску анонимизацију: што је више података доступно, то је лакше особу идентификовати. Уз то, трагање за "великим подацима", и то на све софистицираније начине, води до стварања профила. Премда се ти профили користе за уочавање ретких појава (нпр. да се у великом сету података, као што су евиденције авио-компанија о именима путника, пронађу терористи), они су непоуздани и несвесно могу да доведу до дискриминације на основу расне припадности, пола, вероисповести или националности. Ти профили се састављају на тако сложене начине да одлуке које се на њима заснивају могу да постану суштински неоспориве: чак и они који такве одлуке примењују не схватају у потпуности разлоге на којима се заснивају.

Дигитално окружење може, самом својом природом, да уруши приватност и друга основна права, те да поткопа одговорно доношење одлука. Постоји велики потенцијал за поткопавање владавине закона – слабљењем или уништавањем права на приватност, ограничавањем слободе комуникације или слободе удруживања – као и за произвољно мешање.

### Глобално и приватно, али не на небу

С обзиром на отворену природу интернета (што је и једна од његових највећих снага), сваки излаз на мрежи може да комуницира са дословно сваким другим излазом, следећи било коју руту коју израчуна као најефикаснију, уз податке који теку разним врстама прекидача, усмеривача и каблова: физичком инфраструктуром интернета. Систем електронских комуникација је по природи транснационалан, заправо, глобалан, а његова инфраструктура је физичка и смештена на стварне локације, без обзира на сву причу о "облаку". У овом моменту је значајан део тих компоненти у Сједињеним Америчким Државама, а многе од њих су под контролом и управом приватних тела, а не владиних.

Основна инфраструктура интернета састоји се од фиброптичких каблова великог капацитета, који пролазе испод светских океана и мора, те за њих

везаних земљаних каблова и усмеривача. Најзначајнији каблови за Европу су они који иду с европског континента ка Уједињеном Краљевству, те они који испод Атлантског океана пролазе до Сједињених Држава. С обзиром на доминацију Сједињених Држава на интернету и на "облаку", ти каблови преносе велики део укупног интернетског промета и комуникационих података, укључујући скоро све податке према Европи и из ње.

## Ко има контролу?

### Управљање интернетом

Савет Европе и други су понудили битне принципе управљања интернетом, којима се наглашава потреба да се међународно јавно право и међународно право људских права подједнако примењују онлајн и офлајн, те да се и на интернету поштују владавина закона и демократија. Ти принципи признају и промовишу различите актере у управљању интернетом, те траже и од приватних и од јавних актера да у свим својим операцијама, укључујући стварање нових технологија, услуга и апликација, поштују људска права. Исто тако, позивају државе да поштују суверенитет других нација, те да се суздрже од деловања које би могло да нанесе штету појединцима или органима изван њихове територијалне надлежности.

Међутим, ти принципи су у великој мери још увек само на нивоу изјава и аспирација: још увек недостаје аранжмана за стварно управљање интернетом, који би се могли поуздано користити за обезбеђење примене тих принципа у пракси.

Исто тако, управљање интернетом мора да узме у обзир чињеницу да – делом због доминације корпорација, а делом због историјских аранжмана – Сједињене Америчке Државе (даље у тексту: САД) имају већу контролу над интернетом него било која друга држава (или чак све друге државе заједно). Уз свог блиског партнера Уједињено Краљевство (даље у тексту: УК), САД има приступ највећем делу инфраструктуре интернета.

Бивши ванјски сарадник Агенције за националну безбедност САД-а Едвард Сноуден је открио да САД и УК користе ту контролу и приступ да би вршили масовно праћење интернета, система глобалне електронске комуникације и друштвених мрежа. Страхује се да би на Сноуденово откриће државе могле да одговоре тако што ће испарчати интернет, па би државе или регије инсистирале на томе да се њихови подаци усмеравају искључиво путем локалних усмеривача и каблова, те да се похрањују у локалним *облацима*. То ствара ризик да ће се интернет какав познајемо уништити, и то стварањем националних баријера у једној глобалној мрежи. Ако Сједињене Америчке Државе не унапреде поштивање међународних стандарда људских права у својим активностима које погађају интернет и системе глобалних комуникација, кретање ка таквом испарчаном интернету биће тешко зауставити.

### Контрола приватног сектора

Велики део инфраструктуре интернета и ширег дигиталног окружења је у рукама приватних тела, од којих су многа америчке корпорације. Ово је проблематично,

јер компаније нису директно обавезане међународним правом људских права – које се директно примењује само на државе и владе – и све је теже против таквих компанија предузимати активности којима ће се нешто преиначити. Уз то, приватна тела подлежу домаћим законима земаља у којима су основане или у којима делују, а ти закони се не поклапају увек с међународним правом или међународним стандардима људских права: могуће је да активностима на интернету намећу ограничења (обично у вези са слободом изражавања) која представљају кршење међународног права људских права; могу да намећу или дозвољавају мешање, као што је праћење активности на интернету или електронских комуникација, што је супротно међународном праву људских права; такве активности могу да се примењују екстратериторијално, што представља кршење суверенитета других држава.

Примена домаћих закона на активности приватних тела која контролишу (у значајном делу) дигитални свет изузетно је сложена и осетљива. Наравно да државе имају право, али и дужност, да се боре против криминалних активности које користе интернет или системе електронских комуникација. Ту, природно, користе помоћ релеватних приватних актера. Одговорне компаније ће желети и да избегну могућност да се њихови производи и услуге користе у криминалне сврхе. У таквим околностима, државе би у својим активностима требале да у потпуности поштују и своје међународне обавезе у погледу људских права, али и да у потпуности поштују суверенитет других држава. Државе нарочито не би требале да заобилазе уставне и међународноправне обавезе тако што ће подстицати ограничења људских права кроз "добровољне" активности посредника, а компаније би требале да поштују људска права појединаца.

## Владавина закона у новом дигиталном окружењу

### Владавина закона

Владавина закона је принцип власти према којем су сва лица, институције и тела, јавна и приватна, укључујући и саму државу, одговорна по законима који су јавно усвојени, у једнакој примени на све, по којима се независно суди, и који су у складу с међународним нормама и стандардима људских права. То подразумева придржавање принципâ супремације закона, једнакости пред законом, одговорности по закону, праведности у примени закона, раздвајања власти, учешћа у доношењу одлука, правне извесности, избегавања произвољности, те процесне и правне транспарентности.

### Основни тест "владавине закона" који је развио Европски суд за људска права

Европски суд за људска права је, кроз своју судску праксу, развио детаљне тестове "владавине закона", а усвојила су их и друга међународна тела за заштиту људских права. Да би се прошли тестови, сва ограничења основних права морају да се заснивају на јасним, прецизним, доступним и предвидивим законским правилима и да буду у сврху остварења видљиво легитимних циљева; морају да буду "неопходна" и "пропорционална" релевантном легитимном циљу (уз одређени

"степен слободне процене"), те мора да постоји "ефикасан [по могућности судски] лек" за наводна кршења ових захтева.

## "Свако", без дискриминације

Један од заштитних знакова међународног права људских права још од 1945. године и један од његових највећих успеха је да се људска права морају обезбедити "свакоме", свим људским бићима: то нису само права грађанина, то су права човека.

Сходно томе, уз веома ограничене изузетке, сви закони, свих држава, који се тичу људских права или се у њих мешају, морају се примењивати на "свакога", без дискриминације "било које врсте", укључујући дискриминацију по основу места боравишта или држављанства.

Пошто САД и америчке компаније имају тако јединствено место у функционисању интернета, уставни и корпоративно-законски оквир у САД-у је посебно значајан. Међутим, за разлику од горе поменутог принципа међународног права људских права, многа јемства људских права у Уставу САД-а и у различитим америчким законима која уређују дигитално окружење се односе само на америчке држављане и лица која нису држављани, али су тамо стално настањена ("америчка лица"). Само "америчка лица" уживају корист од Првог амандмана на Устав, који третира слободу говора и слободу удруживања, и од Четвртог амандмана, који америчке држављане штити од "неразумних претреса", те од већине (ограничене) заштите од претераног надзора предвиђеног кључним прописима о националној безбедности и обавештајном раду (тзв. Измена Закона о страном обавештајном надзору, енгл. FISA Amendment, те Закон о патриотском деловању, енгл. The Patriot Act).

## "Под јурисдикцијом[и на територији] [државе уговорнице]"

### Дужност државе да поштује своје обавезе према међународном праву људских права и када делује екстратериторијално

Основни међународни уговори о људским правима, укључујући и Међународни пакт о грађанским и политичким правима (ICCPR) и Европску конвенцију о људским правима (ECHR), обавезују државе да "обезбеде" и "пруже" људска права одређена тим уговорима, "свакоме под својом јурисдикцијом" (или "у оквирима своје јурисдикције"). Такав захтев све више има функционално, а не територијално значење – како су недавно потврдили Комитет за људска права и Европски суд за људска права. Другим речима, свака држава мора да обезбеди или пружи та права свакоме ко је под њеном физичком контролом или на чија права делују њене радње (или радње њених агенција).

Сходно томе, државе морају да поштују своје међународне обавезе у односу на људска права, и то у свим радњама које предузимају, а које могу да делују на људска права појединаца – чак и кад поступају екстратериторијално или кад предузимају радње које могу да имају екстратериторијално деловање.

Оваква обавеза посебне последице има за податке – од којих се и састоји дигитални свет – и то нарочито за личне податке, како то потврђује европско право о заштити података, које штити све појединце чије податке обрађују европски контролори, без обзира на место становања, држављанство или други статус. Међутим, Сједињене Америчке Државе формално одбијају овакву примену међународног права људских права. У светлу доминације САД-а (и америчких корпорација, које подлежу јурисдикцији те земље) у дигиталном окружењу, то представља опасну претњу владавини права у овом новом окружењу.

### Тешкоће с конкурентним и сукобљеним прописима који се истовремено примењују на активности онлајн, с посебним освртом на слободу изражавања

Проблем конкурентне – и сукобљене – примене различитих домаћих прописа на материјале на интернету и интернетске активности је питање које се мора хитно разматрати како би се јамчила владавина закона на интернету.

Овде питање није право влада да предузимају радње којима ће поштивати међународно право и које су неопходне и пропорционалне у демократском друштву. Владе би свакако требале да задрже слободу да доносе одлуке о прописима у својој јурисдикцији. Питање је способности и права влада и судова у земљи да предузимају мере које за последицу имају наметање ограничења трећим земљама, где дати појединци делују у складу са законима своје земље држављанства или боравишта, а који би, за разлику од страних закона, њима требали да буду познати (или уз могућност да за њих знају) и предвидиви у примени.

У принципу, појединци и компаније који из своје земље боравишта или регистрације чине информације доступним требали би да поштују само законе те земље; од појединаца који приступају материјалима или их преузимају са страних веб-страница, кад знају и требају да знају да су такви материјали у њиховим земљама боравишта незаконити, могло би се очекивати да поштују законе своје земље. Државе би јурисдикцију над страним материјалима који нису противзаконити по међународном праву требале да примењују у ограниченим околностима, тј. када постоји јасна и блиска веза између тих материјала и њихове дистрибуције и државе која предузима дату радњу. Ако је веза државе мање јасна, она би ипак требала да има право да поступа, али генерално би требала да предузима радње на самој локацији кршења или близу ње.

## Људска права и приватна лица

### Право људских права и тзв. Руџијеви принципи, смернице Савета Европе и других

Међународно право људских права се, у суштини, примењује само на државе и на радње (или пропусте) јавних власти. Појављују се, пак, нови међународни стандарди, којима је циљ да их примењују и компаније. Најзначајнији су *Основни принципи УН-а у вези с пословним активностима и људским правима* (тзв. Руџијеви принципи), које је израдио Специјални представник Генералног секретара Уједињених нација за пословне активности и људска права професор Џон Руџи.

Међутим, Руђијеви принципи су још увек усмерени на дужност држава домаћина да поступају против кршења људских права чији су починиоци компаније. Они се не баве детаљно обратним ситуацијама – када државе компанијама постављају захтеве који би те компаније довели у ситуацију да крше међународно право људских права.

Чини се битним да и Савет Европе и други наставе да стварају даљње смернице о одговорности пословних организација које се суочавају са (или се стављају у ситуацију где би се могле суочити са) захтевима влада или других приватних лица, којима се подржавају мере које би могле да представљају кршење међународног права људских права (како се даље разрађује у делу о приватизованој борби против криминала).

### Филтрирање и блокирање које врше интернетске и компаније за електронске комуникације по упутству – или на основу "подстицаја" – држава

Уз инкриминацију материјала на интернету – што се све чешће дешава када су материјали произведени у другој земљи, и то, *ex post facto*, након што се материјали објаве и приступи им се – државе све више покушавају да спрече (блокирају) приступ одређеним материјалима и информацијама доступним онлајн. Такво блокирање и филтрирање се обавља софтвером и хардвером који ревидира комуникације и на основу унапред одређених критеријума одлучује о томе да ли ће спречити прослеђивање материјала примаоцу којем је упућен, често некоме ко само претражује интернет.

Можда не изненађује то што репресивне државе покушавају да блокирају приступ опозиционим веб-страницама, те што теократски режими исто чине с веб-страницама које сматрају богохулним. С друге стране, и државе које наводно поштују владавину закона – укључујући и државе чланице Савета Европе – покушавају да блокирају приступ материјалима које сматрају неприхватљивим. Или, у границама прикривенијег и мање одговорног оквира, једноставно "подстичу" чуваре интернета (пружаоце услуга приступа интернету и пружаоце услуга мобилне телефоније) да то раде "добровољно", изван јасног и јавног законског оквира.

У демократским земљама су блокирање и филтрирање обично, барем званично и иницијално, углавном усмерени на строго легитимне циљеве: расистички или верски "говор мржње" или дечију порнографију. Међутим, такви системи пате од великих недостатака у погледу начина на који делују:

- неминовно је да блокирање може да произведе (ненамерне) лажно позитивне резултате (блокирање страница без икаквог забрањеног материјала) и лажно негативне резултате (кад странице са забрањеним материјалима исклизну мимо филтера);
- критеријуми за блокирање одређених страница, а не неких других, и листе блокираних страница су често, у најмању руку, нетранспарентни, а у најгорем случају тајни;

- процеси за подношење жалби могу да буду тешки, мало познати или непостојећи, нарочито ако се одлуке о томе шта се блокира а шта не – намерно – остављају приватним телима;
- мере за блокирање је лако заобићи, чак и људима који немају неке посебне техничке вештине;
- посебно је важно, нарочито у вези с дечијом порнографијом, то што блокирање ни на који начин не третира стварни проблем – злостављање те деце.

Горе наведене проблеме појачава чињеница да државе, када уведу блокирање за најтежа питања, као што су дечија порнографија и говор мржње, обично то прошире и на разне друге ствари које не одобравају. Глобално говорећи, укључујући и Европу, било је покушаја држава да се блокирају не само странице које садрже говор мржње и заговарање тероризма, већ и, на пример, политичку дискусију или информације о сексуалним и мањинским правима.

Корисно је направити разлику између две ситуације: блокирања садржаја које јесте и које није засновано на закону. Неупитно је да постоји одређени садржај који представља легитиман циљ мера блокирања (законито блокирање нелегалног садржаја). Међутим, циљ мере блокирања и стварна техничка средства којима се она извршава и даље су кључна ствар у одређењу да ли је мера пропорционална и, сходно томе, законита – на пример, ако нема никаквих доказа о значајном нивоу случајног приступа датом садржају, те ако је намерни приступ једноставан и након мере блокирања, пропорционалност блокирања је далеко упитнија.

Ствар постаје сложенија ако се одлука о томе које странице блокирати препушта приватним телима, које држава "подстиче", али тврди да за блокирање не сноси одговорност (блокирање садржаја које није засновано на закону). Неке земље, укључујући Уједињено Краљевство и Шведску, увеле су системе блокирања на основу добровољних аранжмана с пружаоцима услуга приступа интернету. Сва питања везана за ефикасност и пропорционалност мера остају релевантна и за ову врсту блокирања, али се поставља генералније и фундаменталније питање на које треба одговорити: колико су такве мере блокирања заиста добровољне и/или да ли подразумевају одговорност државе? Чињеница да се члан 10 Европске конвенције о људским правима односи само на мешање у права које врше "јавне власти" не значи да држава може тек тако да се ослободи одговорности за мере које предузимају приватна тела, а имају такав ефекат – нарочито не ако држава *de facto* снажно подстиче такве мере. У таквим околностима, држава јесте одговорна што за такав систем није успоставила законодавни основ: без таквог основа, ограничења нису заснована на "закону".

У својој новијој судској пракси, Европски суд за људска права јасно примећује опасност неселективног блокирања. Суд је, у својој пресуди у предмету *Јилдирим против Турске*, приметио да је дата мера – блокирање приступа свим веб-страницама којима хостинг у Турској даје платформа Google Sites да би се блокирала једна Гуглова страница за коју се сматрало да је увредљива према Кемалу Ататурку – произвела произвољне ефекте, те се не може сматрати да је усмерена само на блокирање приступа датој проблематичној страници,

јер се састојала од свеукупног блокирања страница којима хостинг пружа платформа Google Sites. Уз то, процедура судске ревизије у вези с блокирањем интернетских страница сматрала се недовољном да задовољи критеријум избегавања злоупотребе, јер домаћи закон није предвиђао никакво јемство заштите, којим би се обезбедило да налог за блокирање одређене странице не буде употребљен као средство блокирања приступа генерално. Суд је, сходно томе, утврдио кршење члана 10 Европске конвенције о људским правима.

### Неселективна дубинска инспекција пакета *(DPI)* компанија на основу судског налога издатог на захтев других компанија, у сврху остварења ауторских права

Носиоци права интелектуалне својине све више траже да се филтери и блокаде, слични горе описанима, намећу страницама које наводно омогућавају размену пиратског садржаја, те се све више тражи приступ подацима о корисницима интернета у вези с таквим наводним размена, укључујући и то да пружаоци услуга приступа интернету аутоматски користе дубинску инспекцију пакета како би открили вероватне (или могуће) кршиоце права.

Дубинска инспекција пакета (енгл. DPI) тражи да "инспектор" испита не само шире метаподатке везане за порекло или одредиште "пакета", већ и садржај целе комуникације. Сами "пакети" се одређују на основу шеме или алгоритма везаног за одређени садржај. За носиоце права интелектуалне својине то су одређени маркери одређеног видео-материјала или фотографије на којима постоји заштита ауторских права. Међутим, иста технологија омогућава претраживање дословно било чега: одређеног политичког говора, одређене револуционарне песме, заставе синдикалне организације. Такве мере су изузетно агресивне, јер траже праћење свих корисника неког пружаоца услуге приступа интернету (или мреже мобилне телефоније) са циљем покушаја да се идентификује неколицина њих који можда (или вероватно) крше ауторска права, чиме се постављају озбиљна питања неопходности и пропорционалности.

И Европски суд за људска права и Суд правде Европске уније су донели значајне пресуде којима се јасно сугерише да неселективно филтрирање свих комуникација преко једног пружаоца услуге приступа интернету (или мобилне мреже) – тј. генерални мониторинг или праћење – у сврху идентификације могућих кршилаца права међу масом недужних корисника јесте супротно праву људских права.

## Државе у остваривању екстратериторијалне јурисдикције

Држава која користи своја законодавна овлашћења и овлашћења у борби против криминала да би ухватила или на други начин остваривала контролу над подацима који се физички не чувају на њеној, већ на територији друге државе – обично путем физичке инфраструктуре интернета и глобалних система комуникације – да би се ти подаци преузели са сервера у некој другој држави, или тако што тражи од приватних тела да остваре приступ тим подацима у иностранству да би их преузели са сервера или уређаја у другој земљи и предали држави – представља остваривање њене јурисдикције екстратериторијално, у оквирима јурисдикције друге државе.

Према општим правилима међународног јавног права, у одсуству међународних уговора који дају овлашћење страним агенцијама за екстериторијално остваривање јурисдикције, није законито да прва држава то ради без сагласности друге државе.

## Питања и равнотежа између њих

### Питања

Успостављање владавине закона на интернету и у ширем дигиталном свету ће тражити појашњење правила која се тичу слободе изражавања, приватних тела (нарочито корпорација) и људских права, заштите података и сајбер криминала; након тога ће се морати одговорити на питање: како ће се у том новом окружењу успоставити равнотежа у свему овоме?

### Слобода изражавања

Домаћи прописи везани за активности на интернету и у ширем дигиталном окружењу, нарочито закони везани за слободу изражавања, често су конкурентни и сукобљени: по законима многих држава, лица која дају изјаве онлајн или путем електронских комуникација у једној земљи или из једне земље могу се сматрати одговорнима за то по законима друге земље, у случају да такве изјаве крше законе те друге земље, чак и ако су законите тамо где су настале. Ово представља фундаменталну претњу владавини закона на интернету и у том окружењу. Овим питањем се судска пракса Европског суда за људска права још није детаљно бавила.

Као што је раније сугерисано, једини начин да се ово реши би био када би државе и домаћи судови показали јасну суздржаност тиме што не би наметали своје домаће законске стандарде на изражавање и информације које се путем интернета дистрибуирају из иностранства, осим када су незаконите по међународном праву или представљају јасне везе које оправдавају остваривање јурисдикције државе.

Друго битно питање је питање законске одговорности појединаца или компанија које управљају веб-страницама или, чак, одговорности пружаоца услуга приступа интернету за садржај који се поставља на неку веб-страницу. И у овоме је досада судска пракса на европском нивоу ограничена. У овом моменту се чини да су приватне компаније ухваћене између јасних обавеза (уклонити садржај или се суочити с казном) и нејасних обавеза (корисницима јамчити приступ законитом садржају). Резултат тога је да се приватне компаније могу определити за претерано поштивање, те свим корисницима онемогућити приступ савршено законитом материјалу, а истовремено себе штитити од могућих захтева погођених корисника тако што ће им наметати непрецизне услове коришћења. То су суштинска питања која треба решити.

### Приватизована примена закона

Чињеница да су интернет и глобално дигитално окружење у великој мери под контролом приватних тела (нарочито али не и искључиво америчких корпорација) такође представља претњу владавини закона. Таква приватна

тела могу да наметну (или да буду "подстакнута" да намећу) ограничења на приступ информацијама, а да не подлежу уставним или међународноправним захтевима који се примењују на државна ограничавања права на слободу изражавања. Таква приватна тела могу, исто тако, да добију налог од домаћег суда, који поступа по захтеву другог приватног тела, да врше изузетно агресивне анализе својих података да би открили вероватна (или само могућа) кршења права на приватну имовину, често права на интелектуалну својину. Може им се наложити да "повуку" податке, укључујући владине, комерцијалне и личне, са сервера из других земаља, из разлога борбе против криминала или националне безбедности, без прибављања сагласности те друге земље – или сагласности компанија или носилаца података у тој другој земљи – што представља кршење суверенитета те друге земље, комерцијалне поверљивости на коју компаније имају право, те људских права носилаца података.

Премда указују на значај третирања ових питања, УН-ови Руџијеви принципи на њих не дају одговоре. Како је раније речено, потребни су нови приступи и нове смернице. Савет Европе је тој дискусији дао значајан допринос, сугеришући да би државе требале да буду одговорне за ситуације када не обезбеде да приватна тела не крше људска права њихових грађана, те да државе имају обавезу да обезбеде да се генерални услови приватних компанија који нису у складу с међународним стандардима људских права морају сматрати неважећим.

## Заштита података

Европско право заштите података заснива се на сету основних принципа (праведна обрада, навођење сврхе и ограничење сврхе, минимализација података, квалитет података и сигурност података) и сету права (права носилаца података) и лекова (надзор независних власти за заштиту података), што представља посебан одраз генералних принципа "владавине закона" које је развио Европски суд за људска права. Конвенција Савета Европе о заштити података (Конвенција бр. 108) и прописи Европске уније у овој области наводе како да се одржава поштивање општих захтева права људских права у веома специфичном контексту обраде личних података. Европски модел заштите података се све више преузима и изван подручја Савета Европе: Конвенција бр. 108 (моментално у процесу модернизације) постаје глобални златни стандард у јемству међународне владавине закона у овом специфичном пољу, што је од кључног значаја за интернет и шири дигитални свет.

Европска заштита података додатно је оснажена једном пресудом Суда правде Европске уније, која одбацује обавезно, неусмерено и на сумњи незасновано задржавање података. У вези с дебатом о начину рада обавештајних и безбедносних служби, покренутој након открића Едварда Сноудена, све јасније постаје то да тајни, обимни и неселективни програми праћења и надзора нису у складу с европским правом људских права, те да се не могу оправдати борбом против тероризма или другом значајном претњом националној безбедности. Такво мешање може се прихватити само ако је строго неопходно и пропорционално легитимном циљу.

Европско схватање заштите података представља најзначајнији камен темељац владавине закона на интернету и у ширем дигиталном свету. Резултат тога је да ће бити од пресудног значаја да се обезбеди да ревизија (модернизација) Конвенције бр. 108, која је моментално у току, не води до било каквог снижавања стандарда. Нарочито би било корисно да Конвенцији бр. 108 приступе Сједињене Америчке Државе, и то не само за америчке држављане, већ као корак у смеру свеобухватнијег глобалног приступа поштивању основног људског права на заштиту података и других с тим повезаних права.

## Сајбер криминал

Конвенција о сајбер криминалу тражи од држава потписница да одређене поступке – као што су нелегални приступ компјутерским системима (хакирање), нелегално пресретање електронских комуникација, слање злоћудног софтвера (*malware*), кршење ауторских права и производња и дистрибуција дечије порнографије – домаћим законима прогласи кривичним делима; Додатни протокол уз Конвенцију тражи од држава чланица инкриминацију ширења расистичког и ксенофобичног материјала (говор мржње). Исто тако, она детаљно предвиђа међународну сарадњу у борби против таквог облика криминала, укључујући узајамну правну помоћ у истрагама и чувању доказа, изручењу и сличним стварима. Конвенција је отворена за потпис и за неевропске државе, те ју је ратификовало њих пет, укључујући САД.

Премда је ван сваке сумње евидентна потреба за постојањем сагласности у борби против криминала у глобалном дигиталном окружењу – а Савет Европе заслужује похвалу за покретање таквог процеса – сама Конвенција још није у потпуности у стању да у начину на који је државе потписнице примењују обезбеди поштивање владавине закона.

Један од разлога за то је чињеница да Конвенција не садржи свеобухватну одредбу о људским правима, те тако не предвиђа заштиту од могућности да држава непримерено широко дефинише кривична дела или да у своје материјалне законе не укључи изузетке или могућност одбране (као што су одбрана на основу јавног интереса за тзв. звиждаче, енгл. *whistleblowers*), нити штити од могућности двоструке инкриминације или пружања (формалне или неформалне) помоћи државама потписницама у ситуацијама кад би то могло да представља кршење људских права.

Други разлог је то што Конвенција није повезана с другим кључним инструментима насталим у оквиру Савета Европе који подржавају владавину закона у дигиталном и/или транснационалном контексту. Таква веза чини се све неопходнијом, јер је Конвенција отворена и за државе које нису потписнице Европске конвенције о људским правима или нису у потпуности прихватиле упоредиве захтеве Међународног пакта о грађанским и политичким правима (као, на пример, Сједињене Америчке Државе, у погледу својих екстратериторијалних активности или права "неамеричких лица"). Из угла владавине закона у Европи, приступ Конвенцији о сајбер криминалу би требао тражити и то да државе прихвате обавезе из Европске конвенције о људским правима и/или Међународног пакта о грађанским и политичким правима и ратификацију Конвенције о заштити

података, Европске конвенције о екстрадицији, те Европске конвенције о узајамној помоћи у кривичним стварима.

На крају, могло би се рећи да чланови 26 и 32 Конвенције подржавају тенденцију агенција за борбу против криминала да прибегавају "неформалним" облицима прикупљања података, чак и преко граница, без успостављања јасних јемстава заштите (на пример, да се такве неформалне мере неће користити за агресивне активности прикупљања података које би, у једној држави у којој постоји владавина закона, тражиле судски налог); исто тако се може рећи да та два члана подржавају тенденцију тих власти да све више податке "повлаче" директно са сервера у другим земљама или да траже да компаније које су под њиховом јурисдикцијом – нарочито водећи интернетски дивови – то раде за њих, без коришћења формалних, међудржавних аранжмана за узајамну правну помоћ, што представља, могло би се тврдити, кршење суверенитета државе у којој се такви подаци пронађу.

Овај принцип – установљен чланом 16 Конвенције бр. 108 у погледу узајамне помоћи власти које се баве заштитом података – да постоје јасна ограничења околности под којима се лични подаци могу прикупљати и/или прослеђивати у транснационалним активностима, такође би требао бити боље одражен у Конвенцији о сајбер криминалу. Одређени број препорука и изјава Комитета министара Савета Европе нуди корисне смернице о томе како се успоставља равнотежа између поштивања принципа заштите података и омогућавања примерене борбе против криминала. Потребно је ојачати поштивање тих инструмената у државама чланицама које су потписнице Конвенције о сајбер криминалу.

Израда предложеног новог Додатног протокола уз Конвенцију о сајбер криминалу представља прилику да се реше барем нека од ових питања. Уз те елементе побољшања, Конвенција о сајбер криминалу могла би да представља други камен темељац владавине закона на интеренту и у ширем дигиталном свету.

## Национална безбедност

И Европска конвенција о људским правима и Конвенција Савета Европе о заштити података се, у принципу, примењују на све активности држава које су им потписнице: премда обе садрже одређена специјална правила и изузетке, питања националне безбедности нису експлицитно искључена. У том смислу се мандат Савета Европе и опсег тих инструмената разликују од права Европске уније, које из надлежности и јурисдикције Уније експлицитно искључује националну безбедност. То значи да, када се ради о међународноправном уређењу активности везаних за националну безбедност и обавештајне агенције, Савет Европе мора да преузме водећу улогу, ако не глобално, онда барем у Европи.

Потреба да се обезбеди владавина закона у вези с активностима агенција за националну безбедност и обавештајних агенција постаје очигледнија у светлу открића Едварда Сноудена у вези с глобалним операцијама надзора и праћења, нарочито онима које врше Агенција за националну безбедност (NSA) Сједињених Америчких Држава, Центар за комуникације Владе (GCHQ) Уједињеног Краљевства, те њихови партнери у групи 5EYES (Аустралија, Канада

и Нови Зеланд). Та открића показују да се ове агенције редовно прикључују на фиброоптичке каблове великог капацитета, који представљају "кичму" интернета, те да пресрећу мобилне и друге комуникације у целом свету, у великом обиму, на пример тако што пресрећу радијске комуникације, користећи "стражња врата" која су инсталирали на велике комуникационе системе, те користећи безбедносне слабости таквих система.

У европском и међународном праву људских права, национална безбедност није карта која поништава све друге елементе. Заправо је са́мо питање шта се легитимно може сматрати покривеним концептом "националне безбедности" нешто што би требало судски разматрати: требало би бити на судовима да, у светлу међународног права људских права, одређују шта јесте – и шта није – легитимно обухваћено тим термином. Корисно усмерење долази и из *Јоханесбуршких принципа о националној безбедности, слободи изражавања и приступу информацијама*, које је израдила невладина организација Артицле 19 и које су подржали различити међународни форуми, укључујући и Специјалног известиоца УН-а за слободу мишљења и изражавања. Ти принципи јасно кажу да државе могу да се позову на националну безбедност као разлог за мешање у људска права само у вези с питањима која прете самом ткиву и основним институцијама нације. Понекад тероризам може да достигне тај ниво, али у већини случајева се ради о појави коју би требало третирати путем борбе против криминала, а не кроз парадигму националне безбедности. То важи и за поступке држава који се тичу интернета и електронских комуникација.

Недостају јасна уговорна правила која би усмеравала деловање агенција за националну безбедност и обавештајних агенција, као и основ на којем делују и размењују податке. У многим земљама постоји мало јасних, објављених закона који уређују рад тих агенција. У некима уопште нема објављених правила. Све док не буду позната правила по којима такве агенције и службе раде – на домаћем нивоу, естратериторијално или у сарадњи једних с другима – не може се рећи да су њихове активности у складу с владавином закона. Још једно веома битно питање је очигледна неефикасност бројних надзорних система.

Другим речима, када је у питању национална безбедност, још увек не постоји никакав прави камен темељац на који би се наслонила владавина закона – премда постоје барем основни принципи који би могли да представљају основ за такав суштински део склопа универзалних људских права.

С обзиром на све већа партнерства агенција за борбу против криминала, обавештајних и безбедносних агенција, овакво негирање владавине закона прети да се с њих прошири на полицију и тужилаштва. Одсуство јасног правног оквира у том смислу, и на домаћем и на међународном нивоу, представља додатну претњу владавини закона на интернету и у глобалном дигиталном окружењу.

# Препоруке Комесара

Узимајући у обзир налазе и закључке овог тематског документа, Комесар даје следеће препоруке, са циљем унапређења поштивања владавине закона на интернету и у ширем дигиталном окружењу.

## I. О универзалној природи људских права и о њиховој једнакој примени и онлајн и офлајн

1. Основни захтеви владавине закона важе, а требало би обезбедити да се у пракси примењују подједнако и онлајн и офлајн. То нарочито значи:

- да се Европска конвенција о људским правима и сва правила Савета Европе о заштити података примењују на све активности обраде личних података, свих агенција, у свим државама чланицама Савета Европе, укључујући и њихове агенције за националну безбедност и обавештајни рад;
- да се обавезе везане за владавину закона, укључујући обавезе које произилазе из чланова 8 (право на поштивање приватног и породичног живота) и 10 (слобода изражавања) Европске конвенције о људским правима не могу заобићи путем *ad hoc* аранжмана с приватним актерима који контролишу интернет и шире дигитално окружење; и
- да државе чланице Савета Европе требају настојати да обезбеде да неевропске државе на сличан начин поштују своје међународне обавезе према људским правима у свему што раде, а што погађа појединце који користе интернет или су на други начин активни у ширем дигиталном окружењу;
- да ниједна држава (нити било која њена агенција, укључујући агенције за борбу против криминала, националну безбедност и обавештајни рад), било европска или не, не приступа подацима похрањеним у другој земљи – или који пролазе кроз интернетске или комуникационе "кичмене" каблове који иду између тих земаља – без јасне, експлицитне сагласности друге земље или земаља којих се то тиче. Прибављање сагласности носилаца података (било индиректно, кроз услове коришћења за пружаоце услуга комуникација, или директно, у околностима које не морају да буду очигледно слободне, уз добра обавештења или довољно прецизне) или сарадња приватних тела установљена у првој држави (или циљној држави/државама) није замена за сагласност те циљне државе.

## II. О заштити података

2. Државе чланице које то још нису урадиле би требале да ратификују Конвенцију Савета Европе о заштити појединаца у погледу аутоматске обраде личних података (Конвенција бр. 108). Та Конвенција је отворена и за потпис држава које нису чланице и, ако се прихвати на ширем нивоу, може да постане најзначајнији камен темељац владавине закона на интернету и у ширем дигиталном окружењу.

3. Државе чланице које су већ ратификовале Конвенцију би требале да обезбеде да се она у потпуности спроводи на домаћем нивоу.

4. Ревизија Конвенције бр. 108, која је моментално у току, не би требала да доведе до било каквог смањења европских или глобалних стандарда заштите података. Штавише, требала би да води ка објашњењу и бољем спровођењу правила, нарочито у вези с интернетом и ширим дигиталним светом, те у вези с надзором и праћењем у сврху националне безбедности и обавештајног рада.

5. У контексту текуће реформе правила Европске уније за заштиту података, постојећа правила која би могла да поткопају владавину закона, као што су правила везана за сагласност, профилирање или приступ страних агенција за борбу против криминала личним подацима, требала би да буду појашњена и усклађена с међународним обавезама према људским правима, укључујући оне које произилазе из Конвенције бр. 108 и релевантних препорука и смерница Савета Европе.

6. Масовно, на сумњи незасновано задржавање комуникационих података је фундаментално супротно владавини закона, некомпатибилно с основним принципима заштите података, те неефикасно. Државе чланице не би требале да му прибегавају, нити да намећу обавезно задржавање података код трећих лица.

## III. О сајбер криминалу

7. Државе потписнице Конвенције Савета Европе о сајбер криминалу морају у потпуности да поштују своје међународне обавезе према људским правима у свему што раде (или не раде) по Конвенцији, било да се ради о дефинисању релевантних кривичних дела (или њихових елемената, изузетака или за њих везане одбране), у свакој кривичној истрази или кривичном гоњењу, или у вези с узајамном правном помоћи или екстрадицијом.

8. Ако било која држава потписница предузме радње које погађају појединце ван њене територије, то такву државу потписницу не изузима из обавеза по Конвенцији о сајбер криминалу или по међународним уговорима о људским правима (нарочито по Европској конвенцији о људским правима и Међународном пакту о грађанским и политичким слободама); штавише, те обавезе се подједнако примењују и на екстратериторијално поступање.

9. Све државе потписнице Конвенције о сајбер криминалу би требале и да ратификују и да ригорозно примењују Конвенцију о заштити података, Европску конвенцију о екстрадицији и Европску конвенцију о узајамној помоћи у кривичним стварима.

10. Државе чланице, укључујући њихове агенције за спровођење закона, требале би да примењују Препоруку бр. P (1987) 15 Комитета министара Савета Европе, којом се уређује коришћење личних података у сектору полицијског рада, те Препоруку Рец(2010)13 о заштити појединаца у погледу аутоматске обраде личних података у контексту профилирања, те Декларацију из 2013. о ризицима по основна права који произилазе из дигиталног праћења и других технологија за вршење надзора.

11. Државе чланице би требале да обезбеде да њихове агенције за спровођење закона не прибављају податке са сервера и из инфраструктуре у другим земљама путем неформалних аранжмана. Уместо тога, требале би да користе аранжмане за узајамну помоћ, као и посебне аранжмане за убрзано спасавање података, које је успоставила Конвенција о сајбер криминалу. Агенције за борбу против криминала у једној земљи не могу се ослањати на чињеницу да су приватна тела – као што су пружаоци услуга приступа интернету, друштвене мреже или оператери мрежа мобилне телефоније – у другим земљама прибавила овлашћења да, у складу са својим општим условима коришћења, предочавају податке својих клијената, те је њихово преузимање таквих података у тим околностима супротно владавини закона и до њега не треба да долази.

## IV. О јурисдикцији

12. Ограничења у екстратериторијалном остваривању националне јурисдикције у вези с транснационалним сајбер криминалом би требала да постоје. Та ограничења би требала да узму у обзир ефекте суштинских ограничења на сама кривична дела, као и ефекте изузетака или елемената одбране, у матичној земљи појединца (или земљи где је дело извршено) у вези с јурисдикцијом на коју се позивају друге државе које не признају таква ограничења, изузетке или одбрану.

13. Нарочито у вези с правом на слободу изражавања, појединци и компаније које чине информације доступне из својих земаља боравишта или седишта би, у принципу, требале да поштују само законе те земље, док би се од појединаца који приступају материјалима или их преузимају са страних веб-страница (када би могли и требали да знају да су ти материјали илегални у њиховој земљи боравишта) требало очекивати да поштују законе те друге земље. Независно од садржаја који је нелегалан по међународном праву, државе би своју јурисдикцију над страним дигиталним материјалима требале да остварују у ограниченим околностима, конкретно када постоји јасна и блиска веза између тих материјала и/или оних који их дистрибуирају и дате земље.

## V. О људским правима и приватним телима

14. Државе чланице би се требале престати ослањати на приватне компаније које контролишу интернет и шире дигитално окружење у погледу наметања ограничења која представљају кршење обавеза те државе према људским правима. У том смислу су потребне боље смернице о околностима под којима радње или пропусти приватних компанија који представљају кршење људских

права укључују и одговорност државе. То укључује усмерење у погледу нивоа учешћа државе у кршењу које је неопходно да би се активирала таква одговорност, те у погледу обавеза државе да обезбеди да општи услови коришћења приватних компанија не одступају од људских права. Такође је потребно испитати државну одговорност у погледу мера које приватна лица спроводе из пословних разлога, без директног учешћа државе.

15. Надовезујући се на Основне принципе Уједињених нација у вези с пословним активностима и људским правима (Руђијеви принципи), потребно је градити даљње смернице у погледу одговорности фирми у вези с њиховим активностима на интернету или у ширем дигиталном окружењу (или које их се тичу), нарочито у погледу покривања ситуација у којима се фирме могу суочити или се довести у ситуацију у којој се могу суочити са захтевима влада који би могли да представљају кршење међународног права људских права.

## VI. О блокирању и филтрирању

16. Државе чланице би требале да обезбеде да сва ограничења приступа интернетском садржају која погађају кориснике под њиховом јурисдикцијом буду заснована на строгом и предвидивом законском оквиру који уређује опсег сваког таквог ограничења, те који даје јемство судског надзора (или ревизије *ex post* у истински и евидентно хитним случајевима), у сврху спречавања могућих злоупотреба. Уз то, домаћи судови морају да испитају да ли је свака мера блокирања неопходна, ефикасна и пропорционална, а нарочито да ли је довољно прецизно усмерена, тако да погађа само конкретан садржај који треба да се блокира.

17. Државе чланице нити би требале да подстичу, нити да се ослањају на актере из приватног сектора који контролишу интернет и шире дигитално окружење, да би остварили бокирање ван оквира који задовољава горе описане критеријуме.

## VII. О активностима везаним за националну безбедност

18. Европска конвенција о људским правима и Конвенција бр. 108 морају да се примене на све активности држава које су потписнице тих конвенција, укључујући и активности државе везане за националну безбедност и обавештајни рад.

19. Конкретно, да би се остварило поштивање владавине закона на интернету и у ширем дигиталном окружењу:

- државе би требале да имају могућност да се позову на националну безбедност као разлог за мешање у људска права само у вези с питањима која прете самом ткиву и основним институцијама нације;
- државе које желе да наметну мешање у основна права на основу наводне претње националној безбедности морају да покажу да се на ту претњу не може одговорити уобичајеним кривичноправним мерама, укључујући и посебне законе о борби против тероризма, који се уклапају у прихваћене параметре мирнодопског кривичног права и поступка као и у међународне стандарде везане за кривичноправни поступак;

- горе наведено важи и за радње државе које су везане за интернет и електронске комуникације.

20. Државе чланице би требале да активности агенција за националну безбедност и обавештајни рад доведу под свеукупни законски оквир. Док се не успостави већа транспарентност правила по којима те службе делују – и на домаћем нивоу, и екстратериторијално, и/или у сарадњи једних с другима – не може се претпоставити да су њихове активности у складу с владавином закона.

21. Државе чланице би требале да обезбеде и постојање ефикасног демократског надзора над службама националне безбедности. За ефикасан демократски надзор би требало промовисати културу поштивања људских права и владавине закона, нарочито међу службеницима безбедносних агенција.

Значајан део својих људских права данас остварујемо користећи интернет и шире дигитално окружење. Међутим, наша људска права могу се и кршити управо коришћењем тих истих средстава.

Постоји општа сагласност да би се људска права требала уживати онлајн у истој мери колико и офлајн. У пракси, пак, актери који могу да обезбеде да уживамо људска права нису исти у та два окружења. Нарочито, два суштинска елемента те разлике су несразмеран утицај и контрола које одређене државе и приватне компаније имају на интернету и његовој физичкој инфраструктури на глобалном нивоу.

Овај тематски документ разматра како се владавина закона може одржати у окружењу које карактеришу ова специфична питања управљања, уз фокус на неке области политике рада које су посебно релевантне за људска права: слобода изражавања, заштита података и приватност, сајбер криминал и државна безбедност. Документ указује и на то како би се могло ићи напред у обезбеђењу да се можемо поуздати у то да ће се владавина закона примењивати на наше онлајн активности.

**www.commissioner.coe.int**

PREMS 216914 SRP

SRP

**www.coe.int**

Савет Европе је водећа организација за људска права на континенту. Обухвата 47 држава, од којих су 28 чланице Европске уније. Све државе чланице Савета Европе потписале су Европску конвенцију о људским правима, споразум чији је циљ заштита људских права, демократије и владавине права. Европски суд за људска права надгледа примену Конвенције у државама чланицама.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE