K R I V I Č N O P R O C E S N O P R A V O

https://doi.org/10.7251/CEST1322205T **UDK** 343.1:621.39

МАСОВНИ НАДЗОР КОМУНИКАЦИЈА: ДА ЛИ ТОНЕМО У ТОТАЛИТАРИЗАМ?

Др Вељко Турањанин

Ванредни професор Правног факултета Универзитета у Крагујевцу

Др Емир Ћоровић

Ванредни професор Државног универзитета у Новом Пазару

Апстракт. *Аутори се у овом раду баве масовним пресретањем комуникација и његовим односом са правом на приватност. У средишту дебате су нове пресуде Европског суда за људска права у предметима Big Brother Watch and Others v. the United Kingdom and Centrum för Rättvisa v. Sweden. ЕСЉП је почео да развија нове критеријуме у вези са масовним надзором, будући да су досадашњих шест критеријума стари више од десет година. Међутим, овај приступ може бити упитан с обзиром на релативно нове пресуде у истој ствари, али у којима се користи стари приступ. Овај рад је подељен на неколико делова. Након уводних напомена, аутори објашњавају приступ Европског суда за људска права. На првом месту, објашњавају опште принципе који се односе на тајне мере надзора, укључујући пресретање комуникација, након чега објашњавају приступ ЕСЉП у случајевима масовног надзора и приступ ЕСЉП који треба следити у случајевима масовног надзора комуникација.*

Кључне речи: *масовни надзор комуникација, тајни надзор комуникације, Big Brother Watch and Others v. the United Kingdom, Centrum för Rättvisa v. Sweden, право на приватност*

1. УВОД

Однос између технологије и друштва деценијама је био ноторно комплексна и клизава област науке. У модерном времену добија нови облик (Kiernan & Mueller, 2021:22). Поред бројних промена, технологија је променила начин на који се односимо према другом и према влади (Leavens, 2015:709). Џорџ Орвел би се вероватно сложио да је један од најефикаснијих начина на који репресивна влада може да елиминише личне слободе својих грађана лишавање њихове приватности (Weber, 1971:358; Turanjanin, 2020:268). У идеалном свету, државни надзор мора да буде вођен интересима јавне безбедности и спровођења и проверен правом на приватност, али последњих година ова равнотежа се постепено мења као резултат растућих националних и глобалних немира, развоја способности надзора и ерозије заштите приватности (Yadin, 2017:709). Наше комуникације и активности данас рутински остављају богате дигиталне трагове који се могу прикупљати,

анализирати и чувати по ниској цени (Wong, 2015). Државни надзор сајбер простора је, нажалост, неоправдано обиман и сталан, углавном неометан законским ограничењима; надзор над физичким просторима није толико распрострањен нити толико необуздан (Yadin, 2017:709). У Сједињеним Државама, 11. септембар 2001. године значајно је изменио правила приватности (Heymann, 2016:428), али можемо рећи да је то проблем и у остатку света који иде ка тоталитарном друштву (Nomikos, 2017:122; Jacobs, 2009). Иако надзор није нова појава, масовни надзор јесте (Franks, Democratic Surveillance, 2017).

У последњих неколико година велику улогу имају открића Едварда Сноудена, што је последично подстакло међународну дебату о приватности, шпијунирању и надзору интернета (Geist, 2015; Clement & Obar, 2015: 13-44; Kampmark, 2014: 2), а што је довело до напора да се реформишу савремени системи надзора (Lee, Perlin & Schottenfeld, 2019: 123; Hu, 2015; Arnbak & Golberg, 2015; Eoyang & Ashcroft, 2017: 1; Klein, Flournoy & Fontaine, 2016). Његова открића су открила техничку и правну инфраструктуру савременог државног надзора, што је довело до појаве појма *законите незаконитости* (Austin, 2015) и поново нагласила дебату у ком моменту надзор владе представља кршење приватности (Eoyang, 2016: 3).

Укратко, електронски надзор комуникација представља пресретање комуникације између две или више страна (Banks, 2017: 514). Ово је веома сложено питање, које такође потпада под члан 8. Коненције. ЕСЉП је у чувеној пресуди *Klass and Others v. Germany* нагласио да су телефонски разговори обухваћени појмовима „приватни живот“ и „преписка“ у смислу члана 8. То је поновљено у предмету *Malone v. The United Kingdom* и у бројним одлукама након тога. Као што знамо, ова одредба је подељена у четири категорије: приватни живот, породични живот, дом и преписка (Schabas, 2015: 366). Чланови 8-11 су подложни ограничењима због бројних „легитимних сврха“ које се налазе, иако не уједначено, у другим ставовима (Greer, 2006: 257). Права заштићена чланом 8. могу се ограничити само у складу са законом и на основу потреба демократског друштва, а органи Конвенције су развили флексибилну методологију за тумачење и примену става 2. члана 8. Конвенције (Schabas, 2015: 40).

У данашњем свету, значај развоја дигиталне технологије за надзор и приватност не може се преценити (Cole, 2016: 679) и право на приватност треба да иде у корак са технолошким развојем (Jayawickrama, 2017: 650). Иако изазов да осигурамо да наши закони и уставна заштита иду у корак са променљивим временима није нов, истовремена појава брзог технолошког

развоја створила је опасно широк јаз између постојеће заштите приватности и владиног капацитета и овлашћења да заобиђе те заштите (Siemion, 2015: 20). Интернет је увео нову динамику у вековне тензије између безбедности и слободе (Banks, 2017: 513). Развој способности органа за спровођење закона да спроводе истраге и надзор и масовно усвајање дигиталних комуникационих технологија од стране јавности створило је огромне нове истражне мете, тако да су полиција и приватни продавци искористили технолошке иновације да креирају нове и раније незамисливе истражне алате (Manes, 2019: 505; Solove, 2004: 1267). Органи кривичног поступка морају да користе савремене технологије у борби против нових и софистицираних облика криминалне активности (Muharremi, 2015: 87). Међутим, један од кључних проблема лежи у чињеници да се већи део овог надзора спроводи без налога или потребног степена сумње (Slobogin, 2015).

Усред дебата о балансирању приватности и безбедности, неки политичари су предложили одрицање од права на приватност ради безбедности (van Genderen, 2017: 338; Czerniak, 2021: 126), што није без присталица (Schoenfeld, 2015). Многе земље широм света уводе законе о надзору комуникације (Hosein & Palow, 2013: 1072), али то није правило. Остаје чињеница да правни оквир често дозвољава превише дискреције властима, остављајући простор за произвољан надзор (Gräf, 2017: 446). У развоју софистициране технологије јавља се потреба за бољом борбом против тешких облика криминала и многе земље су спровеле мере тајног надзора. Старе методе истраге у модерном времену нису ефикасне за успешно кривично гоњење (Fenyvesi, 2006; Clark , 1990). Дакле, изазов је како ускладити право на приватност са потребом пресретања комуникација ради превенције и истраге кривичних дела (Esen, 2012; Moonen, 2010: 97, 98). Сасвим је нормално да обични људи, уз разумна очекивања приватности (Donohue, 2006), протестују против неразумног надзора комуникација и то није повезано са кривичним делима (Joh, 2013: 1002). Док су многи људи широм света често вољни да слободу и приватност мењају за безбедност, у случају масовног надзора, показали су интересовање за програме и изразили огорчење због њих (Leonetti, 2015: 231).

Прислушкивање и други облици пресретања телефонских разговора представљају озбиљно мешање у приватни живот и преписку и стога морају бити засновани на закону који је посебно прецизан (Jayawickrama, 2002). Ни имовинска питања нису искључена на овом пољу (Woodburn, 2016). Ово је, поред тога, веома осетљива област због заштите података (Norris, de Hert, L'Hoiry, & Galleta, 2017). Дакле, друштва вођена владавином права сматрају

да владе треба да прикупљају информације о нама само када је корисно да се постигне циљ важнији од нашег личног права да будемо менаџери онога што се о нама зна (Moonen, 2010: 98).

Значајан допринос у овој области произилази са становишта Европског суда за људска права да законодавци треба да јасно препознају круг субјеката који би могли бити изложени овој мери, али и природу (врсту) кривичног дела, где је применљиво; временска ограничења примене; записник; начин контроле ове евиденције и разлози уништавања прикупљеног материјала. Пресретање комуникација је веома сложено питање (Rona & Aarons, 2016: 512) и ЕСЉП је, од случаја *Леандер* па надаље, увек ишао ка прогресивном проширењу делокруга члана 8. (Sicurella & Scalia, 2013: 434-435).

2. МАСОВНИ НАДЗОР КОМУНИКАЦИЈА И ЕСЉП

2.1. Општи принципи

На првом месту, потребно је подсетити се општих принципа везаних за надзор комуникација. ЕСЉП је у бројним пресудама нагласио да су телефонски разговори обухваћени појмовима „приватни живот" и „преписка" у смислу члана 8. Такво мешање је оправдано одредбама става 2. члана 8. само ако је „ у складу са законом", тежи једном или више легитимних циљева из става 2. и „неопходан је у демократском друштву" да би се постигао циљ или циљеви. Мера тајног надзора може се сматрати у складу са Конвенцијом само ако је строго неопходна за заштиту демократских институција и, штавише, ако је апсолутно неопходна, за добијање виталних обавештајних података у појединачној операцији. Иначе, то је озбиљна претња демократији у данашњем свету (Nash, 2002). Израз „у складу са законом" подразумева услове који превазилазе постојање правног основа у домаћем закону и захтева да правни основ буде „доступан" и „предвидив".[1]

Генерално, ЕСЉП је у својој пракси дефинисао значење израза „у складу са законом". Овај термин имплицира да оспорена мера треба да има неку основу у домаћем закону, али се такође односи и на квалитет дотичног закона, захтевајући да буде компатибилан са владавином права и доступан дотичном лицу које мора, штавише, бити у стању да предвиди последице по себе.[2] У домаћем закону мора постојати мера правне заштите од произвољног

[1] *Amann v. Switzerland* Application No. 27798/95, 16 February 2000, 55.

[2] *Kruslin v. France*, 27; *Lambert v. France*, supra note 18, 23; *Huvig v. France*, 26; *Kopp v. Switzerland* Application No. 23224/94, 15 March 1998, 55; *Perry v. the United Kingdom* Application No. 63737/00, 17 July 2003, 45; *Dumitru Popescu v. Romania (No. 2)* Application

мешања јавних власти у права загарантована ставом 1. члана 8.[3] Поред тога, ЕСЉП је нагласио чињеницу да су ризици произвољности евидентни посебно када се овлашћење извршне власти врши у тајности.[4]

Хуан Антонио Гарсија Амадо нас подсећа да је, према Речнику Шпанске краљевске академије, предвидљиво „оно што се може предвидети или је у оквиру нормалног предвиђања", тако да, предвидети значи видети у ишчекивању или знати, нагађати по неким знацима или индикацијама шта треба да се деси или да има или да припреми ресурсе против будућих непредвиђених ситуација (Amado, 2017: 177). Када говоримо о предвидивости у контексту прикривеног пресретања комуникације, захтеви Конвенције не могу бити потпуно исти у посебном контексту пресретања комуникација за потребе полицијских истрага.[5] ЕСЉП је у предмету *Kvasnica* навео да захтев правне „предвидивости" у посебном контексту тајних мера надзора, као што је пресретање комуникација, не може значити да би појединац требало да буде у стању да предвиди када ће власти вероватно пресрести његову комуникацију тако да да може да прилагоди своје понашање у складу са тим.[6] Овај стандард се, између осталих, понавља у предмету *Weber and Saravia v. Germany*[7] или слично у *Leander v. Sweeden*. Након тога, потребно је испитати да ли надзор има легитиман циљ и да ли је неопходан у демократском друштву.

2.2. Приступ Европског суда за људска права у случајевима масовног надзора

Масовно пресретање прекограничних комуникација,[8] што се обично подразумева у оквиру ширег појма дигиталног надзора (Ünver, 2018), представља посебан проблем данас.[9] Велико веће ЕСЉП донело је одлуку у два важна предмета: *Big Brother Watch and Others v. the United Kingdom* и

No. 71525/01, 16 April 2007, 61; *Liberty and Others v. the United Kingdom* Application No. 58243/00, 1 July 2008, 59.

3 *Malone v. The United Kingdom*, 67.

4 *Klass and Others v. Germany*, 42, 49.

5 *Malone v. The United Kingdom*, supra note 4, at para 67.

6 *Kvasnica v. Slovakia*, supra note 19, at para 79.

7 *Weber and Saravia v. Germany*, Decision as to the Admissibility of Application No. 54394/00, 29 June 2006, 93.

8 *Big Brother Watch and Others v. the United Kingdom* Application Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, 322-323; *Centrum för Rättvisa v. Sweden* Application No. 35252/08, 25 May 2021, 236-237.

9 У великом броју случајева, надзора није ни чисто домаћи ни чисто страни (Freiwald, 2008: 333). Истовремено, морамо имати на уму да наша комуникација на даљину никада није била потпуно приватна (Landau, 2016: 61).

Centrum för Rättvisa v. Sweden. Члан 8. Конвенције не забрањује употребу масовног пресретања комуникација ради заштите националне безбедности и других суштинских националних интереса од озбиљних спољних претњи, а државе уживају широко поље процене у одлучивању о томе која врста режима пресретања је неопходна. Међутим, у таквом систему поље слободне процене које им се даје мора бити уже и одређени број заштитних мера ће морати да буде присутан у случају масовног надзора.

Током година, ЕСЉП је успоставио одређене минималне заштитне мере које би требало да буду прописане у закону како би се избегла злоупотреба овлашћења: природа кривичних дела која могу довести до налога за пресретање, дефиниција категорија људи за које постоји обавеза пресретања њихове комуникације, ограничење трајања пресретања, поступак који треба следити за испитивање, коришћење и чување добијених података, мере предострожности које треба предузети када се подаци саопштавају другим странама и околности у којима пресретнути подаци могу или морају бити избрисани или уништени. Поред тога, ЕСЉП води рачуна о уређењу надзора над спровођењем мера тајног надзора, постојању механизама обавештавања и свим правним лијековима предвиђеним националним законом.[10]

Можемо се сложити са ставом Европског суда за људска права да је масовно пресретање постепени процес у којем се степен мешања у право појединца на приватност повећава како процес напредује.[11] Режими масовног пресретања можда неће сви пратити потпуно исти модел, а различите фазе процеса неће нужно бити дискретне или праћене у строгом хронолошком редоследу. Према ЕСЉП, фазе процеса масовног пресретања које треба узети у обзир могу се описати на следећи начин:

(а) пресретање и почетно задржавање комуникација и сродних комуникационих података (тј. података о саобраћају који припадају пресретнутим комуникацијама);

(б) примена специфичних селектора на задржане комуникационе/сродне комуникационе податке;

(ц) испитивање одабраних комуникација/сродних комуникационих података од стране аналитичара; и

(д) накнадно задржавање података и коришћење „коначног производа“, укључујући дељење података са трећим лицима.[12]

[10] *Roman Zakharov v. Russia* Application No. 47143/06, 4 December 2015.

[11] *Big Brother Watch and Others v. the United Kingdom*, 325; *Centrum för Rättvisa v. Sweden*, 238.

[12] Ibid., 325; ibid., 239.

У првој фази обавештајне службе ће масовно пресретати електронске комуникације. Обично ће ове комуникације припадати великом броју појединаца и неке комуникације могу бити филтриране у овој фази.[13] Иницијално претраживање се одвија у другој фази, када се различити типови селектора, укључујући „јаке селекторе“ (као што је адреса е-поште) и/или сложени упити примењују на задржане пакете комуникација и сродних комуникационих података. Ово може бити фаза у којој процес почиње да циља појединце кроз употребу јаких селектора.[14] У трећој фази, пресретнути материјал први пут испитује аналитичар.[15] Последња фаза постоји када обавештајне службе заиста користе пресретнути материјал. То може укључивати израду обавештајног извештаја, прослеђивање материјала другим обавештајним службама у држави која их пресреће, или чак преношење материјала страним обавештајним службама.[16] На крају овог процеса, потреба за заштитним мерама биће највећа, што је приступ у складу са мишљењем Венецијанске комисије.

У *Weber and Saravia* и *Liberty and Others* ЕСЉП је утврдио да режими масовног пресретања спадају у оквир процене држава, али данас, 2022. године, развијених шест поменутих критеријума стари су више од десет година, тако да је ЕСЉП морао да развије нове критеријуме у вези са масовним надзором. Међутим, овај приступ може бити упитан с обзиром на релативно нове пресуде у истој ствари, али у којима се користи стари приступ. Ипак, данас све више живимо на мрежи, генеришући како знатно већи обим електронских комуникација, тако и комуникација знатно другачије природе и квалитета, од оних које су вероватно настале пре деценију, а обим активности надзора је био много ужи.[17] Оно што је посебно важније, циљано пресретање и масовно пресретање се разликују у низу важних аспеката од *Weber and Saravia* и *Liberty and Others*.

Основна сврха масовног надзора и пресретања је праћење комуникација лица ван територијалне јурисдикције државе, иако је могуће пресретање и испитивање комуникација лица унутар исте државе, ради истраге одређених тешких кривичних дела. Ова врста пресретања је углавном усмерена на међународне комуникације.[18] За разлику од тајног пресретања комуникација, масовно пресретање се не користи нужно за циљање

[13] Ibid., 326; ibid., 240.
[14] Ibid., 327; ibid., 241.
[15] Ibid., 328; ibid., 242.
[16] Ibid., 329; ibid., 243.
[17] Ibid., 341; ibid., 255.
[18] *Big Brother Watch and Others v. the United Kingdom*, 345; *Centrum för Rättvisa v. Sweden*, 258.

комуникације одређених појединаца. У овој процедури, појединци су на мети применом јаких селектора за комуникацију коју масовно пресрећу обавештајне службе. „На овај начин ће бити пресретнути само они „пакети“ комуникација циљаних појединаца који су путовали преко носилаца које су одабрале обавештајне службе, а само оне пресретнуте комуникације које су одговарале или снажном селектору или сложеном упиту могле су бити испитане од стране аналитичара.”[19]

У контексту тајних мера надзора или пресретања од стране јавних органа, неопходно је имати јасна, детаљна правила о пресретању телефонских разговора, посебно зато што технологија доступна за коришћење постаје све софистицираниja.[20] У случају када домаћи закон не регулише употребу прикривених прислушних уређаја у релевантном тренутку, ометање није „у складу са законом”.[21] Затим, у бројним пресудама ЕСЉП је навео да, с обзиром на то да примена мера тајног надзора комуникације у пракси није подложна контроли јавности у целини, то би било у супротности са владавином права. Сходно томе, закон мора навести обим сваког таквог дискреционог права датог надлежним органима и начин његовог коришћења са довољно јасноће да се појединцу пружи адекватна заштита од произвољног мешања.[22]

2.3. Приступ Европског суда за људска права који треба следити у случајевима масовног пресретања

У сфери масовног пресретања, очигледно је да неки од *Weber and Saravia* критеријума нису у потпуности применљиви. Пре свега, то је природа кривичних дела која могу довести до наредбе за пресретање и дефинисања категорија људи за које постоји обавеза пресретања њихове комуникације. Поред тога, то је случај са захтевом „разумне сумње“.[23] Овај критеријум се може наћи у судској пракси ЕСЉП о циљаном пресретању у контексту кривичних истрага, али је мање релевантан у контексту масовног пресретања. Без обзира на то, ЕСЉП сматра да је императив да када држава води такав режим, домаћи закон треба да садржи детаљна правила о томе када власти

[19] Ibid., 346; ibid., 260.

[20] *Valenzuela Contreras v. Spain* Application No. 27671/95, 30 July 1998, 67; *Kopp v. Switzerland*, 72.

[21] *P. G. and J. H. v. the United Kingdom* Application No. 44787/98, 25 December 2001, 39.

[22] *Weber and Saravia v. Germany*, 46; *Malone v. The United Kingdom*, 68; *Leander v. Sweeden*, 51; *Huvig v. France*, 29; *Bykov v. Russia* Application No. 4378/02, 10 March 2009, 78.

[23] Стернберг је још 1978. нагласио да амерички четврти амандман такође захтева да све владине претраге и заплене, укључујући и операције електронског надзора, морају бити разумне (Sternberg, 1978: 205).

могу да прибегну таквим мерама и да довољно јасно наведе разлоге на основу којих би масовно пресретање могло бити одобрено и околности у којима би комуникација појединца могла бити пресретнута.[24]

У контексту масовног пресретања, важност надзора се мора појачати. Данас постоји инхерентан ризик од злоупотребе, док ће легитимна потреба за тајношћу неизбежно значити да, из разлога националне безбедности, државе често неће бити слободне да обелодане информације које се тичу деловања оспореног режима.[25] Стога, како би се смањио ризик од злоупотребе моћи масовног пресретања, ЕСЉП сматра да процес мора бити подвгнут „заштити од почетка до краја“: у свакој фази процеса треба извршити процену неопходности и пропорционалност мера које се предузимају; масовно пресретање треба да буде предмет независног овлашћења на самом почетку, када се дефинишу предмет и обим операције; и да операција треба да буде предмет надзора и независног *ex post facto* прегледа.[26]

Судско одобрење је важна гаранција против произвољности и злоупотребе у овој области (van der Sloot & Kosta, 2019: 258), али према ЕСЉП, то није „неопходан услов“, јер масовно пресретање треба да буде одобрено од стране независног органа - органа који је независан од извршне власти. Ово тело треба да буде обавештено и о сврси пресретања и о носиоцима или комуникационим путевима који ће вероватно бити пресретнути, што би омогућило органу да процени неопходност и пропорционалност операције масовног пресретања, као и да процени да ли је избор носилаца неопходан и сразмеран сврси због које се пресретање спроводи.[27]

Штавише, употреба снажних селектора је један од најважнијих корака у процесу масовног пресретања, јер је то тачка у којој обавештајне службе могу да нађу на мети комуникације одређеног појединца.[28] Узимајући у обзир карактеристике масовног пресретања, велики број ангажованих селектора и инхерентну потребу за флексибилношћу у избору селектора, која се у пракси може изразити као техничке комбинације бројева или слова, очигледно је да

---

[24] *Big Brother Watch and Others v. the United Kingdom*, 348; Centrum för *Rättvisa v. Sweden*, 262. Судије Леменс, Вехабовић и Бошњак наглашавају да је помињање „основа“ и „околности“ прилично нејасно, посебно у одсуству било каквог упућивања на то шта ти разлози и околности могу или не морају бити. Судија Пинто де Албукерки такође сматра да је језик Европског суда за људска права недопустиво нејасан.

[25] Ibid., at § 349; ibid., at § 263.

[26] Ibid., at § 350; ibid., at § 264.

[27] *Big Brother Watch and Others v. the United Kingdom*, 351-352; *Centrum för Rättvisa v. Sweden*, 265-266.

[28] Ibid., 353; ibid., 267.

је укључивање свих селектора у овлашћењу не може бити изводљиво у пракси. Ипак, имајући у виду да избор селектора и термина за упите одређују које ће комуникације бити квалификоване за испитивање од стране аналитичара, овлашћење би у најмању руку требало да идентификује типове или категорије селектора који ће се користити.[29] Штавише, требало би да постоје појачане заштитне мере када се у обавештајним службама ангажују јаки селектори повезани са појединцима који се могу идентификовати. Обавештајне службе морају да оправдају употребу сваког таквог селектора и то оправдање треба да буде пажљиво евидентирано и да подлеже процесу претходног интерног овлашћења којим се обезбеђује посебна и објективна провера да ли је оправдање у складу са претходно наведеним принципима.[30]

Свака фаза процеса масовног пресретања такође треба да буде предмет надзора од стране независног органа и тај надзор треба да буде довољно снажан да задржи мешање на оно што је неопходно у демократском друштву.[31] У свакој фази процеса обавештајне службе треба да воде детаљну евиденцију.[32] Коначно, ефикасан правни лек треба да буде доступан свакоме ко сумња да су његове комуникације пресреле обавештајне службе. Његов циљ би могао бити двострук: или да оспори законитост пресретања на које се сумња или да се испита компатибилост пресретања са Конвенцијом. У контексту циљаног пресретања, накнадно обавештавање о мерама надзора треба да буде релевантан фактор у процени ефикасности правних лекова пред судовима, а самим тим и постојање делотворних заштитних мера против злоупотребе овлашћења надзора.[33] Обавештавање о мерама надзора је нераскидиво повезано са делотворношћу правних лекова пред судом[34] а

[29] Ibid., 354; ibid., 268.

[30] Ibid., 355; ibid., 269.

[31] *Roman Zakharov v. Russia*, 232; *Klass and Others v. Germany*, 49, 50 и 59; *Weber and Saravia v. Germany*, 106 и *Kennedy v. the United Kingdom* Application No. 26839/05, 18 May 2010, 153-154. Међутим, како Владецк истиче, заиста свеобухватна шема за контрадикторну судску ревизију програма тајног надзора у ствари може бити недостижна (Vladeck, 2014: 578).

[32] *Big Brother Watch and Others v. the United Kingdom*, 356; *Centrum för Rättvisa v. Sweden*, 270.

[33] Обавештење није неопходно ако систем домаћих правних лекова дозвољава било којој особи која сумња да је њена комуникација пресретнута да се обрати судовима; другим речима, где надлежност суда не зависи од обавештења субјекту пресретања да је било пресретања његових комуникација (*Roman Zakharov v. Russia*, 234 и *Kennedy v. the United Kingdom*, 167).

[34] Ефикасност правних лекова је повезана са обавештењем. Међутим, питање правних лекова се односи на ретроактивну примену правних лекова након надзора, јер субјект надзора треба да има право да испитује законитост тајне мере надзора. Анализа члана 13 у *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* је најкомплетнија анализа у судској пракси у вези са питањем накнадног обавештења

самим тим и са постојањем делотворних заштитних механизама против злоупотребе овлашћења надзора, пошто у принципу постоји мало простора за обраћање судовима од стране појединаца о којима је реч.[35] ЕСЉП је искористио пресуду *Klass* као прилику да одреди основне принципе који балансирају између овлашћења државног тајног надзора и права циљаних појединаца, посебно права да буду обавештени о мерама надзора и могућности да се обрате судовима након престанка таквих мера (Boehm, 2012). У *Klass*, ЕСЉП није директно захтевао обавештавање дотичне особе, али у новијим случајевима ЕСЉП све више инсистира на обавези обавештавања (Boehm & de Hert, 2012), почев од *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*.

Међутим, чињеница да лица која су била под тајним надзором нису накнадно обавештена након престанка надзора не може сама по себи да оправда закључак да мешање није било „неопходно у демократском друштву", јер је само одсуство знања о надзору оно што осигурава ефикасност. Заиста, такво обавештење би могло открити радне методе и поља деловања. Чим се обавештавање може извршити без угрожавања сврхе ограничења након престанка мере надзора, информације треба, међутим, да буду пружене заинтересованим лицима.[36] У предмету *Szabó and Vissy v. Hungary* такође није постојала обавеза обавештења, па је из тог разлога, између осталих, ЕСЉП утврдио повреду члана 8. Последњих година ЕСЉП је у више наврата доносио одлуке о заштити право на приватност када је у питању масовни надзор комуникација (Vogiatzoglou, 2018; van der Sloot & Kosta, 2019).

У *Big Brother Watch and Others v. the United Kingdom*, ЕСЉП је даље развио своје схватање правног лека и обавештења, и сматра да правни лек који не зависи од обавештења субјекту пресретања такође може бити ефикасан правни лек у контексту масовног пресретања; у ствари, у зависности од околности, може чак понудити боље гаранције правилног поступка од система заснованог на обавештењу. Без обзира на то да ли је материјал добијен циљаним или масовним пресретањем, постојање изузетка за националну безбедност могло би да лиши било каквог стварног практичног ефекта обавештајном захтеву. Вероватноћа да захтев за обавештавање има мали или никакав практичан ефекат биће акутнији у контексту масовног

(*видети Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* Application No. 62540/00, 28 June 2007; (Murphy, 2016: 296)).

35 *Klass and Others v. Germany*, 57; *Weber and Saravia v. Germany*, 135.

36 *Klass and Others v. Germany*, 58; *Weber and Saravia v. Germany*, 135; *Leander v. Sweeden*, 66; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, 90.

пресретања, пошто се такав надзор може користити у сврхе прикупљања страних обавештајних података и углавном ће бити усмерен на комуникацију особа изван територијалне надлежности државе. Стога, чак и ако је идентитет мете познат, власти можда неће бити свесне његове локације.[37]

Овлашћења и процесне гаранције које орган поседује су релевантне за утврђивање да ли је правни лек ефикасан. Стога, у одсуству захтева за обавештавањем, императив је да правни лек буде пред органом који је, иако није нужно судски, независан од извршне власти и обезбеђује правичност поступка, нудећи, у мери у којој је то могуће, контрадикторност поступка. Одлуке овог органа биће образложене и правно обавезујуће у погледу, између осталог, престанка незаконитог пресретања и уништавања незаконито прибављеног и/или ускладиштеног пресретнутог материјала.[38]

Процењујући да ли је држава деловала у оквиру свог поља слободне процене, ЕСЉП је почео да развија нови, шири спектар критеријума од шест Веберових заштитних мера. ЕСЉП је додао осам критеријума:

1. разлози због којих се може одобрити масовно пресретање;
2. околности у којима комуникација појединаца може бити пресретнута;
3. процедура за давање дозволе;
4. процедура која треба бити поштована за одабир, испитивање и коришћење пресретнутог материјала;
5. мере предострожности које треба предузети приликом саопштавања материјала другим странама;
6. ограничења трајања пресретања, складиштења пресретнутог материјала и околности у којима се такав материјал мора избрисати и уништити;
7. процедуре и модалитете за надзор од стране независног органа над поштовањем наведених заштитних мера и овлашћења за решавање неусаглашености;
8. процедуре за независно *ex post facto* преиспитивање такве усклађености и овлашћења која су дата надлежном органу у решавању случајева непоштовања.[39]

[37] *Big Brother Watch and Others v. the United Kingdom*, 358; *Centrum för Rättvisa v. Sweden*, 272.

[38] Ibid., 360; ibid., 273; види, *mutatis mutandis*, *Segerstedt-Wiberg and Others v. Sweden* Application No. 62332/00, 6 June 2006, 120.

[39] *Big Brother Watch and Others v. the United Kingdom*, 361; *Centrum för Rättvisa v. Sweden*, 275.

Неке државе данас деле материјал са својим обавештајним партнерима и чак, у неким случајевима, дозвољавају тим обавештајним партнерима директан приступ њиховим сопственим системима. Нажалост, ЕСЉП није дао конкретне смернице у вези са мерама предострожности које треба предузети када се преноси пресретнути материјал другим странама. ЕСЉП сматра да би пренос материјала који се добија масовним пресретањем од стране једне државе страним државама или међународним организацијама требало да буде ограничен на материјал који је прикупљен и ускладиштен на начин у складу са Конвенцијом и да подлеже одређеним додатним посебним заштитним мерама које се односе на сам трансфер.

ЕСЉП је у *Big Brother Watch and Others* нагласио четири важна правила која се морају поштовати у овим случајевима. Пре свега, околности у којима се такав трансфер може десити морају бити јасно наведене у домаћем закону. Друго, држава која преноси податке мора осигурати да држава прималац, у руковању подацима, има успостављене заштитне мере које могу спречити злоупотребу и несразмерно ометање. Конкретно, држава пријема мора гарантовати безбедно складиштење материјала и ограничити његово даље откривање. Ово не значи нужно да држава пријема мора имати заштиту упоредиву са заштитом државе која преноси; нити нужно захтева да се пре сваког трансфера да гаранција. Треће, појачане мере заштите ће бити неопходне када је јасно да се преноси материјал који захтева посебну поверљивост. Коначно, ЕСЉП сматра да би пренос материјала страним обавештајним партнерима такође требало да буде подвргнут независној контроли.[40]

ЕСЉП не сматра да је прикупљање сродних комуникационих података путем масовног пресретања нужно мање наметљиво од прибављања садржаја и стога сматра да пресретање, задржавање и претраживање сродних комуникационих података треба анализирати позивајући се на исте мере заштите као и оне које су применљиве на садржај.[41] Док ће пресретање сродних комуникационих података обично бити одобрено у исто време када је дозвољено пресретање садржаја, обавештајне службе их могу другачије третирати када се добију. С обзиром на различит карактер сродних комуникационих података и различите начине на које их обавештајне службе користе, све док постоје поменуте заштитне мере, ЕСЉП сматра да законске

[40] Ibid., 362; ibid., 276.
[41] Ibid., 363; ibid., 277.

одредбе које регулишу њихово поступање не морају нужно бити идентични у сваком погледу онима који регулишу третман садржаја.[42]

3. ЗАКЉУЧАК

Успостављање равнотеже између заштите права на приватност и људских права с једне стране и заштите друштва од криминалитета и националне безбедности с друге, требало би да буде један од кључних циљева државе у савременим облицима реаговања државе на криминалитет. Дефинитивно није лак задатак поштовати приватност, обезбедити сигурност и заштитити се од злоупотребе у савременом, модерном, дигитално повезаном свету (Daskal, 2017: 143). Као што пракса ЕСЉП често показује, државе врло лако склизну у поље кршења људских права.

У области масовног надзора произилазе два кључна захтева: употреба масовних техника мора бити ограничена на околности које су стриктно неопходне за заштиту демократских институција, а тест крајње нужде захтева да овлашћења на оперативном нивоу морају бити од виталног значаја' за појединачну операцију (Murray & Fussey, 2019: 56). Када говоримо о пресудама у предметима *Big Brother Watch and Others v. the United Kingdom* и *Centrum för Rättvisa v. Sweden*, оно што је неизбежно сумњиво јесте зашто је ЕСЉП затворио очи на број међународних објављених докумената у вези са масовним пресретањем. Са позитивне стране, ЕСЉП је почео да развија нове критеријуме за масовни надзор. Међутим, ови принципи ће морати да се тумаче и даље развијају на начин који ће правилно подржавати демократско друштво и вредности за које се оно залаже. У свом садашњем облику, наведени принципи заиста могу изазвати и изазиваће проблеме у њиховој примени.

Литература

Lambert and Others v. France, Application No. 23618/94 (ECtHR August 24, 1998).

Addis, M., & Morrow, P. (2005). *Your Rights: The Liberty Guide to Human Rights.* Pluto press.

Alhogbani, A. (2015). Going Dark: Scratching the Surface of Government Surveillance. *23 COMMLAW Conspectus*, 469-501.

Amado, J. A. (2017). On the Foreseeability of Legal Consequences: Which Normative Provisions Are and Which Are Not Protected? U P. Manzano, L. Sánchez, & M. Rosique, *Multilevel Protection of the Principle of the Legality in Criminal Law* (str. 177-193). Cham: Springer.

Amann v. Switzerland, Application No. 27798/95 (ECtHR February 16, 2000).

[42] *Big Brother Watch and Others v. the United Kingdom*, 364; *Centrum för Rättvisa v. Sweden*, 278.

Anderson, T. (2014). Toward Institutional Reform of Intelligence Surveillance: A Proposal to Amend the Foreign Intelligence Surveillance Act. *8 Harvard Law & Policy Review*, 413-436.

Arnbak, A., & Golberg, S. (2015). Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad. *21 Michigan Telecommunications & Technology Law Review*, 317-361.

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, Application No. 62540/00 (ECtHR June 28, 2007).

Austin , L. M. (2015). Lawful Illegality: What Snowden Has taught Us about the Legal Infrastructure of the Surveillance State. U M. Geist, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (103-126). University of Ottawa Press.

Banks, W. (2017). Next Generation Electronic Surveillance Law: Imagining the Future. *49 Connecticut Law Review*, 671-703.

Banks, W. C. (2017). Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage. *66 Emory Law Journal*, 513-525.

Banks, W., & Bowman, M. (2000). Executive Authority for National Security Surveillance. *50 American University Law Review*, 2-130.

Bellia, P. L. (2005). Spyware and the Limits of Surveillance Law. *20 Berkeley Technology Law Journal*, 1283-1344.

Berman, E. (2016). The Two Faces of the Foreign Intelligence Surveillance Court. *91 Indiana Law Journal*, 1192-1250.

Big Brother Watch and Others v. the United Kingdom , Application Nos. 58170/13, 62322/14 and 24960/15 (ECtHR May 25, 2021).

Boehm, F. (2012). *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonized Data Protection Principles for Information Exchange at EU-level 34.* Berlin: Springer.

Boehm, F., & de Hert, P. (2012). Notification, an important safeguard against the improper use of surveillance - finally recognized in case law and EU law. *3 European Journal of Law and Technology*, 346-359.

Boroi, A. (2013). Examination of the Provisions Governing the Interceptions of Conversations and Communications according to the European Court of Human Rights Jurisprrudence. *9 AUDJ*, 58–70.

Buono, I., & Taylor, A. (2017). Mass Surveillance in the CJEU: Forging a European Consensus. *76 Cambridge Law Journal*, 250 - 253.

Bykov v. Russia, Application No. 4378/02 (ECtHR March 10, 2009).

Cahall, B., Bergen, P., Sterman, D., & Schneider, E. (2014). Do NSA's Bulk Surveillance Programs Stop Terrorists? *New America*, 1-32.

Calo, R. (2016). Can Americans Resist Surveillance. *83 The University of Chicago Law Review*, 23-43.

Centrum för Rättvisa v. Sweden , Application No. 35252/08 (ECtHR May 25, 2021).

Clark, W. (1990). Electronic Surveillance and Related Investigative Techniques. *128 Military Law Review*, 155-224.

Clement, A., & Obar, J. (2015). Canadian Internet “Boomerang” Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges. U M. Geist, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (13-44). University of Ottawa Press.

Cole, D. (2016). After Snowden: Regulating Technology-Aided Surveillance in the Digital Age. *44 The Capital University Law Review*, 677-691.

Czerniak, D. (2021). Collection of location data in criminal proceedings European (the EU and Strasbourg) standards. *7 Revista Brasileira de Direito Processual Penal*, 123-159.

Daskal, J. (2017). Public and Private Eyes: Surveillance in the Digital Age. *96 Foreign Affairs*, 139-143.

de Biolley, S., & Weyembergh, A. (2006). The EU Mutual Legal Assistance Convention of 2000 and the Interception of Telecommunications. *8 European Journal of Law Reform*, 285-287.

Deeks, A. (2015). An International Legal Framework for Surveillance. *55 Virginia Journal of International Law*, 293-368.

Donohue, L. (2006). Anglo-American Privacy and Surveillance. *96 Journal of Criminal Law and Criminology*, 1061-1208.

Donohue, L. (2014). Bulk Metadata Collection: Statutory and Constitutional Considerations. *37 Harvard Journal of Law & Public Policy*, 757-900.

Donohue, L. K. (2006). Anglo-American Privacy and Surveillance. *96 Journal of Criminal Law and Criminology*, 1164-1167.

Dumitru Popescu v. Romania (No. 2) , Application No. 71525/01 (ECtHR April 16, 2007).

Eoyang, M. (2016). Statement for the Record: Beyond Privacy & Security: The Role of the Telecommunications Industry in Electronic and Surveillance. *Third Way 1*, 3.

Eoyang, M., & Ashcroft, G. (2017). Why Electronic Surveillance Reform is Necessary. *Third Way*, 1.

Esen, R. (2012). Intercepting Communications 'In Accordance with the Law. *76 The Journal of Criminal Law*, 164-178.

Feldman, D. (2002). *Civil Liberties and Human Rights in England and Wales.* OUP Oxford; 2nd edition.

Fenyvesi, C. (2006). The Legal and Criminalistic Aspects of Secret Data and Information Collection. *47 Acta Jur. Hng.*, 183-199.

Flaherty, D. (1989). *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States.* The University of North Carolina Press.

Franks, M. A. (2017). Democratic Surveillance. *30 Harvard Journal of Law & Technology no. 2*, 425-489.

Franks, M. A. (2017). Democratic Surveillance. *30 Harvard Journal of Law & Technology no. 2*, 425-489.

Freiwald, S. (2008). Electronic Surveillance at the Virtual Border. *78 Miss. L.J.*, 333-368.

Friedman, L. (2017). Remnants of Information Privacy in the Modern Surveillance State. *52 New England Law Review*, 15-29.

Geist, M. (2015). Why Watching the Watchers Isn't Enough: Canadian Surveillance Law in the Post-Snowden Era. U M. Geist, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (103). University of Ottawa Press.

Gräf, E. (2017). When automated profiling threatens our freedom: neo-republican perspective. *3 European Data Protection Law Review*, 441-451.

Greer, S. (2006). *The European Convention on Human Rights: Achievements, Problems and Prospects.* Cambridge University Press.

Hartzog, W., & Selinger, E. (2015). Surveillance as Loss of Obscurity. *72 Washington and Lee Law Review*, 1343-1386.

Henderson, S. (2016). A Rose by Any Other Name: Regulating Law Enforcement Bulk Metadata Collection. *94 Texas Law Review*, 28-59.

Heymann, P. (2016). An Essay on Domestic Surveillance. *8 Journal of National Security Law & Policy*, 421-435.

Hosein, G., & Palow, C. (2013). Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques. *74 Ohio State Law Journal*, 1071-1104.

Hu, M. (2015). Small Data Surveillance v. Big Data Cybersurveillance. *42 Pepperdine Law Review*, 773-843.

Hu, M. (2018). Bulk Biometric Metadata Collection. *96 The North Carolina Law Review*, 1426-1474.

Huvig v. France, Application No. 11105/84 (ECtHR April 24, 1990).

Jacobs, B. (2009). Keeping Our Surveillance Society Non-Totalitarian. *1 Amsterdam Law Forum*, 19-34.

Jayawickrama, N. (2002). *The Judicial Application of Human Rights Law: National, Regional and International Jurisprudence.* Cambrige University Press.

Jayawickrama, N. (2017). *The Judicial Application of Human Rights Law: National, Regional and International Jurisprudence.* Cambridge University Press.

Jeffreys-Jones, R. (2017). *We Know all about You: The Story of Surveillance in Britain and America.* Oxford University Press.

Joh, E. (2013). Privacy Protests: Surveillance Evasion and Fourth Amendment Suspicion. *55 Arizona Law Review*, 997-1029.

Kadidal, S. (2014). NSA Surveillance: The Implications for Civil Liberties. *10 Journal of law and policy for the information society*, 433-479.

Kalanges, S. (2014). Modern Private Data Collection and National Security Agency Surveillance: A Comprehensive Package of Solutions Addressing Domestic Surveillance Concerns. *34 The Northern Illinois University Law Review*, 644-679.

Kampmark, B. (2014). Restraining the Surveillance State: A Global Right to Privacy. *2 Journal of Global Faultlines 1*, 1-16.

Kennedy v. the United Kingdom, Application No. 26839/05 (ECtHR May 18, 2010).

Kerr, O. (2014). A Rule of Lenity for National Security Surveillance Law. *100 Virginia Law Review*, 1513-1543.

Kiernan, C., & Mueller, M. (2021). Standardizing Security: Surveillance, Human Rights, and the Battle Over Tls 1.3. *11 Journal of Information Policy*, 1-25.

Klass and Others v. Germany , Application No. 5029/71 (ECtHR September 6, 1978).

Klein, A., Flournoy, M., & Fontaine, R. (2016). Post-Snowden Responses and Reforms Surveillance Policy: A Pragmatic Agenda for 2017 and Beyond. (str. 23). Center for a New American Security.

Kopp v. Switzerland, Application No. 23224/94 (ECtHR March 15, 1998).

Kris, D. (2014). On the Bulk Collection of Tangible Things. *7 Journal of National Security Law & Policy*, 209-295.

Kruslin v. France, Application No. 11801/85 (ECtHR April 24, 1990).

Kvasnica v. Slovakia , Application No. 72094/01 (ECtHR June 9, 2009).

Lagerwall, A. (2008). *Privacy and Secret Surveillance from a European Convention Perspective.* Stockholm University Faculty of Law.

Landau, S. (2016). Choices: Privacy & Surveillance in a Once & Future Internet. *145 Daedalus*, 54-64.

Leander v. Sweeden, Application No. 9248/81 (ECtHR March 26, 1987).

Leavens, A. (2015). The Fourth Amendment and Surveillance in a Digital World. *27 Journal of Civil Rights and Economic Development*, 709-746.

Lee, D., Perlin, P., & Schottenfeld, J. (2019). Gathering Intelligence: Drifting Meaning and the Modern Surveillance Apparatus. *10 Journal of National Security Law & Policy*, 77-123.

Leonetti, C. (2015). If a Tree Falls: Bulk Surveillance, the Exclusionary Rule, and the Firewall Loophole. *13 Ohio State Journal of Criminal Law*, 211-231.

Liberty and Others v. the United Kingdom , Application No. 58243/00 (ECtHR July 1, 2008).

Lin, H. (2014). Technology's limited role in resolving debates over digital surveillance. *345 Science*, 728-730.

Lüdi v. Switzerland, Application No. 12433/86 (ECtHR June 15, 1992).

Malone v. The United Kingdom , Application No. 8691/79 (ECtHR August 2, 1984).

Manes, J. (2015-2016). Online Service Providers and Surveillance Law Transparency. *125 The Yale Law Journal*, 343-358.

Manes, J. (2019). Secrecy & Evasion in Police Surveillance Technology. *34 Berkeley Technology Law Journal*, 504-566.

Marshall, J. (2009). *Personal Freedom through Human Rights Law? Autonomy, Identity and Integrity under the European Convention on Human Rights.* Brill Nijhoff .

Mayer, J., Mutchler, P., & Mitchell, J. (2016). Evaluating the privacy properties of telephone metadata. *113 Proceedings of the National Academy of Sciences of the United States of American*, 5536-5541.

Moonen, T. (2010). Special Investigation Techniques, Data Processing and Privacy Protection in the Jurisprudence of the European Court of Human Rights. *1 Pace International Law Review Online Companion*, 97-136.

Muharremi, D. (2015). Measures of Concealed (Secret) Criminal Investigation. *5 International Review of Law and Economics*, 83-90.

Mulligan, A. (2016). Constitutional Aspects of International Data Transfer and Mass Surveillance. *55 Irish Jurist*, 199-208.

Murphy, M. H. (2016). Surveillance and the Right to Privacy: Is an 'Effective Remedy' Possible? U A. Diver, & J. Miller, *Justiciability of Human Rights Law in Domestic Jurisdictions* (289–306). Heidelberg-New York-Dordrecht-London: Springer.

Murray, D., & Fussey, P. (2019). Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. *52 Israel Law Review*, 31-60.

Nash, S. (2002). Balancing Convention Rights: P.G. and J.H. v United Kingdom. *6 The International Journal of Evidence & Proof*, 125-129.

Nomikos, L. (2017). Are We Sleepwalking into a Surveillance Society. *Bristol Law Review*, 111-122.

Norris, C., de Hert, P., L'Hoiry, X., & Galleta, A. (2017). *The Unaccoumtable State of Surveillance: Exercising Access Rights in Europe.* Springer International.

P. G. and J. H. v. the United Kingdom, Application No. 44787/98 (ECtHR December 25, 2001).

Perry v. the United Kingdom, Application No. 63737/00 (ECtHR July 17, 2003).

Persinger, A. (2015). Reforming the Foreign Intelligence Surveillance Court to Curb Executive Branch Abuse of Surveillance Techniques. *37 Campbell Law Review*, 519-546.

Propp, K. (2019). US Surveillance on Trial in Europe: Will Transatlantic Digital Commerce be Collateral Damage? *Atlantic Council*, 1-6.

Ram, N., & Gray, D. (2020). Mass Surveillance in the Age of COVID-19. *7 Journal of Law and the Biosciences*, 1-17.

Rapisarda, M. (2016). Privacy, Technology, and Surveillance: NSA Bulk Collection and the End of the Smith v. Maryland Era. *51 Gonzaga Law Review*, 122-158.

Robertson, R. (2017). The Unconstitutionality of Bulk Data Collection. *26 Boston University Public Interest Law Journal*, 151-176.

Robis, L. A. (2014). When Does Public Interest Justify Government Interference and Surveillance. *5 Asia Pacific Journal on Human Rights and the Law*, 203-218.

Roman Zakharov v. Russia, Application No. 47143/06 (ECtHR December 4, 2015).

Romero, A. (2015). Mass E-Mail Surveillance: The Next Battle. *21 Sur - International Journal on Human Rights*, 1-3.

Rona, G., & Aarons, L. (2016). State responsibility to respect, protect and fulfill human rights obligations in cyberspace. *8 Journal of National Security Law & Policy*, 503-530.

Rozenshtein, A. (2018). Surveillance Intermediaries. *70 Stanford Law Review*, 99-189.

S. and Marper , Applications Nos. 30562/04 and 30566/04 (ECtHR December 4, 2008).

Sales, N. (2014). Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy. *10 Journal of law and policy for the information society*, 523.

Schabas, W. (2015). *The European Convention on Human Rights: A Commentary.*

Schoenfeld, G. (2015). In Defense of the American Surveillance State. *63 Drake Law Review*, 1121-1134.

Schweda, S. (2015). UK surveillance under judicial scrutiny: GCHQ intelligence sharing with nsa contravened human rights, but is now legal. *1 The European Data Protection Law Review*, 61-69.

Scott, P. (2017). General Warrants, Thematic Warrants, Bulk Warrants: Property Interference for National Security Purposes. *68 Northern Ireland Legal Quarterly*, 99-121.

Segerstedt-Wiberg and Others v. Sweden , Application No. 62332/00 (ECtHR June 6, 2006).

Setty, S. (2015). Surveillance, Secrecy, and the Search for Meaningful Accountability. *51 Stanford Journal of International Law*, 69-103.

Sicurella, R., & Scalia, V. (2013). Data Mining and Profiling in the Area of Freedom, Security and Justice: State of Play and New Challenges in the Balance between Security and Fundamental Rights Protection. *4 New Journal of European Criminal Law*, 409-460.

Siemion, R. (2015). Protecting Privacy in the Digital Age: Beyond Reforming Bulk Telephone Records Collections. *41 Human Rights Law Review*, 17-20.

Silver and Others v. the United Kingdom, Application Nos. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 (ECtHR March 25, 1983).

Slobogin, C. (2015). Standing and Covert Surveillance. *42 Pepperdine Law Review*, 517-548.

Solove, D. (2004). Reconstructing Electronic Surveillance Law. *72 The George Washington Law Review*, 1701-1747.

Spencer, S. (2013). The Surveillance Society and the Third-Party Privacy Problem. *65 Scottish Constitution Law Review*, 374-410.

Sternberg, R. (1978). Covert Entry in Electronic Surveillance: The Fourth Amendment Requirements. *47 Fordham Law Review*, 203-222.

Swire, P. (2004). The System of Foreign Intelligence Surveillance Law. *72 The George Washington Law Review*, 1307-1372.

Szabó and Vissy v. Hungary, Application No. 37138/14 (ECtHR June 6, 2016).

Tene, O. (2014). A New Harm Matrix for Cybersecurity Surveillance. *12 Colorado Technology Law Journal*, 391-425.

Tokson, M. (2021). Inescapable Surveillance. *106 Cornell Law Review*, 409.

Turanjanin, V. (2020). Video Surveillance of the Employees Between the Right to Privacy and Right to Property After Lopez Ribalda and Others v. Spain. *5 University Bologna Law Review*, 268-293.

Ünever, A., & Kim, G. (2016). *Data Privacy and Surveillance in Turkey: An Assessment of the Draft Law on the Protection of Personal Data.* EDAM.

Ünver, A. (2018). *Politics of Digital Surveillance, National Security and Privacy.* EDAM, Oxford CTGA & Kadir Has University.

Valenzuela Contreras v. Spain, Application No. 27671/95 (ECtHR July 30, 1998).

van der Sloot, B., & Kosta, E. (2019). Big Brother Watch and Others v UK: Lessons from the Latest Strasbourg Ruling on Bulk Surveillance. *5 The European Data Protection Law Review*, 252 - 261.

van Genderen, R. (2017). Privacy and data protection in the age of pervasive technologies in AI and robotics. *3 European Data Protection Law Review*, 338-352.

Vladeck, S. (2014). Standing and Secret Surveillance. *10 A Journal of Law and Policy for the Information Society*, 551-579.

Vogiatzoglou, P. (2018). Centrum for Rattvisa Sweden: Bulk interception of communications by intelligence services in Sweden does not violate the right to privacy. *4 The European Data Protection Law Review*, 563 - 567.

Weber and Saravia v. Germany, Decision as to the Admissibility of Application No. 54394/00 (ECtHR June 29, 2006).

Weber, S. (1971). Habeas Data: The Right of Privacy Versus Computer Surveillance. *5 University of San Francisco Law Review*, 358-377.

Wong, C. (2015). Internet at a Crossroads: How Government Surveillance Threatens How We Communicate. *World report, Human Rights Watch*, 1-13.

Woodburn, N. (2016). NSA Surveillance and Interference with Citizens' Property Rights. *7 Faulkner Law Review*, 287-299.

Yadin, G. (2017). Virtual Reality Surveillance. *35 Cardozo Arts and Entertainment Law Journal*, 709-746.

Yoo, J. (2014). The Legality of the National Security Agency's Bulk Data Surveillance Programs. *10 Journal of Law and Policy for the Information Society*, 901-930.

BULK INTERCEPTIO OF COMMUNICATIONS: ARE WE DROPPING IN TOTALITARIANISM?

Veljko Turanjanin, PhD

Associate professor, Faculty of Law, University of Kragujevac

Emir Ćorović, PhD

Associate professor, State University of Novi Pazar, Department of Law

Abstract: *Authors in this work deal with bulk interception of communications and its relationship with the right to privacy. At the center of the debate are new ECtHR's judgments in cases Big Brother Watch and Others v. the United Kingdom and Centrum för Rättvisa v. Sweden. The ECtHR decided to develop new criteria regarding bulk surveillance because the developed six criteria are more than ten years old. However, this approach may be questionable given the relatively new judgments in the same matter but in which the old approach is taken. This work is divided into several parts. After introductory remarks, the authors briefly explain the main human rights documents regarding the bulk interception of communications and the right to privacy. After that, they explain the approach of the European Court of Human Rights. In the first place, they explain the general principles relating to secret measures of surveillance, including the interception of communications, after which he explains ECtHR's approach in bulk surveillance cases and the ECtHR approach to be followed in bulk interception cases.*

Keywords: *bulk interception, mass surveillance, Big Brother Watch and Others v. the United Kingdom, Centrum för Rättvisa v. Sweden, right to privacy.*