PËR PANOPTIKON QYTETAR

Studim për politikë publike
Baraspeshë më e mirë ndërmjet
mbrojtjes së privatësisë dhe
nevojës për
ndjekjen e komunikimeve

Proektin e finanson Unioni Europian

МРЕЖА 23

"ЖЕНСКА АКЦИЈА"

Shkup, 2017

Асоцијација за унапредување на статусот на жената во современите општествени процеси во Македонија
Associacion for improving the status of women in contemporary social processes in Macedonia
"ЖЕНСКА АКЦИЈА" "WOMEN'S ACTION"

МРЕЖА 23

Studim për politikë publike

PËR PANOPTIKON QYTETAR

Baraspeshë më e mirë ndërmjet mbrojtjes së privatësisë dhe nevojës së ndjekjes së komunikimeve

Shkup, 2017

Projekti “Edhe meta të dhënat janë personale. Si të arrihet një baraspeshë më e mirë ndërmjet privatësisë dhe nevojës së ndjekjes së komunikimeve?” është financuar nga Bashkimi Evropian.

Botues:
„Zhenska akcija“ – asociacion për përparimin e statusit të gruas në proceset bashkëkohore te shoqërisë

Për botuesin:
Dragica Milloshevska

Redaktor:
Aleksandar Nikollov

Autorë:
Aleksandar Nikollov
Dushko Todoroski

Hulumtues:
Mirjana Apostollova
Natasha Najdenova-Leviq
Dragica Milloshevska

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

342.738(497.7)

NIKOLLOV, Aleksandar
Studim për politikë publike për panoptikon qytetar : baraspeshë më e mirë ndërmjet mbrojtjes së privatësisë dhe nevojës së ndjekjes së komunikimeve / Aleksandar Nikollov, Dushko Todoroski. - Shkup : Zhenska akcija, 2017. - 70 стр. ; 25 см

ISBN 978-608-66103-3-3

1. Todoroski, Dushko [автор]
а) Право на приватност - Заштита на лични податоци - Македонија б) Јавна политика - Македонија
COBISS.MK-ID 104194314

Ky publikim qe mundësuar me përkrahje të Bashkimit Evropian në kuadër të projektit Rrjeti 23+ i cili është implementuar nga Instituti për politike evropiane dhe nga Komiteti i Helsinkit për të drejtat e njeriut në Republikën e Maqedonisë. Mendimet e theksuara në këtë publikim janë mendime të autorëve dhe nuk i reflektojnë çdoherë mendimet e Bashkimit Evropian.

PËRMBAJTJA

Përmbledhje ekzekutive

Ku dokument ka për qëllim të inicojë forcimin e respektimit të së drejtës së privatësisë dhe ruajtjes së të dhënave personale gjatë komunikimeve elektronike në Republikën e Maqedonisë, përmes paraqitjes dhe përfaqësimit të rekomandimeve për ndryshime të kornizës juridike dhe mbikëqyrëse në bazë të së drejtës së BE dhe praktikave më të mira nga shtetet anëtare të Bashkimit, në drejtim të përkufizimit të mundësisë për ndjekje masive dhe joselektive të komunikimeve, meta të dhënave dhe përcaktimit të qartë të kompetencave të shërbimeve të të zbulimit dhe organeve hetimore.

Publikimi i "bombave" politike në vitin 2015 të cilat nxorën në pah ndjekjen jolegale të komunikimeve telefonike të elitave të biznesit dhe të politikës , të mediave dhe aktivistëve civilë. Kjo ishte hera e dytë, që nga pavarësia e Maqedonisë- pas aferës "Veshi i madh" në vitin 2000- të zbulohet një përgjim jolegal masiv, që ka cënuar privatësinë, mbrojtjen e të dhënave personale dhe lirinë e shprehjes. Skandalet e këtilla tregojnë keqpërdorime serioze të sistemit shtetërorpër ndjekjen e komunikimeve, më konkretisht, të paisjes dhe personelit të Drejtorisë së sigurisë dhe kundërzbulimit. Komisioni evropian shfaqi brengosje në raportet për Maqedoninë për vitin 2015 dhe 2016 për ndjekjen masive të komunikimeve elektronike ndërsa në Prioritetet urgjente të reformave, vuri në pah reforma serioze që i pret për tejkalimin mangësive në kornizën ligjore për ndjekjen e komunikimeve dhe zbatimin e tyre.

Ligji i komunikimeve elektronike (LKE) i vitit 2014 solli risi në ndjekjen e përmbajtjes së komunikimeve si dhe në ruajtjen masive të të dhënave për qarkullimin e komunikimit të qytetarëve. Ligji mundësoi që Ministria e punëve të brendshme të ketë *qasje të pakufizuar* deri te *të gjitha* komunikimet elektronike të *të gjithë* qytetarëve. Përveç kësaj qe futur obligimi që çdo provajder (ofrues) telefonash dhe interneti t'i ruajnë të ashtuquajturat "meta të dhënash" për të gjithë shfrytëzuesit, për një vjet. Dispozitat për ruajtje masive të të dhënave ishin të arsyetuara si transponim të Direktivës 2006/24/BE, e cila qe hequr nga Gjykata Evropiane e drejtësisë menjëherë pas miratimit të LKE. Megjithatë, Republika e Maqedonisë ende nuk ka marrë masa adekuate me qëllim që t'i tejkalojë sfidat serioze të imponuara nga situata e këtillë.

Duke i pasur parasysh sfidat e detektuara, autorët propozojnë më shumë rekomandime të cilat duhet të mundësojnë që në vend të panoptikonit- sistem , në të cilin qytetarët janë të friksuar sepse janë nën mbikëqyrje të vazhdueshme nga pushteti- në Maqedoni të ndërtohet panoptikon qytetar- sistem në të cilin transparenca krijon llogaridhënie te bartësit e pushtetit ndaj qytetarëve. Rekomandimet janë dhënë të detajuara nën titullin përkatës në këtë studim, e në vazhdim janë dhënë shkurtimisht:

- Të hiqen nenet 176-178 të Ligjit të komunikimeve elektronike të cilat e përshkruajnë ruajtjen e meta të dhënave, për shkak të heqjes, nga ana e Gjykatës evropiane të drejtësisë, të Direktivës 2006/24/BE, e cila është transpozuar në këtë ligj. Ndjekja dhe qasja në meta të dhënat për komunikimet elektronike të përfshihen në Ligjin për ndjekjen e komunikimeve.

- Të rishqyrtohet arsyeshmëria e lejimit të ndjekjes së komunikimeve, për një gamë aq të gjerë të veprave penale, në bazë të vlerësimit – a është vallë cënimi i privatësisë në përputhshmëri me peshën e veprës penale, për të cilën bëhet fjalë, dhe me dëshmitë që pritet të grumbullohen me masat e veçanta hetuese, përkatësisht me ndjekjen e komunikimeve.
- Të pamundësohet qasje e drejtpërdrejtë në përmbajtjen e komunikimeve nga ana e shërbimeve, përkatësisht, organet kompetente, paraprakisht, do të duhet ta njoftojnë operatorin dhe të dorëzojnë urdhërgjykate për ndjekje, e pastaj operatori ta mundësojë qasjen në komunikimet e personave të përfshirë.
- Në kërkesën për ndjekjen e komunikimeve duhet theksuar dhe arsyetuar dyshimi i bazuar për kryerje të mundshme të një vepre penale ose për veprën penale tani më të kryer, e jo vetëm baza për dyshim, si shkallë shumë e ulët e dyshimit.
- Të futet edhe një palë në procedurën për lejimin e ndjekjes së komunikimeve, që do t'i përfaqësojë interesat e personave, komunikimet e të cilëve propozohet që të ndiqen (për shembull panel ekspertësh, përfaqësues i Drejtorisë për mbrojtjen e të dhënave personale ose Avokati i popullit). Kjo palë të ketë të drejtë ankese në kërkesën për ndjekjen e komunikimeve, si dhe në urdhërat për ndjekjen e komunikimeve, nëse konsideron se me këtë bëhet shkelje e pa arsyeshme e privatësisë dhe të dhënave personale të qytetarëve.
- Të rishqyrtohet arsyeshmëria e afateve të përcaktuara të gjata maksimale për ndjekjen e komunikimeve.
- Të bëhet ndarja ligjore e kompetencës dhe rregullave të ndjekjes së komunikimeve gjatë hetimeve penale nga ato që kanë karakter sigurie dhe të kundërzbulimit.
- Të forcohet kontrolli i brendshëm në MPB që kryejë kontroll edhe në rastet kur është keqpërdorur autorizimi për ndjekjen e komunikimeve.
- Nëse me ndjekjen e komunikimeve fitohen njohuri të cilat implikojnë persona të tjerë në veprat penale, ose, me të cila, konfirmohen bazat për vepra të tjera penale, ndryshe nga ato, për të cilat ka të bëjë urdhëresa e vazhdueshme për ndjekjen e komunikimeve, të jetë e nevojshme dhënia e urdhëresës së re nga gjykatësi që të vazhdojë ndjekja e komunikimeve dhe që regjistrimet nga ato komunikime të mund të përdoren në gjyq.
- Të parashikohet pasja e kujdesit për kategoritë e veçanta të të dhënave personale (të përcaktuara me Ligjin për mbrojtjen e të dhënave personale), përkatësisht, gjatë ndjekjes së komunikimeve, të përjashtohen ose të fshihen deklarime të lidhura me këto të dhëna.
- Të futet obligimi që personat e prekur të informohen për masat e veçanta hetuese pas ndërprerjes së tyre, përveç kur mund të dëshmohet se kjo do të ndikonte në pengimin ose prejudikimin e ndjekjes penale.
- Të sigurohen *mjete juridike* efektive që mund të përdoren në rastet kur ndonjë person i caktuar konsideron se i janë shkelur të drejtat me ndjekjen e komunikimeve nga ana e organeve kompetente. Organizata relevante jofitimprurëse të fitojnë të drejtën ligjore që të mund të paraqesin ankesa dhe t'i përfaqësojnë personat e prekur nga ndjekja e komunikimeve.
- Të forcohen dispozitat ligjore për sigurinë e të dhënave nga ndjekja e komunikimeve dhe për asgjësimin e tyre, në rastet kur ata nuk janë më të nevojshme për qëllimin për të cilin janë grumbulluar.
- Të sigurohet mundësia që mbikëqyrje së pa paralajmëruar të ketë çdo anëtar i koisioneve kompetente kuvendore, të shoqëruar nga persona profesionistë të komisioneve, me ç'rast do të kishin qasje edhe në të dhënat e grumbulluara për ndjekjen e komunikimeve

deri te emrat e njerëzve dhe arsyet pse ndiqen. Përveç kësaj, të miratohet rregullore që do të sigurojë zhvillim efikas të procedurës për të fituar certifikatë sigurie anëtarët e komisioneve mbikëqyrëse kuvendore.

- Të formohet komision qytetarësh për mbikëqyrje të ndjekjes së komunikimeve, të cilin do ta emëronte Kuvendi nga radhët e ekspertëve dhe përfaqësuesve të shoqërisë civile.
- Të zgjerohet obligimi i informimit edhe te gjykatat edhe te operatorët e telekomunikimit, lidhur me kërkesat dhe urdhëresat për ndjekjen e komunikimeve. Raportet e prokurorit publik t'i përmbajnë të gjitha elementet e përshkruara, përfshirë këtu edhe atë për shpenzimet dhe arsyetimin në rastet kur masat nuk i kanë dhënë rezultatet e pritura dhe të shpallen më së voni deri në fund të shkurtit në vitin vijues, për vitin paraprak. Raportet të përmbajnë edhe pasqyrën e kërkesave të miratuara, të modifikuara ose të refuzuara për ndjekjen e komunikimeve, numrin e lëndëve të ndjekuratë veprës penale, numrin e kërkesave për sigurimin e meta të dhënave nga provajderë të huaj të shërbimeve të internetit, numrin e shënimeve të asgjësuara nga masat e veçanta hetimore.
- Dhënësit e shërbimeve elektronike të komunikimeve të kenë obligim për disejn të orientuar kah privatësia, përkatësisht masat teknike dhe arganizative që sigurojnë mbrojtje të të dhënave personale, t' i parashikojnë qysh gjatë disejnimit të sistemeve, e jo pastaj. Organet kompetente të kryejnë kontrolle të rregullta te operatorët për qasjen dhe përpunimin e të dhënave përqarkullimin e komunikimeve dhe të dhënave për vendndodhjen e parapaguesve.
- Në ligjin për ndjekjen e komunikimeve të përfshihen dispozita ndëshkimore për organet kompetente dhe njerëzit përgjegjës në to.
- Të zhvillohet fushatë për ngritjen e vetëdijes së qytetarëve rreth rreziqeve gjatë komunikimeve elektronike, si dhe të drejtave të tyre për mbrojtjen e privatësisë dhe të dhënave personale gjatë komunikimit.
- Të forcohet profesionalizmi dhe etika te prokurorët publikë, gjykatësit, si dhe të sigurohet mbështetje e jashtme për implementimin e standardeve dhe për trajnimin dhe specializimin e prokurorëve publikë dhe gjykatësve në fushën e ndjekjes së komunikimeve, privatësisë dhe mbrojtjes së të dhënave personale.

Hyrje

Panoptikoni është simbol i shoqërisë bashkëkohore, në të cilën ndjekja e komunikimeve është aq e përhapur, sa që njerëzit parapëlqejnë vetëcensurën dhe frikohen të thonë diçka që ndryshon nga mendimi dominant, ose nga ajo që është korrektësi politike. Ky nocion rrjedh nga një qasje arqitekturore e shekullit të 19, që mundëson mbikëqyrje të lehtë mbi njerëzit. Te arqitektura e panoptikonit, njerëzit të cilët janë objekt mbikëqyrjeje, për shembull, të burgosur, pacientë, fëmijë ose punëtorë, janë vendosur në dhoma që kanë qenë të shpërndara rreth kullës qendrore, që ka qenë e mbikëqyrësit. Kulla i ndriçon të gjitha dhomat për rreth, që të mundet mbikëqyrësi të shohë se çfarë bëjnë të gjithë. Por, kulla është e bërë asisoj që njerëzit nuk mund të shohin a është ndokush në të. Ata. megjithatë, kanë ndjenjën se dikush i vëzhgon vazhdimisht, dhe mundohen të jenë "të disiplinuar" dhe "shembullorë".

Fjala panoptikon rrjedh nga fjala e vjetër greke **panoptis** *, që do të thotë ai që shikon çdo gjë. Në mitologjinë e vjetër greke Argus Panoptis ka qenë kolos i cili ka pasur shumë sy dhe nuk ka fjetur asnjëherë. Hera, bashkëshortja e Zeusit, e ka detyruar që të kujdeset për nimfën Ija, për të cilën ka dyshuar se është dashnore e Zeusit.*

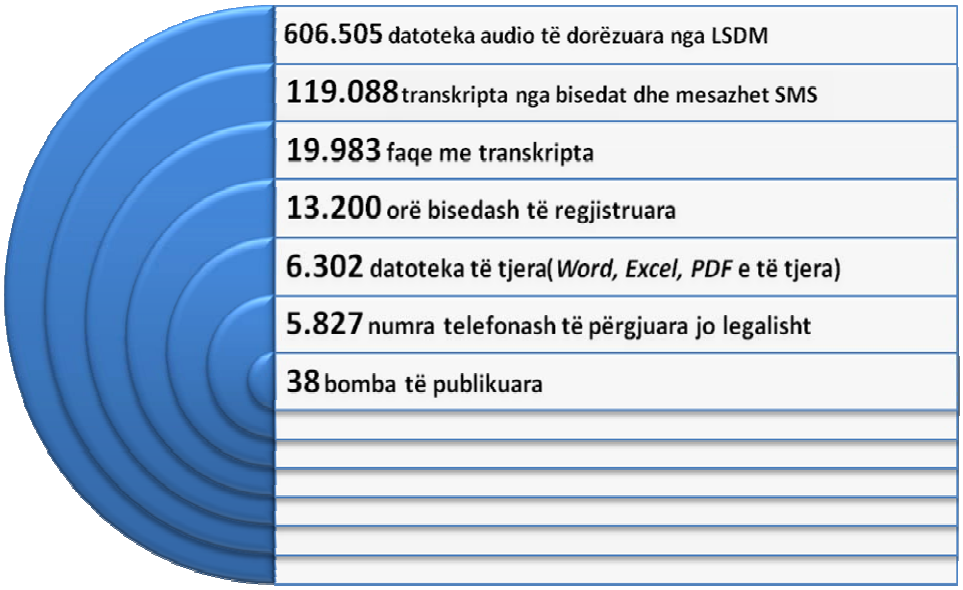
Edvard Snouden[1] dhe Vikiliks[2] treguan se panoptikoni ekziston, duke zbuluar programe globale për ndjekje masive të komunikimeve telefonike, të internetit dhe të radio komunikimeve. Objekt i kësaj ndjekjeje të gjerë të komunikimeve nuk është vetëm përmbajtja e komunikimeve, por edhe e të ashtuquajturave meta të dhëna, përkatësisht të dhënave për atë se me kë, kur dhe sa shpesh komunikojmë si dhe me çfarë pajisjesh dhe nga cilat vendndodhje. Mossuksesi i shteteve dhe i pushteteteve mbinacionale që të sigurojnë mbrojtje adekuate të privatësisë dhe të dhënave personale të shfryt[zuesve të komunikimeve elektronike, rezultoi me atë që gjashtëdhjetë përqind e evropianëve të mos kenë besim në kompanitë e telekomunikimit dhe në provajderët e internetit, ndërsa shtatëdhjetë përqind të jenë të brengosur se të dhënat e tyre të përdoren për qëllime krejtësisht tjera, nga ato për të cilat grumbullohen.[3]

Në Maqedoni, ndjenja se jetojmë në panoptikon ishte përforcuar edhe më shumë në vitin 2015 me publikimin e "bombave" të cilat vunë në dukje ndjekjen jolegale të komunikimeve telefonike të elitave politike dhe të biznesit, mediave dhe aktivistëve qytetar në periudhën prej vitit 2008 deri në 2015.[4] Kjo është hera e dytë që, pas aferës "Veshi i

[1] https://edwardsnowden.com/revelations/
[2] https://wikileaks.org/
[3] Raport i "Dojçe Telekom" për privatësinë dhe sigurinë e të dhënave, 2015. I disponueshëm në: https://www.telekom.com/resource/blob/323750/a7b17936956c92c23c07f433084e21d6/dl-report-datasecurity-2015-data.pdf
[4] Periudha kohore në të cilën është zhvilluar ndjekja joligjore e komunikimeve është përcaktuar në Ligjin për mbrojtjen e privatësisë ("gazeta zyrtare e Republikës së Maqedonisë" nr. 196/2015). "Bombat" janë të disponueshme në: http://vistinomer.mk/të gjitha bisedat e përgjuara të publikuara nga opozita – transkripte video-audio/.

madh" të vitit 2000, të zbulohet përgjim jolegal masiv, që ka cënuar privatësinë, mbrojtjen e të dhënave personale dhe lirinë e shprehjes. Efekti i vetëcenzurës, karakteristikë e panoptikonit, akceptohet edhe në Maqedoni, dhe u bë gjë normale që njerëzit, gjatë bisedave telefonike, t'i tërheqin vërejtje bashkëbiseduesit që të ketë kujdes për gjithë atë që flet dhe që e zbulon.

Grafikon: Bombat e LSDM në shifra[5]



Ndonëse pushteti dhe opozita kishin sqarime të ndryshme rreth motiveve dhe aktorëve që shpien deri te përgjimi i cili ishte publikuar me "bombat", si dhe rreth kanaleve përmes të cilave u derdhën këta të dhëna personale, edhe të parët edhe të dytët u pajtuan se është keqpërdorur edhe sistemi shtetëror për ndjekjen e komunikimeve, më konkretisht pajisja dhe personeli i Drejtorisë së sigurisë dhe kundërzbulimit.[6] Dhe, diçka plotësuese, fakti që nga sistemi dolën dokumente me komunikimet e ndjekura, është i mjaftueshëm që të konkludohet se nuk ekzistojnë standarde adekuate , procedura dhe mekanizma mbrojtës për siguri informatike.

[5] Raport për aktivitetet e Prokurorisë publike speciale për periudhën prej 15.09.2016 deri në 15.03.2017, i disponueshëm në http://www.jonsk.mk/wp-content/uploads/2017/03/6-MESECEN-IZVESTAJ.pdf; Raport i aktiviteteve të Prokurorisë publike speciale për periudhën prej 15.09.2015 deri në 15.03.2016 i disponueshëm në http://www.jonsk.mk/wp-content/uploads/2016/03/izvestaj-konecen-zaklucen.docx; „PPS përfundimisht hyri në Telekom", SDK.MK, 24.04.2017, i disponueshëm në http://sdk.mk/index.php/makedonija/sjo-konechno-vleze-vo-telekom/.

[6] VMRO-DPMNE pohonte që ndjekja e komunikimeve ishte kryer në disa mënyra. Përpos keqpërdorimit të pajisjes të DSK, kinse përmes bashkëpunëtorëve të një shërbimi të zbulimit, ish kryeministri Gruevski në deklaratën e dhënë më datë 25.02.2015 theksoi se "përgjimi dhe regjistrimi jolegal i bisedave telefonike" ishte kryer nga ana e kryerësve të pa njohur me përdorimin e pajisjes mobile vendndodhja e së cilës qe ndryshuar vazhdimisht, dhe e cila funksionon sipas parimit të klonimit të të ashtuquajturave stacione bazike të operatorëve të rrjeteve të komunikimit mobil. " Si ka funksonuar skema e përgjimit në "Puç"?", TV Alfa, , 26.02.2015, e disponueshme në:http://www.alfa.mk/News.aspx?id=90130.

Ekzistojnë edhe probleme të tjera në privatësinë e komunikimeve elektronike. Ligji i komunikimeve elektronike (LKE) i vitit 2014[7] futi mbajtjen masive të të dhënave për qarkullimin telekomunikativ të qytetatëve. Pa ndonjë diskutim të rëndësishëm në opinion, u imponua obligimi që të gjithë provajderët telefonik dhe të internetit, për të gjithë shfrytëzuesit e vet, t'i mbajnë një vit të ashtuaujturat "meta të dhëna", dhe pas kërkesës nga organet e shtetit, t'ua dorëzojnë atyre. Këtu bëjnë pjesë këto të dhëna për shërbimet telefonike dhe të internetit (duke përfshirë edhe e-postën): emri dhe adresa e personave që komunikojnë, numri i telefonit ose IP adresa e pajisjes elektronike me të cilën bëhet komunikimi, pajisja telefonike dhe vendndodhja gjeografike e personave që komunikojnë; koha e fillimit dhe e mbarimit të komunikimit; lloji i shërbimit telefonik ose të internetit. Dispozitat për mbajtjen masive të të dhënave ishin të arsyetuara si transpozim të Direktivës 2006/24/BE[8], e cila qe hequr[9] nga Gjykata evropiane e drejtësisë, menjëherë pas miratimit të ligjit të ri në Maqedoni

Në mënyrë plotësuese, LKE i vitit 2014 mundësoi që Ministria e punëve të brendshme të ketë qasje *të drejtpërdrejtë dhe të pakufizuar* në përmbajtjen e *të gjitha* komunikimeve elektronike *të të gjithë qytetarëve.* Sipas vendimit të vjetër ligjor, operatorët mundësonin qasje në përmbajtjen e komunikimeve të një shfrytëzuesi *të caktuar* vetëm në bazë të urdhëresës së gjykatës kompetente.

Jotransparenca nga ana e Prokurorisë publike për efektet e ndjekjes së komunikimeve si dhe mospunimi dhe mospasja qasje në të dhënat relevante të Komisionit kuvendor për mbikëqyrjetë ndjekjes së komunikimeve dhe Komisionit për mbikëqyrje të punës së shërbimeve të zbulimit dhe kundërzbulimit, edhe më shumë i shton rreziqet e keqpërdorimit të sistemit për ndjekjen e komunikimeve, përfshirë edhe meta të dhënat e ruajtura për komunikimet e shfrytëzuesve të shërbimeve lektronike.

Në vend të lirisë së shprehjes- vetëcenzurë dhe izolim

Hulumtimi ndërkombëtar i vitit 2014 i Pen qendrës amerikane, tregoi se shkrimtarët, nën presionin e frikës nga ndjekja masive e komunikimeve, parapëlqenin vetëcenzurën. Varësisht nga vendi, për shkak të një frike të këtillë ndërmjet 34% dhe 61% e shkrimtarëve i shmangeshin të folurit ose të shkruarit në temë të caktuar, ose mendoheshin seriozisht që ta bëjnë këtë. Ndërmjet një të katërtës dhe dy të tretave të shkrimtarëve kishin filluar që tu ikin qëllimisht temave të caktuara në komunikim telefonik ose përmes mejl-it, që tu largohen rrjetave sociale ose të përmbahen nga kërkimet e caktuara në internet ose të vizitojnë veb-faqet të cilat do të mund të llogariteshin si kontraverze dhe të dyshimta. Efekti i panoptikonit ka ndikuar që, madje edhe shkrimtarët – nga të cilët do të priteshte që si intelektuale të kenë tendenca progresive dhe liberale- të heqin dorë nga një pjesë e identitetit të tyre , qëndrimeve dhe lirive të tyre.

P

[7] „Gazeta zurtare e Republikës së Maqedonisë" numër 39/14, 188/14 dhe 44/15.

[8] E disponueshme në: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

[9] Aktgjykimi i Gjykatës evropiane të drejtësisë. I disponueshëm në: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

Ky studim i analizon mangësitë ligjore, teknike, institucionale dhe edukative që rezultojnë me cënim masiv të privatësisë dhe mbrojtjes së të dhënave personale gjatë komunikimeve elektronike në Maqedoni. Situatat e këtilla kanë ndikim të fuqishëm negativ ndaj tërë shoqërisë përmes:

- **Keqpërdorimit të institucioneve për realizimin e interesit privat në vend të atij publik.** „Bombat“ treguan se Drejtoria e sigurisë dhe kundërzbulimit, operatorët e rrjeteve publike të komunikimit dhe funksionarët mund ta cënojnë lehtë privatësinë e qytetarëve dhe t'i keqpërdorin të dhënat e tyre personale për të realizuar favor personal ose grupor që është në kundërshtim me interesin publik.
- **Keqsimit të besimit në institucione.** Zbulimi i ndjekjes masive dhe jolegale të komunikimeve e gërryen besimin e publikut në organet e sigurimit, në sundimin e së drejtës dhe shtetin juridik.
- **Rrezikimit të demokracisë.** Ndjekja masive dhe, shpeshherë jolegale, e komunikimeve e rrezikon edhe lirinë e shprehjes dhe shpie në paraqitjen e vetëcenzurës te qytetarët, ose në terheqjen e tyre nga jeta publike. Ekziston rreziku i presionit ndaj opozitës, funksionarëve individualë ose i arritjes së një përparsie jo të drejtë të politikanëve të caktuar dhe partive politike kundrejt të tjerëve.
- **Shtimit të rreziqeve të sigurisë.** Funksionarët dhe politikanët të cilët kanë urdhëruar përgjim jolegal ose masiv ose të cilët kanë qenë viktima të së njëjtës, mundet lehtë të jenë të kompromituar në publik me qëllim të krijimit të krrizës, ose, mund të bëhen objekt shantazhimi. Përveç kësaj, resurset e mëdha të nevojshme për ndkeje masive të komunikimeve, krijojnë rrezik se nuk do të mbeten resurse të mjaftueshme për funksionimin optimal të segmenteve të tjera të sistemit të sigurimit. Nga ana tjetër, besimi i humbur i publikut krijon rrezik sigurie se do të vështirësohet bashkëpunimi i organeve të sigurimit me qytetarët.
- **Rritjes së rreziqeve ekonomike**. Keqpërdorimi i sistemit për ndjekjen e komunikimeve për spiunim industrial dhe për realizimin e interesave të biznesit personal dhe familjar mund ti destimulojë investimet private dhe ta çrregullojë konkurencën e tregut.

Sëkëndejmi, Komisioni evropian shfaqi brengosjen në raportet për Maqedoninë për vitin 2015 dhe 2016 për ndjekjen masive të komunikimeve elektronike, kurse në Prioritetet urgjente të reformave, vuri në pah edhe reformat serioze që i pret, për tejkalimin e mangësive në kornizën ligjore për ndjekjen e komunikimeve dhe zbatimin e tyre.

Ky dokument ka për qëllim të inicojë forcimin e respektimit të së drejtës së privatësisë dhe mbrojtjen e të dhënave personale gjatë komunikimeve elektronike, përmes përfaqësimit dhe avokomit të rekomandimeve për ndryshimin e kornizës ligjore dhe mbikëqyrëse, në bazë të legjislacionit të BE dhe praktikave më të mira nga shtetet anëtare të Bashkimit, në drejtim të kufizimit të mundësisë për ndjekje masive dhe joselektivetë komunikimeve dhe meta të dhënave. Autorët shpresojnë se në këtë mënyrë do të kontribuojnë që në vend të panoptikonit, në shoqërinë tonë të ndërtohet panoptikon qytetar.

Panoptikoni qytetar është ideal për një sistem krejtësisht më të ndryshëm, në të cilin transparenca krijon llogaridhënie te bartësit e pushtetit. Në mënyrë metaforike, te arqitektura e panoptikonit qytetar, çdonjëri që ushtron funksion publik është i vendosur në një lokal të hapur dhe është i rrethuar nga qytetarë, të cilët e vështrojnë me vëmendje se çfarë bën funksionari dhe i shtrojnë pyetje.

Metodologjia

Ishte zbatuar një analizë e të dhënave nga burime sekondare për gjendjen me mbrojtjen e privatësisë dhe të dhënave personale gjatë të dhënave elektronike, e cila përmban një përmbledhje ndërkombëtare me fokusim në legjislativën e BE dhe përmbledhje të gjendjes në këtë sferë në Maqedoni. Analiza ndërkomëtare krahasuese e mbrojtjes së privatësisë dhe të dhënave personale gjatë komunikimeve elektronike fokusohet në legjislativën e BE, në standarde të tjera evropiane, në vendimet relevante gjyqësore dhe zbatimin e tyre në shtete të caktuara anëtare. Ishin veçuar edhe praktikat më të mira nga shtetet anëtare të Bashkimit.

Analiza e gjendjes në sferën e mbrojtjes së privatësisë dhe të dhënave personale në komunikimet elektronike në Maqedoni, nga aspekti i ndjekjes së komunikimeve, ishte përgatitur përmes hulumtimit të dokumenteve ekzistuese dhe intervistave. Ekipi i projektit e analizoi kornizën ligjore të vendit, me të cilën rregullohet mbrojtja e privatësisë dhe të dhënave personale gjatë komunikimeve elektronike si dhe analliza dhe studime të tjera ekzistuese në këtë temë që i përkasin gjendjes në Maqedoni, me theks në mbajtjen e meta të dhënave. Analiza e dokumenteve ishte plotësuar me takime me përfaqësues të shumë institucioneve kompetente, midis të cilave edhe të Drejtorisë për mbrojtjen e të dhënave personale, Prokurorisë së lartë publike, Gjykatës kushtetuese, Fakultetit të sigurisë në Shkup, Avokatit të popullit dhe Agjencisë për komunikime elektronike (shih "Aneks- listën e përfaqësuesve të intervistuar të institucioneve dhe të ekspertëve"). Gjithashtu, ishin zhvilluar biseda edhe me fuish funksionarë të MPB dhe të Drejtorisë së sigurisë dhe kundërzbulimit, komisioneve të Kuvendit për mbikëqyrje të ndjekjes së komunikimeve dhe për mbikëqyrje të shërbimeve, ish deputetë të Kuvendit, si dhe me ekspertë të tjerë të pavarur të kësaj fushe.

Një vlerë shtesë të dokumentit janë rekomandimet konkrete për përmirësimin e gjendjes së përgjithshme me mbrojtjen e privatësisë dhe të dhënave personale- duke përfshirë edhe meta të dhënat gjatë komunikimeve elektronike në Maqedoni, si dhe përkufizimi i kompetencave të shërbimeve të zbulimit dhe organeve hetimore..

Përkufizimi, të cilin e hasën autorët është ndjeshmëria e temës, për ç'arsye nuk kishin mundësi t'i sigurojnë të gjitha informatat e nevojshme nga institucionet kompetente dhe nga bashkëbiseduesit. Kufizim shtesë ishte fakti që Bashkimi Evropian, gjatë analizës, ishte në proces të ndryshimit të dukshëm të legjislativës nga sfera e mbrojtjes së të dhënave personale , duke përfshirë edhe ato gjatë komunikimeve elektronike, si dhe në polici dhe në gjyqësor, i cili nuk përfundoi tërësisht deri në botimin e këtij publikimi. Në rastet kur ka të miratuara akte të reja ligjore të Bashkimit, studimi u referohet atyre, bile edhe kur ende nuk kanë hyrë në fuqi.

Studimi nuk merret drejtpërdrejtë me rreziqet e cënimit të privatësisë së qytetarëve nga kapja e komunikimeve dhe e të dhënave personale nga shërbimet e huaja ose nga bartja e të dhënave ndërmjet shteteve. Dokumenti, gjithashtu, nuk analizon se si të arrihet baraspesha ndërmjet mbrojtjes së privatësisë së personave publikë, nga njëra anë, dhe interesit publik që të jenë të njohura aktivitetet dhe qëndrimet e tyre, nga ana tjetër.

Analizë juridike e standardeve kyçe evropiane për mbrojtjen e privatësisë dhe të dhënave personale gjatë komunikimeve elektronike

Në këtë pjesë i referohemi kornizës ligjore të vendosur nga Këshilli i Evropës dhe Bashkimi Evropian.

Gjatë mbrojtjes së privatësisë, vendet evropiane, si anëtare të Këshillit të Evropës, janë të obliguara tu përmbahen detyrimeve ligjore, të cilat dalin nga Konventa Evropiane për mbrojtjen e të drejtave të njeriut dhe lirive themelore dhe nga Konventa për mbrojtjen e personave përkitazi me përpunimin automatik të të dhënave personale.

Sipas **Konventës evropian për të drejtat e njeriut,** "çdo njeri gëzon të drejtën e respektimit të jetës së tij private dhe familjare, shtëpisë dhe korrespondencës".[10] Konceptet e jetës private dhe korrespondencës i përfshijnë edhe të dhënat telefonike dhe telekomunikative.[11] Vendimet e Gjykatës evropiane për të drejtat e njeriut vënë në pah që mbrojtja e kësaj të drejte themelore e përfshin, jo vetëm përmbajtjen e komunikimeve, por edhe meta të dhënat për komunikimin e realizuar. Këtu, për shembull, bëjnë pjesë "data dhe kohëzgjatja e bisedave"dhe numrat telefonik që kërkohen, sepse të dhënat e tilla janë "pjesë përbërëse e komunikimeve përmes telefonit".[12] Konventa e parashikon edhe *të drejtën e informimit* të individit, për të cilin grumbullohen të dhënat, dhe, nëse është e nevojshme, edhe *të drejtën e korrigjimit të tyre.*

Sipas nenit 8, paragrafi 2 të Konventës, përzierja e pushtetit publik në realizimin e të drejtës së jetës private, mund të jetë e lejuar vetëm nëse ajo përzierje është e paraparë me ligj dhe nëse paraqet masë e cila është në interes të sigurisë shtetërore dhe asaj publike, mirëqenies ekonomike të vendit, mbrojtjes së rendit si dhe të pengimit të veprave penale, mbrojtjes së shëndetit dhe moralit ose mbrojtjes së të drejtave dhe lirive të të tjerëve. Sipas Gjykatës evropiane për të drejtat e njeriut, përzierja e tillë mund të konsiderohet si e arsyeshme vetëm nëse është e *domosdoshme*, nëse u përgjigjet *nevojave urgjente të shoqërisë*, nëse është *proporcional* me qëllimin për të cilin ndërmerret dhe nëse shkaqet, të cilat ceken nga autoritetet publike për tu arsyetuar ajo, janë *relevante dhe të mjaftueshme*.[13]Si ilustrim, në rastin e Meloun (Malone) kundër Mbretërisë së Bashkuar , gjykata ka verifikuar që ruajtja masive dhe joselektive e gjurmëve të gishtërinjve dhe të dhënave të DNA-s të personave të cilët janë të dyshuar por jo edhe të dënuar, nuk është e arsyeshme sipas nenit 8, paragrafi 2 të Konventës. Ndërkaq, në kontekstin e Bashkimit Evropian, Gjykata e drejtësisë e Bashkimit Evropian, ka vënë në dukje edhe atë që për përzierjen e autoriteteve në jetën private të llogaritet si *proporcionale me qëllimin për të cilin ndërmerret*, duhet të demonstrohet që nuk janë të disponueshme metoda të tjera, më pak intruzive.[14]

Konventa e Këshillit të Evropës për mbrojtjen e personave përkitazi me përpunimin automatik të të dhënave personale, që është ratifikuar edhe nga Republika e Maqedonisë, synon drejt mbrojtjes së të drejtave dhe lirive themelore të individëve, e veçanërisht të

[10] Neni 8, paragrafi 1 nga Konventa.

[11]Shihni ECtHR, Klass et al, 6 shtator 1978, pas. 41.

[12]Shihni ECtHR, Malone v. the United Kingdom, 2 gusht 1984, pas. 84.

[13]Shihni ECtHR, S. and Marper v. the UK, 4 dhjetor 2008, pas. 101.

[14]Shikoni CJEU, Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, 9 nëntor 2010, pas. 81.

drejtës së tyre për privatësi në lidhje me përpunimin automatik të të dhënave personale në sektorin publik dhe atë privat. Konventa është instrumenti i parë ndërkombëtarisht detyrues që i mbron individët nga keqpërdorimet të cilat mund të paraqiten gjatë grumbillimit dhe përpunimit të të dhënave personale. Përpunimi i të dhënave me fjalë të thjeshta mund të definohet si çdo gjë që mund të bëhet me të dhënat, për shembull, grumbullimi, ruajtja ose fshirja e tyre.

Neni 5 i Konventës përcakton që të dhënat personale në procesin e përpunimit të automatizuar duhet të jenë: a)të grumbulluara dhe të përpunuara ndrshmërisht dhe ligjërisht; b)të ruajtura për qëllime konkrete dhe legjitime dhe nuk do të përdoren për qëllime që nuk janë të përputhshme; c)adekuate, relevante dhe jo të tepruara përkitazi me qëllimet për të cilat janë ruajtur; ç) të sakta, dhe nëse e do nevoja, të përditësuara; d)të ruajtura në formën që lejon identifikimin e të dhënave jo më gjatë se që është e nevojshme për qëllimet për të cilat janë ruajtur. Në përputhje me këtë Konventë, duhet ndërmarrë masa adekuate sigurie për mbrojtjen e të dhënave personale , të ruajtura në baza të automatizuara të dhënash, kundër asgjësimit të rastësishëm ose të paatorizuar, humbjes ë rastësishme si dhe kundër qasjes së paautorizuar, ndryshimit dhe shpërndarjes.[15] Konventa e ndalon përpunimin automatik *të të dhënave personale të ndjeshme* – siç janë ato për prejardhjen etnike dhe racore, për bindjet politike apo religjioze, për shendetin, jetën seksuale ose të dhënat për dënime për vepra penale – nëse legjislativa nacionale nuk ka vendosur mekanizma adekuate mbrojtëse. [16] Konventa, gjithashtu, vendos të drejtën e individit që të mund të kuptojë se janë ruajtur të dhëna për të, ta kuptojë qëllimin për çka janë ruajtur, përmbajtjen dhe, nëse është e nevojshme, të mund të sigurojë korrigjimin ose fshirjen e tyre, nëse janë përpunuar në kundërshtim me legjislacionit kombëtar.[17] Përjashtime nga dispozitat për mbrojtjen e të dhënave personale mund të ketë vetëm nëse janë të lejuara me legjislacionin, kombëtar dhe nëse paraqesin masë të domosdoshme në një shoqëri demokratike, e në interes të mbrojtjes së sigurisë shtetërore , sigurisë publike, të interesave monetare të shtetit, pengimit të kryerjes së veprave penale ose mbrojtjes së subjekteve të të dhënave ose të drejtave dhe lirive të të tjerëve.[18]

Komisioni i Venedikut[19] ka krijuar një **Listë kontrolli të sundimit të ligjit,** që duhet të shërbejë si instrument për vlerësimin e sundimit të ligjit në një vend të caktuar nga aspekti i strukturave të tij kushtetuese dhe ligjore, legjislacionit dhe praktikën ekzistuese ligjore.[20] Ndonëse nuk është akt ligjor, ky dokument është i rëndësishëm sepse në mënyrë koncize i ekspozon kriteret sipas të cilave mund të vlerësohet sundimi i ligjit në një vend, duke përfshirë edhe aspektin e ndjekjes së komunikimeve. Sipas Listës, ndjekja e komunikimeve mundet ta cënojë seriozisht të drejtën e privatësisë, prandaj është me rëndësi thelbësore që të mos i lejojë shtetit forcë të pakufizuar që ta kontrollojë jetën e individëve. Për këtë qëllim, ndjekja e komunikimeve duhet të jetë e kufizuar me parime, si për shembull, parimi i proporcionalitetit. Është e nejoshme të ekzistojnë edhe kontrolle procedurale dhe

[15] Neni 7 i Konventës.
[16] Neni 6 i Konventës.
[17] Neni 8 i Konventës.
[18] Neni 9 i Konventës.
[19] Komisioni Evropian për demokraci ligjërisht është trup këshilldhënës i Këshillt të Evropës për ndihmë dhe këshillim të shteteve individuale, anëtare, në çështje kushtetuese, me qëllim që të përparohet funksionimi i institucioneve demokratike dhe mbrojtja e të drejtave të njeriut. .
[20] Alista është e disponueshme në http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)007-e

mbikëqyrje, përfshirë edhe dhënien e autorizimit nga ana e gjykatësit ose një trupi të pavarur, bile edhe në rastet e ndjekjes së të dhënave për trafikun telekomunikativ të një personi konkret , përkatësisht meta të dhënave. Përveç kësaj, është e nevojshme të ekzistojnë mjete efektive ligjore që mund të përdoren në rastet kur një person i caktuar konsideron se i janë shkelur të drejtat. Dokumenti bën një saktësim të rëndësishëm që edhe grumbullimi i meta të dhënave për komunikime elektronike, paraqet ndjekje të komunikimeve. Me këtë do të kufizohej grumbillimi, ruajtja dhe shpërndarja e të dhënave të grumbulluara- përfshirë edhe rastet në bazë të parimit të proporcionalitetit.

Në Bashkimin Evropian, e drejta e privatësisë dhe mbrojtjes së të dhënave personale jynë dy të drejta të ndryshme të njeriut të mbrojtura me **Marrëveshjen për funksionimin e Bashkimit Evropian dhe me Kartën e Bashkimit Evropian për të drejtat themelore,** si dhe nga sistemi ligjor i 28 vendeve anëtare të BE.

Sipas **Marrëveshjes për funksionimin e Bashkimit Evropian**[21], çdokush gëzon të drejtën e mbrojtjes së të dhënave personale. Neni 16 i Marrëveshjes vë në dukje se Parlamenti dhe Këshilli i Evropës i caktojnë rregullat për mbrojtjen e individëve sa i përket përpunimit të të dhënave personale nga ana e Bashkimit dhe institucioneve, trupave, zyrave dhe agjencive të tij si dhe nga ana e shteteve anëtare, në aktivitetet që bëjnë pjesë në gamën ligjore të Bashkimit. Neni 87, paragrafi 2 i Marrëveshjes aplikon sistem të bashkëpunimit policor dhe gjyqësor në lëndë penale. Për këtë qëllim, Parlamenti Evropian dhe Këshilli mund të miratojnë masa lidhur me grumbullimin, mbajtjen, përpunimin, analizën dhe këmbimin e informatave relevante.

Karta e Bashkimit Evropian për të drejtat themelore[22] i garanton të drejtën e privatësisë (neni7) dhe mbrojtjen e të dhënave personale (neni 8). Neni 8, sa i përket mbrojtjes së të dhënave personale, thekson se të njëjtat duhet të përpunohen vetëm për qëllime konkrete dhe me pëlqimin e personit të prekur ose mbi ndonjë bazë tjetër legjitime, të përcaktuar me ligj. Çdokush ka të drejtë qasjeje në të dhënat e grumbulluara për të si dhe të drejtë korrigjimi të të njëtëve. Rrjedhimisht kësaj, në të njëtin nen theksohet se respektimi i këtyre rregullave do të kontrollohet nga organe të pavarura.

Direktiva[23]për përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimit elektronik, si dhe ndryshimet e miratuara me Direktivën 2009/136/BE të vitit 2009, kanë për qëllim, midis tjerash, t'i harmonizojnë aktet nacionale të shteteve anëtare, që të sigurojnë nivel të njëjtë të mbrojtjes së të drejtave dhe lirive themelore, veçanërisht të drejtës së privatësisë, gjatë përpunimit të të dhënave personale në sektorin e komunikimit elektronik. Direktiva, e njohur edhe si Direktivë për e- privatësi, vendos rregulla sigurie gjatë përpunimit të të dhënave personale , për informim gjatë cënimit të të dhënave personale si dhe për besueshmëri të telekomunikimeve dhe qarkullimit të të dhënave.

Dhënësit e shërbimeve të komunikimeve elektronike duhet të ndërmarrin masa adekuate teknike dhe organizative me qëllim që:

- të sigurojnë që vetëm persona të autorizuar të kenë qasje te të dhënat personale;
- t'i mbrojnë të dhënat personale nga shkatërrimi, humbja ose ndryshimi i rastësishëm ose nga çdo lloj forme tjetër joligjore ose të paautorizuar të përpunimit;

[21] Marrëveshja për funksionimin e Bashkimit Evropian 2012/C 326/01
[22]Karta e Bashkimit Evropian për të drejtat themelore, 2012 O.J. (C 326) 391
[23] Direktiva 2002/58/BE e Parlamendit evropian dhe e Këshillit e datës 12.07.2002, O.J. 2002 L 201.

- të sigurojnë zbatim të politikës së sigurisë, gjatë përpunimit të të dhënave personale.

Dhënësi i shërbimeve mund t'i përdorë të dhënat për komunikimin dhe të dhënat për vendndodhjen e personave që komunikojnë (meta të dhënat) vetëm për qëllim pagese dhe për mundësim teknik të shërbimit. Kur meta të dhënat nuk janë më të nevojshme për këta qëllime, ata duhet patjetër të fshihen ose të anonimizohen.

Në raste të rrezikut të veçantë nga cënimi i sigurisë së rrjetit, dhënësi i shërbimeve të komunikimeve elektronike , duhet t'i informojë parapaguesit , edhe nëse rreziku është jashtë fushëveprimit të masave të sigurisë, që duhet të ndërmerren nga ana e dhënësit të shërbimit, duhet t'ua vë në pah shfrytëzuesve të gjitha zgjidhjet e mundshme dhe masat e mbrojtjes që mund t'i ndërmarrin. Dhënësi i shërbimeve të komunikimeve elektronike është i detyruar të ndërmarrë edhe masa adekuate për tu përballur me rreziqe të reja, të pa parashikuara, të sigurisë dhe ta kthejë nivelin e rëndomtë të sigurisë së shërbimit.

Kur do të ndodh cënim i të drejtave personale, si rezultat i qasjes së pautorizuar, humbjes ose shkatërrimit të të dhënave, dhënësi i shërbimeve të komunikimeve elektronike, duhet menjëherë ta informojë organin kompetend mbikëqyrës. Parapaguesit duhet patjetër të informohen nëse ka të ngjarë që të dhënat e tyre personale ose privatësia do të rrezikohen, si pasojë e shkeljes së të dhënave.[24]

Sipas Direktivës së e-privatësisë, shtetet anëtare duhet të sigurojnë besueshmëri të komunikimeve, përmes rrjeteve të komunikimit, e veçanërisht:

- të ndalojnë dëgjimin, përgjimin, ruajtjen ose cilindo lloj të ndjekjes ose kapjes së komunikimeve ose të dhënave për trafikun telekomunikativ, pa pëlqimin e shfrytëzuesve të shërbimeve, përveç kur ekziston autorizim ligjor;
- të garantojnë se ruajtja e të dhënave ose qasje në të dhënat, të ruajtua në pajisjen personale të shfrytëzuesit, është e mundshme vetëm me informim të qartë dhe të plotë të shfrytëzuesit për qëllimet dhe i është dhënë e drejta që të refuzojë.

Çfarëdolloj përufizimesh të të drejtave dhe bligimeve të përpunuara në Direktivën, duhet patjetër të jenë të arsyetuara si të domosdoshme, adekuate dhe proporcionale në një shëqëri demokratike dhe të shërbejnë për qëllime konkrete të rendit publik, siç janë siguria nacionale, mbrojtja, siguria publike ose preventiva, hulumtimi dhe ndjekja e krrimit serioz. ENë vitin 2017, Komisioni evropian ka publikuar **draft- rregulloren për e-privatësi** [25] e cila duhet ta zëvendësojë Direktivën ekzistuese për e-privatësi dhe të jetë *lex specialis* me rregulla specifike për privatësi gjatë komunikimeve elektronike, duke duke mbizotëruar aktet e përgjithshme në këtë sferë, në rast mospërputhjeje. Kalimi nga Direktiva në rregullativë bëhet me qëllim që të harmonizohet legjislacioni për mbrojtjen e privatësisë në BE. Rregullativa për e- privatësi, do të jetë drejtpërdrejtë e zbatueshme dhe ligjëridht obliguese në të gjitha anëtaret e BE, për dallim nga Direktiva për e- privatësi, për të cilën nevojiteshin dispozita nacionale për zbatim, që , ndërkaq, kishte si pasojë zbatimin jokonzistent.

Teksti i draft-rregullores prasheh që garantohet privatësia e përmbajtjes së komunikimeve dhe meta të dhënave si për personat fizikë ashtu edhe për ata juridikë. Ndalohet ndjekja e komunikimeve dhe meta të dhënave , përveç në rastet kur kjo lejohet me legjislacionin nacional- për shembull gjatë hetimeve penale. Analiza e përmbajtjes së

[24] Neni13 nga Direktiva e ndryshuar.

[25]Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), e disponueshme në:http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2017:0010:FIN.

komunikimeve dhe meta të dhënave është e lejuar vetëm me pëlqimin e shfrytëzuesit(në rastin kur dëshiron të fitojë shërbime specifike për të cilat kjo është e domosdoshme), ose me pëlqimin e të gjithë pjesëmarrësve në komunikimin, si dhe në raste të tjera të përcaktuara me ligj. Përpunimi i meta të dhënave që janë grumbulluar për qëllimet e faturimit nga ana e dhënësve të shërbimeve është lejuar për këtë qëllim, por me kufizim se meta të dhënat relevante nuk mund të ruhen më gjatë se periudha në të cilën ligjërisht mund të kontestohet llogaria ose mund të kryhet pagesa.

Zbatimi i rregullave për besueshmëri të komunikimeve elektronike do të jetë përgjegjësi e organeve nacionale për mbrojtjen e të dhënave personale. Fillimisht, qëllimi ishte rregullorja të hyjë në fuqi në maj të vitit 2018, por rregullorja ende nuk është miratuar, dhe prandaj pritet një datë e mëvonshme për të hyrë në fuqi.

Zbulimet e Snoudenit ishin kthesë në diskutimet për reformën e mbrojtjes së ë dhënave në BE, duke e theksuar nevojën për një kornizë të fuqishme ligjore, e cila nuk i pasqyron mundësitë e reja teknologjike për ndjekje masive të komunikimeve. Pas negociatave katërvjeçare, në vitin 2016, BE miratoi një paketë që përbëhet nga Rregullorja e përgjithshme për mbrojtjen e të dhënave[26] (RPMDH) dhe **Direktiva 2016/680 për mbrojtjen e të dhënave në polici dhe në të drejtën penale**[27] – e cila ka të bëjë me mbrojtjen e të dhënave të lidhura me vepra penale dhe me dënime penale. RPMDH do të zbatohet prej 25 maj 2018, ndërsa shtetet anëtare kanë kohë deri në 6 maj 2018 ta inkorporojnë të ashtuquajturën Direktivë policore në legjislacionin nacional.

Është e rëndësishme që në definimin e të dhënave personale në RPMDH në mënyrë eksplicite janë përfshirë të dhëna për vendndodhjen si dhe identifikuesit onlajn, si një lloj meta të dhënash. Është zgjeruar definimi për *të dhëna personale të ndjeshme* dhe ai tani mbulon këtë përcaktim: prejardhjen etnike ose racore, mendimet politike, besimet fetare ose filosofike, anëtarsimin në sindikata, të dhënat për shëndetin, për jetën ose orientimin seksual , të dhënat gjenetike dhe biometrike. Të dhënat e ndjeshme u ekspozohen kushteve të veçanta që duhet të plotësohen që të lejohet përpunimi i tyre. Të dhënat për *dënime për vepra penale* mund të përpunohen dhe për to të mbahet një regjistër adekuat vetëm nga ana e pushteteve nacionale.

Është me rëndësi që RPMDH vendos kusht ligjor për disejn, orientuar kah privatësia, përkatësisht, masat teknike dhe organizative që sigurojnë mbrojtje të të dhënave personale, duhet të parashikohen qysh në disejnimin e sistemeve, e jo më vonë.

Kur do të ndodh cënimi i të dhënavepersonale, si rezultat i qasjes së paautorizuar, humbjes ose asgjësimit të të dhënave, kontrolluesi i të dhënave duhet patjetër ta informojë

[26]Rregullativa (BE) 2016/679 e Parlamentit Evropian dhe e Këshillit për mbrojtjen e individëve lidhur me përpunimin e të dhënave personale dhe qarkullimin e lirë të atyre të dhënave. (Rregullativa e përgjithshme për mbrojtjen e të dhënave), OJ L 119, 27.04.2016, e disponueshme në: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[27]Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, e disponueshme në: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680

organin mbikëqyrës kompetent dhe menjëherë t'i informojë personat me të cilat kanë të bëjnë të dhënat, nëse pretendohet se shkelja do të rezultojë me "rrezik të madh ndaj të drejtave dhe lirive të tyre".[28]

RPMDH e proklamon parimin e minimizimit të të dhënave, përkatësisht përpunimit vetëm të të dhënave që janë të domosdoshme për kryerjen e obligimeve, si kufizim të qasjes në të dhënat personale të atyre të cilët duhet ta zbatojnë përpunimin.

Neni 17 i RPMDH e siguron "të drejtën e harresës". Nëse këtë e kërkon personi të cilit i përkasin të dhënat personale, të njëjtat duhet të fshihen pa shtyerje, nëse nuk janë më të nevojshme për qëllimin për të cilin janë grumbulluar dhe përpunuar, ose personi e ka tërhequr dhënien e pëlqimit, në bazë të të cilit janë përpunuar të dhënat personal, e me këtë rast, nuk ekziston ndonjë bazë tjetër ligjore për përpunimin e tyre, ose, nëse janë përpunuar në mënyrë joligjore.

Duke shënuar një hap të qartë përpara në mbrojtjen e të drejtave themelore, edhe RPMDH edhe Direktiva 2016/680 përfshijnë masa të shumta mbrojtëse për të dhënat personale. Rregullativa dhe Direktiva mundësojnë një mbikëqyrje të fuqishme nga organe të pavarura nacionale për mbrojtjen e të dhënave, të cilat mund të pranojnë ankesa dhe tu ndajnëkompensime aubjekteve të të dhënave. Më tutje, duhet theksuar përshkrimi i të drejtës për për mjet efektiv gjyqësor kundër procesorit ose kontrollorit të të dhënave, dhe i së drejtës të kompensimit për personin i cili ka p[suar dëm material dhe jomaterial, si rezultat i përpunimit joligjor të të dhënave personale.[29] Direktiva u jep të drejtë organizatave jofitimprurëse, që veprojnë në interes të individëve, për të paraqitur ankesa dhe për t'i përfaqësur personat e prekur.[30] Ngjashën si në RPMDH, edhe Direktiva fut obligimin për informim të njerëzve në rastet e cënimit të të dhënave personale.

Edhe përkrah ngjashmërive të këtilla, institucionet e BE e veçojnë sferën e policisë dhe të drejtës penale për shkak të specifikave të saj, dhe pikërisht për këtë, është miratuar direktivë e veçantë për të, për përpunimin e të dhënave për preventivë, hulumtim, detektim ose ndjekje të veprave penale ose ekzekutim të dënimeve penale. (**Direktiva 2016/680)**. Zgjidhja që në këtë sferë të miratohet direktivë, përkundër rregullativës për mbrojtjen e të dhënave në sferat tjera, mund të shpjegohet me faktin që direktiva do tu japë anëtareve të BE një fleksibilitet më të madh gjatë inkorporimit të saj në legjislacionin nacional, ndërsa rregullativa e përgjithshme për mbrojtjen e të dhënave personale (RPMDH) do të zbatohet drejtpërdrejtë.

Ekzistojnë edhe dallime të tjera ndërmjet dy akteve ligjore. Për shembull, Direktiva nuk i thekson të gjitha karakteristikat, të cilat , sipas RPMDH, duhet t'i kenë të dhënat për përpunimin e tyre që të llogaritet si ligjore dhe e drejtë. Së këndejmi, nuk nevojitet pëlqim nga subjekti i të dhënave kur orgnanet kompetente u urdhërojnë personave fizikë me qëllim parandalimi, hetimi, detektimi ose ndjekjeje të veprave penale. Gjithashtu, Direktiva 2016/680 ua kufizon të drejtat e informimit subjekteve të të dhënave, qasjen e tyre në të dhënat e grumbulluara si dhe korrigjimin e lëshimeve në të dhënat e grumbulluara. Të paktën, informatat në vijim, duhet patjetër të jenë të disponueshme për personat, të dhënat personale të të cilëve janë grumbulluar: identiteti i kontrollorit, ekzistimi i operacionit të grumbullimit si dhe qëllimi i operacionit, e drejta për të parashtruar ankesë dhe e drejta për të kërkuar qasje në të dhënat e grumbulluara por edhe të kërkojë ngrirje

[28] Nenet 31 dhe 31.
[29] Neni 56.
[30] Nenet 52–55.

dhe restrikcion të përpunimit të mëtejshëm. Megjithatë, anëtaret e BE mund ta kufizojnë të drejtën e këtillë të informimit, me qëllim të shmangies së pengimit ose prejudikimit të hetimeve, si dhe për shkak të mbrojtjes së sigurisë nacionale ose publike.[31]

Direktiva 2016/680 nuk do të zbatohet në procedurat penale gjyqësore, përkatësisht, në ato raste anëtaret e BE mund ta zbatojnë legjislacionin nacional në aspekt të së drejtës së informimit, qasjes në të dhënat dhe korrigjimit ose fshirjes të dhënave personale.[32] Direktiva nuk mund të zbatohet gjithashtu në sferat që janë jashtë fushës së të drejtës të BE- siç është siguria nacionale[33] – e as gjatë përpunimit të të dhënave nga institucionet, trupat dhe agjencitë e BE.

Sipas Direktivës 2016/680, të dhënat personale duhet të grumbullohen për qëllim specifik, eksplicit dhe legjitim dhe nuk guxojnë të përpunohen jashtë mënyrave të lajuara.Nëse të dhënat e grumbulluara personale përpunohen nga i njëjti ose nga një organ tjetër për qëllimin qëndryshon nga ai , për të cilin fillimisht janë grumbulluar , kjo duhet të lejohet në suazat e kufizimeve ligjore. Të dhënat e grumbulluara personale ruhen në formën që mundëson identifikimin e subjekteve të të dhënave, jo më gjatë se që nevojitetpër qëllimin për të cilin janë përpunuar .[34] Anëtaret e BE duhet të caktojnë kufizime kohore për ruajtjen e të dhënave të këtillaose për rishqyrtim periodik të nevojës së ruajtjes së tyre. [35] Kufizimi i grumbullimittë të dhënave vetëm në atë që është drejtpërdrejtë e nevojshme dhe relevante për dedikimin konkret si dhe mbajtja e tyre vetëm aq sa është e nevojshme për atë qëllim, e shpreh në praktikë *parimin e minimizimit të të dhënave.* Si një prej teknikave dhe masave organizative për zbatimin e parimit të minimizimit të të dhënave, që i thekson direktiva, është "*pseudoanonimizimi*" [36] Kjo nënkupton përpunimin e të dhënave në atë mënyrë që të dhënat personale nuk mundet më t'i përshkruhet një personi konkret, pa përdorimin e informatave shtesë, që ruhet në vend të veçantë dhe janë objekt i masave teknike dhe organizative të sigurisë.

Përpunimi patjetër duhet të kryhet në mënyrë të sigurtëqë mundëson mbrojtje nga përpunimi i paautorizuar dhe joligjor si dhe nga humba e rastësishme, asgjësimi ose dëmtimi. Për këtë qëllim, në nenin 29 të Direktivës, janë caktuar një varg masash sigurie gjatë përpunimit të të dhënave, edhe atë:

- pengimi i qasjes së personave të paautorizuar te pajisja për përpunimin e të dhënave ("kontroll i qasjes deri te pajisja");
- pengimi i leximit, kopjimit, modifikimit ose heqjes së paautorizuar të mbajtësve të të dhënave ("kontroll i mbajtësve të të dhënave");
- pengimi i futjes së paautorizuar të të dhënave personale dhe shikimit të paautorizuar, modifikimit ose fshirjes së të dhënave personale të magazinuara („kontroll i magazinimit");
- pengimi i përdorimit të sistemeve të automatizuara për përpunimin e të dhënave nga persona të paautorizuar, përmes pajisjes së komunikimit ("kontroll i shfrytëzuesve");
- sigurimi që persona të autorizuar që të përdorin sistem për përpunim automatik të të dhënave, të kenë qasje vetëm te të dhënat personale të përfshira me autorizimin e tyre për të pasur qasje ("kontroll i qasjes tek të dhënat")

[31] Nenet 13, 15 dhe 16.
[32] Neni 18; recitalet 20, 49 dhe 107.
[33] Neni 2, paragrafi 3; recitali 14.
[34] Neni 4, paragrafi 1.
[35] Neni 5.
[36] Neni 20.

- sigurimi se është e mundur të kontrollohen dhe të verifikohen trupat në të cilat transferohen ose ose lehen në dispozicion, me përdorimin e pajisjes për komunikim me të dhënat ("kontroll i komunikimit");
- sigurimi se mundet më vonë të konfirmohet dhe të përcaktohet cilat të dhëna personale janë bartur në sistemet për përpunim automatik, si dhe kur dhe prej kujt kanë qenë të bartura të dhënat ("kontroll i bartjes së të dhënave");
- pengimi i leximit, kopjimit, ndryshimit ose fshirjes së paatorizuar të të dhënave personale gjatë bartjes së të dhënave personale ose gjatë transportit të mbajtësve të të dhënave ("kontroll i transportit");
- sigurimi që sistemet e instaluara munden, në raste të ndërprerjes, të përterihen ("përtrirje");
- sigurimi që funksionon sistemi, ndërsa gabimet në funksionet paraqiten ("besueshmëri") dhe se të dhënat personale të magazinuara nuk mund të jenë të dëmtuara me defektin e sistemit("integriteti").

Neni 27 i Direktivës i obligon kontrollorët të bëjnë *vlerësimin e ndikimit ndaj* mbajtjes *së të dhënave,* kur një formë e caktuar e përpunimit, veçanërisht se përdor teknologji të reja, është e sigurtë që do të rezultojë me rrezik të lartë ndaj të drejtave dhe lirive të personave fizikë. Vlerësimi duhet ti caktojë rreziqet, mekanizmat mbrojtës dhe masat e sigurisë.

Personat duhet të jenë të informuar, pa shtyerje, për të dhënat personale të grumbulluara, të cilat i espozohen rrezikut të lartë nga rrezikimi i të drejtave dhe lirive të personave, me qëllim që ata në kohë të mund të ndërmarrin masa adekuate.

Sipas Direktivës, kontrollorët duhet të kenë të caktuar një *nëpunës për mbrojtjen e të dhënave*, i cili duhet t'i informojë kontrollorët për detyrimet ligjore dhe ta ndjek zbatimin e tyre.

Çdo vend anëtar i BE duhet të vendos *një organ të pavarur mbikëqyrës* në territorin e vet, i ngarkuar për ndjekjen e zbatimit të ë drejtës për mbrojtje të të dhënave , në përputhje me Direktivën. Direktiva lejon që këtë detyrë ta kryejë organi i përgjithshëm për të drejtën e mbrojtjes së të dhënave. Ky organ duhet ta mbikëqyrë dhe nxis zbatimin praktik të direktivës, të promovojë ngritjen e vetëdijes publike dhe të kuptuarit e rreziqeve, rregullave, mënyrave të mbrojtjes, t'i këshillojë në përputhje me të drejtën e BE, parlamentit nacional, qeverisë dhe institucioneve të tjera që kanë lidhje me grumbullimin dhe procesimin e të dhënave personale. Direktiva u mundëson organeve të mbikëqyrjes për mbrojtjen e të dhënave në këtë sferë, të kenë forcë korrigjuese në raport me kontrollorët dhe përpunuesit e të dhënave, ashtu që mund të caktojnë një përkufizim të përkohshëm ose të përhershëm, përfshirë këtu edhe ndalimin e përpunimit të të dhënave. Organeve mbikëwyrëse, gjithashtu, u është besuar detyra që të pranojnë ankesa nga individë për përdorimin e të dhënave të tyre personale, si dhe të bëjnë hetime të domosdoshme.

Mbajtja e meta të dhënave

Në vitin 2006 qe miratuar **Direktiva 2006/24/BE për mbajtjen e të dhënave,** të krijuara ose të përpunuara në lidhje me dhënien e shërbimeve të disponueshme publike për komunikime elektronike ose rrjeta publike të komunikimit. Kjo direktivë më shumë e njohur si Direktivë për mbajtjen e të,[37] ishte krijuar me qëllim që të mundësojë që meta të dhënat të jenë në dispozicion për hetime, identifikim dhe ndjekje të veprave serioze penave, të definuara nga çdo shtet anëtar në legjislacionin kombëtar. Në meta të dhënat bëjnë pjesë të dhënat për shfrytëzuesit e shërbimeve telefonike dhe të internetit(përfshirë edhe e- postën), siç janë: emri, adresa e thirrësit dhe të thirrurit, numri i telefonit/ ip adresa, pajisja telefonike dhe vendndodhja e personave të cilët komunikojnë; koha e fillimit dhe përfundimit të komunikimit; lloji i shërbimit telefonik/të internetit.

Ish deputeti gjerman Malt Shpic me analizën e meta të dhënave të cilat "Dojçe Telekom" i ka mbajtur për të, ka ardhur në përfundimin se e ndjekin vendndodhjen e tij 78% të kohës.

Me analizën e meta të dhënave komunikative të një personi të caktuar, mund të kumptohet më shume se me ndjekje fizike të të njëjtit person. Për shmbull, e dhëna se personi i caktuar i ka dërguar mesazhe SMS avokatit të të drejtave familjare, или СМС порака до адвокат за семејно право, ndjekur nga thirrjet telefonike te agjencia e patundshmërive, mund të bëjë të kuptohet për shkurorëzim martese. Meta të dhënat gjenerohen edhe pa qenë njerëzit të vetëdijshëm për këtë, përkatësisht pa ndërmarrë ndonjë aktivitet komunikimi. Për shembull, aplikimet për postë elektronike të telefonave të mençur kontaktojnë me të ashtuquajtura stacione të bazës të operatorëve mobilë në intervale shumë të shkurtëra kohore, me çka vazhdimisht gjenerohet e dhëna për vendndodhjen e telefonit mobil dhe në çfar drejtimi lëviz. Me analizën e meta të dhënave është e mundshme të nxirren përfundime të sakta për jetën private të njerëzve, siç janë lidhjet e tyre sociale, shprehitë e tyre, aktivitetet e përditshme , interesat dhe shijet.[38]

ÇFARË ZBULOJNË PËR NE META TË DHËNAT E KOMUNIKIMIT?	
Me kë komunikojmë	Emrat dhe adresat e personave me të cilët komunikojmë
Kur komunikojmë	Fillimi dhe përfundimi i komunikimeve,kohëzgjatja e tyre dhe shpeshtësia e komunikimeve
Si komunikojmë	Lloji i komunikimit (p.sh. thirrje telefonike, mesazhe SMS/MMS , telefoni përmes internetit, mesazh përmes mejl-it, surfim në internet); lloji i pajisjes (p.sh. telefon mobil)
Ku jemi	Vendndodhja e pajisjes nga e cila komunikojmë

[37] Data Retention Directive.

[38] Draft report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communication), 2017/0003 (COD), Committee on Civil Liberties, Justice and Home Affairs of the European Parliament, 2017. Të disponueshëm në: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-606.011%2B01%2BDOC%2BPDF%2BV0%2F%2FEN

Direktiva për mbajtjen e të dhënave vendosi kritere kur e drejta e mbrojtjes së të dhënave është e pazbatueshme, përkatësisht rastet kur bëhet fjalë për siguri nacionale, siguri publike, mbrojtje ttë territorit, preventivë dhe hulumtim të aktiviteteve krriminale që e rrezikojnë sigurinë dhe ekominë në një ose më tepër vende anëtare të Bashkimit.

Irektiva për mbajtjen e të dhënave kërkonte nda dhënësit e shërbimeve të komunikimit elektronik publikisht të disponueshme ode rrjetet publike të komunikimit ti mbajnë të dhënat e qarkullimit dhe vendndodhjen, që u përkasin individëve ose personave juridikë. Periudha e mbajtjes duhej të zgjaste minumum gjashtë muaj, e më së shumti dy vjet.

Në vitin 2011, Komisioni Evropian përgatiti raport për vlerësimin e zbatimit të Direktivës 2006/26/BE për mbajtjen e të dhënave.[39] Sipas raportit, Komisioni ishte i kënaqur nga zbatimi i Direktivës dhe vlerësoi se mbajtja e të dhënave paraqet një mjet i vlefshëm për sistemet e drejtësisë dhe zbatimin e drejtësisë. Sa u përket vërejtjeve për kohëzgjatjen e mbajtjes dhe shpenzimeve të shkaktuarapër operatorët, raporti thekson se Bashkimi Evropian duhet të vazhdojë të vendos dhe t'i përmirësojë standardet , përmes rregullave të përbashkëta që do të jenë valide për nevojat e të gjitha palëve të interesuara.

Megjithatë, më 8 prill 2014, Këshilli i lartë gjyqësor i **Gjykatës së drejtësisë të Bashkimit Evropian (GjED)**, anuloi Direktivën nr. 2006/24/BE. Përkundër faktit që Gjykata vlerësoi se direktiva zbaton një qëllim legjitim në luftën kundër krrimit të rëndë edhe në mbrojtjen e sigurisë kombëtare, konfirmoi se Direktiva e shkel të drejtën e jetës private dhe të drejtën e mbrojtjes së të dhënave personale të individëve, të garantuara me nenet 7 dhe 8 të Kartës së Bashkimit Evropian për të drejtat themelore. Këto të drejta ishin shkelur për shkak se direktiva e organeve të shtetit u siguronte qasje joselektive dhe masive në të dhënat e qytetarëve, që ishte edhe arsyeja kryesore për anulimin e saj.[40]Hulumtimi i zhvilluar nga Agjencia e Bashkimit Evropian për të drejtat themelore, tregoi se të gjitha gjykatat themelore të cilat ishin marrë me këtë çështje, kishin vlerësuar se sistemet nacionale për mbajtjen e meta të dhënave janë pjesërisht ose krejtësisht jokushtetuese.[41]

Rasti doli para GJED, si çështje preliminare nga Gjykata supreme e Irlandës dhe gjykata kushtetuese e Austrisë. Në të vërtetë, gjykatat nacionale gjatë zgjidhjes së rasteve, kanë të drejtë të referojnë çështje drejtësie në GJED. Pastaj GJED vendos për validitetin e aktit ligjor të Bashkimit Evropian, ose për interpretimin e marrëveshjeve ose akteve nënligjore, kurse vendimi për rastin konkret u është lënë gjykatave nacionale. Në këtë rast, Gjykata supreme e Irlandës duhej ta zgjidhte kontestin në mes të kompanisë irlandeze "Digital Rights Ireland" dhe autoriteteve irlandeze lidhur me ligjshmërinë e masave nacionale për mbajtjen e të dhënave nga komunikimet elektronike. Nga ana tjetër, në Gjykatën kushtetuese të Austrisë paraprakisht një numër i madh personash kishin dërguar disa padi, të cilët kërkonin anulimin e ligjit austriak të telekomunikimeve, me të cilin transpozohej Direktiva për mbajtjen e të dhënave në legjislacionin kombëtar. Gjykata kushtetuese e Austrisë e përkrahu pikëpamjen se mbajtja ndikon te një numër i madh personash, kurse mbajtja e të dhënave të tyre për një kohë të gjatë krijon rrezikun që organet e pushtetit do të kenë qasje në përmbajtjen e të dhënave dhe do ta shkelin privatësinë e tyre. Gjykata kushtetuese e Austrisë shqaqi brengosje për atë se a mundet

[39]E disponueshme në http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF
[40]CJEU, Digital Rights Ireland v. Seitlinger and Others, C-293/12, 8 April 2014.
[41]FRA (2015), Fundamental rights: challenges and achievements in 2014, Luxembourg, Publications Office.

Direktiva për mbajtjen e të dhënave t'i arrijë qëllimet e vendosura, pa i shkelur parimet e mbrojtjes së privatësisë dhe të dhënat personale.

Gjatë shqyrtimit të kategorisë së gjerë të të dhënave, e cila ishte objekt i mbajtjes, GJED vërejti që të dhënat e tila mund të mundësojnë që të nxirren përfundime shumë të saktalidhur me jetët private të personave, të dhënat e të cilëve ishin mbajtur, siç janë shprehitë e përditshme vendet e përhershme ose të përkohshme të banimit, lëvizjet ditore ose të tjera, aktivitetet që kryhen, lidhjet sociale të atyre njerëzve dhe rrethi social. Gjykata vuri në pah që nln rrethana të atilla, edhe përkundër faktit që nuk është e lejuar që të mbahet përmbajtja e komunikimeve, por vetëm e meta të dhënave, mund të rrezikohet liria e shprehjes të parapaguesve ose shfrytëzuesve të regjistruartë dhënësve të shërbimeve elektronike të komunikimit. GJED erdhi në përfundim se mbajtja e të dhënave , me qëllim që të mundësohet qasje nga organet kompetente të shtetit, paraqet përpunim të të dhënave dhe me këtë ndikohet në dy të drejtat themelore nga Karta e Bashkimit Evropian për të drejtat themelore: a) e drejta e jetës private, e garantuar me nenin 7, dhe b) mbrojtja e të dhënave personale , garantuar me nenin 8.

Gjatë shqyrtimit të çështjes për shkeljen e të drejtës për privatësi dhe mbrojtjen e të dhënave personale , GJED ka ardh në përfundimin:

- obligimi i dhënësve të shërbimeve të komunikimit elektronik, "vetëvetiu paraqet pengim të të drejtave të garantuara me nenin 7 të Kartës"
- qasja e pushteteve nacionale në të dhënat "paraqet përzierje shtesë në atë të drejtë themelore", dhe
- mbajtja, gjithashtu, e shkel të drejtën e mbrojtjes së të dhënave personale.

Neni 52 i Kartës kërkon që cilatdo kufizime të realizimit të të drejtave të garantuara, duhet patjetër të vendosen me ligj dhe duhet patjetër të respektohet thelbi i atyre të drejtave. Të gjitha kufizimet janë objekt i testit të proporcionalitetit dhe mund të vendosen vetëm nëse janë të nevojshme dhe i përmbushin kërkesat e interesit të përgjithshëm, të definuara nga BE ose nevojës për mbrojtjen e të drejtave të të tjerëve.

Gjykata evropiane e drejtësisë vështroi qëllimin themelor të Direktivës për mbajtjen e të dhënave, e cila duhet tu ndihmojë vendeve anëtare të BE në luftën kundër krrimit serioz dhe t'i kontribuojë ruajtjes së sigurisë publike. Gjykata u pajtua që lufta kundër terrorizmit ndërkombëtar është qëllim i interesit të përgjithshëm, dhe për këtë konfirmoi se mbajtja e të dhënave është mjet i rëndësishëm për organet nacionale në zhvillimin e luftës kundër krrimit serioz. Në bazë të këtyre analizimeve, Gjykata evropiane e drejtësisë solli përfundimin se mbajtja e të dhënave , me qëllim që tu japë mundësi pushteteve nacionale tu qasen të dhënave të tilla, për pengimin dhe zbulimin e veprave të rënga penale "vërtet përmbush qëllimin e interesit të përgjithshëm".

GJED më tutje analizonte a ka qenë përzierja nga ana e pushteteve nacionale në proporcion me qëllimin për të cilin realizohet. Në këtë kuptim, në përputhje me praktikën gjyqësore, standardet që duhet të plotësohen është që kjo të jetë "adekuate" dhe "e domosdoshme", me qëllim që të arrihen qëllimet. Sa i përket pyetjes, a ka qenë vallë mbajtja e të dhënave masë adekuate për arritjen e qëllimeve të Direktivës 2006/24/BE, Gjykata evropiane e drejtësisë, duke vënë në pah se mjetet e komunikimit elektronik luajnë një rol jetik në zbulimin e veprave penale, e njëherësh, edhe nevoja e organeve nacionale që të kenë asje në të dhënat, konfirmoi se mbajtja e meta të dhënave është "mjet i rëndësishëm" dhe "mund të konsiderohet se është adekuate" që të arrihen qëllimet e Direktivës.

Sa i përket testit të domosdoshmërisë, dhe a ësëtë përzierja e kufizuar vetëm në atë që është e domosdoshme, gjykata dha tre vërejtje të rëndësishme: a) Direktiva parashikon mbajtje të të gjitha të dhënave nga trafiku telekomunikativ, të gjeneruara nga spektri i gjerë i mënyrave elektronike të komunikimit, duke përfshirë edhe telefoninë fikse, telefoninë mobile, qasjen në internet, postën elektronike dhe telefoninë me internet; b) shtrirja e Direktivës përfshin të gjithë parapaguesit dhe përdoruesit e regjistruar të shërbimeve për komunikim elektronik; dhe c) Direktiva i cënon të drejtat themelore të të gjithë qytetarëve të Bashkimit Evropian. Gjykata konstatoi se mbajtja e meta të dhënave ndikon jo vetëm te personat , të dhënat e të cilëve mund të kontribuojnë për inicimin e procedurës gjyqësore, por edhe te ata për të cilët nuk ekziston gjurmë të dëshmive të cilat tregojnë se sjellja e tyre mund të jetë e lidhur me krrim serioz. Gjithashtu, u konstatua që askush nuk është i liruar nga kjo rregull; kjo vlen bile edhe për ata, komunikimet e të cilëve janë objekt i sekretit zyrtar, në pajtim me rregullat nacionale. Në duskutimin e mëtejshëmpër Direktivën, GJED vërejti mungesë të çfarëdo lidhjeje në mes të të dhënave të mbajtura dhe kanosjes për sigurinë publike. Gjykata gjithashtu theksoi se mbajtja nuk është kufizuar vetëm në meta të dhënat e personave të lidhur me një periudhë të caktuar kohore ose me një zonë të caktuar gjeografike, ose të një grupi personash të cilët do të mund të kishin lidhje me një vepër penale serioze. Përveç kësaj, GJED shqyrtoi a i përmban Direktiva të gjitha kufizime e të drejtës së pushteteve nacionale për qasje në meta të dhënat e mbajtura. Në këtë pikëpamje, GJED vërejti mungesën e kufijve të përgjithshëm. Së këndejmi, Gjykata konstatoi se Direktiva: a) nuk ka vendosur as kufizime materiale e as procedurale për qasje të organeve kompetente të shtetit në të dhënat e mbajtura, b) nuk e ka kushtëzuar qasjen e autoriteteve nacionale në meta të dhënat, kushtëzuar me kontroll paraprak, të kryer nga një gjykatë ose ndonjë organ tjetër i pavarur administrativ do ta kufizonte qasjen në të dhënat dhe përdorimin e tyre të asaj që është apsolutisht e domosdoshme, dhe c) nuk kërkon nga vendet anëtare të vendosin kufizime të atilla. Sa i përket periudhës së mbajtjes, që zgjat prej gjashtë muajsh deri në dy vjet, GJED theksoi se Direktiva nuk cakton kurrfarë kriteresh objektike që të caktohet periudha adekuate e mbajtjes së “asaj që është e domosdoshme”.

Në bazë të këtyre elementeve, Gjakata vlerësoi se Direktiva nuk ka vendosur rregulla të qarta dhe precize me të cilat rregullohet “shkalla e pëerzierjes me të drejtat themelore të nenit 7 dhe 8 të Kartës”. Prandaj, qe sjell përfundim se Direktiva “përfshin një përzierje të gjerë dhe mjaft serioze në ato të drejta themelore në rendin juridik të BE, pa përzierjen e tillë të jetë të jetë e kufizuar me dispozita që do të sigurojnë se është reduktuar vetëm në atë që është krejtësisht e domosdoshme”.

Sa i përket sigurisë dhe mbrojtjes së të dhënave që janë mbajtur, GJED caktoi se Direktiva 2006/24/BE nuk përmban masa të mjaftueshme mbrojtëse, në përputhje me nenin8 të Kartës, që tësigurohet mbrojtje efikase e të dhënave të mbajtura sa i përket rrezikut nga keqpërdorimit dhe kundër çdo qasjeje joligjore dhe shfrytëzimit të të dhënave. Sipas nenit 8 të Kartës, midis tjerash, nevojitet pëlqim i subjektit të të dhënave për përpunim të të dhënave të tij personale. Gjykata konstatoi se Direktiva 2006/24/BE nuk përmban rregulla për rregullimin e mbrojtjes dhe sigurisë së të dhënave në mënyrë të qartë dhe të saktë të cilat përkojnë me: a)sasinë e madhe të të dhënave mbajtja e të cilave kërkohet me atë direktivë; b)natyrën e ndjeshme të atyre të dhënave; dhe c)rrezikun nga qasja joligjore në ato të dhëna. Gjithashtu, nuk janë caktuar obligime të veçanta të vendeve anëtare që të vendosin rregulla të këtilla.

Gjykata evropiane e drejtësisë gjithashtu konsideronte se siguria dhe mbrojtja e të dhënave personale nuk mund të garantohet në tërësi, në mungesë të mbikëqyrjes një organ

i pavarur për mbrojtjes e të dhënave personale, si kërkohet me nenin 8 të Kartës së Bashkimit Evropian për të drejtat themelore.Së këndejm, GJED ka ardh në përfundim se trupat ligjvënëse të BE, me miratimin e Direktivës 2006/24/BE, i kanë tejkaluar kufijt e imponuar nga parimi i proporcionalitetit përkitazi me nenet 7, 8 dhe 52 të Kartës. Si rezultat i kësaj Direktiva u shfuqizua.

Mbajtja e të dhënave në BE pas shfuqizimit të Direktivës 2006/24/BE

Pas shfuqizimit të Direktivës 2006/24/BE në vitin 2014 nga Gjykata evropiane e drejtësisë, Komisioni evropian u deklarua se nuk do të punojë në hartimin e direktivës së re e cila do ta zëvendësonte atë të shfuqizuarën.[42] Bashkimi evropian u sugjeronte shteteve anëtare dhe institucioneve relevante evropiane të përgatisin ndryshime përkatëse në përputhje me aktvendimin, i cili vendos standard të ri për legjislacionet nacionale për mbajtjen e të dhënave.[43] Gjatl krijimit të rregullave të reja , duhet mbajtur llogari të njëjtat të jenë edhe në përputhje me të drejtat për privatësi dhe mbrojtjen e të dhënave private, të theksuara në nenin 15 të Direktivës 2002/58/BE për e-privatësi si dhe me parimet e përgjithshme që i përmban Karta e Bashkimit Evropian për të drejtat themelore.

Në këtë raport vjetor, të vitit 2017, Agjencia e Bashkimit Evropian për të drejtat themelore, vë në pah se anëtaret e BE, në kuadër të legjislacionit nacional duhet t'i shmangen mbajtjes së përgjithshme dhe jodiskriminuese të të dhënavenga operatorët e telekomunikimit. Legjislacioni nacional duhet të fus kontrolle rigoroze të proporcionalitetit si dhe masa mbrojtëse adekuate procedurale për garantimin efektiv të të drejtave për privatësi dhe mbrojtje të të dhënave personale.

Supervizori evropian për mbrojtjn e të dhënave (SEMDH) dhe Grupi i punës për nenin 29[44] e theksuan nevojën e shmangies së kërkesës për mbajtjen e të dhënave në kornizën e re për e- privatësi, në përputhje me vendimin e GJED.[45]

Përkundër asaj që vendimi i GJED ndikoi që disa shtete më hollësisht ta shqyrtojnë problemin me mbajtjen e të dhënave, megjithatë, nuk kishte ndonjë tërheqje gjerësisht të përhapur, të sistemeve të vendosura për mbajtjen e të dhënave nëpër tërë Evropën.

Shumica e vendeve u orvatën, kokë më vete, të bëjnë balancin ndërmjet vendimit të GJED dhe nevojës për mbajtjen e të dhënave për qëllime të lidhura me sigurinë e shtetit dhe ndjekjen efikase të grupeve krriminale. Më posht janë paraqitur disa raste të shteteve anëtare të BE lidhur me veprimet e marra, pas shfuqizimit të Direktivës për mbajtjen e të dhënave , së bashku me një pasqyrë të shkurtër të dispozitave ligjore për ndjekjen e përmbajtjes së komunikimeve dhe dhe statistikave për ndjekjen që janë në dispozicion.

[42] European Commission statement on national data retention laws,16.09.2015. E disponueshme në: http://europa.eu/rapid/press-release_STATEMENT-15-5654_en.htm

[43]Qëndrimi i BE lidhur me aktvendimin e GJED për shfuqizimin e Direktivës: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp220_en.pdf

[44] Emër i shkurtuar për grupin e punës për mbrojtjen e të dhënave, që është vendosur në përputhje me nenin 29 të Direktivës 95/46/BE. Grupi i jep këshilla të pavarura Komisionit evropian dhe ndihmon në zhvillimin e politikave të harmonizuara për mbrojtjen e të dhënave.

[45]European Data Protection Supervisor, Opinion 5/2016 Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC), 22 July 2016; Art. 29 Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), 19 July 2016.

Republika Federale e Gjermanisë

Qysh ara shfuqizimit të Direktivës për mbajtjen e të dhënave në vitin 2014, Gjykata federale kushtetuese e Gjermanisë në vitin 2010 e shpalli për të pavlefshëm[46]aktin e implementimit me të cili ishte transponuar Direktiva 2006/24/BE në të drejtën nacionale. Sidoqoftë, vendimi i këtille ishte marrë në bazë të asaj që kjo Direktivë nuk është në përputhje me të drejtat e fshehtësisë së komunikimeve dhe vetëpërcaktimit informatik, me atë që implementimi i saj nuk ishte shpallur si jokushtetuese. Në vitin 2015, ministri i drejtësisë propozoi ligj të ri i cili qe miratuar me qëllim që arrihet kompromis ndërmjet çështjeve të sigurisë së shtetitdhe shkeljes së lirive dhe të drejtave të qytetarëve. Në përputhje me këtë Ligj, të miratuar me shumicë të madhe në Bundestag, kohëzgjatja e e mbajtjes së të dhënave u shkurtua prej 6 muajsh në 10 javë, u hoq mbajtja e tërë trafikut përmes postës elektronike dhe ishte proklamuar nevoja e urdhërit gjyqësor për dorëzimin e të dhënave të mbajtura organeve shtetërore. Në mënyë plotësuese, dispozitat e reja ligjore u kushtojnë vemendje të dukshme sigurisë, përmes obligimit për enkripcion dhe krijimin e të dhënave për të pasur qasje në dosjet, si dhe autorizim nga të paktën dy persona të utorizuar për qasje teknike te të dhënat.

Lidhur me ndjekjen e përmbajtjes së komunikimeve, në vitin 2016 nga "Dojçe Telekom" ishte siguruar qasje në 44.238 linja[47] me kërkesë të organeve shtetërore. Megjithatë, në raport theksohet se operatorët në Gjermani janë të detyruar të dorëzojnë të dhëna specifike në Shërbimin federal të zbulimit (BND) , por shtrirja dhe numri i të dhënave të këtilla të dorëzuara nuk shpallet.

Republika e Austrisë

Gjykata kushtetuese e Austrisë ishte gjykata e parë nacionale e cila shpalli të pavlefshëm një pjesë të madhe ë Ligjit për mbajtjen e të dhënave, pas vedimit të marrënga GJED. Operatorët austriakë nuk kanë më obligim t'i mbajnë të dhënatdhe t'i dorëzojnë te autoritetet nacionale. Megjithatë, operatorëve u është lejuar që të mbajnë të dhëna për komunikim, për qëllime të tyre legjitime, siç janë faturimi, preventiva nga mashtrimet e të ngjashme. Edhe një gjë, këto të dhëna rishtazi lehen që të jenë të disponueshme edhe pr pushtetet publike, kur ekzistojnë rreziqe sigurie dhe kanosje për sigurinë e shtetit.

Në Austri, në vitin 2016, nga "T-mobajl Austria" ishte siguruar përmbajtja e bisedave nga gjithsej 2.183 linja[48], me kërkesë të organeve kompetente.

Republika e Estonisë

[46] European Digital Rights. German Federal Constitutional Court rejects data retention law. https://edri.org/edrigramnumber8-5german-decision-data-retention-unconstitutional/

[47]Raporti i transparencës i "Dojçe Telekom" për Gjermani. I disponueshëm në: https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/news/germany-363566

[48] Raport për transparencë të "Dojçe telekom" për Austrinë. I disponueshëm në : https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/news/austria-363540

Legjislacioni në Estoni, i cili rregullon mbrojtjen e privatësisë dhe të të dhënave personale është tërësisht i harmonizuar me direktivat evropiane në këtë sferë. Pjesa e Ligjit për komunikime elektronike[49] që ka të bëjë me mbajtjen e të dhënave, mbështetet në Direktivën 2006/24/BE. Pas shfuqizimit të kësaj direktive nuk janë bërë kurrfarë ndryshimesh në zgjidhjet ligjore, me çka operatorët janë të detyruar t'i ruajnë meta të dhënat në afat prej një viti. Inspektorati estonas për mbrojtjen e të dhënave ka publikuar disa udhëzues në të cilat paraqiten të drejtat e qytetarëve dhe obligimet e operatorëve dhe organeve kompetente shtetërore sa i përket mbikëqyrjes dhe ndjekjes së koëm.

Republika e Lituanisë

Në Ligjin e komunikimeve elektronike të Lituanisë është transponuar Direktiva 2006/24/BE, ndërsa mbajtja e të dhënave kryhet në periudhëm më të shkurër të të paraparë me direktivën e shfuqizuar- gjashtë muaj. Regjimi i mbajtjes së të dhënave u përket edhe trafikut telekomunikativ edhe atij të internetit. Në vitin 2015 kanë filluar konsultime të caktuara lidhur me nevojën e ndryshimeve në këtë sferë, por gjithsesi, ndonëse ishin bërë disa amendamente për ligjin kompetent, nuk kishte ndryshime sa i përket mbajtjes së të dhënave. Në përputhje me Kodin penal të Lituanisë të dhënat e mbajtura përdoren kryekëput për hulumtime, identifikim dhe ndjekje të krrimit serioz.

Republika e Irlandës

Gjatë kohë para miratimit të Direktivës për mbajtjen e të dhënave në vitin 2006, Irlanda kishte vendosur sistem për mbajtjen e meta të dhënave në kohëzgjatje prej 7 vitesh. Mbajtja e tillë ishte zbatuar pa kurrfarë mbikëqyrjeje dhe kontrolli ndaj punës së operatorëve. Këto dispozita ishin ndryshuar me miratimin e Direktivës 2006/24/BE me të cilën u vendos periudha maksimale e mbajtjes së të dhënave , prej 2vitesh për telekomunikimet dhe prej një viti për komunikimet me internet. Organizata "Digital Rajts Irland" (*DRI*) [50] filloi procedurë për tu verifikuar kushtetutshmëria e Ligjit para Gjykatës evropiane të drejtësisë. Në vitin 2014, Gjykata vendosi që Direktiva, e cila është bazë e të drejtës irlandeze në këtë fushë, i cënon të drejtat e qytetarëve të BE, të garantuara në Kartën e Bashkimit për të drejtat themelore.

Veç kësaj, Gjykata kushtetuese e Irlandës e ngriti çështjen se, ai i bën Direktiva dëshmitë e grmbulluara me mbajtjen e të dhënave, të palejuara. Prap se prap, autoritetet nacionale nuk kanë inicuar ndryshiin e legjislacionit . "Digital Rajts Irland" ka filluar edhe procedurë para Gjykatës kushtetuese të Irlandës lidhur me ligjin nacional për të cilin ende pritet mendim.

Republika e Çekisë

Në Çeki, Ligji i komunikimeve elektronike përshkruante mbajtje të meta të dhënave në kohëzgjatje prej 6 deri në 12 muaj. Por, Gjykata kushtetuese e Çekisë në vitin 2011 e shpalli ligjin jokushtetues, me arsyetim se e cënon të dretën e qytetarëve për privatësi. Në

[49] Ligji për komunikime elektronike të Estonisë, I disponueshëm në: https://www.riigiteataja.ee/en/eli/501042015003/consolide

[50] Organizata i është përkushtuar mbrojtjes së të drejtave të njeriut në epokën digjitale. https://www.digitalrights.ie/

korriktë vitit 2012 ishin miratuar ndryshime të Ligjit të komunikimeve elektronike, me çka u forcuan masat teknike dhe organizative, për mbrojtjen e të dhënave për trafik dhe vendndodhje. Më tutje, shërbimet e sigurisë dhe ato të zbulimit mund të kërkojnë qasje në meta të dhënat nën kushte të caktuara, vetëm me lejen e gjykatësit të Gjykatës kushtetuese.

Në vitin 2016, "T-mobajl Çeki" ka siguruar qasje të organeve kompetente shtetërore deri te 8.492 linja.[51] Qasja e këtillë është siguruar në përputhje me Ligjin e komunikimeve elektronike i cili definon kushtet për ndjekje legale të komunikimeve dhe mbajtjen e të dhënave.

Republika e Kroacisë

Ligji kroat për komunikime elektronike [52] në nenin 109 cakton që operatorët kanë obligim ti mbajnë meta të dhënat në kohëzgjatje prej një viti. Si arsye për mbajtjen e të dhënave theksohen: a) nevoja e zhvillimit të hetimeve, zvulimit, ndjekjes dhe dënimit të krriminelëve seriozë; dhe b) nevoja e sigurisë dhe mbrojtjes dhe ruajtjes së sigurisë nacionale. Edhe pas shfuqizimit të Direktivës për mbajtjen e të dhënave, ligji në Kroaci mbeti në fuqi. Ndënëse ishin nicuar hulumtime dhe analiza të gjendjes nga Agjencia rregullatore e Kroacisë për veprimtari rrjetore dhe Agjencia për mbojtjen e të dhënave personale, megjithate mbajtja e të dhënave do të vazhdojë derisa nuk miratohen ndryshimet ligjore.

Në raportin për transparencëpër vitin 2016, Telekomi kroat (Hrvatski telekom)thekson se nuk ka informata për numrin e linjave të ndjekura, sepse autoritetet e shtetitkanë qasje të drejtpërdrejtë në përmbajtjen e komunikimeve. Më tutje, sqarohet se, në përputhje me dispozitat ligjore, operatorët duhet të sigurojnë qasje të vazhdueshme dhe të drejtpërdrejtë në pajisjen teknike për ndjekjen e komunikimeve, me çka "Telekomi kroat" nuk ka kurrfarë të dhënash sa i përket numrit të linjave të ndjekura.

Sa i përket mbikëqyrjes së punës së agjencive informative të sigurisë, Kroacia ka vendosur sistem shumëshkallësh, me qëllim që të pengohen keqpërdorimet e mundshme të cilat mundësohen me ndjekjen e komunikimeve të qytetarëve. Në të vërtetë, Kuvendi i Kroacisë, përveç Këshillit të sigurisë nacionale, që është në përbërje të tij, ka formuar edhe Këshill për mbikëqyrje qytetare të agjencive informative të sigurisë. Anëtarët e Këshillit i zgjedh Kuvendi, nga radht e profesorëve universitarë nga fusha e sigurisë, drejtësisë, sigurisë së sistemeve të komunikimit , përfaqësues të organizatave civile, avokatëve dhe eksertëve të sferës.

[51]Raport për transparencë i „Dojçe Telekom" Për Republikën e Çekisë. I disponueshëm në : https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/news/czech-republic-363568

[52] Ligji i komunikimeve elektronike të Kroacisë. I disponueshëm në: https://www.zakon.hr/z/182/Zakon-o-elektroni%C4%8Dkim-komunikacijama

Analizë e kornizës ligjore për mbrojtjen e privatësisë dhe të dhënave personale gjatë komunikimeve elektronike në Maqedoni

Mbrojtja e privatësisë dhe e të dhënave personale gjatë komunikimeve elektronike në Maqedoni është rregulluar me Kushtetutën, Ligjin e mbrojtjes së të dhënave personale dhe me Ligjin e komunikimeve elektronike. Më posht është bërë një vështrim i shkurtër i këtyre akteve ligjore.

Kushtetuta e Repubkës së Maqedonisë në nenin 17 e garanton lirinë dhe pacënueshmërinë e letrave dhe të gjitha formave të tjera të komunikimeve. Vetëm me vendim të gjykatës kushtetuese, nën kushtet dhe procedurën e caktuar me ligj, mund të hiqet dorë nga e drejta e pacënueshmërisë së letrave dhe të gjitha formave të tjeta të komunikimit, nëse kjo është e domosdoshme për shkak të pengimit ose zbulimit të veprave penale, për shkak të zhvillimit të procedurës penale si dhe për shkak të sigurisë dhe mbrojtjes së Republikës. Ligji miratohet me shumicë prej dy të tretat e votave nga numri i përgjithshëm i deputetëve. Neni 18 i garanton sigurinë dhe fshehtësinë e të dhënave personale. Qytetarëve u garantohet mbrojtje nga cënimi i integritetit personal, që del nga regjistrimi i informatave për to, përmes përpunimit të të dhënave.

Ligji i parë për mbrojtjen e të dhënave personale[53] në frymën e Konventës së Këshillit të Evropës 109/81 dhe Direktivës 95/46/BE, është miratuar në vitin 2005. Ligji për mbrojtjen e të dhënave personale , si pjesë e lirive dhe të drejtave themelore të personave fizikë, e veçanërisht të drejtën e privatësisë. Ky ligj zbatohet në përpunimin e automatizuar të plotë dhe të pjesërishëm të të dhënave personale dhe përpunim tjetër të të dhënave personale, që jannë pjesë e përmbledhjes ekzistuese të të dhënave personale ose janë dedikuar që të jenë pjesë e përmbledhjes së të dhënave personale.

DEFINIMET KYÇE NGA LIGJI PËR MBROJTJEN E TË DHËNAVE PERSONALE	
E dhëna personale	Çdo informatë që i përket një personi të identifikuar fizik ose personit fizik i cili mund të identifikohet
Përpunimi i të dhënave personale	Operacioni ose një grumbull operacionesh që kryhen ndaj të dhënave personale në mënyrë automatike ose në ndonjë mënyrë tjetër, siç është: grumbullimi, evidentimi, organizimi, ruajtja, përshtatja ose ndryshimi, tërheqja, konsultimi, përdorimi, zbulimi përmes transferimit, publikimit ose të bërit të disponueshëm me ndonjë mënyrë tjetër, barazimi, kombinimi, bllokimi fshirja ose asgjësimi
Kontrollor i përmbledhjes së të dhënave personale	Një person fizik ose juridik, organ i pushtetit shtetëror ose trup tjetër, i cili i cakton qëllimet dhe mënyrën e përpunimit të të dhënave personale
shfrytëzuesi	Një person fizik ose juridik, organ i pushtetit shtetëror ose tru tjetër të cilit i zbulohen të dhënat

Mbrojtja e të dhënave personale i garantohet çdo personi fizik, pa diskriminim, përfshirë edhe shtetësinë. Si kategori të veçanta të të dhënave personale , të cilat nuk guxon të përpunphen, përkatësisht mund të përpunohen vetëm në ushte të veçanta, nëligj janë caktuar:të dhënat personale që e zbulojnë prejardhjen racore ose etnike , bindjen politike,

[53] Ligji për mbrojtjen e të dhënave personale, „Gazeta zyrtare e Republikës së Maqedonisë“ nr.7/2005, 103/2008, 124/2010 dhe 135/2011.

fetare, filosofike ose ndonjë bindje tjetër, anëtarësimi në organizatë sindikale dhe të dhënat që kanë të bëjnë me shëndetin e njerëzve, duke përfshirë edhe të dhënat gjenetike, të dhënat biometrike ose të dhënat që kanë të bëjnë me jetën seksuale. Definimi i këtillë i të dhënave të ndjeshme është në përputhje me Rregullativën e përgjithshme të BE për mbrojtjen e të dhënave.

Ligji përshkruan se të dhënat personale përpunhen në mënyrë të drejtë dhe në përputhje me ligjin; grumbulllohen për qëllime konkrete, të qarta dhe pëtcaktuara me ligj dhe përpunohen në mënyrën që është në përputhje me ato qëllime. Eshë paraparë edhe që do të ndërmerren të gjitha masat adekuate për fshirjen ose korrigjimin e të dhënave personale të cilat janë të pa sakta ose ose jo të plota, duke i pasur parasysh qëllimet për të cilat janë grumbulluar dhe përpunuar. Gjithashtu, ligji parasheh ruajtjen e të dhënave personale , jo më gjatë se që nevojitet, për tu arritur qëllimet për të cilat janë grumbulluar të dhënat për përpunim të mëtejshëm.Pas skadimit të afatit për ruajtjen e të dhënave prsonaëe , mund të përpunohen vetëm për qëllime historike, shkencore dhe statistikore, duke respektuar të drejtën e ruajtjes së privatësisë, jetës personale dhe familjare nga përdorimi i tyre i paautorizuardhe anonimizimi i tyre.

Ligji për ruajtjen e të dhënave personale përshkruan që përpunimi i të dhënave personale mund të kryhet: pas marrjes paraprake të pëlqimit nga subjekti i të dhënave personale; për realizim të marrëveshjes në të cilën subjekti i të dhënave personale është palë marrëveshëse ; për oërmbushjen e dispozitës ligjore ; për mbrojtjen e jetës ose interesave thelbësore të subjektit të të dhënave personale; për kryerjen e punëve në interes publik ose autorizimit zyrtar të kontrollorit ose të personit të tretë, të cilit i janë zbuluar të dhënat, përveç nëse liritë dhe të drejtat e subjektit të të dhënave personale nuk mbisundojnë ndaj interesave të tilla.

Ligji i komunikimeve elektronike (LKE),[54] midis tjerash, ka për qëllim që të sigurojë mbrojtje tl t drejtave tl shfrytëzuesve dhe besueshmëri të komunikimeve.[55] Për punën e komunikimeve eletronike ligji i përcakton si institucione kompetente, Ministrinë e shoqërisë dhe administratës informatike dhe Agjencinë e komunikimeve elektronike.

Ligji i obligon operatorët të ndërmarrin masa adekuate teknike dhe organizative me qëllim ë të menaxhojnë me rreziqet për sigurinë e rrjetave dhe shërbimeve, veçanërisht që të pengohet dhe minimizohet ndikimi ndaj shfrytëzuesve.[56]Në rast të cënimit të sigurisë së të dhënave personale, operatori është i detyruar në afat prej 24 orësh të informojë për këtë Agjencinë e komunikimeve elektronike dhe Drejtorinë për mbrojtjen e të dhënave personale.[57] Nëse cënimi i sigurisë së të dhënave personale mund të ndikojë negativisht në të dhënat personale ose privatësia e parapaguesit ose e ndonjë personi tjetër fizik, operatori është i obliguar në afat prej 24 orësh për këtë ta informojë parapaguesin në fjalë ose personin fizik, përveç nëse Agjencia nuk vendos ndryshe.[58]

Ligji e rregullon edhe besueshmërinë e komunikimeve,[59] që u përket përmbajtjes së komunikimeve, të dhënave për trafik komunikimi dhe të dhënave për vendndodhjen dhe faktet e rrethanat për ndërprerjen e lidhjes ose për përpjekjet e pasuksesshme për

[54] Ligji i komunikimeve elektronike, „Gazeta zyrtare e Republikës së Maqedonisë" nr. 39/2014, 188/2014 dhe 44/2015.
[55] Neni 2 i Ligjit të komunikimeve elektronike.
[56] Neni 166 i Ligjit të komunikimeve elektronike.
[57] Neni 167 i Ligjit të komunikimeve elektronike.
[58] Njëlloj.
[59] Neni 168 i Ligjit të komunikimeve elektronike.

vendosjen e lidhjes. Qartësisht janë ndaluar të gjitha format e dëgjimit, ndjekjes, incizimit, mbajtjes ose çdo lloj tjetër i ndjekjes ose mbikëqyrjes së komunikimeve, pa marrë pëlqim nga shfrytëzuesit për të cilët është fjala. Përjashtime nga ndalimi i këtillë kanë të bëjnë me zbatimin e Ligjit për ndjekjen e komunikimeve, për mbajtjen e meta të dhënave për parapaguesit, rregulluar me Ligjin e komunikimeve elektronike, me ruajtjen teknike të të dhënave të domosdoshme për transmetim të komunikimeve, si dhe me incizimin e komunikimeve dhe të dhënave adekuate për trafik komunikimi, për shkak të sigurimit të dëshmisë për transaksione komerciale, por jo më gjatë se afatet ligjore në të cilat mund të kontestohet llogaria ose të kryhet pagesa.[60]

Qasje në të dhënat për trafik komunikimi, si një lloj meta të dhënash, u lejohet vetëm personave të autorizuar të operatorit, të cilët punojnë në llogaritjen e shpenzimeve të parapaguesve dhe shpenzimeve të komunikimit të ndërsjellë, menaxhimin me trafikun e komunikimit , kërkimin e konsumatorëve, zbulimin e mashktrimeve, marketingun ose sigurimin e shërbimeve me vlerën e shtuar.[61]

Të dhënat për venndodhjen e parapaguesve ose shfrytëzuesve të shërbimeve elektronike të komunikimit, si një lloj i veçantë i meta të dhënave , mund të përpunohen nga operatori, vetëm në rastin kur janë bërë në mënyrë anonime ose në bazë të pëlqimit të marrë paraprakisht nga parapaguese ose shfrytëzuesi i shërbimeve, në atë masë dhe në atë kohëzgjatje, që janë të nevojshme për sigurimin e shërbimeve me vlerën e shtuar.[62] Parapaguesi ose shfrytëzuesi i shërbimeve në çdo kohë mund ta tërheq pëlqimin e vet të dhënë për përpunimin e të dhënave për vendndodhjen.[63]

Ligji i komunikimeve elektronike parashikon gjobë në lartësi prej 4% deri në 7% të të ardhurave të përgjithshme vjetore të operatorit të shërbimeve të komunikimeve elektronike, si dhe 1.500 deri 3.000 euro për personin përgjegjës në operatorin, nëse:[64]

- kryen dëgjimin, ndjekjen, ruajtjen, incizimin, mbajtjen ose çdo formë të ndjekjes ose mnikëqyrjes së komunikimeve, pa marrë pëlqim nga shfrytëzuesit;
- Ruan informata ose jep qasje deri te informatat të cilat tanimë janë të ruajtura në pajisje terminale të parapaguesit ose shfrytëzuesit, në kundërshtim me Ligjin;
- Nuk i fshin ose nuk i bën anonimë të dhënat e qarkullimit të komunikimeve (përveç kur nevojiten per transferim komunikimesh dhe sigurimin e dëshmive për transaksione komerciale);
- Përpunon të dhëna për qarkullim komunikimesh dhe vendndodhjen, në kundërshtim me ligjin;
- Lejon qasje në përpunimin e të dhënave për qarkullim komunikimesh dhe për vendndodhjen, personave të paautorizuar;
- Të dhënat për qarkullim komunikimesh nuk i ruan në Republikën e Maqedonisë;
- Nuk i respekton barimet e sigurisë së meta të dhënave të mbajtura;
- Mban të dhëna që e zbulojnë përmbajtjen e komunikimit.

[60] Njëlloj.
[61] Njëlloj.
[62] Neni 171 i Ligjit të komunikimeve elektronike.
[63] Njëlloj.
[64] Neni 181 i Ligjit të komunikimeve elektronike.

Analizë e kornizës ligjore dhe institucionale për ndjekjen e komunikimeve dhe mbajtjen e të dhënave në Maqedoni

Ndjekja e komunikimeve dhe mbajtja e meta të dhënave gjatë komunikimeve elektronike në Maqedoni është rregulluar me Ligjin për ndjekjen e komunikimeve, me Ligjin për procedurë penaledhe Ligjin e komunikimeve elektronike. Të tre ligjet dhe përvojat nga zbatimi i tyre janë analizuar paralelisht, janë zbërthyer në disa nëntituj tematikë të dhënë në vazhdim.

Definimi i dhe përfshirja e ndjekjes së komunikimit

Ligji për ndjekjen e komunikimeve[65] i rregullon kushtet dhe procedurën e ndjekjes së komunikimeve, mënyrën e veprimit, ruajtjen dhe shfrytëzimin e të dhënave dhe dëshmive si dhe kontrollin e ligjshmërisë së ndjekjes së komunikimeve.[66] Me këtë ligj, ndjekja e komunikimeve është definuat si njohuri sekrete dhe njëherësh krijim të një regjstri teknik të përmbajtjes së komunikimeve. Me mundësi që të riprodhohet. Ndjekja mund t'i përfshijë të gjitha llojet e komunikimeve telefonike dhe të tjera elektronike, si protokol i internetit, bisedë përmes protokolit të internetit, faqen e internetit dhe pos tën elektronike.[67] Ndjekja e komunikimeve në Maqedoni, të definuara kësisoj, i përfshin edhe komunikimet përmes aplikacioneve për transmetimin e zërit, përmbajtjet video dhe përmbajtjet tjera përmes internetit (p.sh. *Skype, Viber, Snapchat, WhatsApp, FaceTime*), por nuk e përfshin qasjen në meta të dhënat për komunikimet e realizuara elektronike. E fundit, nuk është në përputhje me listën për kontrollin e mbisundimit të së drejtës të Komisionit të Venecias, ku është saktësuar se edhe grumbullimi sekret i meta të dhënave për komunikime elektronike, paraqet ndjekje të komunikimeve.

Përveç përmbajtjes së bisedave dhe komunikimeve të tjera elektronike, **Ligji i procedurës penale** lejon qasje edhe te meta të dhënat. Në të vërtetë, si një prek masave të veçanta hetimore është përshkruar qasja në komunikimet e realizuara telefonike dhe të tjera elektronike, që për shkak të formulimit të keq, mund t'i përfshijë edhe meta të dhënat por edhe përmbajtjen e komunikimeve të këtilla. Nëse kjo masë duhet tu përkasë meta të dhënave , është e paqartë se cili është dallimi sa i përket nenit 287 të të njëjtit ligj. Në të vërtetë, në pjesën qe e rregullon procedurën parahetimore, me këtë nen përcaktohet se, me kërkesë të prokurorit publik, oparatorët e rrjeteve publike të komunikimit dhënësit e shërbimeve publike të komunikimit , janë të detyruar të dorëzojnë të dhëna për kontakte të realizuara në qarkullimin komunikativ për një person të caktuar.[68] Kjo paraqet një formë e meta të dhënave.

[65] Ligji për ndjekjen e komunikimeve, "Gazeta zyrtare e Republikës së Maqedonisë" nr. 121/2006, 110/2008 dhe 116/2012.
[66] Neni 1 nga Ligji për ndjekjen e komunikimeve.
[67] Neni 7 nga Ligji për ndjekjen e komunikimeve.
[68] Neni 287 i ligjit.

Baza për ndjekjen e komunikimeve

Ligji për ndjejen e komunikimeve lejon ndjekjen e komunikimeve për zbulimin dhe ndjekjen e kryerësve të veprave penale, si dhe për shkak të mbrojtjes së interesave të sigurisë dhe mbrojtjes së vendit.Teksti nën këtë titurr ndalet në ndjekjen , që lidhet me kryerësit e veprave penale, ndërsa ndjekja për shkak sigurie dhe mbrojtjeje është përpunuar nën titull të veçantë më posht.

Ndjekja e komunikimeve është caktuar si masë e veçantë hetimore në Ligjin e procedurës penale.[69] Këto masa janë rregulluar në kreun XIX, ku ligji vë në paj se mund të ndërmerren masa të veçanta hetimore- ndër të cilat është edhe ndjekja dhe incizimi i komunikimeve telefonike dhe të tjera elektronike- kur kjo është e domosdoshme për sigurimin e të dhënave dhe dëshmive për zhvillimin e procedurës penale, e **të cilat nuk mund të grumbulloren në tjetër mënyrë.**

Me ndryshimet dhe plotësimet e Ligjit për ndjekjen e komunikimeve në vitin 2012, u fshi dispozita që jepte definim më të ngushtë, për shkak të pengimit dhe ndjekjes të të cilave vepra penale, mund të ndiqen komunikimet.[70] Megjithatë, dispozita të tilla ekzistojnë në Ligjin e procedurës penale. Sipas këtij ligji, ndjekja e komunikimeve mund të përshkruhet si masë e veçantë hetimore në rastet në të cilat ato janë kryer, ndërmerren veprime për t'i kryer ose janë duke i përgatitur:[71]

- Vepra penale për të cilat parashihet dënimi me burg prej , të paktën katër vjet, ndërsa janë duke i përgatitur, në vijim e sipër është kryerja e saj ose janë kryer nga një grup i organizuar, nga një bandë ose nga ndonjë shoqëri tjetër krriminale;
- Vepra penale kundër shtetit dhe vepra penale kundër njerëzimit dhe të drejtës ndërkombëtare;
- Një varg veprash të tjera të rënga penale, prej vrrasjes e deri te terrorizmi dhe finansimi i terrorizmit.

Urdhëri mund të bëhet edhe për një person i cili praon ose çon dërgesa nga i dshuari ose i dyshuari përdor mjetin e tij të komunikimit.[72]

Nëse krahasohen këto baza me dispozitën e fshirë të Ligjit për ndjejen e komunikimeve, mund të përfundohet se janë zgjerur bazat për ndjekjen e e komunikimeve me këto vepra penale:

- Shfaqje e filmit pornografik për fëmijë;
- Grabitje (paraprakisht ishte përfshirë vetëm grabitja e personit të mitur);
- Joshje për marrëdhënie seksuale ose veprim tjetër seksualtë fëmijës që nuk ka mbushur 14 vjet;
- Dëmtim ose hyrje e paatorizuar në sistemin kompjuterik (neni 251, paragrafet 4 dhe 6 nga Kodi Penal; paraprakisht kjo sanksionohej vetm nëse vepra ishte kryer përmes mjeteve të komunikimit elektronik);
- Keqpërdorimi i procedurës së falimentimit;
- Nxjerrja jashtë vendit e të mirave që janë nën mbrojtje të përkohshme ose trashëgimive kulturore ose rrallësi natyrore (neni 266, paragrafi 1 të Kodit penal;

[69] Ligji i procedurës penale, „Gazeta zyrtare e Republikës së Maqedonisë" nr. 150/2010, 100/2012 dhe 142/2016.
[70] Ishte fshirë neni 8 i Ligjit.
[71] Nenet 253 dhe 255 të Ligjit për procedurë penale.
[72] Neni 255 i Ligjit për procedurë penale.

paraprakisht kjo përfshinte të mirat e rëndësishme ose e mirë e një rëndësie të veçantë për Republikën e Maqedonisë);

- Tjetërsim i trashëgimisë kulturore me rëndësi të veçantë, në pronësi shtetërore.

Mbetet përshtypja se është mjaft e gjerë gama e veprave penale, për të cilat lejohet përdorimi i ndjekjes së komunikimeve. Sipas rekomandimit relevant të Këshillit të Evropës, masa të veçanta hetuesie duhet të përdorur për zbulimin dhe hulumtimin e krrimit të rëndë.[73] Sipas konventës së Kombeve të Bashkuara, krrim i rëndë është ai që sipas legjislacionit nacionalështë i ndëshkueshëm me dënim me burg prej 4 e më shumë vjet.[74] Megjithatë, në mesin e veprave penale të cekura më lartë, për të cilat me ndryshime ligjore është mundësuar ndjekja e kounikimeve, ka edhe të atillë për të cilat dënimi i përshkruar minimal është gjatë muaj burg kurse, thuaja në të gjitha rastet e cekura , është nën 4 vjet burg. Sëkëndejmi, **është e nevojshme që të rishqyrtohet arsyeshmëria që të lejohet përdorimi i kësaj mase invazive për një gamë aq të gjere të veprave penale**, në bazë të analizës, a është cënimi i privatësisë proporcional me peshën e veprës penale për të cilën bëhet fjalë dhe dëshmitë ë pritet të grumbullohen me masat e veçanta të hetimit, përkatësisht me ndjekjen e komunikimeve.

Kërkesa për ndjekjen e komunikimeve

Teksti nën këtë titull i përket ndjekjes së komunikimeve, që lidhet me kryerësit e veprave penale, ndërsa ndjekja për shkak të sigurisë dhe mbrojtjes është përpunuar nën titull të veçantë më posht.

Sipas nenit 9 të Ligjit, kërkesë për ndjekjen e komunikimeve për zbulimin dhe ndjejen e kryerësve të veprave penale, gjykatësit kompetent i paraqet prokurori publik kompetent, me inisiative personale ose me propozim të Ministrisë së punëve të brendshme, Drejtorisë së policisë financiare ose të Drejtorisë së doganave. Kërkesa me shkrim për ndjekjen e komunikimeve i dorëzohet gjykatësit në procedurë paraprake dhe, midis tjerash, duhet të përmbajë: emrin e veprës penale; personin ose objektet ndaj të cilave do të kryhet ndjekja e komunikimeve (për shembull, numri i telefonit ose adresa e postës elektronike); mjetet teknike që do të përdoren; njohuritë dhe dëshmitë në bazë të të cilave mbështeten bazat e dyshimit dhe arsyetim për shkaqet për të cilat të dhënat dhe dëshmitë nuk mund të grumbullohen në mënyrë tjetër; kohëzgjatja e ndjekjes së komunikimeve si dhe lloji i sistemit telekomunikativ, numri i telefonit ose ndonjë e dhënë tjetr për identifikimin e lidhjes telekomunikative.[75]

[73] Council of Europe Committee of Ministers, Recommendation Rec (2005) 10 of the Committee of Ministers to member states on "special investigative techniques" in relation to serious crimes including acts of terrorism, i disponueshëm në https://wcd.coe.int/ViewDoc.jsp?id=849269&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.

[74] The United Nations Convention Against Transnational Organized Crime, Article 2i disponueshëm në:https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

[75] Neni 10 i Ligjit për ndjekjen e komunikimeve.

Brengos fakti që, **për ndjekjen e komunikimeve mjafton të theksohet vetëm baza e dyshimit- e jo dyshimi i bazuar-** për kryerjen e mundshme ose tanimë të kryer të veprës penale, që është një shkallë shumë e ulët e dyshimit.[76]

Urdhër për ndjekjen e komunikimeve

Teksti nën këtë titull ka të bëjë me ndjekjen e komunikimeve , që lidhet me kryerësit e veprave penale, ndërsa ndjekja për arsye të sigurisë dhe mbrojtjes është përpunuar nën tutull të veçantë, më posht.

Masëv e veçantë hetimore "ndjekja dhe regjistrimi i komunikimeve telefonike dhe komunikimeve të tjera elektronike" , pas kërkesës së arsyetuar nga prokurori publik, e përcakton gjykatësi në procedurë paraprake, me urdhër me shkrim. Masën e të pasurit qasje në komunikimet e realizuara telefonike dhe në komunikimet tjera elektronike, e cakton prokurori publik, me urdhër me shkrim.[77]

Sipas Ligjit për ndjekjen e komunikimeve, gjykatësi në procedurë paraprake, duhet të vendos lidhur me kërkesën e pranuar për ndjekjen e komunikimeve, në afat prej 48 orësh.[78] Afati i këtillë është mjaft i shkurtër, duke pasur parasysh se ekzistojnë raste në praktikë kur kërkesa ka të bëjë me mbi 100 persona, e do të duhej të përmbajë njohuri dhe dëshmi, të arsyetuara në mënyrë përkatëse, për bazat e dyshimit. Afati i shkurtër që është dhënë për të marrë vendim gjykatësi, mund të arsyetohet vetëm me ekzistimin e rasteve urgjente, për shemull, kur duhet të pengohet një vepër penale, të dokumentohet kryerja e saj , të shmanget ikja e kryerësve të mundshëm ose shkatërrimi i dëshmive. Prap se prap, për rastet urgjente, ligji në nenin 11 parashikon mundësinë që të kryhet ndjekja e komunikimeve , përkohësisht, në bazë të urdhërit gojor të gjykatësit, të dhënë me kërkesë gojore nga prokurori publik kompetent, dhe i cili është i vlefshëm në afat prej 48 orësh. Sëkëndejmi, **brengos afati i përshkruar prej 48 orësh se , vallë, a është i mjaftueshëm që gjyatësi të mundet në mënyrë adekuate ta shqyrtojë kërkesën** për ndjekjen e komunikimeve dhe të vendos a do të japë urdhër përkatës, kurse nuk është logjike që për kërkesën për vazhdimin e kohëzgjatjes së masës, është caktuar afat prej 72 orësh- që është më shumë se koha e caktuar për lejimin e parë të ndjekjes së komunikimeve . Me ndryshimet e ligjit për ndjekjen e komunikimeve në vitin 2012, është caktuar që urdhër gojor mund të jepet në raste urgjente, kur ekziston "rreziku që t'i shaktohet dëm i pakompensueshëm procedurës penale". Zgjidhja e vjetër ligjore ishte shumë më precize dhe më restriktive, sepse përshkruante që urdhër gojor mund të jepet vetëm kur ekziston rrezik nga:

- Shkaktimi i vdekjes ose lëndim i rëndë;
- Shkaktimi i dëmit material të pronës me përmasa të mëdha;
- Ikja e kryerësit të veprës penale për të cilën është caktuar dënim me burg të përjetshëm.

Prandaj, **nevojitet të saktësohen, në mënyrë më restriktive, kushtet në të cilat lejohet që ndjekja e komunikimeve të kryhet në bazë të urdhërit gojor.**

Me qëllim që **gjykatësi të marrë vendim të informuar për arsyeshmërinë e kërkesës për ndjekjen e komunikimeve, si dhe të vlerësojë a janë përmbushur kushtet për cënimin**

[76] Sipas Ligjit të procedurës penale, bazat e dyshimit janë njohuri të cilat, në bazë të njohurisë dhe përvojës mund të vlersohen si dëshmi për vepër të kryr penal, kurse dyshimi i bazuar është shkallë më e lartë e dyshimit, bazuar në dëshmitë e grumbulluara, të cilat shpiejnë në përfundimin se një person i caktuar ka kryer vepër penale.

[77] Neni 256 i Ligjit për procedurë penale.

[78] Neni 11 i Ligjit për ndjekjen e komunikimeve.

e privatësisë dhe të dhënave personale, është e domosdoshme që të përfshihet edhe një palë në procedurë, që do t'i përfaqësonte interesat e personave, komunikimet e të cilëve propozohet që të ndiqen. Këtë rol mund ta kryejë paneli i ekspertëve, përfaqësuesi i Drejtorisë për mbrojtjen e të dhënsve personale ose avokati i popullit, si "përfaqësues i interesit publik". [79]

Sa i përket sigurimit të urdhërit nga autoritetet gjyqësore për ndjekjen e komunikimeve, bashkëbiseduesit të cilët më parë kanë qenë pjesë e MPB theksuan se ekzistojnë raste që urdhëri nga gjykatësi të kërkohet në mënyrë retroaktive, me ç'rast nga gjykatësit kërkohet ta nënshkruajnë urdhërin , bile edhe pa e ditur se mbi çfarë baze autorizojnë ndjekjen e komunikimeve dhe ndaj kujt. Me këtë rast, ishin theksuar raste në të cilat, pa urdhër të dhënë nga gjykatësi ka filluar ndjekja e komunikimeve, e në momentin kur është gjetur indicia për vepër penale, është kërkuar urdhëri në mënyrë retroaktive. Në të kaluarën, kur ka akzistuar evidencë e shkruar me dorë e dokumentacionit , është bërë edhe përshkrimi i librave të tërë të evidencës që të fshihet dhënia e urdhërave gjyqësore retroaktive, kurse me zbatimin e evidencës elektronike, procesi i këtillë i falsifikimit të evidencës, kinse, vetëm është lehtësuar. Dyshim në efektivitetin e mbikëqyrjes së mëparshme gjyqësore të ndjekjes së komunikimeve, krijon edhe e dhëna se deri më tash nuk ka pasur rast të refuzimit të kërkesë nga gjykatat për zbatimin e masave të veçanta hetimore.

Ligji i procedurës penale, në nenin 257, e përshkruan përmbajtjen e urdhërit për ndjekjen e komunikimeve , që e sjell gjykatësi. Është kontestuese që **ky nen nuk përshkruan obligimin që në urdhë të ceket organi me kërkesë të të cilit urdhërohet ndjekja e komunikimeve.** Ku element i urdhërit ishte i domosdoshëm, në përputhje me nenin13 të Ligjit për ndjekjen e komunikimeve, që ishte fshire, me ndryshimet dhe plotësimet në vitin 2012.

Thënë kushtimisht, ligji përshkruan procedurë ankimimi, nëse gjykatësi nuk pajtohet me kërkesën për ndjekjen e komunikimeve ose me kërkesën për vazhdimin e kohëzgjatjes. Në këtë rast, rreth kërkesës duhet të vendos këshilli treanëtarësh i gjykatës kompetente të shkallës së parë.[80] **Është brengosëse që "e drejta respektive e ankesës" nuk është vendosur edhe për mbrojtjen e të drejtave dhe interesave të personave , komunikimet e të cilëve propozohet të ndiqen.** Në të vërtetë, ligji nuk përmban dispozita me të cilat do t'i mundësohet entitetit përkatës, për shembull, Drejtorisë për mbrojtjen e të dhënave personale, ose avokatit të popullit të marrë pjesë në procedurën e dhënies së urdhërit për ndjekjen e komunikimeve dhe të ketë mundësi, para një instance tjetër, ta kontestojë arsyeshmërinë e dhënies eventuale të urdhërit nga gjykatësi në procedurë paraprake**.**

Kohëzgjatja e ndjekjes së komunikimeve

Me ndryshimet dhe plotësimet e Ligjit për ndjekjen e komunikimeve në vitin 2012 ishte fshirë dispozita , sipas së cilës, ndjekj a e komunikimeve mund të zgjas një kohë të caktuar, që e imponoi pyetjen- në çfarë mënyre do të sigurohet që ndjekja e komunikimeve

[79] Mekanizën i këtillë eziston në Kvinslend, Austri
[80] Neni 11-a i Ligjit për ndjekjen e komunikimeve.

të një subjekti të caktuar të mos bëhet vazhdimisht.[81] Edhe pse dispozitat tjera të ligjit definojnë përkufizime kohore për ndjekjen e komunikimeve, për një vetër konkrete penale, megjithatë, nuk ekziston dispozitë me të cilën do të pengohej ndjekja e vazhdueshme e komunikimeve të dikujt. Ndjekja e vazhdueshm e komunikimeve të dikujt është e mundur , nën arsyetimin hipotetik se vazhdimisht paraqiten dyshime të reja të bazuara për ndonjë vepër të re penale.

Afati që e përmban kërkesa për ndjekjen e komunikimeve është kufizuar në 4 muaj dhe mund të vazhdohet edhe për 4 muaj.[82] Kërkesa për vazhdim i dërgohet Ministrisë së punëve të brendshme, Drejtorisë së policisë finansiare ose Drejtorisë së doganave, e cila, nëse pajtohet, e dërgon te gjykatësi kompetent.[83] Për veprat penale për të cilat është caktuar dënim me burg prej, të paktën, katër vjet, për të cilat ekziston dyshim i bazuar se janë kryer nga një grup i organizuar, nga një bandë ose shoqëri tjetër krriminale, gjykatësi i procedurës paraprake mund ta vazhdojë këtë afat më së shumti edhe për gjashtë muaj.[84]

Së këndejmi, ndjekja nuk guxon t'i kalojë 14 muaj. Afatet e këtilla janë dukshëm më të gjata se ata që ishin parashikuar para ndryshimeve në Ligjin për ndjekjen e komunikimeve në vitin 2012. Paraprakisht masa lejohej në kohëzgjatje perj një muaji, me mundësi që me kërkesë shtesë të vazhdohet edhe me nga një muaj çdo herë, por e tërër kohëzgjatja të mos kalonte një vit.

Gjetjet kuçe të Pribes

Grupi i ekspertëve të lartë për çështjet sistemore të sundimit të drejtësisë, udhëhequr nga Rajnhard Pribe, në raportet e vitit 2015 dhe 2017 si arsye kryesore për skandalin me përgjimin e thekson koncentrimin e pushtetit në Drejtorinë e siguris dhe kundërzbulimit (DSK) dhe mbikëqyrjen e keqe të saj. Në raportin e vitit 2015 theksohet se DSK vepron jashtë autorizimeve ligjore në emër të Qeverisë, për kontrollin e funksionarëve më të lartë në administratën publike, prokurorëve,gjykatësve dhe oponentëve politikë me përzierje në pavarësinë e gjyqësorit dhe institucioneve të tjera relevante.Në raportin e shtatorit të vitit 2017 theksohet se nuk janë ndërmarrë hapa konkretë për tejkalimin e problemeve.

Sipas grupit të ekspertëve, vetëm DSK ka aftësi teknike për ndjekjen e komunikimeve edhe gjatë hetimeve të zbulimit edhe gjatë hetimeve penale. Ndjekja kryhet nga DSK në emrin personal dhe në emër të Policisë, Drejtorisë së doganave dhe Policisë financiare Në bazë të neneve 175 dhe 176 të Ligjit për komunikime elektronike çdo provajder nacional i telekomunikimeve nacionale i mundëson kopjim të tërë komunikimit , me çka DSK mundet drejtpërdrejtë t'i ndjek komunikimet-në mënyrë të pavarur dhe të pa penguar – pa marrë parasysh a është dhënë ose jo urdhër gjyqësor.

[81] Raport nga debati publik i Këshillit nacional për integrime evropiane rreth versionit punues të Propozimligjit për ndryshime dhe plotësime të Ligjit për ndjekjen e komunikimeve, Kuvendi i Republikës së Maqedonisë, 16.07.2012 Raporti është i disponueshëm në:https://www.sobranie.mk/WBStorage/Files/JRSledenjenakomunikacii.pdf

[82] Neni 260 i Ligjit për procedurë penale.

[83] Neni 15 i Ligjit për ndjekjen e komunikimeve.

[84] Neni 260 260 i Ligjit për procedurë penale.

Ligji për procedurë penale përcakton që, kur të arrihen qëllimet, për të cilat edhe janë caktuar masa të veçanta hetimore, ose do të pushojnë së ekzistuari bazat për shkak të të cilave janë lejuar, organi i cili e ka dhënë ose e ka vazhduar urdhërin, është i detyruar menjëherë të urdhërojë ndërprerjen e masave. Megjithatë, në praktikë është e mundur që gjykatësi ose prokurori publik të mos kuptojë menjëherë për rrethanat e ndryshuara, dhe **është e rekomandueshme që kushti i këtillë të përfshihet në mesin e elementeve të domosdoshme të urdhërit për ndjekjen e komunikimeve dhe ta obligojë organin i cili duhet ta realizojë urdhërin**.[85] Për këtë nevojitet plotësim në nenin 257 të Ligjit të procedurës penale.

Pribe për reformimin e DSK

Në raportin e grupit të ekseprtëve të vitit 2017 është theksuar se kanë filluar proceset e reformave përmes projektit me mbështetje ndërkombetare, me ç'rast është përgatitur analizë dhe janë cekur modelet e menaxhimit, zbatimit dhe mbikëqyrjes së përgjimit. Njëra prej kahjeve të propozuara për tejkalimin e situatës momentale është marrja e qasjes së drejtpërdrejtë të DSK në përmbajtjen e komunikimeve dhe kthimi i riorientimit të komunikimeve te operatorët, të cilët sipas urdhërit gjyqësor, do të jenë të detyruar të mundësojnë kushte për përgjim, ndërsa

Alternativa tjetër e mundshme është krijimi i një qendre të veçantë operative teknike e cila do të jetë e obliguar për ndjekjen e komunikimeve, por vetëm nëse vlerësohet se trupi i këtillë i ri do të kishte mundësi t'u rezistonte presioneve dhe ndikimeve të jashtme. Në vend të lirisë së shprehjes- vetëcenzurë dhe izolim

Hulumtimi ndërkombëtar i vitit 2014 i Pen qendrës amerikane, tregoi se shkrimtarët, nën presionin e frikës nga ndjekja masive e komunikimeve, parapëlqenin vetëcenzurën. Varësisht nga vendi, për shkak të një frike të këtillë ndërmjet 34% dhe 61% e shkrimtarëve i shmangeshin të folurit ose të shkruarit në temë të caktuar, ose mendoheshin seriozisht që ta bëjnë këtë. Ndërmjet një të katërtës dhe dy të tretave të shkrimtarëve kishin filluar që tu ikin qëllimisht temave të caktuara në komunikim telefonik ose përmes mejl-it,

Zbatimi oparativ i ndjekjes së komunikimeve

Sipas Ligjit për procedurë penale, masat e veçanta hetimore- përfshirë edhe ndjekjen e komunikimeve- zbatohen nga prokurori publik ose policia gjyqësore nën kontrollin e prokurorit publik. Kjo nuk është harmonizuar me ligjin për ndjekjen e komunikimeve, as në praktikë ku zbatimi operativ i ndjekjes së komunikimeve i është deleguar Ministrisë së punëve të brendshme, më saktesisht, Drejtorisë së sigurisë dhe kundërzbulimit.

Sipas nenit 175 të Ligjit për kmunikime elektronike, operatorët janë të detyruar t'i sigurojnë të gjitha kushtet e domosdoshme teknike që të mundësojnë ndjekjen e komunikimeve

[85] Current practices in electronic surveillance in the investigation of serious and organized crime, United Nations Office On Drugs And Crime, Vienna, 2009, E disponueshme në: https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf

në rrjetat e tyre, në përputhje me Ligjin për ndjekjen e komunikimeve.

Operatorët janë të obliguar , me shpenzime të veta, të sigurojnë dhe mirëmbajnë pajisjen, interfejs adekuat dhe të vendosin linja elektronike të komunikimit për transmetim deri te organi i autorizuar për ndjekjen e komunikimeve. Ligji e rregullon edhe specifikimin teknik të pajisjes dhe interfejsit për ndjekjen e komunikimeve, përkatësisht për këtë operatorët duhet t'i ndjekin instrukcionet e organit të autorizuar për ndjekjen e komunikimeve. Operatorët obligohen wë të mundësojnë ndjekje të komunikimeve në kohë reale.

Kjo që u theksua shpie në atë që edhe në Ligjin e komunikimeve elektronike të vitit 2014 mbeti qasja e pakufizuar dhe e drejtpërdrejtë e MPB në tërë trafikun telekomunikativ në Maqedoni. Në të vërtetë, me ndryshime dhe plotësimet e vitit 2010të Ligjit ë vjetër për komunikime elektronike[86] , u përfshinë risi në mënyrën e ndjekjes së komunikimeve. Në të vërtetë, përveç obligimit të operatorëve që të sigurojnë pajisje adekuate dhe interfejs për zbatimin e masës së përgjimit të komunikimeve, u shtua edhe obligimi që pajisja nënkupton vendosje të linjave telekomunikative dhe pajisjes telekomunikative për transmetim deri te vendi i organit të autorizuar për ndjekjen e komunikimeve. Së këndejmi, DSK mund ta kryejë ndjekjen pa veprime plotësuese nga ana e operatorëve dhe pa dijen e tyre. Pajisja që e ka operatori (e siguruar në bazë të specifikimeve të dhëna nga MPB), përdoret kryekëput për t'i orientuar përmbajtjet e komunikimeve drejt DSK-s. Për shkak të obligimit ligjor për sigurimin e qasjes së drejtpërdrejtë të MPB në komunikimet, gjatë porositjes së pajisjes, vetë "Telekomi i Maqedonisë" ka kërkuar që aktivitetet e ndjekjes të jenë të padukshme pr operatorin, përkatësisht operatori të mos kuptojë se kush, kur dhe sa ndiqet, me qëllim që të mos ketë kurrfarë përgjegjësie.

Qasja e drejtpërdrejtë në përmbajtjen e komunikimeve e shton rrezikun e keqpërdorimeve, prkatësisht rasteve që ndjekja të kryhet pa urdhër adekuat nga gjykatësi. Rreziku shtesë paraqitet edhe për shkak të mundësisë teknike që MPB t'i riorientojë komunikimet e ndjekura drejt entiteteve tjera dhe lokacione të tjera. Bashkëbiseduesit theksuan se riorientimi i tillë kryhet edhe përmess rrugës pa tel deri te tre lokacione të MPB, që krijon rreziqe të mëdha për ndjekjen e komunikimeve nga persona të tretë, ndërsa u dhanë edhe pretendime për riorientimin e komunikimeve të ndjekura në lokale partiake.

Për dallim nga qasja e tashme e MPB në përmbajtjen e komunikimeve, deri në vitin 1998, për shkak të përdorimit të llojit tjetër të pajisjes, që të kryejë ndjekje të ndonjë komunikimi, ka qenë e nevojshme që MPB paraprakisht ta njoftojë operatorin përkatës dhe të dorëzojnë urdhër nga gjykatësi në bazë të të cilit, operatori do ta mundësojë ndjekjen. Sistemi i vjetër ka mundësuar që edhe operatorët të përfshihen në mbikëqyrjen paraprake, duke siguruar që janë përmbushur kushtet për ndjekjen e komunikimeve. Me këtë, ka ekzistuar edhe një pikë në sistem- jashtë MPB- në të cilën organet e mbikëqyrjes kanë mundur të inspektojnë dhe të kontrollojnë.

Në vitin 2010, Gjykata kushtetuese mori vendim me të cilin shfuqizohen nenet kontestuese që kanë të bëjnë me ndjekjen e komunikimeve, në Ligjin e komunikimeve elktronike të miratuar në vitin 2005.[87] Në përputhje me këtë vendim,[88] Gjykata u deklarua se

[86] Ligji për ndryshime dhe plotësime të Ligjit për komunikime elektronike ("Gazeta zyrtare e Republikës së Maqedonisë", nr. 83/2010).

[87]Neni 4 pikat 47 dhe 48, neni 112 paragrafet 7 dhe8, neni 114 paragrafet 7, 8 dhe 9, neni 115 dhe neni 138 paragrafi 1 pikat 28 dhe 29 të Ligjit për komunikime elektronike („Gazeta zyrtare e Republikës së Maqedonisë" nr.13/2005, 14/2007, 55/2007, 98/2008 dhe83/2010).

dispozitat e këtij ligji përmbajnë rrezik nga ndërhyrja jokushtetuese dhe e paautorizuar në privatësinë dhe të njëjtat nuk janë precize, u ekspozohen improvizimeve ose interpretimeve dhe u japin forcë direkte organeve të autorizuara për zbatimin e masës së ndjekjes së komunikimeve pa e vendos autorizimin e tyre në kornizë të fuqishme ligjore. Gjykata vlerësoi se dispozitat kontestuese të Ligjit nuk përmbajnë garanci të mjaftueshme kundër keqpërdorimit eventual nga organi i autorizuar , me dhënien e mundësisë teknike për ndjekje të vazhdueshme dhe të pavarur të përmbajtjes së komunikimit si dhe gjatë grumbullimit të të dhënave të nevojshme lidhur me komunikimin e realizuar. Në mungesë të dispozitave të qarta ligjore lidhur me ndjekjen e komunikimeve, ekziston rrezik i madh për krijimin e forcës së pakufishme, në kundërshtim me parimin e sundimit të së drejtës.

Përkundër vendimit të këtillë të Gjykatës kushtetuese, Ligji i komunikimeve elektronike i vitit 2014 mundësoi rishtazi që Ministria e punëve të brendshme të ketë *qasje të drejtpërdrejtë dhe të pakufizuar* në përmbajtjen e *të gjitha* komunikimeve elktronike të *të gjithë* qytetarëve. Përkundër kësaj, zgjidhja ligjore që ishte në fuqi deri në vitin 2010 ishte shumë më e volitshme për mbrojtjen e privatësisë, e në përputhje me të, operatorët mundësonin qasje në përmbajtjen e komunikimeve të një shfrytëzuesi të caktuar, vetëm në bazë të urdhërit nga gjykata kompetente. Në vitin 2015 ishte paraqitur iniciativa për rishqyrtiin e kushtetutshmërisë së nenit 175 të Ligjit për komunikime elektronike. Kryetari i Gjykatës kushtetuese nuk e fuste këtë lëndë në rend dite dy vjet edhe pse gjykatësi i ngarkuar-raportues e kishte përgatitur lëndën ndërsa Gjykata mund të thirret në vendimin paraprak dhe përsëri ta shfuqizojë dispoziten kontestuese. Gjykata kushtetuese më 21.06.2017 vendosi të zhvillojë procedurë pr vlerësimin e kushtetutshmerisë së nenit të përmendur. Vendimi i Gjykatës Kushtetuese ishte paralajmëruar se do të dorëzohet në Kuvend, i cili do të ketë 30 ditë afat për përgjigje.

Ligji i komunikimeve elektronike dhe Ligji për ndjekjen e komunikimeve nuk i ndajnë kompetencat, rregullat dhe teknikat e ndjekjes së komunikimeve gjatë hetimeve penale nga ato që kanë karater të sigurisë dhe zbulimit- që është cekur si një problem tjetër në përparësitë urgjente të reformave.[89].

Qeveria e Republikës së Maqedonisë në **Planin 3-6-9**[90] e thekson nevojën e reformës së shërbimeve të zbulimit dhe të sigurisë me qëllim të kthimit të besimit në to. Me këtë plan, Qeveria mori si obligim të përgatis plan për realizimin e rekomandimeve të grupit të ekspertëve të lartë për çështjet sistemore të sundimit të drejtësisë, lidhur me ndjekjen e komunikimeve, me proces transparent dhe inkluzivtë konsultimeve me të gjitha palët e interesuara. Plani parashikonedhe pjesëmarrje të organeve të përfshira në ndjekjen e komunikimeve në mbledhje të rregullta të komisionit përkatës të Kuvendit për mbikëqyrje të punës së tyre si dhe pjesëmarrje të Drejtorisë së sigurisë dhe kundërzbulimit dhe Agjencisë sl zbulimit në mbledhje të rregullta të komisionit të Kuvendit i cili kryen mbikëqyrjen e tyre.

---

[88] Vndim i Gjykatës kushtetuese, nr. 139/2010-0-1 i datës 15.12.2010, i disponueshëm në: http://www.ustavensud.mk/domino/WEBSUD.nsf/ffc0feee91d7bd9ac1256d280038c474/7119424dde39fdadc1257809002db948?OpenDocument

[89] Prioritete reformash urgjente për Maqedoninë ,qershor 2015. I disponueshëm në: https://eeas.europa.eu/sites/eeas/files/urgent_reform_priorities_en.pdf

[90] Plani 3-6-9 i Qeverisë së Republikës së Maqedonisë, i disponueshëm në: http://vlada.mk/sites/default/files/programa/2017-2020/Plan%203-6-9%20MKD.pdf

Përdorimi i informacioneve nga ndjekja e komunikimeve

Të plotësohet neni 258 i ligjit për procedurë penale në pjesën e raportit të policisë gjyqësore për ndjekjen e komunikimeve që i dorëzohet prokurorit publik. Detyrimisht në raport duhet të evidentohet numri i telefonit , linja e përdorur ose adresa e postës elektronike (apo lloj tjetër identifikuesi) që janë ndjekur.

- Te rishqyrtohen nenet 255 dhe 263 të ligjit për procedurë penale për t'u siguruar se të dhënat e grumbulluara nga ndjekja e komunikimeve janë konform qëllimit për të cilin është dhënë urdhëri për ndjekje. Në të vërtetë, ky qëllim është grumbullimi i të dhënave për rastet e caktuara të veprave penale apo vërtetimin e personave që janë përdorues të linjave telefonike, e-mail adresave apo të tjerave, e që janë objekt i veprës penale. Përderisa nga ndjekja e komunikimeve merren informacione për përfshirjen e personave të tjerë në vepra penale, apo me të cilat vërtetohet dyshimi për vepra të tjera penale, të lëshohet urdhër i ri nga ana e gjykatësit që të mund të vazhdojë ndjekja e komunikimeve, ndërsa procesverbalet e ndjekjes të mund të përdoren në gjyq. Arsyetimi që do të mund t'i jepej gjykatësit për përfshirje më të gjerë të masës nuk duhet të bazohet në komunikimet e regjistruara që e tejkalojnë urdhërin dhe në bazë të të cilit janë grumbulluar.
- Të kihet kujdes për kategoritë e veçanta të të dhënave personale (ashtu siç është paraparë me ligjin për mbrojtjen e të dhënave personale), respektivisht gjatë ndjekjes së komunikimeve të hiqen apo fshihen dëshmitë të lidhura me me këtë kategori të të dhënave personale.

Njoftimi i personave, komunikimet e të cilëve janë ndjekur, e drejta për t'i kontestuar komunikimet e ndjekura, e drejta për ankesë dhe kompensim të dëmit

Ndryshimet ligjore duhet të paraqesin një detyrim për të informuar personat e interesuar për masat e posaçme hetimore pas përfundimit të tyre. Të paktën personi, të cilit i janë grumbulluar të dhënat personale, të mund të disponojë me informatat siç janë: identiteti i kontrollorit, ekzistimi i operacionit për grumbullim, qëllimi i operacionit, e drejta për të shtruar ankesë, e drejta për të kërkuar qasje deri te të dhënat e grumbulluara, por edhe të kërkojë ngrirje dhe restrikcion të përpunimit të mëtejmë. E drejta për të patur qasje deri te informacionet të mund të shmanget vetëm në rast kur mund të dëshmohet se mund ta pengojë apo prejudikojë ndjekjen penale dhe këtë të mund ta bëjë ndonjë organ i pavarur.

- Të parashihen mjete efektive juridike që mund të përdoren në rastet kur një person beson se të drejtat e tij janë shkelur nga autoritetet kompetente gjatë ndjekjes së komunikimeve. Ndër të tjera, personat, komunikimet e të cilëve ndiqen, të kenë mundësi ligjore për ankesë deri te Drejtoria për Mbrojtjen e të Dhënave Personale për përdorimin e të dhënave të tyre personale. Organizatat joprofitabile që veprojnë në sferën e mbrojtjes së fshehtësisë së të dhënave personale të kenë të drejtë ligjore të paraqesin ankesa dhe t'i përfaqësojnë personat e përfshirë në ndjekjen e komunikimeve.

Mbrojtja, ruajtja dhe shkatërrimi i komunikimeve të ndjekura

• Nevojitet **forcimi** i dispozitave ligjore për sigurinë e të dhënave të grumbulluara nga ndjekja e komunikimeve dhe për shkatërrimin e tyre në rastet kur ato nuk janë më të nevojshme për qëllimin për të cilin janë mbledhur. Në ligjin për ndjekjen e komunikimeve të parashihen masa të detajizuara për sigurinë gjatë përpunimit të të dhënave në pajtim me Direktivën 2016/680 për mbrojtjen e të dhënave në polici dhe të drejtën penale. Mes tjerash, të zbatohet parimi i minimizimit i të dhënave gjatë ndjekjes së komunikimeve, duke përfshirë edhe pseudoanonimizimin-përpunimin e të dhënave në mënyrë që të dhënat personale të mos mund t'i përshkruhen një personi pa patur informacione shtesë të cilat ruhen si të veçanta dhe janë objekt I masave teknike e organizative të sigurisë. Të sigurohet se gjatë shkatërrimit të të dhënave të shkatërrohen edhe procesverbalet dhe të gjitha kopjet në të gjitha institucionet që kanë qenë të kyçura në ndjekje.

• Kur si rezultat i qasjes së paautorizuar do të ketë shkelje të të dhënave personale të mbledhura nga ndjekja e komunikimeve, organi kompetent duhet menjëherë të informojë organin mbikëqyrës për mbrojtjen e të dhënave personale dhe të personave, të dhënat personale të të cilëve janë rrezikuar.

Veçantitë e ndjekjes së komunikimeve me qëllim të mbrojtjes së interesave të sigurisë dhe mbrojtjes së vendit

Për shkak të mbrojtjes së interesave të sigurisë dhe mbrojtjes së vendit është i domosdoshëm vlerësimi paraprak i sigurisë se a duhet të kërkohet që dikujt t' i ndiqen komunikimet.

Mbikëqyrja dhe kontrolli gjatë ndjekjes së komunikeve

• Të miratohet një rregullore që do të sigurojë zbatim efikas të një procedure për marrjen e certifikatës së sigurisë për anëtarët e komisioneve mbikëqyrëse parlamentare. Deputetët të cilët nuk do të marrin një certifikatë të tillë brenda një kohe të arsyeshme, nuk do të kenë mundësi të jenë anëtarë të këtyre komisioneve.

• Të evidentohen të gjitha të dhënat për qasje kah sistemi për ndjekjen e komunikimeve.

Përdorimi i ipnformacioneve të marra nga ndjekja e komunikimeve

Në vitin 2012 u fshinë disa dispozita të Ligjit për ndjekjen e komunikimeve, me të cilat përcaktohej obligimi i Ministrisë së Punëve të Brendshme që të përgatit raport për

gjykatësin në procedurë paraprake , për çdo lëndë të përfunduar nga ndjekja e komunikimeve, duke e rregulluar përmbajtjen e raportit të tillë konform ligjit.[91]

Megjithatë, në Ligjin e Procedurës Penale, ka dispozitë ku thuhet se pas zbatimit të masave të posaçme hetimore, policia gjyqësore e përgatit raportin, të cilin ia dorëzon Prokurorit Publik.[92] Në raport figuron koha e fillimit dhe e mbarimit të masës, numri dhe identiteti i personave të përshirë me masën, jep një përshkrim të shkurtër për rrjedhën dhe rezultatet nga zbatimi i masës. **Përcaktimi i këtillë ka nevojë të plotësohet me detyrimin që në raport të figuron edhe numri i linjës telefonike që është ndjekur, apo i linjave tjera që përdoren si dhe adresa e postës elektronike**. Kjo për faktin se ndjekje të komunikimeve mund të urdhërohet edhe për objekte, si lëndë të veprës penale (linja telefonike apo adresa e postës elektronike).

Të gjitha të dhënat, njoftimet, dokumentet dhe objektet e prokuruara gjatë zbatimit të masës së posaçme hetimore, mund të përdoren si dëshmi në procedurën penale.

Sipas nenit 255 të Ligjit për Procedurë Penale, përderisa gjatë zbatimit të masës janë ndjekur dhe inçizuar komunikimet e personave që nuk kanë qenë të përfshirë me urdhëresë, Prokurori Publik është i obliguar t'i ndajë ato dhe ta informojë gjykatësin për procedurën paraprake. Me propozim të Prokurorit Publik, gjykatësi i procedurës paraprake mund të urdhërojë që nga dokumentacioni i plotë i zbatimit të masës, të veçojë vetëm pjesët që kanë të bëjnë me veprën penale, për të cilën është lëshuar urdhëri.

Në nenin 263 të Ligjit për Procedurë Penale, gjithashtu thuhet se nëse gjatë zbatimit të masës fitohen të dhëna për ndonjë vepër tjetër penale, që nuk është e përfshirë me urdhërin, masa do të vazhdojë vetëm nëse bëhet fjalë për vepër penale, për të cilën janë paraparë masa të posaçme hetimore. Të dhënat e grumbulluara mund të shfrytëzohen si dëshmi gjatë procedurës penale.

Nenet 255 dhe 263 kanë nevojë për rishqyrtim, për t 'u siguruar se të dhënat e grumbulluara nga ndjekja e komunikimeve, janë konform qëllimit për të cilin është dhënë urdhëri dhe janë mbledhur të dhënat.

Domethënë, ky qëllim është mbledhja e të dhënave për veprat penale dhe personat e paracaktuar ose identifikimin e personave duke përdorur një linjë telefonike, linjë tjetër ose adresë e-mail, që është objekt i një vepre penale. Sëkëndejmi, përfshirja e personave të rinjë ose ngritja e veprave të reja penale, kërkon një urdhër të ri nga gjykatësi, ndërsa kërkesa për një gjë të tillë nuk duhet të bazohet në komunikimet e regjistruara që e tejkalojnë urdhërin, në bazë të të cilit janë mbledhur.

Sipas Ligjit të Procedurës Penale, te njëra nga masat e parashikuara[93] inçizimi do të ndërpritet nëse gjatë regjistrimit ekzistojnë tregues se dëshmitë prekin sferën e jetës private dhe familjare. Dokumentacioni për dëshmitë e këtilla menjëherë duhet të shkatërrohet.[94] Mbetet e paqartë përse ligjvënësi nuk ka parashikuar kujdes të këtillë edhe për kategoritë e veçanta të të dhënave personale, të cilat sipas Ligjit për Mbrojtjen e të Dhënave Personale nuk guxojnë të përpunohen, gjegjësisht mund të përpunohen vetëm në kushte të veçanta,[95]

[91] Nenet 19 dhe 21 të ligjit për ndjekjen e komunikimeve.

[92] Neni 258 i ligjit të procedurës penale.

[93] Ndjekja dhe inçizimi në shtëpi, në hapësirë të mbyllur apo të rrethuar që i takon asaj shtëpie apo hapësirën e biznesit të caktuar si privat ose në një automjet dhe hyrjen në ato mjedise me qëllim krijimin e kushteve për ndjekjen e komunikimit.

[94] Neni 268 i ligjit për procedurë penale.

[95] Ligji për mbrojtjen e të dhënave personale përcakton kategoritë e veçanta të të dhënave personale që nuk mund të përpunohen ose mund të përpunohen vetëm në kushte të veçanta të përcaktuara në ligj: të dhënat

dhe të cilët , në këtë rast, mund të grumbullohen me zbatimin e masës për ndjekje dhe inçizim të komunikimeve telefonike dhe të tjera elektronike.

Informimi i personave, komunikimet e të cilëve ndiqen, e drejta për t'i kundërshtuar komunikimet e ndjekura, e drejta për paraqitjen e kundërshtimit dhe kompensimi i dëmit

Ligji për ndjekjen e komunikimeve përcakton se personi, të cilit i ndiqet komunikimi, ka të drejtë të kundërshtojë vërtetësinë e të dhënave të mbledhura dhe ligjshmërinë e procedurës për ndjekjen e komunikimeve të tij, në një procedurë të përcaktuar me Ligjin për Procedurën Penale të Republikës së Maqedonisë.[96] Megjithatë, është simptomatike që me ndryshimet dhe plotësimet e ligjit në vitin 2012, u fshi përcaktimi i ligjit me të cilin ndaloheshte ndjekja e komunikimeve pa urdhër të gjykatës kompetente.[97]

Në nenin 4 të ligjit , me të cilin klasifikoheshin informatat e grumbulluara përmes ndjekjes së autorizuar, u fshi fjala "e autorizuar ". Përveç kësaj, Ligji për Procedurë Penale të Republikës së Maqedonisë nuk përcakton një procedurë të veçantë për të vënë në dyshim vërtetësinë e të dhënave të mbledhura dhe ligjshmërinë e ndjekjes së komunikimeve.

Në rast të një vendimi gjyqësor se komunikimi është ndjekur në kundërshtim nga dispozitat e ligjit për ndjekjen e komunikimeve, personi e ka të drejtën e kompensimit nga buxheti i shtetit.[98] Por, **nuk është saktësuar se si këta individë do të jenë në gjendje të shfrytëzojnë të drejtën për të kundërshtuar dhe për të kompensuar dëmin, kur në ligjin për ndjekjen e komunikimeve shlyhet dispozita sipas së cilës, pas miratimit të një vendimi për të kryer një hetim, ata duhet të ishin të njoftuar me raportin për ndjekjen e komunikimeve,** të përgatitur nga Ministria e Brendshme.[99] Ligji për Procedurën Penale përcakton që pas përfundimit të masave të posaçme hetimore, nëse nuk e cënon procedurën, me kërkesë të personit të interesuar, Prokurori Publik ia dorëzon urdhërin me shkrim. Si në rastin e mëparshëm, personat në fjalë, që të mund të paraqesin një kërkesë të tillë, së pari duhet të dijnë se komunikimet e tyre janë ndjekur, por ligji nuk parashikon një mekanizëm të qartë në këtë drejtim. Prandaj, **ndryshimet ligjore janë të nevojshme për të futur një detyrim për të informuar personat në fjalë për masat e posaçme hetimore, pas përfundimit të tyre.**

Mbrojtja, ruajtja dhe shkatërrimi i komunikimeve të ndjekura

Me ndryshimet e ligjit të ndjekjes së komunikimeve në vitin 2012, u fshinë edhe masat mbrojtëse për ruajtjen e të dhënave për ndjekjen e komunikimeve, të cilat rekomandonin

---

personale që zbulojnë origjinën racore ose etnike, politike, fetare, filozofike dhe përkatësi të tjera, anëtarësim në Sindikata dhe të dhëna në lidhje me shëndetin e njeriut, duke përfshirë të dhëna gjenetike, të dhëna biometrike ose të dhëna që lidhen me jetën seksuale.

[96] Neni 6 i ligjit për ndjekjen e komunikimeve.

[97] Ligji për ndryshimin dhe plotësimin e Ligjit për ndjekjen e komunikimeve, Gazeta Zyrtare e Republikës së Maqedonisë nr.116 / 2012.

[98] Neni 28 i ligjit për ndjekjen e komunikimeve.

[99] Ligji për ndryshimin dhe plotësimin e ligjit për ndjekjen e komunikimeve, Gazeta zyrtare e Republikës së Maqedonisë nr.116/2012.

ruajtjen e tyre nëpër dosje të vulosura te gjykatësi në procedurë paraprake dhe te prokurori kompetent, për hapjen e të cilave domosdo nevojitet urdhër të lëshuar gjyqësor, si dhe procerverbal të mbajtur gjatë hapjes. E njëjta ka të bëjë edhe me përcaktimet, sipas të cilave, pas afatit të vjetërsimit për ndjekjen e një vepre penale , për të cilën ka patur urdhër për ndjekjen e komunikimeve, asgjësohen të dhënat që i ka Prokuroria Publike si dhe materialet origjinale nga ndjekja e komunikimeve, që janë ruajtur në Ministrinë e Punëve të Brendshme.[100]

Edhepse ligji i procedurës penale ka një dispozitë për shkatërrimin e të dhënave, ajo nuk është e detajuar ashtu siç ishte në dispozitat e fshira të Ligjit për ndjekjen e komunikimeve. Në të vërtetë, sipas nenit 261 të Ligjit të Procedurës Penale, nëse Prokurori Publik refuzon të ndjekë penalisht ose nëse të dhënat e mbledhura me masat e posaçme hetimore nuk kanë rëndësi për kryerjen e procedurës, parashikohet që ato të shkatërrohen nën mbikëqyrjen e gjykatësit, ndërsa Prokurori Publik do të përgatisë një procesverbal. Nëse procedura penale nuk ndërmerret brenda 15 muajve pas përfundimit të masave, të gjitha të dhënat e grumbulluara personale duhet të fshihen ose të shkatërrohen nën mbikëqyrjen e gjykatësit të procedurës paraprake, Prokurorit Publik dhe përfaqësuesit të Drejtorisë për Mbrojtjen e të Dhënave Personale, për çka Prokurori Publik duhet të hartojë procesverbal.[101] Këto dispozita nuk parashikojnë se çfarë do të ndodhë me materialet origjinale nga ndjekja e komunikimeve, të grumbulluar nga Drejtoria e Sigurisë dhe Kundërzbulimit. Andaj, **ndryshimet në dispozitat ligjore për ruajtjen dhe shkatërrimin e të dhënave nga ndjekja e komunikimeve, në mënyrë të konsiderueshme dhe të paarsyeshme e kanë përkufizuar mbrojtjen e të dhënave të grumbulluara.**

Personat të cilët në ndonjë mënyrë kanë mësuar të dhëna, që kanë të bëjnë ose dalin nga zbatimi i masave të posaçme hetimore, janë të detyruar t'i ruajnë ato si sekret zyrtar.[102]

Veçantitë e ndjekjes së komunikimeve me qëllim të mbrojtes së interesave të sigurisë dhe mbrojtjes së vendit

Gjykata mund të urdhërojë ndjekjen e komunikimeve edhe për mbrojtjen e interesave të sigurisë dhe të mbrojtjes së vendit. Tabela më poshtë jep një pasqyrë të ngjashmërive dhe dallimeve kryesore midis dispozitave ligjore për ndjekjen e komunikimeve mbi këtë bazë,[103] për dallim prej ndjekjes së komunikimeve me qëllim të zbulimit dhe ndjekjes së kryerësve të veprave penale.

	Përgjimi i komunikimeve me qëllim të zbulimit dhe ndjekjes së kryerësve të veprave penale	Përgjimi i komunikimeve me qëllim të mbrojtjes së interesave të sigurisë dhe mbrojtjes së vendit
Arsye	Zbulimi dhe ndjekja e kryerësve të veprave penale	Përgatitja e veprës penale kundër shtetit, forcave të armatosura ose kundër njerëzimit dhe të drejtës

[100] Nenet 22-25 të ligjit për ndjekjen e komunikimeve
[101] Neni 267.
[102] Neni 264 i Ligjit për ndjekjen e komunikimeve.
[103] Nenet 29-34 të Ligjit për ndjekjen e komunikimeve.

	Përgjimi i komunikimeve me qëllim të zbulimit dhe ndjekjes së kryerësve të veprave penale	Përgjimi i komunikimeve me qëllim të mbrojtjes së interesave të sigurisë dhe mbrojtjes së vendit
		ndërkombëtare, si dhe përgatitjen, nxitjen, organizimin ose pjesëmarrjen në një sulm të armatosur kundër Maqedonisë apo në pamundësimin e sistemit të sigurisë
Paraqitësi i kërkesës	Prokurori kompetent Publik në bazë të iniciativës së tij ose në bazë të propozimeve të Ministrisë së Punëve të Brendshme, Drejtorisë së policisë financiare apo Drejtorisë së doganave	Prokurori Publik i Republikës së Maqedonisë, me propozim të Ministrit të punëve të brendshme, Ministrit të mbrojtjes ose personit të autorizuar nga këto dy institucione
Kohëzgjatja	Deri në 4 muaj, me mundësi për zgjatje të shumëfishtë deri në 4 muaj, por jo më shumë se 14 muaj në total	Deri në 6 muaj, me mundësinë e zgjatjes, por jo më shumë se 24 muaj në total
Gjykatësi që lëshon urdhërin	Gjykatësi i procedurës paraprake	Gjykatës i caktuar i Gjykatës Supreme
Afati për vendimin e gjykatësit	48 orë, ndërsa në raste urgjente mund të lëshohet një urdhër me gojë që vlen 48 orë	72 orë, ndërsa në raste urgjente 5 orë
Ankimimi gjatë refuzimit të kërkesës i drejtohet	Këshillit tre anëtarësh i gykatësve të Gjykatës kompetente të shkallës së parë	Këshillit tre anëtarësh i gjykatësve të Gjykatës Supreme
Ankimimi gjatë pranimit të kërkesës (nga një subjekt që i përfaqëson interesat e personave)	Nuk është paraparë	Nuk është paraparë
Periudha më e gjatë e ruajtjes së shënimeve	Nuk ka përkufizime	Pesë vjet pas skadimit të kohës së përcaktuar me urdhër
E drejta e informimit të personave, komunikimet e të cilëve po përgjohen	Nuk është paraparë	Nuk është paraparë
E drejta për kompensimin e dëmeve ndaj personave të cilët janë përgjuar në kundërshtim me dispozitat ligjore	Me procedurë urgjente vendos Gjykata kompetente për lëshimin e urdhërit për përgjimin e komunikimeve, e cila nuk mund të zgjasë më shumë se tre muaj	Nuk është paraparë
E drejta për kompensimin e dëmeve ndaj personave, komunikimi i të cilëve është përgjuar pa mos i vërtetuar dyshimet	Nuk është paraparë	Nuk është paraparë

Bashkëbiseduesit të cilët më parë kanë punuar në Shërbimin e sistemit të sigurisë të Republikës së Maqedonisë, deklarojnë se në këtë shërbim, gjatë hetimit, nuk bëhet asnjë vlerësim paraprak i sigurisë, me qëllim që të vendoset nëse duhet të hapet procedurë dhe të kërkohet urdhër nga gjykatësi për ndjekjen e komunikimeve.

Mbikëqyrja dhe kontrolli mbi ndjekjen e komunikimeve

Mbikëqyrja mbi zbatimin e masës së posaçme hetimore, ndjekjen e komunikimeve, e kryen komisioni pesë anëtarësh i Kuvendit, i përbërë nga tre përfaqësues të opozitës dhe dy

përfaqësues nga partitë politike në pushtet. Pengesë të veçantë paraqet përcaktimi i shtuar[104] në ndryshimet e ligjit, në vitin 2012, se komisioni sjell vendim për mbikëqyrje me shumicë votash. **Mbetet e paqartë se përse ka nevojë që të përcaktohet se komisioni duhet të sjell vendim të posacëm për mbikëqyrje, kur ai është i formuar pikërisht për këtë qëllim.**

Në mënyrë plotësuese, **Komisioni duhet të paraqet raport vjetor deri te Kuvendi i Republikës së Maqedonisë në afat prej dy muajsh, pas përfundimit të vitit rrjedhës, por nuk ekzistojnë përcaktime me të cilat do të garantojnë se do t'iu sigurohen të dhënat që në kohë ta kryejnë obligimin e këtillë**.[105] Prokurori Publik i Republikës së Maqedonisë është i obliguar që një herë në vit të paraqet raport para Kuvendit të Republikës së Maqedonisë për masat e veçanta hetimore, masa këto që janë kërkuar për vitin paraprak [106] por, nuk ka afatizim për këtë obligim, gjë që do t'i mundësonte komisionit përkatës kuvendor ta respektojë afatin e përcaktuar për raportin e vet. Komisionet mbikëqyrëse kuvendore nuk kanë qasje kah asnjë të dhënë plotësuese nga shërbimet.

Komisioni kuvendor për mbikëqyrjen e ndjekjes së komunikimeve dhe Komisioni për mbikëqyrjen e punës së shërbimeve të sigurisë dhe të kundërzbulimit, deri tani nuk kanë arritur mbikëqyrje efektive **për shkak të mungesës së qasjes kah të dhënat relevante, si dhe për shkak të opstrukcioneve duke i ndryshuar vazhdimisht anëtarët nga radhët e partive të qeverisë së mëparshme,** gjë që ka pamundësuar mbajtjen e mbledhjeve deri në marrjen e certifikatave për anëtarët e rinjë. Sipas bisedave me ish anëtarët e këtyre komisioneve, **dhënja e certifikatave të sigurisë është stërgjatur nga ana e MPB-së më shumë se 6 muaj,** madje deri në një vit, me çka është bllokuar puna e komisioneve. Janë potencuar edhe shembuj të ndërrimit të anëtarëve të komisionit nga ana e partive në pushtet me qëllim që të paraqitet nevoja e dhënies së certifikatave të reja për siguri, që në ndërkohë ta pamundësojnë sërish mbajtjen e mbledhjeve. E gjithë kjo situatë është ironike meqë ministrat me automatizëm e marrin certifikatën më të lartë të sigurisë, ndërsa për deputetët kjo qasje nuk vlen.

Inspektimi në vendin e ngjarjes nga komisionet parlamentare gjithashtu është penguar nga fakti se shumica në komisionin për mbikëqyrjen e Drejtorisë së Sigurisë dhe Kundërzbulimit dhe Agjencisë së Inteligjencës kanë qenë nga pozita, ndërsa në komisionin për mbikëqyrjen e masës së posaçme hetimore, ndjekjen e komunikimeve, shumicën e ka patur opozita, por, madje edhe në rastin e dytë, anëtarët e pozitës kanë insistuar që të vendoset me konsenzus.

Komisionet nuk kanë në dispozicion as ekspertë, ndërsa vet deputetët nuk janë ekspertë të lëmisë së teknologjisë apo informatikës. Edhe sikur t'iu jipet mundësia për të bërë inspektime, pa praninë e ekspertëve, nuk kanë njohuri përkatëse për ta kryer inspektimin (njohuri teknologjike, informatike madje edhe juridike). Andaj, komisionet kuvendore për mbikëqyrje kanë vetëm rol formal.

Kontrollin për zbatimin e masës së posaçme, ndjekjen e komunikimeve, e bën Prokurori kompetent Publik, ndërsa në rastin kur masa është dhënë për shkak të mbrojtjes së interesave të sigurisë dhe mbrojtjes së vendit, kontrolli bëhet nga ana e gjykatësit të Gjykatës Supreme, i cili e ka lëshuar urdhërin.

[104] Neni 36 i ligjit për ndjekjen e komunikimeve
[105] Neni 37 i ligjit për ndjekjen e komunikimeve
[106] Neni 271 i ligjit për procedurë penale

Në pajtim me nenin 7 të ligjit për komunikime elektronike, Agjencia për Komunikime Elektronike është e obliguar të sigurojë ruajtjen e integritetit dhe të sigurisë së rrjeteve publike elektronike të komunikimit. Agjencia është e obliguar të zbatojë procedurë për mbikëqyrjen e operatorëve lidhur me plotësimin e obligimeve në raport me sigurimin e kushteve të duhura teknologjike, që të mundësohet ndjekja e komunikimeve, në pajtim me ligjin për ndjekjen e komunikimeve dhe në bazë të kërkesës së organit të autorizuar. Megjithatë, Agjencia për Komunikime Elektronike nuk ka mundur as të pohojë e as të mohojë se a është kryer mbikëqyrja mbi pajisjen për ndjekjen e komunikimeve tek operatorët.

Pas publikimit të " bombave" politike, ishte shokuese heshtja e institucioneve kompetente. Me vonesë reaguan tre institucione:

- **Ministria e Punëve të Brendshme,** edhe atë pas emërimit të ministrit "opozitar" Oliver Spasovski, i cili inicoi formimin e grupit punues, të përbërë nga përfaqësues të më shumë institucioneve.

- **Drejtoria për Mbrojtjen e të Dhënave Personale (DMDHP),** e cila në bazë të "bombave" me detyrë zyrtare ka kryer inspektim mbikëqyrës[107] në Drejtorinë e Sigurimit dhe Kundërzbulimit, gjatë periudhës qershor-nëntor të vitit 2016. Mbikëqyrja është bërë për ligjshmërinë e aktiviteteve të ndërmarra gjatë përpunimit të të dhënave personale dhe mbrojtjes së tyre. Në procesverbalin për mbikëqyrjen e kryer inspektuese, janë verifikuar parregullësi dhe lëshime, edhe atë : mospasje të dokumentacionit për masat teknike dhe organizative të sigurimit të fshehtësisë dhe mbrojtjes së përpunimit të të dhënave personale, moszbatim të masave teknike dhe organizative për sigurimin e fshehtësisë dhe mbrojtjes së përpunimit të të dhënave personale, si dhe mos kryerjen e kontrollit mbi sistemin e vendosur të mbrojtjes së të dhënave personale.

Në fillim të vitit 2017 është marrë vendim nga ana e DMDHP-së lidhur me mbikëqyrjen e zbatuar. Me këtë vendim obligohet Ministri i Punëve të Brendshme të ndërmerr veprime dhe aktivitete konkrete për eliminimin e parregullësive dhe lëshimeve të verifikuara, me ç'rast është dhënë afati kohor deri në korrik të vitit 2017, të vendoset sipas vendimit. DMDHP-ja gjatë dhjetorit të vitit 2016 ka filluar me zbatimin e mbikëqyrjeve inspektuese të aktiviteteve të ndërmarra lidhur me ligjshmërinë e aktiviteteve gjatë përpunimit të të dhënave personale dhe mbrojtjen e tyre tek të dy operatorët. Nga mbikëqyrja e kryer është konstatuar se operatorët e telekomunikacionit kanë krijuar linja elektronike të komunikimit me lidhjen e duhur të transmetimit tek organi i autorizuar për ndjekjen e komunikimeve në rrjetin e tyre.

Është vërtetuar se ato aplikojnë masa teknike dhe organizative për të siguruar fshehtësinë dhe mbrojtjen e përpunimit të të dhënave personale nga shkatërrimi aksidental ose i paligjshëm, humbja aksidentale ose ndryshimi, apo mbajtja e paautorizuar ose e paligjshme e përpunimit, qasjes ose zbulimit të personave të paautorizuar.

- **Avokati i Popullit** mori një ankesë nga një gazetare, person i cili u përmend në bisedat, me ç'rast kanë filluar procedurën e kërkimit të infomacioneve dhe zbatimin e kontrollit mbi DSK-në, Ministrinë e Brendshme dhe Parlamentit, por nuk kanë marrë asnjë informacion. Avokati i Popullit është një institucion që gëzon rejtingun dhe besimin më të lartë të qytetarëve, por, ende ka kapacitete të vogla (burime njerëzore), pasi që Qeveria nuk lejon punësime të reja dhe kështu pengon punën e këtij institucioni**.**

[107] Drejtoria për Mbrojtjen e të Dhënave Personale **,**Raporti vjetor për vitin 2016: https://dzlp.mk/sites/default/files/u4/godisen_izvestaj_dzlp_2016.pdf

Siguria te operatorët e rrjeteve publike të komunikimeve elektronike dhe ofruesve të shërbimeve

Kishte mungesë reagimi publik ndaj "bombave" politike edhe nga ana e operatorëve të telekomunikacioneve, të cilët nuk i njoftuan abonentët e tyre për shkeljen e privatësisë dhe të dhënave personale, si dhe për masat që po i ndërmarrin për të hetuar se si ndodhi një çrregullim i tillë dhe si do të minimizoheshin rreziqet për të mos u përsëritur më.

Sipas Telekom-it të Maqedonisë, operatorët kanë revizione të rregullta të sistemeve nga ana e Dojçe Telekom-it, i cili ka vendosur standarde të veçanta për shfrytëzimin e pajisjes dhe për personat që kanë qasje në to. Është publikuar se Magjar Telekom-i ka hapur hetim të brendshëm në maj të vitit 2014, lidhur me bombat, tre muaj pas publikimit të inçizimeve të para tonike nga përgjimet, por nuk është publikuar rezultati i atij hetimi. [108] Gjithsej 3 persona nga Telekom-i kanë qasje te pajisjet për përgjimin e komunikimeve, por vetëm në aspekt të funksionalitetit të saj, ndërsa mund të reagojnë vetëm në rastet kur ka ankesë nga MPB-ja për ndonjë problem eventual. Operatori ka shumë të dhëna personale, të cilat ruhen për nevojat sistemore (si psh. për faturat) dhe ekzistojnë mundësi të caktuara për keqpërdorimin e tyre, edhe përkundër sistemeve të mira mbrojtëse, por deri tani nuk ka patur rast që të zbulohet një keqpërdorim i këtillë, apo të dënohet ndonjë i punësuar.

Dispozitat ndëshkuese ndaj organeve kompetente për ndjekjen e komunikimeve

Në ligjin për ndjekjen e komunikimeve mungojnë dispozitat ndëshkuese për organet kompetente dhe personat përgjegjës, që është e pashpjegueshme, duke patur parasysh faktin se mosrespektimi i ligjit mund të rezultojë me shkelje të rënda të të drejtave të personave, komunikimi i të cilëve ndiqet, si dhe demokracisë dhe sundimit të ligjit në vend. Fakti që Kodi Penal[109] penalizon përgjimin e paautorizuar dhe regjistrimin audio, si dhe shkeljen e fshehtësisë së korrespondencës (duke përfshirë edhe postën e siguruar elektronike), është e pamjaftueshme për t'i mbuluar të gjitha situatat dhe pasojat eventuale nga moszbatimi ose zbatimit të pamjaftueshëm të dispozitave të ligjit për ndjekjen e komunikimit. .[110]

[108] http://fokus.mk/kako-familijata-na-gruevski-ja-gradeshe-mrezhata-za-prislushuvane/

[109] Kodi Penal, „Gazeta zyrtare e Repubkës së Maqedonisë “ numër 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 87/2007, 7/2008, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 42/2012, 166/2012, 55/2013, 82/2013, 14/2014, 27/2014, 28/2014, 41/2014, 115/2014, 132/2014,160/2014, 199/2014, 226/2015, 97/2017.

[110] Sipas nenit 151, nëse bëhet përgjimi apo inçizimi audio i paautorizuar, nga ndonjë person zyrtar i shërbimit qoftë person përgjegjës apo person juridik, do të dënohet me vuajtje burg prej më së paku 4 vitesh. Këtë dënim mund ta vuajë edhe personi i punësuar si person juridik, të cilit në kuadër të punës i është besuar zbatimi i masës për përgjimin e komunikimeve. Personi juridik dënohet me gjobë ndërsa personi juridik i cili veprimtari kryesore e ka patur dhënien e shërbimeve të telekomunikacionit dënohet me 10% të të ardhurave totale nga viti aktual, kur edhe është kryer vepra. Me nenin 147 për shkeljen e konfidencialitetit të letrave

Ruajtja e meta të dhënave

Në ligjin e komunikimeve elektronike të vitit 2014 u inorkorporuan risi në pjesën e ndjekjes së komunikimeve dhe ruajtjes masive të meta të dhënave nga ana e shfrytëzuesve. Nenet 176 dhe 178 i obligojnë të gjithë ofruesit e shërbimeve të telefonit dhe të internetit t'i ruajnë për një vit, për të gjithë shfrytëzuesit këto të dhëna të shërbimeve për telefon dhe internet (përfshirë edhe e-postën): emrin, adresën, numrin e telefonit / IP adresën, pajisjen telefonike dhe lokacionin e personave që komunikojnë; koha e fillimit dhe mbarimit të komunikimit, lloji i shërbimit për telefon/internet. Operatorët janë të obliguar që të dhënat e këtilla t'i ruajnë me harxhimet e veta, edhe pas kërkesës për t'ia dorëzuar organeve shtetërore. Arsyetimi ishte se meta të dhënat do të ruhen për shkak të "pengimit apo zbulimit të veprave penale, hapjes së procedurave penale ose për shkak të interesave të sigurisë dhe mbrojtjes". Pastaj, qasja te meta të dhënat bëhet në bazë të një kërkese, respektivisht urdhëri nga prokurori publik, dhe nuk kërkohet urdhëri nga gjykatësi. Problemi paraqitet se legjislacioni ynë parashikon një standard më të ulët drejt qasjes në këto të dhëna, në kushtet kur telefonat modern celularë ofrojnë të dhëna për lëvizjen dhe vendndodhjen e përdoruesve të tyre, madje edhe më mirë dhe më thjeshtë se sa me ndjekjen fizike të dikujt. Një qasje e tillë është në kundërshtim me Konventën Evropiane për të Drejtat e Njeriut. Dispozitat për ruajtjen masive të të dhënave ishte justifikuar si një zhvendosje e Direktivës 2006/24/EC, e cila ishte anuluar nga Gjykata Europiane e Drejtësisë, menjëherë pas miratimit të Ligjit të ri për komunikimet elektronike në Republikën e Maqedonisë. Pas revokimit të Direktivës, në Maqedoni janë ndërmarrë hapa për të hequr nenet kontestuese që rregullojnë ruajtjen e të dhënave. Sipas një përfaqësuesi të Agjencisë për Komunikime Elektronike, "në vitin 2015 ose 2016," ata kanë dorëzuar propozim për ndryshimin e ligjit për komunikime elektronike në Ministrinë e Shoqërisë Informatike dhe Administratës, në mënyrë që të përputhen me ligjin e BE-së. Megjithatë, përfaqësuesi i Agjencisë nuk ishte në gjendje për të konfirmuar nëse në këtë projekt-tekst e kanë propozuar edhe heqjen e detyrimit për të mbajtur meta të dhëna". [111]

Ligji për komunikime elektronike e definon detyrimin për ruajtjen e të dhënave gjatë sigurimit të shërbimeve nëpërmjet një rrjeti publik të komunikimit fiks ose celular, si dhe gjatë sigurimit të qasjes në internet, në postën elektronike deri te shërbimet telefonike përmes internetit. Të dhënat e mëposhtme, operatorët janë të detyruar t'i ruajnë për një periudhë njëvjeçare:

1. Të dhëna që nevojiten për ndjekjen dhe identifikimin e burimit të komunikimit (numri i thirrjes; emri dhe adresa e shfrytëzuesit; kodi shfrytëzues për identifikim; kodi shfrytëzues për identifikim si dhe numri i telefonit që shërben për çfarëdo lloj komunikimi dhe qasje drejt rrjetit publik telefonik; emri dhe mbiemri i parapaguesit apo i shfrytëzuesit të regjistruar, të cilit i është dhënë adresë për IP; kodi shfrytëzues për identifikim ose numri i telefonit gjatë komunikimit).
2. Të dhënat e nevojshme për të identifikuar destinacionin e komunikimit (numrat e thirrur ose numrin/numrat ku barten thirrjet; emri dhe adresa e përdoruesit; kodi i

përcaktohet dënimi me gjobë ose me burgim deri në një vit, por nëse është person zyrtar, dënohet me vuajtje burg, prej tre muajsh deri në pesë vjet.

[111] Ministria nuk iu përgjigj kërkesës për bisedë në këtë temë.

identifikimit të përdoruesit ose numri i telefonit të marrësit të thirrjes telefonike nëpërmjet internetit; emri dhe adresa e përdoruesit dhe kodi i përdorur për identifikim të marrësit të thirrjes telefonike përmes internetit).

3. Të dhënat që nevojiten për të identifikuar datën, orën dhe kohëzgjatjen e komunikimit (data dhe koha në fillim dhe në fund të komunikimit; data dhe koha e kyçjes dhe e çkyçjes në internet, në bazë të një zone të caktuar kohore, së bashku me IP adresën; kodi identifikues i përdoruesit; data dhe ora e kyçjes dhe e çkyçjes nga shërbimet e postës elektronike ose nga shërbimet telefonike nëpërmjet Internetit, bazuar në një zonë të caktuar kohore).

4. Të dhënat që janë të nevojshme për identifikimin e llojit të komunikimit (shërbimi i përdorur telefonik; shërbimi i përdorur përmes internetit).

5. Të dhënat e nevojshme për të identifikuar pajisjen e komunikimit të përdoruesit ose atë që konsiderohet të jetë i tij (numrat e thirrësve dhe të marrësve të thirrjes, identiteti ndërkombëtar i parapaguesit celular- IMSI i thirrësit, identiteti ndërkombëtar i pajisjes celulare (IMEI) i marrësit të thirrjes; IMSI i thirrësit, IMEI i palës së thirrur, data dhe koha e aktivizimit fillestar të shërbimit dhe lokacioni prej nga është aktivizuar shërbimi, në rast të thirrjes anonime nga shërbimi pripejd; numri i thirrjes për qasje dial-up, linjë parapaguese digjitale (DSL) ose ndonjë shërbim tjetër i inicuesit të komunikimit).

6. Të dhënat që janë të nevojshme për të identifikuar vendndodhjen e pajisjeve të komunikimit me celularë (shenja e vendndodhjes në fillim të komunikimit; të dhënat për identifikimin e vendndodhjes gjeografike të celularit duke iu referuar simboleve të vendndodhjes së tyre për periudhën kohore, për të cilën ruhen të dhënat e komunikimit).

Neni 177 i Ligjit të komunikimeve elektronike, përcakton një detyrim për operatorët që të zbatojnë masat e duhura teknike dhe organizative për mbrojtje nga shkatërrimi aksidental ose i paligjshëm i meta të dhënave, humbjes ose ndryshimit aksidental dhe ruajtjes së paautorizuar ose të paligjshëm, përpunimit, qasjes apo zbulimit. Më pas, në të njëjtin nen, është definuar se operatori duhet të zbatojë teknika dhe masa përkatëse organizative për të dhënat, që të sigurohet se tek të dhënat do të kenë qasje vetëm personat e autorizuar nga operatori. Mbrojtja e këtyre të dhënave te operatorët, mbështetet në faktin se sistemi i ruajtjes së meta të dhënave, krijon logo gjatë çdo përdorimi dhe çdo aktivitet mund të ndiqet (kush ka patur qasje, kur dhe të ngjashme) ndërkohë që, është i përkufizuar numri i personave që kanë qasje. Por, shtrohet pyetja athua deri tani a është kryer ndonjë mbikëqyrje për zbatimin e masave të këtilla nga ana e operatorëve. Agjencia e Komunikimeve Elektronike as nuk ka mundur të pohojë e as të mohojë.

Operatorët, gjithashtu janë të obliguar që t'i shkatërrojnë meta të dhënat pas skadimit të afatit prej 12 muajsh, përveç disa të dhënave me interes, që do të thotë se për meta të dhënat që mbahen tek operatorët e telekomunikimit, të cilat janë kërkuar nga ana e Prokurorit Publik, nuk ka përkufizim kohor për ruajtjen e tyre. Sipas Prokurorisë Publike, përmes meta të dhënave, Prokuroria mund të detektojë lëvizjen dhe kontaktet e të akuzuarëve, pas çka. mund të merren konkluza të sakta për përfshirjen e tyre në krim. Megjithatë, deri më sot, nuk është bërë ndonjë analizë për implementimin e ligjit, arsyeshmërinë dhe efikasitetin nga zbatimi i tij. Nuk ekzistojnë dëshmi statistikore të cilat do të ndihmonin për ta mbështetur pohimin se rëndësia e meta të dhënave është e madhe në luftën kundër krimit, pavarësisht ndikimit masiv dhe shumë negativ në privatësinë dhe të dhënave personale te të gjithë përdoruesit e shërbimeve të komunikimit elektronik, si dhe

implikimet negative financiare për operatorët, të cilët janë të detyruar të blejnë pajisjet për ruajtjen e këtyre të dhënave me shpenzimet e tyre.[112]

Analiza e Raporteve të Prokurorit Publik për ndjekjen e komunikimeve

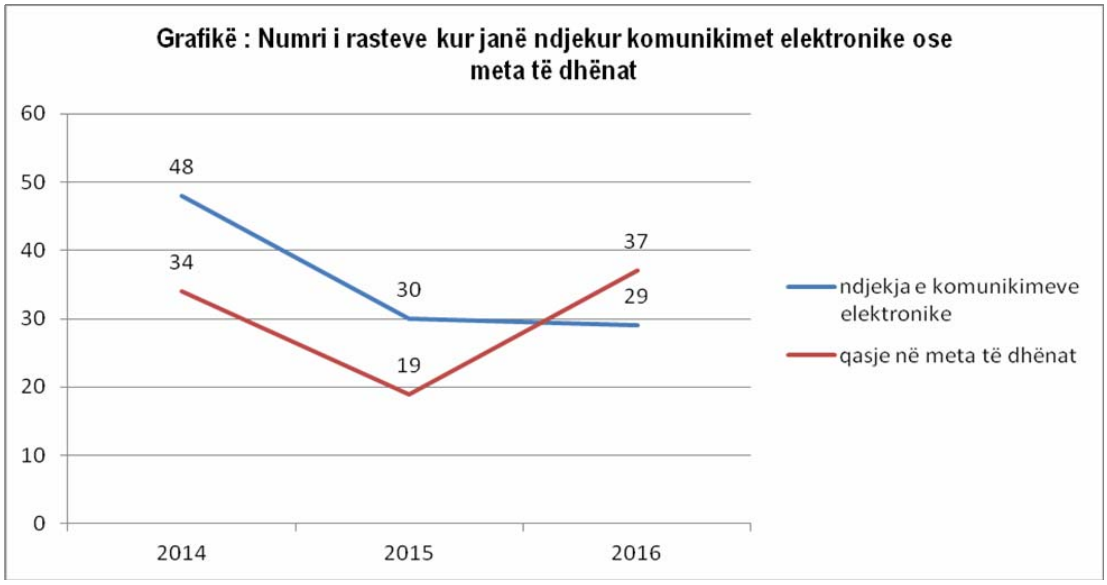
Në pajtim me nenin 271 të ligjit të procedurës penale, Prokurori Publik i Republikës së Maqedonisë, njëherë në vit para Parlamentit të Maqedonisë, paraqet Raport për zbatimin e masave të posaçme hetimore gjatë vitit paraprak. Analiza e Raporteve të Prokurorit Publik për ndjekjen e komunikimeve dhe zbatimit të masave tjera të posaçme hetimore për periudhën 2014-2016, flet se Prokuroria Publike, këto raporte ia dërgon Parlamentit madje 7 muaj pas përfundimit të vitit kalendarik, që është një periudhë tejet e gjatë për përgatitjen e një raporti prej 10 deri në 16 faqesh. Raportet nuk publikohen në web faqen e Prokurorisë Publike, gjë që flet për nivelin brengosës të transparencës. Madje, raportet nuk i përfshijnë elementet konform ligjit, e ato janë me sa vijon:

- Nëse masa e posaçme hetimore, respektivisht përgjimi, nuk ka dhënë rezultate relevante për procedurën dhe arsyetimin për shkaqet, në mënyrë të diferencuar sipas shkaqeve teknike dhe të tjera. Për rastet kur ndjekja e komunikimeve elektronike dhe përdorimi i meta të dhënave është ndërprerë, pa u siguruar dëshmia për procedurën, raportet e Prokurorisë Publike nuk japin sqarime për shkaqet.
- Harxhimet që dalin nga zbatimi i masës së posaçme hetimore.

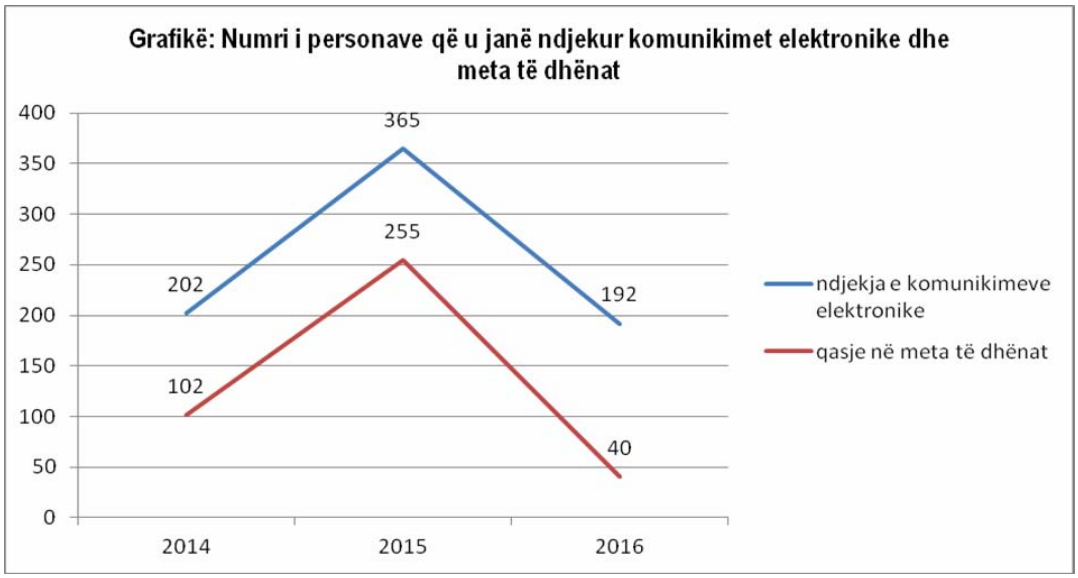
Raportet për vitet 2014 dhe 2015 konstatojnë se "nuk ka patur harxhime plotësuese për Prokurorinë Publike apo për Gjykatën, për faktin se Ministria e Punëve të Brendshme në mënyrë të drejtpërdrejt i i zbaton këto masa dhe për këtë nuk shtron kërkesë për mjetet." Megjithatë, neni 271 i ligjit përcakton se raportet duhet me doemos ta kenë të përfshirë edhe informatën për harxhimet për këto masa, ndërsa nuk i përkufizon harxhimet e bëra në Prokurorinë Publike apo Gjykatë. Mosparaqitja e informacioneve për harxhimet dedikuar këtyre masave, i parandalon ekspertët dhe deputetët në Kuvendin e Republikës së Maqedonisë, që të japin vlerësime për efikasitetin e tyre.

Në grafikën më poshtë janë shënuar të dhënat për periudhën e viteve 2014-2016, të përfshira në këto raporte, për dy masa të posaçme hetimore: ndjekje dhe inçizim të komunikimeve telefonike dhe të tjera elektronike (në tekstin më poshtë: përgjim të komunikimeve elektronike) dhe inspektimin e komunikimeve të realizuara telefonike dhe të tjera elektronike (në tekstin më poshtë: inspektim të meta të dhënave për komunikime elektronike)

[112]Në Çeki, për shembull, Telekom-i çek ka marrë mjete nga shteti për ta blerë pajisjen e nevojshme.



Paraqiten paqëndrueshmëri në të dhënat e paraqitura në raportet. Për shembull, në Raportin për vitin 2016, paraqitet se masa për të ndjekur komunikimet elektronike është zbatuar në 29 raste, por, kur shënohet kohëzgjatja dalin në total 30 raste, ndërsa, pas rezultatit të procedurës paraqiten 31 raste. Nëse supozojmë se dallimi te ndarja pas përfundimit të procedurës paraqitet për faktin se në raste të caktuara mund të ketë më shumë se një rezultat,[113] megjithatë, nuk mund të vërtetohet se përse paraqitet një rast më shumë gjatë shënimit të kohëzgjatjes së masës, në raport me numrin e përgjithshëm të rasteve të përfshira me këtë masë.



Fatkeqësisht, raportet japin një analizë tejet të varfër për numrat e paraqitura në to. Në vitin 2015 paraqitet rrënie prej 37% te masa për ndjekjen e komunikimeve elektronike dhe rrënie prej 44% te masa për inspektimin e meta të dhënave. Rrënia e këtillë e numrit të rasteve paraqitet në vitin 2015, kur ka rritje drastike të numrit të personave (81%–150%) të cilëve u janë përgjuar komunikimet elektronike apo meta të dhënat. Kjo ka të bëjë në dy

[113] Për personat e ndryshëm të përfshirë në rastin.

raste ku janë përfshirë një numër i madh personash për kërcënim terrorist ndaj rendit kushtetues dhe sigurisë (1 rast kundër 126 personave) dhe pjesëmarrje në ushtri të huaj, polici, formacione paraushtarake dhe parapolicore (1 rast kundër 102 personave). Rritja e numrit të personave të përfshirë pasuar nga një rrënie në numrin e rasteve, në raport shumë shkurt arsyetohet me "fokusimin e Prokurorisë Publike kah shkatërrimi i grupeve më të mëdha të organizuara kriminele, ku anëtarësojnë një numër i madh i personave". Por, konstatimi i njëjtë paraqitet edhe në raportin e vitit 2016, edhepse atë vit numri mesatar i personave të ndjekur është zvogëluar në mënyrë drastike, prej 1-7 persona për një rast.

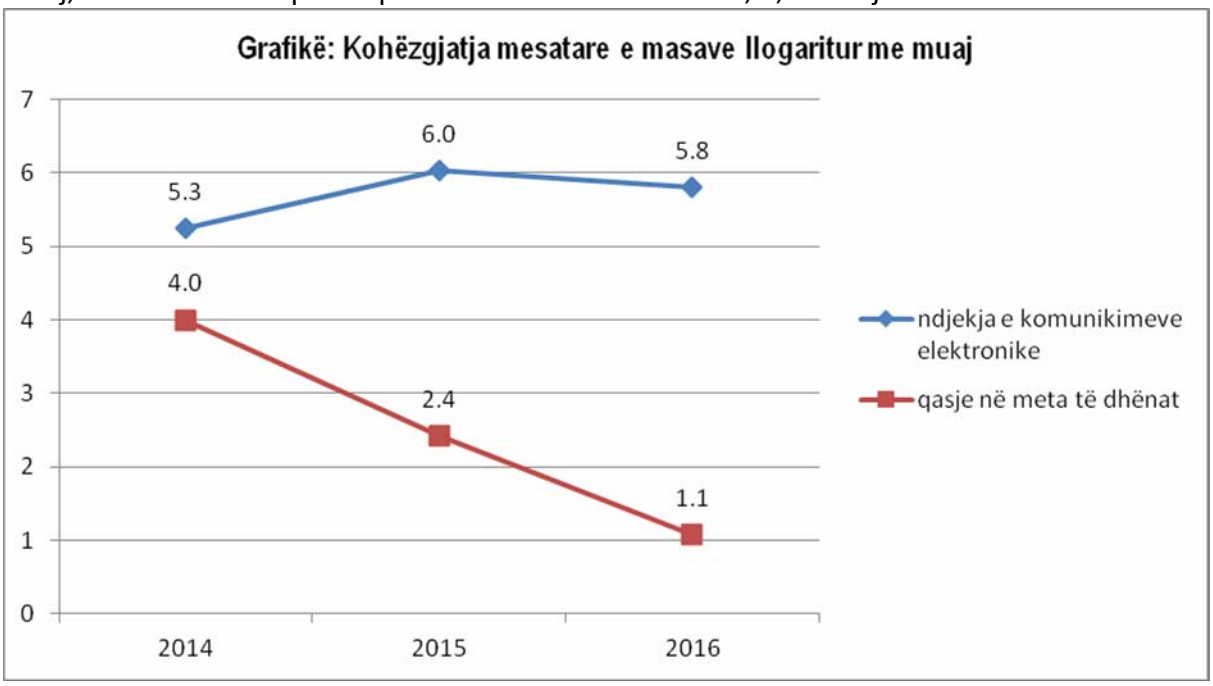
Ligji i procedurës penale i definon edhe mundësitë për përcaktimin e masave të posaçme hetimore ndaj objektit të veprës penale (për shembull, linja telefonike apo adresa e postës elektronike), në rastet ,kur nuk është i njohur identiteti i kryerësit të veprës penale. Sipas statistikës së publikuar në raportin e Prokurorit Publik për zbatimin e masave të posaçme hetimore në vitin 2016, masa "ndjekje dhe inçizim të komunikimeve telefonike dhe të tjera elektronike " të zbatuara ndaj 74 lëndëve, siç janë linja telefonike që e përdor një person i panjohur në momentin kur zbatohet masa. Në raportet e viteve 2014-2015 nuk janë paraqitur të dhëna të caktuara për numrin e masave hetimore për lëndët e veprave penale.

Tabela e rradhës pasqyron dyshimet më të shpeshta për veprat penale, për të cilat janë zbatuar që të dyja masat e posaçme hetimore:

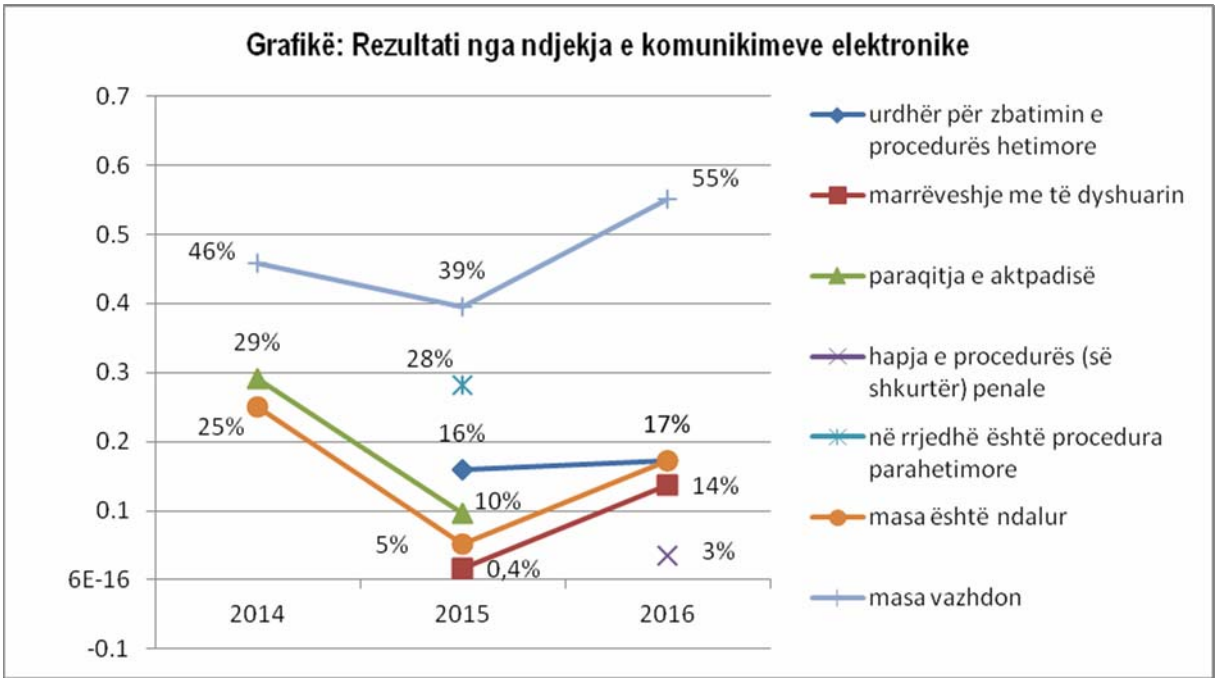
	Përgjimi i komunikimeve elektronike	Inspektimi i të dhënave meta
2014	• Trafikimi i migrantëve (10 raste) • Marrja e ryshfetit (5 raste) • Kriminalitet (4 raste)	• Prodhimi dhe tregtimi i paautorizuar i drogave narkotike, substancave psikotrope dhe perkusorëve (10 raste) • Keqpërdorim të detyrës zyrtare dhe autorizimit (5 raste) • Parandalimi i provave (5 raste)
2015	• Kërcënim terrorist ndaj rendit kushtetues dhe sigurisë (1 rast kundër 126 personave) • Pjesëmarrje në formacionet e huaja ushtarake, policore, paramilitare ose parapolicore (1 rast kundër 102 personave) • Terrorizëm (6 raste kundër 36 personave)	• Kërcënim terrorist ndaj rendit kushtetues dhe sigurisë (1 rast kundër 116 personave) • Pjesëmarrje në formacionet e huaja ushtarake, policore, paramilitare ose parapolicore (1 rast kundër 102 personave) • Prodhimi dhe tregtimi i paautorizuar i drogave narkotike, substancave psikotrope dhe perkusorëve (8 raste kundër 20 personave)
2016	• Terrorizëm (7 raste) • Prodhimi dhe tregtimi i paautorizuar i drogave narkotike, substancave psikotrope dhe perkusorëve (6 raste) • Pjesëmarrje në formacionet e huaja	• Trafikimi i migrantëve (22 raste) • Prodhimi dhe tregtimi i paautorizuar i drogave narkotike, substancave psikotrope dhe perkusorëve (9 raste)

	ushtarake, policore, paramilitare ose parapolicore (2 raste)	• Keqpërdorim të detyrës zyrtare dhe autorizimit (2 raste) • Organizimi i një grupi dhe nxitja për kryerjen e veprave, trafikimit të qenieve njerëzore, trafikimit të të miturve dhe kontrabandimit të migrantëve (2 raste)

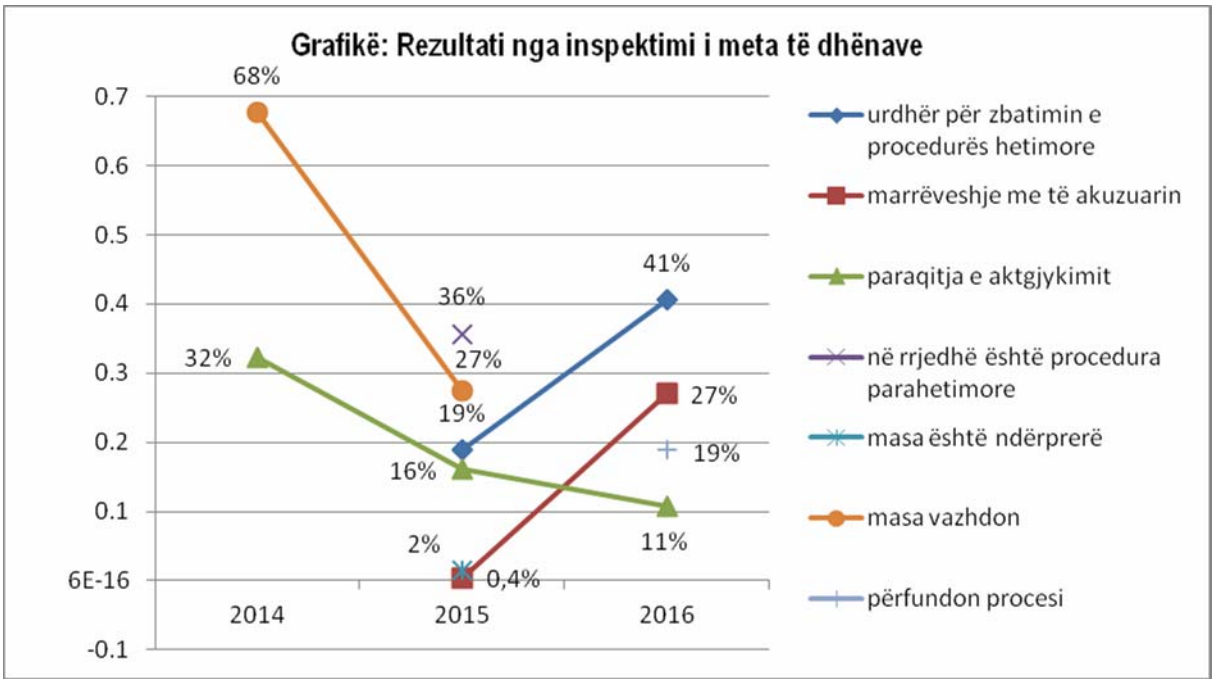
Mesatarisht , kohëzgjatja e masës për ndjekjen e komunikimeve elektronike është 5,6 muaj, ndërsa e masës për inspektimin e meta të dhënave, 2, 5 muaj.



Paqëndrueshmëria plotësuese te raportet qëndron te të dhënat e rezultateve nga zbatimi i masës. Në Raportet e viteve 2014 dhe 2016 janë paraqitur sipas rasteve, ndërsa në Raportin e vitit 2015, të dhënat paraqiten sipas personave dhe nuk ka të dhëna të rezultateve për raste. Kjo dhe paqëndrueshmëritë tjera, e vështirësojnë krahasimin e të dhënave gjatë viteve si dhe dhënien e vlerësimit për masat e ndjekjes të komunikimeve dhe meta të dhënave.



Tek masa për inspektimin e meta të dhënave, në Raportin e vitit 2016 për një rast në të cilin është zbatuar masa, nuk ka të dhëna për rezultatin as edhe për kohëzgjatjen e saj.



Është për tu habitur që në raportet e analizuara për tre vite rradhazi, vetëm në një vend hasim se zbatimi i njërës nga dy masat e analizuara ka rezultuar me grumbullimin e dëshmive për 7 aktgjykime. Megjithatë, nuk është e sqaruar në mënyrë eksplicite sa të akuzuar ka nga këto aktgjykime dhe a janë ende në fuqi apo jo. Është e paqartë nëse gjatë viteve tjera ka patur apo jo aktgjykime në bazë të dëshmive të grumbulluara nga masat e

posaçme hetimore, apo ndoshta nuk është ndjekur ky tregues. Poashtu, mungojnë shembujt e zbulimit apo parandalimit të krimeve të rënda nga aplikimi i masave të posaçme hetimore, më konkretisht, nga zbatimi i ndjekjes së komunikimit.

Raportet nuk përmbajnë të dhëna se sa propozime për ndjekjen e komunikimit i janë dorëzuar Prokurorit Publik, për sa prej tyre Prokurori ka rënë dakord, sa iniciativa vetanake ka patur për të ndjekur komunikimet dhe për sa kërkesa të paraqitura është lëshuar urdhër nga gjykatësi. Nuk ka as edhe një tregues për sa urdhëra gjykatësi është pajtuar plotësisht me kërkesën, sa janë modifikuar (për shembull, përsa i përket personave ose kohëzgjatjes) dhe sa i ka refuzuar. Raportet, gjithashtu, nuk japin statistika nëse janë bërë kërkesa për të siguruar meta të dhëna për ofruesit e huaj të shërbimeve të internetit, siç janë Twitter, Facebook, Gmail dhe të tjerë.

Rekomandime

Definimi dhe përfshirja e ndjekjes së komunikimeve

- Ndjekja dhe inspektimi i meta të dhënave, komunikimet elektronike të përfshihen në definicionin për " ndjekjen e komunikimeve " në ligjin për ndjekjen e komunikimeve.
- Në ligjin e procedurës penale, të saktësohet dallimi midis inspektimit të komunikimeve të realizuara telefonike dhe komunikimeve tjera elektronike, si masë e posaçme hetimore, nga detyrimi i operatorëve që t i ofrojnë Prokurorit Publik të dhëna për kontaktet e realizuara në trafikun komunikues, në pajtim me nenin 287 të po njëjtit ligj.

Arsyeja për ndjekjen e komunikimeve

- Të rishqyrtohet arsyeshmëria për tu lejuar ndjekja e komunikimeve për një gamë të gjerë veprash penale, në bazë të vlerësimit, athua shkelja e privatësisë është në proporcion me rëndësinë e një vepre penale dhe dëshmive që priten të sigurohen me masat e posaçme hetimore, respektivisht me ndjekjen e komunikimeve. Një zgjidhje e mundshme është që zbatimi i kësaj mase, të lejohet vetëm për veprat penale, për të cilat është paraparë vuajtje me burg prej katër e më shumë vitesh.

Kërkesa për ndjekjen e komunikimeve

- Të instalohet obligimi që Gjykata për çdo vit të publikojë se sa kërkesa janë pranuar për ndjekjen e komunikimeve, sa persona kanë qenë të përfshirë, nga cili organ janë kërkuar, për çfarë arsyesh dhe sa kërkesa të tilla janë refuzuar dhe sa nga to janë miratuar.
- Në kërkesën për ndjekjen e komunikimeve të deklarohet dhe sqarohet dyshimi për kryerje të mundshme apo kryerje të veprës penale, e jo vetëm një bazë për dyshim si një shkallë shumë e ulët dyshimi.

Urdhëri për ndjekjen e komunikimeve

- Të rishqyrtohet afati i paraparë prej 48 orësh, prej nenit 11 të ligjit të procedurës penale, se a është i mjaftueshëm për gjykatësin për ta studjuar në mënyrë përkatëse kërkesën për ndjekjen e komunikimeve dhe të vendos a do të lëshojë urdhër përkatës.
- Të saktësohen në mënyrë më restriktive kushtet ku është e lejuar ndjekja e komunikimeve në bazë të urdhërit me gojë, në pajtim me zgjidhjen e vjetër ligjore të ligjit për ndjekjen e komunikimeve. Në fakt, kjo mundësi u lejua vetëm kur ekzistonte rreziku i shkaktimit të vdekjes ose lëndimit të rëndë, shkaktimi i dëmit material mbi pronat me përmasa të gjera, ose arratia e kryerësit të krimit, për të cilin parashihet dënimi me burgim të përjetshëm.
- T'i mundësohet gjykatësit të sjell vendim korrekt për arsyeshmërinë e kërkesës për ndjekjen e komunikimeve si dhe të vlerësojë athua janë plotësuar kushtet për prishjen e privatësisë dhe të dhënave personale, është e domosdoshme që të përfshihet edhe një palë në procedurë, që do t'i përfaqësojë interesat e personave, komunikimet e të cilëve propozohet të ndiqen. Këtë rol mund ta kenë paneli i ekspertëve, përfaqësuesi nga Drejtoria

për Mbrojtjen e të Dhënave Personale ose Avokati i Popullit si "përfaqësues i interesit publik".

- Në nenin 257 të ligjit për procedurë penale, të shtohet edhe një element obligues në përmbajtjen e urdhërit që e lëshon gjykatësi, për ndjekjen e komunikimeve. Urdhëri duhet ta përmbajë emrin e organit i cili e shtron kërkesën për ndjekjen e komunikimeve.
- „E drejta për ankesë" për vendimin e gjykatësit për ndjekjen e komunikimeve të mos jetë e drejtë vetëm e organeve kompetente, kërkesat e të cilëve janë refuzuar, por, të jetë e zbatueshme edhe për mbrojtjen e të drejtave dhe interesave të personave, komunikimet e të cilëve propozohet të ndiqen. Në të vërtetë, ligji për ndjekjen e komunikimeve duhet të plotësohet me përcaktime, të cilat do t' i mundësojnë pjesëmarrje adekuate institucioneve tjera, gjatë përpilimit të urdhërit për ndjekjen e komunikimeve, siç është Drejtoria për Mbrojtjen e të Dhënave Personale apo Avokati i Popullit. Njëherit, kjo do të mundësojë që para një instance tjetër të kundërshtohet qëndrueshmëria e një urdhëri eventual, të lëshuar nga gjykatësi në një procedurë paraprake.

Kohëzgjatja e ndjekjes së komunikimeve

- Të rishqyrtohet arsyeshmëria e afateve maksimale kohore për ndjekjen e komunikimeve (afati kohor i deritanishëm prej maksimum 4 muaj me mundësi për zgjatje deri në 14 muaj, kundrejt afateve të mëparshme kohore prej 1 muaj me mundësi të zgjatjes deri në 12 muaj, nga versioni i vjetër i ligjit për ndjekjen e komunikimeve)
- Të plotësohet neni 257 i ligjit për procedurë penale, me qëllim që në mesin e elementeve obligativ të urdhërit për ndjekjen e komunikimeve të sendërtohet detyrimi për organin që e zbaton ndjekjen, që ta ndal masën kur do të arrihen qëllimet, për të cilat janë përcaktuar masat e posaçme hetimore, ose të mos vlen më qëndrueshmëria e kërkesës.

Zbatimi operativ i ndjekjes së komunikimeve

- Në mënyrë ligjore të ndahen kompetencat dhe rregullat për ndjekjen e komunikimeve gjatë hetimeve penale, nga ato të karakterit të sigurisë dhe kundërzbulimit.
- Të pamundësohet qasja e drejpërdrejt e shërbimeve në përmbajtjen e komunikimeve, respektivisht, organet kompetente paraprakisht duhet ta informojnë operatorin dhe të dorëzojnë urdhër gjyqësor për ndjekje, që pastaj operatori t'ua mundësojë qasjen deri te komunikimet e personave të përfshirë.
- Të mbahet evidenca e ndjekjes së komunikimeve te operatorët, ndaj të cilës do të kenë qasje organet kompetente. Mes tjerash, të evidentohet, cilët të punësuar të operatorit dhe kur kanë patur qasje në përmbajtjen e komunikimeve dhe meta të dhënave. Të praktikohen dënime të rrepta për të punësuarit e operatorëve të cilët në mënyrë të pautorizuar kanë patur qasje, apo iu kanë mundësuar dikujt qasje te meta të dhënat apo te përmbajtja e komunikimeve.
- Të përforcohet kontrolli i brendshëm në MPB-së që të kryhet kontrolli edhe për rastet kur është keqpërdorur autorizimi për ndjekjen e komunikimeve.

Përdorimi i informacioneve nga ndjekja e komunikimeve

- Të plotësohet neni 258 i ligjit për procedurë penale në pjesën e Raportit të policisë gjyqësore për ndjekjen e komunikimeve që i dorëzohet Prokurorit Publik. Detyrimisht në raport duhet të evidentohet numri i telefonit , linja e përdorur ose adresa e postës elektronike (apo lloj tjetër identifikuesi) që janë ndjekur.

- Te rishqyrtohen nenet 255 dhe 263 të ligjit për procedurë penale, për t'u siguruar se të dhënat e grumbulluara nga ndjekja e komunikimeve janë konform qëllimit për të cilin është dhënë urdhëri për ndjekje. Në të vërtetë, ky qëllim është grumbullimi i të dhënave për rastet e caktuara të veprave penale apo vërtetimin e personave që janë përdorues të linjave telefonike, e-mail adresave apo të tjerave, e që janë objekt i veprës penale. Përderisa nga ndjekja e komunikimeve merren informacione për përfshirjen e personave të tjerë në vepra penale, apo me të cilat vërtetohet dyshimi për vepra të tjera penale, të lëshohet urdhër i ri nga ana e gjykatësit që të mund të vazhdojë ndjekja e komunikimeve, ndërsa procesverbalet e ndjekjes të mund të përdoren në gjyq. Arsyetimi që do të mund t'i jepej gjykatësit për përfshirje më të gjerë të masës, nuk duhet të bazohet në komunikimet e regjistruara që e tejkalojnë urdhërin dhe në bazë të të cilit janë grumbulluar.
- Të kihet kujdes për kategoritë e veçanta të të dhënave personale (ashtu siç është paraparë me ligjin për mbrojtjen e të dhënave personale), respektivisht gjatë ndjekjes së komunikimeve të hiqen apo fshihen dëshmitë të lidhura me këtë kategori të të dhënave personale.

Njoftimi i personave, komunikimet e të cilëve janë ndjekur, e drejta për t'i kontestuar komunikimet e ndjekura, e drejta për ankesë dhe kompensim të dëmit

Ndryshimet ligjore duhet të paraqesin një detyrim për të informuar personat e interesuar për masat e posaçme hetimore pas përfundimit të tyre. Të paktën, personi të cilit i janë grumbulluar të dhënat personale, të mund të disponojë me informatat siç janë: identiteti i kontrollorit, ekzistimi i operacionit për grumbullim, qëllimi i operacionit, e drejta për të shtruar ankesë, e drejta për të kërkuar qasje deri te të dhënat e grumbulluara, por edhe të kërkojë ngrirje dhe restrikcion të përpunimit të mëtejmë. E drejta për të patur qasje deri te informacionet të mund të shmanget vetëm në rast kur mund të dëshmohet se mund ta pengojë apo prejudikojë ndjekjen penale dhe këtë të mund ta bëjë ndonjë organ i pavarur.

- Të parashihen mjete efektive juridike që mund të përdoren në rastet kur një person beson se të drejtat e tij janë shkelur nga autoritetet kompetente, gjatë ndjekjes së komunikimeve. Ndër të tjera, personat, komunikimet e të cilëve ndiqen, të kenë mundësi ligjore për ankesë deri te Drejtoria për Mbrojtjen e të Dhënave Personale për përdorimin e të dhënave të tyre personale. Organizatat joprofitabile që veprojnë në sferën e mbrojtjes së fshehtësisë së të dhënave personale, të kenë të drejtë ligjore të paraqesin ankesa dhe t'i përfaqësojnë personat e përfshirë në ndjekjen e komunikimeve.

Mbrojtja, ruajtja dhe shkatërrimi i komunikimeve të ndjekura

- Nevojitet forcimi i dispozitave ligjore për sigurinë e të dhënave të grumbulluara nga ndjekja e komunikimeve dhe për shkatërrimin e tyre, në rastet kur ato nuk janë më të nevojshme për qëllimin, për të cilin janë mbledhur. Në ligjin për ndjekjen e komunikimeve të parashihen masa të detajizuara për sigurinë gjatë përpunimit të të dhënave, në pajtim me Direktivën 2016/680 për mbrojtjen e të dhënave në polici dhe të drejtën penale. Mes tjerash, të zbatohet parimi i minimizimit i të dhënave gjatë ndjekjes së komunikimeve, duke përfshirë edhe pseudoanonimizimin-përpunimin e të dhënave në mënyrë që të dhënat personale të mos mund t'i përshkruhen një person, pa patur informacione shtesë të cilat ruhen si të veçanta dhe janë objekt i masave teknike e organizative të sigurisë. Të sigurohet se gjatë shkatërrimit të të dhënave, të shkatërrohen edhe procesverbalet dhe të gjitha kopjet në të gjitha institucionet që kanë qenë të kyçura në ndjekje.
- Kur si rezultat i qasjes së paautorizuar do të ketë shkelje të të dhënave personale të mbledhura nga ndjekja e komunikimeve, organi kompetent duhet menjëherë të informojë organin mbikëqyrës për mbrojtjen e të dhënave personale dhe të personave, të dhënat personale të të cilëve janë rrezikuar.

Veçantitë e ndjekjes së komunikimeve me qëllim të mbrojtjes së interesave të sigurisë dhe mbrojtjes së vendit

Për shkak të mbrojtjes së interesave të sigurisë dhe mbrojtjes së vendit është i domosdoshëm vlerësimi paraprak i sigurisë se a duhet të kërkohet që dikujt t' i ndiqen komunikimet.

Mbikëqyrja dhe kontrolli gjatë ndjekjes së komunikimeve

- Të miratohet një rregullore që do të sigurojë zbatim efikas të një procedure për marrjen e certifikatës së sigurisë për anëtarët e komisioneve mbikëqyrëse parlamentare. Deputetët, të cilët nuk do të marrin një certifikatë të tillë brenda një kohe të arsyeshme, nuk do të kenë mundësi të jenë anëtarë të këtyre komisioneve.
- Të evidentohen të gjitha të dhënat për qasje kah sistemi për ndjekjen e komunikimeve.
- Të fshihet dispozita ligjore e ligjit për ndjekjen e komunikimeve, sipas të cilit, komisioni përkatës parlamentar, duhet të miratojë vendim të veçantë për mbikëqyrje. Të krijohet mundësia që çdo anëtar i komisioneve përkatëse parlamentare, të mund të bëjë mbikëqyrje të paparalajmëruar, me ç' rast do të kishin qasje edhe për të dhënat e grumbulluara gjatë ndjekjes, edhe te emrat e personave dhe shkaqet përse janë ndjekur. Emrat nuk duhet të jenë në dispozicion të mbikëqyrësve por, kjo nuk do të vlejë vetëm në rastet kur shkaku për ndjekje ka të bëjë me mbrojtjen e interesave të sigurisë dhe mbrojtjen e vendit.

• Komisionet kuvendore të kenë në dispozicion ekspertë që do t'u ndihmojnë me aspektet teknike dhe juridike të mbikëqyrjes, si dhe për kryerjen e inspektimit në vendngjarje.

• Të formohet një komision civil për mbikëqyrjen e ndjekjes së komunikimeve nga ana e Parlamentit, ku anëtarë do të jenë ekspertë dhe përfaqësues të shoqërisë civile dhe në bazë të një procedure të hapur, transparente dhe objektive do të bëhej nominimi dhe zgjedhja e anëtarëve.

• Trupat mbikëqyrës të bëjnë mbikëqyrjen e ligjshmërisë dhe efekteve nga ndjekja e komunikimeve në të gjitha fazat e saj: përzgjedhja e masave të ndjekjes, grumbullimi i të dhënave por edhe gjatë analizës së tyre.

• Drejtoria për Mbrojtjen e të Dhënave Personale të merr roli mbikqyrës sa i përket të dhënave nga ndjekja e komunikimeve nga ana e organeve kompetente, por të jetë e obliguar edhe ta ndjek zbatimin e të drejtës për mbrojtjen e të dhënave edhe në këto raste.

• Në Raportet e Prokurorit Publik për zbatimin e masave të posaçme hetimore të përfshihen të gjitha të dhënat e përcaktuara ligjore (përfshirë këtu mjetet e harxhuara në rastet kur masat nuk i kanë dhënë rezultatet e pritura) të paraqitura në një mënyrë të qëndrueshme, si dhe të dhëna se sa propozime për ndjekje të komunikimit i janë dorëzuar Prokurorit Publik, për sa prej tyre Prokurori ka rënë dakord, sa iniciativa vetanake ka patur ai për t'i ndjekur komunikimet, dhe për sa kërkesa ka patur urdhër nga gjykatësi. Gjithashtu, në Raport duhet të përfshihen edhe treguesit se në sa urdhëra gjykatësit janë pajtuar plotësisht me kërkesën, sa prej tyre kanë modifikuar (psh. në lidhje me personat ose kohëzgjatjen) dhe sa janë refuzuar. Raportet gjithashtu duhet të përfshijnë statistika nëse ka patur kërkesa apo jo dhe sa prej tyre janë bërë për të siguruar meta të dhëna për ofruesit e huaj të shërbimeve të internetit siç janë Twitter, Facebook, Gmail, etj. Poashtu, duhet të përfshihet edhe numri i lëndëve të ndjekura penale si dhe numri i procerverbaleve të shkatërruara nga masat e posaçme hetimore. Raportet duhet të publikohen në faqen e internetit të Prokurorisë Publike, më së voni deri në fund të shkurtit të vitit aktual, për vitin paraprak.

• Të sigurohet një detyrim për operatorët e shërbimeve të komunikimeve elektronike të publikojnë Raporte vjetore për numrin e urdhërave që ata i kanë marrë për ndjekjen e linjave telefonike ose të linjave të tjera dhe qasjen në meta të dhënat, për cilat vepra dhe për sa persona. Këto Raporte duhet të jenë në dispozicion në formën e të dhënave të grumbulluara në faqet e tyre.

Siguria te operatorët publik të rrjeteve elektronike të komunikimit dhe ofruesit e shërbimeve

• Ofruesit e shërbimeve të komunikimeve elektronike duhet t'i ndërmarrin masat e duhura teknike dhe organizative për të siguruar, që qasjen në të dhënat personale ta kenë të mundur vetëm personat e autorizuar, masa për të mbrojtur të dhënat personale nga çdo formë e paligjshme ose e paautorizuar e përpunimit të tyre dhe masa për zbatimin e politikës së sigurisë gjatë përpunimit të të dhënave personale. Në pajtim me të drejtën e BE-së, ofruesit e shërbimeve të kenë një detyrim për të disejnuar mbrojtjen e fshehtësisë private, që do të thotë, të përfshijnë masa teknike dhe organizative të cilat i mbrojnë të dhënat personale, t'i parashikojnë fillimisht gjatë disejnimit të sistemeve, jo më pas .

• Meta të dhënat të përdoren vetëm për qëllime të pagesës dhe mundësivë teknike të shërbimeve. Kur nuk do të jenë më të nevojshme për këto qëllime, detyrimisht të fshihen ose të anonimizohen.

• Gjatë qasjes drejt meta të dhënave apo gjatë sigurimit të përmbajtjes së komunikimeve, nga ana e operatorëve, për qëllime të ndjekjes ligjore të komunikimeve, detyrimisht të bëhet verifikimi i dyfishtë, gjegjësisht qasja të jetë e mundur vetëm përmes paralajmërimit të më së paku dy personave të autorizuar të operatorit.

• Të rishqyrtohen efektet dhe funksionaliteti i nenit 167 të ligjit për komunikim elektronik për sa i përket raportimit për shkeljen e sigurisë së të dhënave personale nga ana e operatorëve të Agjencisë për Komunikime Elektronike, Drejtorisë për Mbrojtjen e të Dhënave Personale dhe abonuesit.

• Autoritetet kompetente të bëjnë kontrolle të rregullta tek operatorët për qasjen dhe përpunimin e të dhënave nga trafiku i komunikimit dhe të dhënat e vendndodhjes së abonentëve.

Masat ndëshkuese për organet kompetente që kanë ndjekur komunikimet

• Në ligjin për ndjekjen e komunikimeve, duhet të vendosen masa ndëshkuese për autoritetet kompetente dhe personat përgjegjës.

Ruajtja e meta të dhënave

• Të shfuqizohen nenet 176-178 të Ligjit për komunikimet elektronike, të cilat përcaktojnë ruajtjen e meta të dhënave, për dy shkaqe: se nuk ka justifkim ruajtja masive e këtyre të dhënave dhe për shkak të heqjes së Direktivës 2006/24 / EC të inkorporuar në këtë ligj, nga ana e Gjykatës Evropiane të Drejtësisë.

• Të pësojë ndryshime Ligji i ndjekjeve të komunikimit në pjesën e definimit të ndjekjes së komunikimit, pjesë kjo që duhet të ketë të përfshirë ndjekjen, gjegjësisht inspektimin e meta të dhënave.

• Ndjekja e meta të dhënave të bëhet në bazë të kërkesës së Prokurorit Publik, por urdhërin përkatës në procedurë paraprake duhet ta ketë dhënë gjykatësi.

Edukimi

• Të realizohet fushatë për ngritjen e vetëdijes së qytetarëve për rreziqet gjatë komunikimit elektronik, si dhe për të drejtat e tyre për mbrojten e privatësisë dhe të dhënave personale gjatë komunikimit. Sipas Agjencisë së BE-së për të Drejtat Themelore, është e nevojshme të informohen dhe të përkujtohen individët që të jenë të vetëdijshëm për të drejtat e tyre për mbrojtjen e të dhënave dhe t'i shfrytëzojnë mjetet juridike në dispozicion[114].

• DMTP-ja të promovojë ngritjen e vetëdijes te qytetarët për t'i kuptuar rreziqet, rregullat, mënyrën dhe mbrojtjen në raport me komunikimet elektronike dhe ndjekjes së komunikimeve; konform të drejtës së BE-së të këshillojë Kuvendin, Prokurorinë, Ministrinë e

[114] FRA (2013), *Access to data protection remedies in EU Member States*, Luxembourg, Publications Office.

Punëve të Brendshme si dhe operatorët e telekomunikimit dhe organe tjera që kanë lidhshmëri me ndjekjen e komunikimeve.

- Të përforcohet profesionaliteti dhe etika e Prokurorëve Publikë dhe gjykatësve, si dhe të sigurohet mbështetje e jashtme për implementimin e standardeve, për trajnimin dhe specializimin e prokurorëve dhe gjykatësve, në fushën e ndjekjes së komunikimeve, privatësisë dhe mbrojtjes së të dhënave personale.

ANEKS I. LISTA E PËRFAQËSUESVE TË INSTITUCIONEVE DHE EKSPERTËVE ME TË CILËT JANË REALIZUAR INTERVISTA[115]

- Përfaqësuesi i Drejtorisë për Mbrojtjen e të Dhënave Personale.
- Përfaqësuesi i Agjencisë për Komunikime Elektronike
- Përfaqësuesi i Prokurorisë së Lartë Publike
- Gjykatësi i Gjykatës Kushtetuese i Republikës së Maqedonisë
- zv/ Avokati i Popullit i Republikës së Maqedonisë
- Ish kryetari i Kuvendit të Republikës së Maqedonisë dhe anëtar i komisionit kuvendor për mbikëqyrjen dhe ndjekjen e komunikimeve
- Ish Ministri i Punëve të Brendshme dhe anëtari i komisionit kuvendor për mbikëqyrjen dhe ndjekjen e komunikimeve.
- Ish diplomatë dhe zyrtarë në Ministrinë e Punëve të Brendshme.
- Ish zyrtar në Drejtorinë për Siguri dhe Kundërzbulim
- Përfaqësues të Telekomit-it të Maqedonisë
- Profesor në Fakultetin e Sigurisë dhe ish zv/ Ministër i Brendshëm
- Ekspert për mbrojtjen e të dhënave personale dhe privatësinë
- Përfaqësues të organizatave të shoqërisë civile - ekspertë në këtë fushë

[115] Gjatë realizimit të intervistave, të gjithë pjesëmarrësve u është garantuar anonimiteti i tyre, andaj në listë janë dhënë vetëm institucionet që i përfaqësojnë dhe në disa raste edhe funksionet e tyre të mëparshme.

ANEKS II. BIBLIOGRAFIA

- Agjencia e Bashkimit Evropian për të Drejtat Themelore,FRA (2015), Fundamental rights: challenges and achievements in 2014, Luxembourg, Publications Office.
- Ftohja globale - ndikimi i ndjekjes masive të shkrimtarëve ndërkombëtarë, Rezultatet e hulumtimit ndërkombëtar të shkrimtarëve, PEN Qendra Amerikane, 2015
- Direktiva 2002/58/E3 e Parlamentit dhe Këshillit Evropian nga 12.07.2002, O.J. 2002 L 201.
- Direktiva 2006/24/E3 për ruajtjen e të dhënave. Në dispozicion: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF
- Direktiva 2006/24/E3 për ruajtjen e të dhënave. Në dispozicion: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF
- Direktiva 2016/680 për ruajtjen e të dhënave në polici dhe në të drejtën penale Në dispozicion:: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680
- Drejtoria për Mbrojtjen e të Dhënave Personale, Raporti vjetor për vitin 2016. Në dispozicion: https://dzlp.mk/sites/default/files/u4/godisen_izvestaj_dzlp_2016.pdf
- Marrëveshja për funksionimin e Bashkimit Evropian 2012/C 326/01
- Komisioni Evropian. Deklaratë mbi ligjet kombëtare për ruajtjen e të dhënave, 16.09.2015. Në dispozicion: http://europa.eu/rapid/press-release_STATEMENT-15-5654_en.htm
- Konventa Evropiane për të Drejtat e Njeriut
- Të drejtat dixhitale evropiane (European Digital Rights). Gjykata Kushtetuese Federale gjermane e abrogoi ligjin për ruajtjen e të dhënave: https://edri.org/edrigramnumber8-5german-decision-data-retention-unconstitutional/
- Ligji i komunikimeve elektronike i Estonisë. Në dispozicion: https://www.riigiteataja.ee/en/eli/501042015003/consolide
- Ligji i komunikimeve elektronike i Kroacisë. Në dispozicion: https://www.zakon.hr/z/182/Zakon-o-elektroni%C4%8Dkim-komunikacijama
- Ligji i komunikimeve elektronike (LKE), Gazeta Zyrtare e Republikës së Maqedonisë, numër 39/14, 188/14 и 44/15.
- Ligji i komunikimeve elektronike , Gazeta Zyrtare e Republikës së Maqedonisë, nr 39/2014, 188/2014 и 44/2015.
- Ligji për ndryshimin dhe plotësimin e ligjit të komunikimeve elektronike, Gazeta Zyrtare e Republikës së Maqedonisë nr. 83/2010)
- Ligji për ndryshimin dhe plotësimin e Ligjit për ndjekjen e komunikimeve, Gazeta Zyrtare e Republikës së Maqedonisë nr. 116/2012
- Ligji i procedurës penale, Gazeta Zyrtare e Republikës së Maqedonisë nr 150/2010, 100/2012 и 142/2016
- Ligji për ndjekjen e komunikimeve, Gazeta Zyrtare e Republikës së Maqedonisë nr. 121/2006, 110/2008 и 116/2012.
- Raporti për aktivitetet e Prokurorisë Speciale Publike për periudhën prej 15.09.2016 deri 15.03.2017. Në dispozicion: http://www.jonsk.mk/wp-content/uploads/2017/03/6-RAPORT VJETOR.pdf;

- Raporti për aktivitetet e Prokurorisë Speciale Publike për periudhën prej 15.09.2015 deri 15.03.2016, në dispozicion: http://www.jonsk.mk/wp-content/uploads/2016/03/izvestaj-konecen-zaklucen.docx;
- Raport për transparencën e Dojçe Telekom-it për Austri. Në dispozicion: https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/news/austria-363540
- Raport për transparencën e Dojçe Telekom-it për Gjermani. Në dispozicion: https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/news/germany-363566
- Raport për transparencën e Dojçe Telekom-it për Republikën Çeke. Në dispozicion: https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/news/czech-republic-363568
- Raport i Dojçe Telekom-it për privatësinë dhe mbrojtjen e të dhënave, 2015. Në dispozicion: https://www.telekom.com/resource/blob/323750/a7b17936956c92c23c07f433084e21d6/dl-report-datasecurity-2015-data.pdf
- Raporti nga debati publik i Këshillit Kombëtar për Eurointegrime për versionin punues të propozim-ligjit për ndryshimin dhe plotësimin e ligjit për ndjekjen e komunikimeve. Kuvendi i Republikës së Maqedonisë, 16.07.2012. Në dispozicion: https://www.sobranie.mk/WBStorage/Files/JRSledenjenakomunikacii.pdf
- Instituti për të drejtat e informacionit pranë Universitetit të Amsterdamit, Dhjetë standarde për mbikëqyrjen dhe transparencën e shërbimeve kombëtare kundërzbuluese, 2015.
- Prioritetet urgjente reformuese për RM-së, qershor 2015. Në dispozicion: https://eeas.europa.eu/sites/eeas/files/urgent_reform_priorities_en.pdf
- Si ka funksionuar plani për përgjim në "Puç "? TV Alfa 26.02.2015, në dispozicion: http://www.alfa.mk/News.aspx?id=90130.
- Zyra e OKB-së për drogë dhe krime. Praktika nga ndjekja elektronike gjatë hulumtimit të krimit serioz dhe të organizuar, Vienë, 2009. Në dispozicion: https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf
- Konventa për mbrojtjen e personave në raport me përpunimin automatik të të dhënave personale të Këshillit të Evropës.
- Konventa e Kombeve te Bashkuara kundër krimit të organizuar transnacional, në dispozicion:https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf
- Konstanca di Françesko Maesa, Baraspesha mes sigurimit dhe mbrojtjes së të drejtave themelore- analiza e Direktivës 2016/680 për mbrojtjen e të dhënave sektorin e policisë dhe jurisprudencës dhe të Direktivës 2016/681 për përdorimin e listave të emrave të pasagjerëve. (PNR), 2016. Në dispozicion: http://rivista.eurojus.it/balance-between-security-and-fundamental-rights-protection-an-analysis-of-the-directive-2016680-for-data-protection-in-the-police-and-justice-sectors-and-the-directive-2016681-on-the-use-of-passen/
- Kodi Penal, Gazeta zyrtare e Republikës së Maqedonisë nr. 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 87/2007, 7/2008, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 42/2012, 166/2012, 55/2013, 82/2013, 14/2014, 27/2014, 28/2014, 41/2014, 115/2014, 132/2014,160/2014, 199/2014, 226/2015, 97/2017.

- Mendimi i supervizorit evropian për mbrojtjen e të dhënave, 22 korrik 2016
- Vendimi i Gjykatës Kushtetuese nr. 139/2010-0-1 nga 15.12.2010, në dispozicion: http://www.ustavensud.mk/domino/WEBSUD.nsf/ffc0feee91d7bd9ac1256d280038c474/7119424dde39fdadc1257809002db948?OpenDocument
- Zbulimet e Eduard Snouden. Në dispozicion: https://edwardsnowden.com/revelations/
- Zbulimet e publikuara në Vikiliks. Në dispozicion: https://wikileaks.org/
- Vlerësime dhe rekomandime të grupit të lartë të ekspertëve për çështje sistemore nga sundimi i ligjit, 2017. Në dispozicion: https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/2017.09.14_seg_report_on_systemic_rol_issues_for_publication.pdf
- Plani 3-6-9 i Qeverisë së Republikës së Maqedonisë, në dispozicion: http://vlada.mk/sites/default/files/programa/2017-2020/Plan%203-6-9%20MKD.pdf
- Karta e Bashkimit Evropian për të drejtat themelore
- Karta e Bashkimit Evropian për të drejtat themelore, 2012 O.J. (C 326) 391
- „Bombat“ politike në dispozicion:: http://vistinomer.mk/site-prislushuvani-razgovori-objaveni-od-opozitsijata-video-audio-transkripti/.
- Propozim rregullativa e Parlamentit dhe Këshillit Evropian për respektimin e privatësisë dhe mbrojtjen e të dhënave personale. Në dispozicion: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2017:0010:FIN.
- Rekomandimi i Këshillit të Evropës për shfrytëzimin e masave të posaçme hetimore, në dispozicion: https://wcd.coe.int/ViewDoc.jsp?id=849269&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.
- Rekomandimet e grupit të lartë të ekspertëve për çështje sistemore nga sundimi i ligjit, 2015. Në dispozicion: https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/news_corner/news/news-files/20150619_recommendations_of_the_senior_experts_group.pdf
- Aktgjykim i Gjykatës Evropiane të Drejtësisë. Në dispozicion: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf
- Aktgjykim i Gjykatës Evropiane të Drejtësisë.: ECtHR, Klass et al, 6 shtator 1978, pas. 41.
- Aktgjykim i Gjykatës Evropiane të Drejtësisë: ECtHR, Malone v. the United Kingdom, 2 gusht 1984, pas. 84.
- Aktgjykim i Gjykatës Evropiane të Drejtësisë: ECtHR, S. and Marper v. the UK, 4 dhjetor 2008, pas. 101.
- Aktgjykim i Gjykatës Evropiane të Drejtësisë (CJEU), Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, 9 nëntor 2010, pas. 81.
- Aktgjykim: CJEU, Digital Rights Ireland v. Seitlinger and Others, C-293/12, 8 prill 2014.
- Rregullativa (BE) 2016/679 e Parlamentit Evropian dhe e Këshillit për mbrojtjen e individëve lidhur me përpunimin e të dhënave personale dhe qarkullimit të lirë të tyre (Rregullativa e përgjithshme për mbrojtjen e të dhënave), OJ L 119, 27.04.2016, në dispozicion: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
- PPS përfundimisht hyri ne Telekom SDK.MK, 24.04.2017, në dispozicion: http://sdk.mk/index.php/makedonija/sjo-konechno-vleze-vo-telekom/.
- Lista e kontrollit për sundimin e ligjit. Komisioni i Venecias.

- Qëndrimi i BE-së për vendimin e PKE-së për shfuqizimin e Direktivës: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp220_en.pdf
- Electronic Frontier Foundation и Article 19, E domosdoshme dhe proporcionale-parime ndërkombëtare për zbatimin e kornizës juridike për të drejtat e njeriut gjatë ndjekjes së komunikimeve, 2014


152
166
180
193
207