КОН ГРАЃАНСКИ ПАНОПТИКОН

подобра рамнотежа меѓу заштитата на приватноста и потребата од следење на комуникациите

Проектот го финансира Европската Унија

МРЕЖА 23

"ЖЕНСКА АКЦИЈА"

Скопје, 2017

Асоцијација за унапредување на статусот на жената во современите општествени процеси во Македонија

Association for improving the status of women in contemporary social processes in Macedonia

"ЖЕНСКА АКЦИЈА" "WOMEN'S ACTION"

МРЕЖА 23

Студија за јавна политика

КОН ГРАЃАНСКИ ПАНОПТИКОН

Подобра рамнотежа меѓу заштитата на приватноста и потребата од следење на комуникациите

Скопје, 2017

Проектот „И метаподатоците се лични! Како до подобра рамнотежа меѓу приватноста и потребата за следењето на комуникациите?“ е финансиран од Европската Унија.

Издавач:
„Женска акција“ – асоцијација за унапредување на статусот на жената во современите општествени процеси

За издавачот:
Драгица Милошевска

Уредник:
Александар Николов

Лектор: Сашо Костов

Автори:
Александар Николов
Душко Тодороски

Истражувачи:
Мирјана Апостолова
Наташа Најденова - Левиќ
Драгица Милошевска

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

342.738(497.7)

НИКОЛОВ, Александар
Граѓански паноптикон : подобра рамнотежа меѓу заштитата на приватноста и потребата од следење на комуникациите : нацрт-документ за јавна политика / [автори Александар Николов Душко Тодороски]. - Скопје : Женска акција, 2017. - 52 стр. ; 25 см

Фусноти кон текстот. - Содржи и: Анекс 1

ISBN 978-608-66103-1-9
1. Тодороски, Душко [автор]
а) Право на приватност - Заштита на лични податоци - Македонија б) Јавни политики - Македонија
COBISS.MK-ID 103740938

Оваа публикација беше овозможена со поддршка од Европската Унија во рамките на проектот Мрежа 23+ кој е имплементиран од Институтот за европска политика и Хелсиншкиот комитет за човекови права на Република Македонија. Наведените мислења во оваа публикација се мислења на авторите и не секогаш ги одразуваат мислењата на Европската Унија.

СОДРЖИНА

Извршно резиме....5
Вовед....9
Методологија....13
Правна анализа на клучните европски стандарди за заштитата на приватноста и личните податоци при електронските комуникации....14
Задржување метаподатоци....22
Анализа на правната рамка за заштита на приватноста и личните податоци при електронските комуникации во Македонија....31
Анализа на правната и институционална рамка за следење на комуникациите и задржување податоци во Македонија....34
Дефинирање и опфат на следењето комуникации....34
Основ за следење комуникации....35
Барање за следење комуникации....36
Наредба за следење на комуникациите....37
Времетраење на следењето комуникации....39
Клучните наоди на Прибе....39
Оперативно спроведување на следењето комуникации....40
Прибе за реформирањето на УБК....41
Употреба на сознанијата од следењето на комуникациите....43
Известување на лицата чии комуникации се следени, право на оспорување на следените комуникации, право на приговор и надомест на штета....44
Заштита, чување и уништување на следените комуникации....45
Специфики на следење на комуникациите заради заштита на интересите на безбедноста и одбраната на земјата....46
Надзор и контрола над следењето комуникации....47
Безбедност кај операторите на јавните електронски комуникациски мрежи и давателите на услуги....49
Казнени одредби за надлежните органи за следењето комуникации....50
Задржување метаподатоци....50
Анализа на извештаите на јавниот обвинител за следењето на комуникациите....53
Препораки....59
Анекс 1. Список на претставници на институции и експерти со кои беа спроведени интервјуа. 71
Анекс2.
Библиографија.... 72

Извршно резиме

Овој документ има за цел да иницира зајакнување на почитувањето на правото на приватност и заштита на личните податоци при електронските комуникации во Република Македонија, преку претставување и застапување на препораките за измени на правната и надзорната рамка врз основа на правото на ЕУ и најдобрите практики од државите членки на Унијата, во насока на ограничување на можноста за масовно и неселективно следење комуникации, метаподатоци и јасно разграничување на надлежностите на разузнавачките служби и истражните органи.

Објавувањето на политичките „бомби“ во 2015 година коишто укажаа на нелегално следење на телефонските комуникации на политичките и бизнис елити, медиумите и граѓанските активисти, беше вторпат од независноста на Македонија – по аферата „Големото уво“ од 2000 година – да се открие нелегално масовно прислушување што ја нарушило приватноста, заштитата на личните податоци и слободата на изразување. Ваквите скандали покажуваат сериозни злоупотреби на државниот систем за следење на комуникациите, поконкретно, опремата и персоналот на Управата за безбедност и контраразузнавање. Европската комисија изрази загриженост во извештаите за Македонија за 2015 и 2016 година за масовното следење на електронските комуникации, а во Итните реформски приоритети посочи и сериозни реформи што ги очекува за надминување на недостатоците во правната рамка за следење на комуникациите и нивно спроведување.

Законот за електронските комуникации (ЗЕК) од 2014 година воведе новини во следењето на содржината на комуникациите, како и во масовното задржување на податоци за комуникацискиот сообраќај на граѓаните. Законот овозможи Министерството за внатрешни работи да има *директен* и *неограничен* пристап до содржината на *сите* електронски комуникации на *сите* граѓани. Покрај тоа, беше воведена обврска сите телефонски и интернет провајдери да ги задржуваат една година за сите свои корисници т.н. „метаподатоци“. Одредбите за масовно задржување податоци беа оправдани како транспонирање на Директивата 2006/24/ЕЗ, којашто беше поништена од Европскиот суд на правдата непосредно по донесувањето на новиот ЗЕК. Сепак, Република Македонија сè уште нема преземено соодветни мерки со цел да ги надмине сериозните предизвици наметнати од ваквата ситуација.

Имајќи ги предвид детектираните предизвици, авторите предлагаат повеќе препораки што треба да овозможат наместо паноптикон – систем во кои граѓаните се исплашени бидејќи се под постојан надзор од власта – во Македонија да се изгради граѓански паноптикон – систем во којшто транспарентноста создава отчетност кај носителите на власта кон граѓаните. Препораките се детално изложени под соодветниот наслов во студијава, а во продолжение накратко се дадени клучните:

- Да се укинат членовите 176–178 од Законот за електронски комуникации кои го пропишуваат задржувањето метаподатоци поради укинување од Европскиот суд на

правдата на Директивата 2006/24/ЕЗ којашто е транспонирана во овој закон. Следењето и увидот во метаподатоци за електронските комуникации да биде опфатено во Законот за следење на комуникациите.

- Да се преиспита оправданоста да се дозволува следење на комуникациите за толку широк опсег на кривични дела, врз основа на проценка дали нарушувањето на приватноста е пропорционално на тежината на кривичното дело за коешто станува збор и доказите што се очекува да се соберат со посебните истражни мерки, односно следењето комуникации.
- Да се оневозможи директниот пристап до содржината на комуникациите од страна на службите, односно надлежните органи претходно да треба да го известат операторот и да достават судски налог за следење, а потоа операторот да го овозможи пристапот до комуникациите на опфатените лица.
- Во барањето за следење на комуникациите да треба да се наведе и образложи основано сомневање за можно извршување или веќе извршено кривично дело, а не само основ за сомневање како многу низок степен на сомневање.
- Да се воведе уште една страна во постапката на одобрување на следењето комуникации што ќе ги застапува интересите на лицата чии комуникации се предлага да се следат (на пр. панел на експерти, претставник на Дирекцијата за заштита на личните податоци или Народниот правобранител). Оваа страна да има право да приговара на барањата за следење комуникации, како и на наредбите за следење на комуникациите доколку смета дека доаѓа до неоправдано нарушување на приватноста и личните податоци на граѓаните.
- Да се преиспита оправданоста на пропишаните долги максимални рокови за следење на комуникациите.
- Законски да се раздвојат надлежноста и прописите за следење на комуникациите при кривичните истраги, од оние од безбедносен и разузнавачки карактер.
- Да се зајакне внатрешната контрола во МВР за да врши контрола и на случаи во коишто е злоупотребено овластувањето за следење на комуникациите.
- Доколку со следењето комуникации се стекнат сознанија коишто имплицираат други лица во кривичните дела, или со коишто се утврдуваат основи за други кривични дела од оние на коишто се однесува постојната наредба за следење на комуникациите, да биде потребно издавање нова наредба од судијата за да продолжи следењето комуникации и за записите од тие комуникации да може да се користат на суд.
- Да се предвиди претпазливост за посебните категории на лични податоци (утврдени со Законот за заштита на личните податоци), односно при следењето комуникации да се исклучат или избришат искази поврзани со овие податоци.
- Да се воведе обврска засегнатите лица да се известат за посебните истражни мерки по нивното прекинување, освен кога може да се докаже дека тоа ќе доведе до попречување или прејудицирање на кривичното гонење.
- Да се воведат делотворни *правни лекови* што можат да се исползуваат во случаите кога одредено лице смета дека му се прекршени правата со следење на комуникациите од страна на надлежните органи. Релевантни непрофитни организации да добијат законско право да можат да поднесуваат приговори и да ги застапуваат засегнатите лица од следењето комуникации.

- Да се зајакнат законските одредби за безбедност на податоците од следењето на комуникациите и за нивно уништување во случаите кога веќе не се потребни заради целта за којашто биле собирани.
- Да се обезбеди можност за ненајавен надзор да има секој член на надлежните собранискиkомисии, придружени од стручни лица на комисиите, при што би имале пристап и до агрегирани податоци за следењето и до имињата на лицата и основите по коишто се следат. Покрај тоа, да се донесе регулатива што ќе обезбеди ефикасно спроведување постапка за добивање безбедносен сертификат за членовите на надзорните собранискиkомисии.
- Да се воведе и граѓанска комисија за надзор над следењето на комуникациите, којашто ќе ја именува Собранието од експерти и претставници на граѓанското општество.
- Да се прошири обврската за известување за барањата и наредбите за следење на комуникациите и на судовите и телекомуникациските оператори. Извештаите на јавниот обвинител да ги содржат сите пропишани елементи, вклучително и за трошоците и образложение во случаите кога мерките не ги дале очекуваните резултати, а да се објавуваат најдоцна до крајот на февруари во тековната година за претходната година. Извештаите да содржат и преглед на прифатени, модифицирани или отфрлени барања за следење на комуникациите, бројот на следени предмети на кривично дело, бројот на барања за обезбедување метаподатоци од странски провајдери на интернет услуги, бројот на уништени записи од посебните истражни мерки.
- Давателите на електронски комуникациски услуги да имаат обврска за дизајн насочен кон приватност, т.е. техничките и организациските мерки коишто обезбедуваат заштита на личните податоци да ги предвидат уште при дизајнот на системите, а не отпосле. Надлежните органи да прават редовни контроли кај операторите за пристапот и обработката на податоците за комуникациски сообраќај и податоците за локација на претплатниците.
- Во законот за следењето на комуникациите да се воведат казнени одредби за надлежните органи и одговорните лица во нив.
- Да се спроведе кампања за подигнување на свеста на граѓаните околу ризиците при електронските комуникации, како и нивните права за заштита на приватноста и личните податоци при комуникацијата.
- Да се јакне стручноста и етиката кај јавните обвинители, судиите, како и да се обезбеди надворешна поддршка за имплементација на стандардите, и за обука и специјализација на обвинителите и судиите во областа на следење на комуникациите, приватноста и заштитата на личните податоци.

Вовед

Паноптикон е симбол за модерното општество во коешто следењето на комуникациите е толку раширено, што луѓето прибегнуваат кон самоцензура и се плашат да кажат нешто што отстапува од доминантното мислење, или од политички коректното. Поимот потекнува од архитектонски пристап од 19-тиот век што овозможува лесен надзор над луѓето. Кај архитектурата на паноптиконот, луѓето што се предмет на надзор, на пример затвореници, пациенти, деца или работници, се сместени во простории што се распоредени околу централна кула наменета за надзорникот. Кулата ги осветлува околните простории, за да може надзорникот да гледа што прават сите. Но, кулата е направена така што луѓето не можат да видат дали во неа има некој. Тие сепак имаат чувство дека некој постојано ги надгледува, па се трудат да бидат „дисциплинирани“ и „примерни“.

*Зборот паноптикон произлегува од старогрчкиот збор **паноптис**, што значи оној кој гледа сè. Во старогрчката митологија Аргус Паноптис бил џин кој имал многу очи и никогаш не спиел. Хера, сопруга на Зевс, го задолжила да внимава на нимфата Ија, за која се сомневала дека е љубовница на Зевс.*

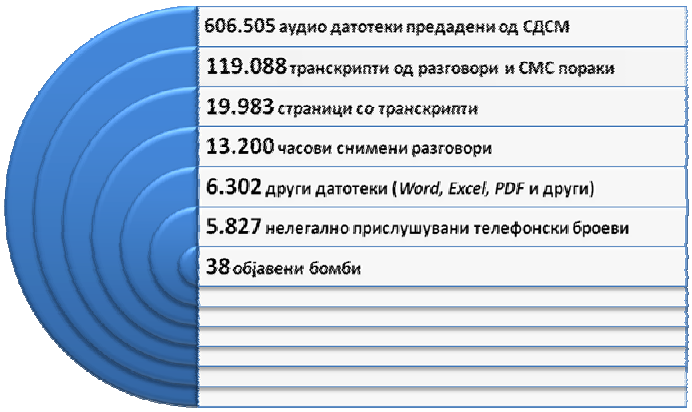
Едвард Сноуден[1] и Викиликс[2] покажаа дека паноптиконот постои, разоткривајќи глобални програми за масовно следење на телефонските, интернет и радио комуникациите. Предмет на ова широко следење на комуникациите не е само содржината на комуникациите, туку и на т.н. метаподатоци, односно податоците за тоа со кого, кога и колку често комуницираме, како и со кои уреди и од кои локации. Неуспехот на државите и наднационалните власти да обезбедат соодветна заштита на приватноста и личните податоци на корисниците на електронските комуникации, резултираше со тоа шеесет проценти од Европејците да немаат доверба во телекомуникациските компании и интернет провајдерите, а седумдесет проценти да бидат загрижени дека нивните податоци се користат за поразлични цели од оние за коишто се собираат.[3]

Во Македонија, чувството дека живееме во паноптикон беше дополнително засилено во 2015 година со објавувањето на политичките „бомби“ кои укажаа на нелегално следење на телефонските комуникации на политичките и бизнис елити,

[1] https://edwardsnowden.com/revelations/
[2] https://wikileaks.org/
[3] Извештај на „Дојче Телеком“ за приватност и безбедност на податоците, 2015. Достапен на: https://www.telekom.com/resource/blob/323750/a7b17936956c92c23c07f433084e21d6/dl-report-datasecurity-2015-data.pdf

медиумите и граѓанските активисти во периодот од 2008 до 2015 година.[4] Ова е вторпат, по аферата „Големото уво“ од 2000 година, да се открие нелегално масовно прислушување што ја нарушило приватноста, заштитата на личните податоци и слободата на изразување. Ефектот на самоцензура, карактеристичен за паноптиконот, се акцептира и во Македонија, па стана нормално луѓето при телефонските разговори да упатуваат на внимателност кај соговорникот во однос на тоа што се кажува или што се открива.

Графикон: Бомбите на СДСМ во бројки[5]



Иако власта и опозицијата имаа различни објаснувања околу мотивите и актерите што довеле до прислушувањето што беше објавено со „бомбите“, како и каналите преку коишто протекле овие лични податоци, и едните и другите се согласија дека е злоупотребен и државниот систем за следење на комуникациите, поконкретно опремата и персоналот на Управата за безбедност и контраразузнавање.[6] Дополнително, фактот што од системот излегле документи со следените комуникации е доволен да се заклучи дека не постојат соодветни стандарди, процедури и заштитни механизми за информациска безбедност.

[4] Временскиот периодот во којшто се одвивало незаконското следење на комуникациите е утврдено во Законот за заштита на приватноста („Службен весник на Република Македонија“ бр. 196/2015). „Бомбите“ се достапни на http://vistinomer.mk/site-prislushuvani-razgovori-objaveni-od-opozitsijata-video-audio-transkripti/.

[5] Извештај за активностите на Специјалното јавно обвинителство за периодот од 15.09.2016 до 15.03.2017, достапен на http://www.jonsk.mk/wp-content/uploads/2017/03/6-MESECEN-IZVESTAJ.pdf; Извештај за активностите на Специјалното јавно обвинителство за периодот од 15.09.2015 до 15.03.2016 достапен на http://www.jonsk.mk/wp-content/uploads/2016/03/izvestaj-konecen-zaklucen.docx; „СЈО конечно влезе во Телеком“, SDK.MK, 24.04.2017, достапно на http://sdk.mk/index.php/makedonija/sjo-konechno-vleze-vo-telekom/.

[6] ВМРО-ДПМНЕ тврдеше дека следењето на комуникациите се вршело на неколку начини. Покрај злоупотреба на опремата на УБК, наводно преку соработници на странска разузнавачка служба, поранешниот премиер Груевски во изјава дадена на 25.02.2015 година наведе дека нелегално „прислушување и снимање телефонски разговори“ било вршено и од страна на непознати сторители со употреба на мобилна опрема чија локација постојано се менува, а која функционира по принцип на клонирање на таканаречените базни станици на операторите на мобилните комуникациски мрежи. „Како функционирала шемата за прислушување во „Пуч“?“, Алфа ТВ, 26.02.2015, достапно на http://www.alfa.mk/News.aspx?id=90130.

Постојат и други проблеми во приватноста на електронските комуникации. Законот за електронските комуникации (ЗЕК) од 2014 година[7] воведе масовно задржување податоци за телекомуникацискиот сообраќај на граѓаните. Без позначајна дискусија во јавноста, се наметна обврска сите телефонски и интернет провајдери да ги задржуваат една година за сите свои корисници т.н. „метаподатоци“ и по барање да им ги достават на државните органи. Тука спаѓаат следниве податоци за телефонски и интернет услуги (вклучително и е-пошта): името и адресата на лицата кои комуницираат, телефонскиот број или ИП адресата на електронскиот уред со којшто се комуницира, телефонскиот уред и географската локација на лицата кои комуницираат; времето на почетокот и крајот на комуникацијата; видот на телефонска или интернет услуга. Одредбите за масовно задржување податоци беа оправдани како транспонирање на Директивата 2006/24/ЕЗ[8], која беше поништена[9] од Европскиот суд на правдата непосредно по донесувањето на новиот закон во Македонија.

Дополнително, ЗЕК од 2014 година овозможи Министерството за внатрешни работи да има *директен* и *неограничен* пристап до содржината на *сите* електронски комуникации на *сите* граѓани. Според старото законско решение, операторите овозможуваа пристап до содржината на комуникациите на *одреден* корисник само врз основа на налог од надлежен суд.

Нетранспарентноста од страна на Јавното обвинителство за ефектите од следењето на комуникациите, како и неработењето и немањето пристап до релевантни податоци на Собраниската комисија за надзор на следењето на комуникациите и Комисијата за надзор над работата на разузнавачките и контраразузнавачките служби, уште повеќе ги зголемува ризиците за злоупотреба на системот за следење на комуникациите, вклучително и на задржаните метаподатоци за комуникациите на корисниците на електронски услуги.

Оваа студија ги анализира правните, техничките, институционалните и едукативните

Наместо слобода на изразување – самоцензура и изолација

Меѓународно истражување од 2014 година на Американскиот ПЕН центар покажа дека писателите, под притисок на стравот од масовно следење на комуникациите, прибегнуваат кон самоцензура. Зависно од земјата, поради ваков страв меѓу 34% и 61% од писателите избегнале да зборуваат или пишуваат на одредена тема, или сериозно размислувале тоа да го направат. Меѓу четвртина и две третини од писателите почнале намерно да избегнуваат одредени теми во телефонска или мејл комуникација, да ги избегнуваат социјалните мрежи, или да се воздржуваат од одредени интернет пребарувања или посета на веб-страници кои би можеле да се сметаат за контроверзни или сомнителни. Ефектот на паноптиконот придонел дури и писателите – кои би се очекувало како интелектуалци да имаат прогресивни и слободарски тенденции – да се откажат од дел од својот идентитет, своите ставови и слободи.

[7] „Службен весник на Република Македонија“ број 39/14, 188/14 и 44/15.
[8] Достапно на: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF
[9] Пресуда на Европскиот суд на правдата. Достапна на: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

недостатоци што резултираат со масовно нарушување на приватноста и заштитата на личните податоци при електронските комуникации во Македонија. Ваквите состојби имаат силно негативно влијание врз целото општеството преку:

- **Злоупотребување на институциите за остварување приватен наместо јавен интерес**. „Бомбите“ покажаа дека Управата за безбедност и контраразузнавање, операторите на јавни комуникациски мрежи и функционерите лесно можат да ја нарушат приватноста на граѓаните и да ги злоупотребат нивните лични податоци за остварување лична или групна корист којашто е спротивна на јавниот интерес.
- **Влошување на довербата во институциите**. Разоткривањето на масовното и нелегално следење на комуникациите ја еродира довербата на јавноста во безбедносните органи, владеењето на правото и правната држава.
- **Загрозување на демократијата**. Масовното и честопати нелегално следење на комуникациите ја загрозува и слободата на изразување и води до појава на самоцензура кај граѓаните, или нивно повлекување од јавниот живот. Постои ризик за притисок над опозицијата, поединечни функционери или стекнување нефер предност на одредени политичари и политички партии наспроти другите.
- **Зголемување на безбедносните ризици**. Функционерите и политичарите кои наредиле нелегално или масовно прислушување или кои биле жртви на истото, можат лесно да бидат компромитирани во јавноста со цел создавање криза или, пак, може да станат предмет на уцени. Покрај ова, големите ресурси потребни за масовно следење на комуникациите создаваат ризик дека нема да останат доволно ресурси за оптимално функционирање на останатите сегменти на безбедносниот систем. Од друга страна, нарушената доверба на јавноста создава безбедносен ризик дека ќе се отежне соработката на безбедносните органи со граѓаните.
- **Зголемување на економските ризици**. Злоупотребата на системот за следење на комуникациите за индустриска шпионажа и остварување лични и семејни бизнис интереси може ги дестимулира приватните инвестиции и да ја наруши пазарната конкуренција.

Оттука, Европската комисија изрази загриженост во извештаите за Македонија за 2015 и 2016 година за масовното следење на електронските комуникации, а во Итните реформски приоритети посочи и сериозни реформи што ги очекува за надминување на недостатоците во правната рамка за следење на комуникациите и нивно спроведување.

Овој документ има за цел да иницира зајакнување на почитувањето на правото на приватност и заштита на личните податоци при електронските комуникации, преку претставување и застапување на препораки за измени на правната и надзорната рамка врз основа на правото на ЕУ и најдобри практики од држави членки на Унијата, во насока на ограничување на можноста за масовно и неселективно следење комуникации и метаподатоци. Авторите се надеваат дека на тој начин ќе придонесат наместо паноптикон, во нашето општество да се изгради **граѓански паноптикон.** Граѓанскиот паноптикон е идеал за сосема поинаков систем во кој транспарентноста создава отчетност кај носителите на власта. Метафорично, кај архитектурата на граѓанскиот паноптикон, секој што извршува јавна функција е сместен во отворена просторија и е опкружен со граѓани кои внимаваат што прави функционерот и му поставуваат прашања.

Методологија

Беше спроведена анализа на податоците од секундарни извори за состојбата со заштитата на приватноста и личните податоци при електронските податоци, којашто содржи меѓународен преглед со фокус на правото на ЕУ и преглед на состојбата во оваа сфера во Македонија. Меѓународната споредбена анализа на заштитата на приватноста и личните податоци при електронските комуникации се фокусира на правото на ЕУ, други европски стандарди, релевантните судски одлуки и нивната примена во одредени држави членки. Беа издвоени и најдобрите практики од државите членки на Унијата.

Анализата на состојбата во сферата на заштита на приватноста и личните податоци во електронските комуникации во Македонија, од аспект на следењето на комуникациите, беше подготвена преку истражување на постојни документи и интервјуа. Проектниот тим ја анализираше домашната законска рамка со којашто се регулира заштитата на приватноста и личните податоци при електронските комуникации, како и други постојни анализи и студии на оваа тема што се однесуваат на состојбата во Македонија, со акцент на задржувањето метаподатоци. Анализата на документите беше надополнета со средби со претставници на повеќе надлежни институции, меѓу кои и Дирекцијата за заштита на личните податоци, Вишото јавно обвинителство, Уставниот суд, Факултетот за безбедност во Скопје, Народниот правобранител и Агенцијата за електронски комуникации (види „Анекс – список на интервјуирани претставници на институции и експерти“). Исто така, беа остварени разговори и со поранешни функционери на МВР и на Управата за безбедност и контраразузнавање, Собраниските комисии за надзор над следењето на комуникациите и за надзор над службите, поранешни пратеници во Собранието, како и со други независни експерти во областа.

Додадена вредност од документот се конкретните препораки за подобрување на општата состојба со заштитата на приватноста и личните податоци – вклучително и метаподатоците при електронските комуникации во Македонија, како и разграничување на надлежностите на разузнавачките служби и истражните органи.

Ограничување со кое се сретнаа авторите е осетливоста на темата поради што не беа во можност да ги обезбедат сите потребни информации од надлежните институции и соговорниците. Дополнително ограничување беше фактот што Европската Унија во текот на анализата беше во процес на значително изменување на законодавството во сферата на заштита на личните податоци, вклучително и при електронските комуникации, како и во полицијата и правосудството, што не заврши целосно до печатењето на оваа публикација. Во случаите кога има донесено нови правни акти на Унијата, студијата се осврнува на нив, дури и кога сè уште не се стапени на сила. Студијата не се занимава директно со ризиците од нарушувањето на приватноста на граѓаните од пресретнување на комуникациите и личните податоци од страна на странските служби, или од пренос на податоците меѓу државите. Документот исто така не навлегува во анализа како да се постигне рамнотежа меѓу заштитата на приватноста на јавните личности од една страна и јавниот интерес да бидат познати нивните активности и ставови од друга страна.

Правна анализа на клучните европски стандарди за заштитата на приватноста и личните податоци при електронските комуникации

Во овој дел се осврнуваме на правната рамка поставена од Советот на Европа и Европската Унија.

При заштитата на приватноста, европските земји, како членки на Советот на Европа се должни да се придржуваат и до правните обврски кои произлегуваат од Европската конвенција за заштита на човековите права и основните слободи и Конвенцијата за заштита на лица во однос на автоматската обработка на личните податоци.

Според **Европската конвенција за човекови права** „секој човек има право на почитување на неговиот приватен и семеен живот, домот и преписката".[10] Концептите на приватен живот и преписка ги вклучуваат и телефонските и телекомуникациските податоци.[11] Одлуките на Европскиот суд за човекови права наведуваат дека заштитата на ова темелно право ја опфаќа не само содржината на комуникациите, туку и метаподатоците за остварениот сообраќај. Тука, на пример, спаѓаат „датумот и времетраењето на разговорите" и телефонските броеви што се барани, затоа што таквите податоци се „составен дел на комуникациите преку телефон".[12] Конвенцијата го предвидува и *правото на информираност* на поединецот за кого се прибираат податоци и, ако е потребно, *правото на нивно коригирање*.

Според член 8, став 2 од Конвенцијата, мешањето на јавната власт во остварувањето на правото на приватен живот може да е дозволено само ако тоа мешање е предвидено со закон и ако претставува мерка што е во интерес на државната и јавната безбедност, економската благосостојба на земјата, заштитата на поредокот и спречувањето на кривични дела, заштитата на здравјето и моралот, или заштитата на правата и слободите на другите. Според Европскиот суд за човекови права, таквото мешање може да се смета за оправдано само ако е *неопходно*, одговара на *итни општествени потреби*, *пропорционално* е на целта за која се презема и ако причините што се наведуваат од јавните власти за да се оправда се *релевантни* и *доволни*.[13] Како илустрација, во случајот на Мелоун (*Malone*) против Обединетото Кралство, судот утврдил дека масовното и неселективно задржување на отпечатоци од прстите и на податоци за ДНК на лица кои се осомничени, но не и осудени, не е оправдано според членот 8, став 2 од Конвенцијата. Во контекстот на Европската Унија, пак, Судот на правдата на Европската Унија има наведено и дека за мешањето на властите во приватниот живот да се смета за *пропорционално* на намената за која се презема, треба да се демонстрира дека не се на располагање други, помалку интрузивни методи.[14]

[10] Член 8, став 1 од Конвенцијата.

[11] Подгледнете ECtHR, Klass et al, 6 септември 1978, пас. 41.

[12] Подгледнете ECtHR, Malone v. the United Kingdom, 2 август 1984, пас. 84.

[13] Подгледнете на пр. ECtHR, S. and Marper v. the UK, 4 декември 2008, пас. 101.

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

Конвенцијата за заштита на лица во однос на автоматската обработка на личните податоци на Советот на Европа, којашто е ратификувана и од страна на Република Македонија, цели кон обезбедување на правата и основните слободи на поединците, а особено нивното право на приватност во однос на автоматското обработување на личните податоци во јавниот и приватниот сектор. Конвенцијата е прв меѓународно обврзувачки инструмент што ги заштитува поединците од злоупотреби што можат да се јават при прибирањето и обработката на личните податоци. Обработката на податоците поедноставено може да се дефинира како сè што може да се прави со податоците, на пример нивно прибирање, зачувување или бришење.

Членот 5 од Конвенцијата налага дека личните податоци во процесот на автоматизираното обработување треба да бидат: а) прибрани и обработени чесно и законито; б) зачувани за конкретни и легитимни цели и нема да бидат употребувани за цели што се неспоиви; в) соодветни, релевантни и непретерани во однос на целите за коишто биле зачувани; г) прецизни и ако е потребно, ажурирани; е) зачувани во облик што дозволува идентификација на податоците не подолго од она што е неопходно за целта за којашто се зачувани. Согласно оваа Конвенција, соодветни безбедносни мерки треба да бидат преземени за заштита на личните податоци чувани во автоматизирани бази на податоци против случајно или неовластено уништување, случајно губење, како и против неовластен пристап, изменување или дистрибуција.[15] Конвенцијата ја забранува автоматската обработка на *осетливи лични податоци* – како што се оние за етничко или расно потекло, политички или религиозни верувања, здравјето, сексуалниот живот или податоците за осуди за кривични дела – доколку националното законодавство нема воспоставено соодветни заштитни механизми.[16] Конвенцијата исто така воспоставува право на поединецот да може да дознае дека се зачувани податоци за него/неа, да ја дознае намената за којашто се зачувани, содржината и ако е потребно, да може да обезбеди нивно коригирање или бришење доколку се обработени спротивно на националното законодавство.[17] Исклучоци од одредбите за заштита на личните податоци може да има само ако се дозволени со националното законодавство и ако претставуваат неопходна мерка во едно демократско општество, а во интерес на заштита на државната безбедност, јавната сигурност, монетарните интереси на државата, спречување на извршување кривични дела, или заштита на субјектите на податоците или пак на правата и слободите на другите.[18]

Венецијанската комисија[19] има утврдено **Список за проверка на владеењето на правото**, што треба да послужи како инструмент за проценка на владеењето на правото во одредена земја од аспект на нејзините уставни и правни структури, законодавството и постојната правна пракса.[20] Иако не е правен акт, овој документ е

[15] Член 7 од Конвенцијата.
[16] Член 6 од Конвенцијата.
[17] Член 8 од Конвенцијата.
[18] Член 9 од Конвенцијата.
[19] Европската комисија за демократија преку правото е советодавно тело на Советот на Европа за помагање и советување на индивидуални држави членки во уставни прашања, со цел да се унапреди функционирањето на демократските институции и заштитата на човековите права.
[20] Списокот е достапен на http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)007-e

битен бидејќи на концизен начин ги изложува критериумите по коишто може да се оцени владеењето на правото во една земја, вклучително и од аспект на следење на комуникациите. Според Списокот, следењето на комуникациите може сериозно да го наруши правото на приватност, па од суштинска важност е да не ѝ овозможи на државата неограничена моќ да го контролира животот на поединците. За таа цел, следењето на комуникациите треба да биде ограничено со принципи, како на пример, принципот на пропорционалност. Потребно е да постојат и процедурални контроли и надзор, вклучително и давање овластување од судија или независно тело, дури и во случаите на следење на податоците за телекомуникацискиот сообраќај на конкретна личност, односно метаподатоците. Покрај тоа, потребно е да постојат делотворни *правни лекови* што можат да се исползуваат во случаите кога одредено лице смета дека му се прекршени правата. Документот прави важно прецизирање дека и собирањето метаподатоци за електронските комуникации претставува следење на комуникациите. Во случаи на масовно следење на комуникациите, документот потенцира дека е потребно со закон да се утврдени детални цели за коишто е оправдано да се примени масовно следење на комуникациите. Со тоа би се ограничило собирањето, задржувањето и дисеминацијата на собраните податоци – вклучително и врз основа на принципот на пропорционалност.

Во Европската Унија, правото на приватност и заштита на лични податоци се две различни човекови права заштитени со **Договорот за функционирањето на Европската Унија** и **Повелбата на Европската Унија за основните права**, како и од правниот систем на 28 земји членки на ЕУ.

Според **Договорот за функционирање на Европската Унија**[21], секој има право на заштита на личните податоци. Членот 16 од Договорот посочува дека Европскиот парламент и Советот ги одредуваат правилата за заштитата на поединците во однос на обработка на личните податоци од страна на Унијата и нејзините институции, тела, канцеларии и агенции, како и од страна на државите членки во активности кои спаѓаат во опсегот на правото на Унијата. Членот 87, став 2 од Договорот воведува систем за полициска и судска соработка во кривични предмети. За таа цел, Европскиот парламент и Советот можат да донесат мерки во врска со прибирањето, зачувувањето, обработката, анализата и размената на релевантни информации.

Повелбата на Европската Унија за основните права[22] ги гарантира правото на приватност (член 7) и заштитата на личните податоци (член 8). Членот 8 што се однесува на заштитата на личните податоци наведува дека истите мора да се обработуваат само за конкретни цели и со согласност на засегнатото лице или врз некоја друга легитимна основа утврдена со закон. Секој има право на пристап до податоците собрани за него, како и право на исправка на истите. Следствено на тоа, во истиот член се наведува дека почитувањето на овие правила ќе биде контролирано од независни органи.

Директивата[23] за обработката на личните податоци и заштитата на приватноста во електронскиот комуникациски сектор, како и измените усвоени со Директивата 2009/136/ЕЗ од 2009 година, имаат за цел, меѓу другото, да ги усогласат националните акти на државите членки за да обезбедат еднакво ниво на заштита на основните права

[21] Договор за функционирање на Европската Унија 2012/С 326/01
[22] Повелба на Европската унија за основните права, 2012 О.Ј. (С 326) 391
[23] Директива 2002/58/ЕЗ на Европскиот парламент и Советот од 12.07.2002, О.Ј. 2002 L 201.

и слободи, и особено правото на приватност, при обработката на личните податоци во електронскиот комуникациски сектор. Директивата, позната и како Директива за е-приватност, воспоставува правила за безбедност при обработката на личните податоци, за известување при повреда на личните податоци, како и за доверливост на телекомуникациите и сообраќајот на податоците.

Давателите на електронските комуникациски услуги треба да преземат соодветни технички и организациски мерки за:

- да обезбедат само овластени лица да имаат пристап до личните податоци;
- да ги заштитат личните податоци од уништување, губење или случајна измена и од кој било друг незаконски или неовластен облик на обработка;
- да обезбедат примена на политика за безбедност при обработката на личните податоци.

Давателот на услугите може да ги користи податоците за сообраќајот и податоците за локацијата на лицата што комуницираат (метаподатоците) само за цели на наплата и за техничко овозможување на услугата. Кога метаподатоците повеќе не се потребни за овие намени, тие мора да се избришат или да се анонимизираат.

Во случај на посебен ризик од нарушување на безбедноста на мрежата, давателот на електронски комуникациски услуги мора да ги информира претплатниците и ако ризикот е надвор од опфатот на безбедносните мерки што треба да се преземат од страна на давателот на услугата, треба да им ги посочи на корисниците сите можни решенија и мерки за заштита што можат да ги преземат. Давателот на електронските комуникациски услуги е обврзан да преземе итни и соодветни мерки за справување со нови, непредвидени безбедносни ризици и да го врати вообичаеното ниво на безбедност на услугата.

Кога ќе настане повреда на личните податоци како резултат на неовластен пристап, загуба или уништување на податоците, давателот на електронските комуникациски услуги веднаш мора да го информира надлежниот надзорен орган. Претплатниците мора да се информираат ако е веројатно дека нивните лични податоци или приватноста ќе бидат загрозени како последица на повредата на податоците.[24]

Според Директивата за е-приватност, државите членки мора да обезбедат доверливост на комуникациите преку јавните комуникациски мрежи, а особено:

- да забранат слушање, прислушување, зачувување или кој било вид на следење или пресретнување на комуникациите или на податоците за телекомуникацискиот сообраќај без согласност од корисниците на услуги, освен кога постои законско овластување;
- да гарантираат дека зачувувањето на податоците, или пристапот до податоци зачувани на личната опрема на корисникот е можна само со јасно и целосно информирање на корисникот за намените и му е дадено право да одбие.

Какви било ограничувања на правата и обврските обработени во Директивата мора да бидат оправдани како неопходни, соодветни и пропорционални во едно демократско општество и да служат за конкретни цели на јавниот ред, како националната безбедност, одбраната, јавната безбедност или превенцијата, истражувањето и гонењето на сериозен криминал.

[24] Член 13 од изменетата Директива.

Во 2017 година, Европската комисија објави **нацрт-регулатива за е-приватност**[25] којашто треба да ја замени постојната директива за е-приватност и да биде *lex specialis* со специфични правила за приватност при електронските комуникации, преовладувајќи над општите акти во областа во случај на неконзистентност. Преминот од директива кон регулатива е со цел да се хармонизира законодавството за заштита на приватноста во ЕУ. Регулативата за е-приватност ќе биде директно применлива и законски обврзувачка во сите членки на ЕУ, за разлика од Директивата за е-приватност за која беа потребни национални прописи за спроведување, што, пак, за последица имаше неконзистентна примена.

Текстот на нацрт-регулативата предвидува дека се гарантира приватноста на содржината на комуникациите и на метаподатоците, како за физичките, така и за правните лица. Се забранува следење на комуникациите и метаподатоците, освен во случаите каде што тоа е дозволено со националното законодавство – на пример при кривични истраги. Анализа на содржината на комуникациите и метаподатоците е дозволена само со согласност на корисникот (во случај ако сака да добие специфични услуги за коишто е тоа неопходно), или со согласност на сите учесници во комуникацијата, како и во други случаи утврдени со закон. Обработка на метаподатоците што се собрани за целите на фактурирање од страна на давателите на услугите е дозволена за таа намена, но со ограничување дека релевантните метаподатоци не може да се чуваат подолго од периодот во кој законски може да се оспори сметката, или може да се изврши наплата.

Спроведувањето на правилата за доверливост на електронските комуникации ќе биде одговорност на националните органи за заштита на личните податоци. Првично, целта беше регулативата да влезе во сила во мај 2018 г., но регулативата сè уште не е донесена, па се очекува и подоцнежен датум на стапување во сила.

Откритијата на Сноуден беа пресвртница во дискусиите за реформата на заштитата на податоците во ЕУ, нагласувајќи ја потребата за силна правна рамка која ќе ги отсликува новите технолошки можности за масовно следење на комуникациите. По четиригодишни преговори, во 2016 година, ЕУ усвои пакет што се состои од **Општа регулатива за заштита на податоците**[26] (ОРЗП) и **Директива 2016/680 за заштита на податоци во полицијата и кривичното право**[27] – којашто се однесува на заштита на податоците поврзани со кривични дела и кривични казни. ОРЗП ќе се применува од 25 мај 2018 година, а државите членки имаат време до 6 мај 2018 година да ја инкорпорираат т.н. Полициска директива во националното законодавство.

[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), достапно на: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2017:0010:FIN.

[26] Регулатива (ЕУ) 2016/679 на Европскиот парламент и на Советот за заштита на поединците во врска со обработката на личните податоци и слободното движење на такви податоци (Општа регулатива за заштита на податоците), OJ L 119, 27.04.2016, достапна на: 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, достапно на: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680

Значајно е што во дефиницијата на лични податоци во ОРЗП експлицитно се вклучени локациските податоци, како и онлајн идентификаторите, како вид метаподатоци. Проширена е дефиницијата за *осетливи лични податоци* и таа сега го опфаќа следново: етничкото или расното потекло, политичките мислења, религиозните или филозофските верувања, членувањето во синдикати, податоците за здравјето, сексуалниот живот или ориентација, генетските и биометриските податоци. Осетливите податоци подлежат на посебни услови што треба да се исполнат за да биде дозволена нивна обработка. Податоците за *осуди за кривични дела* може да се обработуваат и за нив да се води соодветен регистар само од страна на националните власти.

Битно е што ОРЗП воведува законски услов за дизајн насочен кон приватност, т.е. техничките и организациските мерки што обезбедуваат заштита на личните податоци треба да се предвидат уште при дизајнот на системите, а не отпосле.

Кога ќе настане повреда на личните податоци како резултат на неовластен пристап, загуба или уништување на податоците, контролорот на податоците мора да го информира надлежниот надзорен орган, и веднаш да ги информира лицата на кои се однесуваат податоците доколку е извесно дека прекршувањето ќе резултира со „голем ризик по нивните права и слободи“.[28]

ОРЗП го прокламира принципот на минимизација на податоците, т.е. обработка само на податоците што се неопходни за извршување на должностите, како ограничување на пристапот до личните податоци на оние кои треба да ја спроведат обработката.

Членот 17 од ОРЗП го обезбедува „правото на заборавање“. Ако тоа го побара лицето на кое се однесуваат личните податоци, истите мора да се избришат без одлагање доколку не се повеќе потребни за намената за којашто биле прибрани и обработени, или лицето ја повлекло согласноста врз основа на којашто се обработени личните податоци, а притоа не постои друга законска основа за нивното обработување, или, пак, доколку се незаконски обработени.

Означувајќи јасен чекор напред во заштитата на основните права, и ОРЗП и Директивата 2016/680 вклучуваат повеќе заштитни мерки за личните податоци. Регулативата и директивата овозможуваат силен надзор од независни национални органи за заштита на податоците коишто можат да примаат приговори и да доделуваат компензација на субјектите на податоците. Понатаму, треба да се истакне пропишувањето на правото на ефективен судски лек против процесорот или контролорот на податоците, и правото на компензација за лицето што претрпело материјална или нематеријална штета како резултат на незаконска обработка на личните податоци.[29] Директивата им дава право на непрофитните организации што дејствуваат во интерес на поединците да поднесуваат жалби и да ги застапуваат засегнатите лица.[30] Слично како во ОРЗП, и Директивата воведува обврска за известување на луѓето во случај на повреда на личните податоци.

И покрај ваквите сличности, институциите на ЕУ ја издвојуваат сферата на полицијата и кривичната правда поради нејзините специфичности, па токму затоа за неа е донесена посебна директива за обработка на податоците за превенција,

[28] Членови 31 и 31.
[29] Член 56.
[30] Членови 52–55.

истражување, детекција или гонење на кривични дела или извршување кривични казни (**Директивата 2016/680**). Изборот во оваа сфера да се донесе директива наспроти регулативата за заштита на податоците во останатите сфери може да се објасни со фактот што директивата ќе им даде на членките на ЕУ поголема флексибилност при нејзиното вградување во националното законодавство, додека општата регулатива за заштита на личните податоци (ОРЗП) ќе се применува директно.

Постојат и други разлики меѓу двата правни акта. На пример, Директивата не ги наведува сите карактеристики коишто според ОРЗП треба да ги имаат податоците за нивната обработка да се смета за законита и фер. Оттука, не е потребна согласност од субјектот на податоците кога надлежните органи им наредуваат на физичките лица со цел превенирање, истражување, детектирање или гонење кривични дела. Исто така, Директивата 2016/680 ги ограничува правата на информирање на субјектите на податоците, нивно пристапување до собраните податоци, како и исправање на пропустите во собраните податоци. Најмалку, следните информации мора да се достапни до лицето чии лични податоци се собрани: идентитетот на контролорот, постоењето на операцијата за собирање, како и целта на операцијата, правото да поднесе жалба и правото да побара пристап до собраните податоци, но и да побара замрзнување и рестрикција на понатамошно обработување. Сепак, членките на ЕУ можат да го ограничат ваквото право на информирање со цел да се избегне попречување или прејудицирање на истрагите, како и заради заштита на националната или јавната безбедност.[31]

Директивата 2016/680 нема да се применува во судските кривични постапки, односно во тие случаи членките на ЕУ можат да го применат националното законодавство во поглед на правото на информација, пристап до податоците и исправање или бришење на личните податоци.[32] Директивата исто така нема да се применува во сферите што се надвор од доменот на правото на ЕУ – како што е националната безбедност[33] – ниту, пак, при обработката на податоци од институциите, телата и агенциите на ЕУ.

Според Директивата 2016/680, личните податоци треба да бидат прибирани за специфична, експлицитна и легитимна цел и не смее да бидат обработени надвор од дозволените начини. Доколку собраните лични податоци се обработуваат од истиот или од друг орган за цел различна од таа за која првично се собрани, тоа мора да биде одобрено во рамките на законските ограничувања. Собраните лични податоци се чуваат во облик што овозможува идентификување на субјектите на податоците, не подолго од она што е неопходно од целта заради којашто се обработени.[34] Членките на ЕУ треба да утврдат временски ограничувања за чувањето на ваквите податоци или за периодично преиспитување на потребата од нивно чување.[35] Ограничувањето на прибирањето на податоци само на она што е директно потребно и релевантно за конкретна намена, како и нивното задржување само онолку колку што е потребно за таа намена го изразува во пракса *принципот на минимизирање на податоците*. Како една од техничките и организациските мерки за примена на принципот за минимизирање податоци, што ги посочува директивата, е

[31] Членови 13, 15 и 16.
[32] Член 18; рецитали 20, 49 и 107.
[33] Член 2, став 3; рецитал 14.
[34] Член 4, став 1.
[35] Член 5.

„псевдоанонимизацијата“.[36] Тоа подразбира обработка на податоците на начин каде што личните податоци повеќе не можат да се припишат на конкретно лице без употреба на дополнителни информации што се чуваат одделно и се предмет на технички и организациски безбедносни мерки.

Обработката мора да се врши на безбеден начин, што овозможува заштита од неовластено или незаконско обработување, како и од случајно губење, уништување или оштетување. За оваа цел, во членот 29 од директивата се утврдени низа мерки за безбедност при обработката на податоците, и тоа:

- спречување пристап на неовластени лица до опремата за обработка на податоците („контрола на пристапот до опремата“);
- спречување на неовластено читање, копирање, модификација или отстранување на носачите на податоците („контрола на носачите на податоците“);
- спречување на неовластено внесување лични податоци и неовластено прегледување, модификација или бришење на складирани лични податоци („контрола на складирање“);
- спречување на употреба на автоматизираните системи за обработка на податоците од страна на неовластени лица преку комуникациска опрема („контрола на корисници“);
- обезбедување лицата овластени да користат систем за автоматска обработка на податоците да имаат пристап само до личните податоци опфатени со нивното овластување за пристап („контрола на пристап до податоци“);
- обезбедување дека е можно да се проверат и да се утврдат телата на коишто личните податоци се пренесени или ставени на располагање со користење на опрема за комуникација со податоците („контрола на комуникација“);
- обезбедување дека подоцна е можно да се потврди и да се утврди кои лични податоци се внесени во системите за автоматска обработка, како и кога и од кого личните податоци биле внесени („контрола на внесување“);
- спречување неовластеното читање, копирање, менување или бришење лични податоци за време на пренос на личните податоци или за време на транспортот на носачите на податоците („контрола на транспорт“);
- обезбедување дека инсталираните системи можат, во случај на прекин, да бидат обновени („обновување“);
- обезбедување дека функционира системот, а грешките во функциите се пријавуваат („веродостојност“) и дека складираните лични податоци не можат да бидат оштетени со дефект на системот („интегритет“).

Членот 27 од Директивата ги задолжува контролорите да спроведат *проценка на влијанието врз заштитата на податоците*, кога одреден облик на обработка, особено што користи нови технологии, е веројатно дека ќе резултира со висок ризик врз правата и слободите на физичките лица. Проценката треба да ги утврди ризиците, заштитните механизми и безбедносните мерки.

Лицата треба да бидат информирани без одлагање за собраните лични податоци кои подлежат на висок ризик од загрозување на правата и слободите на лицата, со цел тие навреме да можат да преземат соодветни мерки.

[36] Член 20.

Според Директивата, контролорите треба да имаат назначено *службеник за заштита на податоците*, кој треба да ги информира контролорите за законските обврски и да го следи нивното спроведување.

Секоја земја членка на ЕУ треба да воспостави *независен надзорен орган* на својата територија, задолжен за следење на примената на правото за заштита на податоците согласно Директивата. Директивата дозволува оваа улога да ја извршува општиот орган за правото за заштита на податоците. Овој орган треба да ја надгледува и поттикнува практичната примена на директивата, да промовира подигнување на јавната свест и разбирање на ризиците, правилата, начините на заштита, да ги советува во согласност со правото на ЕУ националниот парламент, владата и другите институции што имаат врска со собирањето и процесирањето на личните податоци. Директивата им овозможува на надзорните органи за заштита на податоците во оваа сфера да имаат корективна моќ во однос на контролорите и обработувачите на податоците, со тоа што можат да изречат времено или трајно ограничување, вклучително и забрана на обработка на податоците. На надзорните органи исто така им е доверена задача да примаат приговори од поединци за употребата на нивните лични податоци, како и да спроведат неопходни истраги.

Задржување метаподатоци

Во 2006 година беше донесена **Директивата 2006/24/ЕЗ за задржување податоци** создадени или обработени во врска со давањето јавно достапни услуги за електронски комуникации или јавни комуникациски мрежи. Оваа директива, попозната како Директива за задржување податоци,[37] беше создадена со цел да овозможи метаподатоците да бидат достапни за истрага, препознавање и гонење на сериозни кривични дела, дефинирани од секоја држава членка во националното законодавство. Под метаподатоци се вбројуваат следните податоци за корисниците на телефонски и интернет услуги (вклучително и е-пошта): името, адресата на повикувачот и повиканиот, телефонскиот број/ИП адресата, телефонскиот уред и локацијата на лицата кои комуницираат; времето на почетокот и крајот на комуникацијата; типот на телефонската/интернет услуга.

Поранешниот германски пратеник Малт Шпиц со анализа на метаподатоците кои „Дојче Телеком“ ги задржувал за него, дошол до заклучокот дека ја посочуваат неговата локација 78% од времето.

Со анализа на комуникациските метаподатоци на одредено лице, може да се дознае повеќе одошто со физичко следење на истото лице. На пример, податокот дека одредено лице испратило СМС порака до адвокат за семејно право, проследено со телефонски повици до агенции за недвижности, можат да укажат на неминовен развод на брак. Метаподатоците се генерираат и без луѓето да бидат свесни за тоа,

[37] Data Retention Directive.

односно без да преземат некаква комуникациска активност. На пример, апликациите за електронска пошта на паметните телефони контактираат со т.н. базни станици на мобилните оператори во многу куси временски интервали, со што постојано се генерира податок за локацијата каде се наоѓа мобилниот телефон и во која насока се движи. Со анализа на метаподатоците е возможно да се извлечат прецизни заклучоци за приватните животи на луѓето, како што се нивните социјални врски, нивните навики, секојдневни активности, интереси и вкусови.[38]

ШТО ОТКРИВААТ ЗА НАС КОМУНИКАЦИСКИТЕ МЕТАПОДАТОЦИ?	
Со кого комуницираме	Имињата и адресите на лицата со кои комуницираме
Кога комуницираме	Почетокот и крајот на комуникациите, нивното времетраење и честотата на комуникациите
Како комуницираме	Типот на комуникацијата (пр. телефонски повик, СМС/ММС порака, интернет телефонија, мејл порака, интернет сурфање); типот на уред (пр. мобилен телефон)
Каде сме	Локацијата каде се наоѓа уредот од кој комуницираме

Директивата за задржување податоци воспостави критериуми кога правото на заштита на податоците е неприменливо, односно во случаите кога станува збор за национална безбедност, јавна сигурност, одбрана на територијата, превенција и истражување на криминални активности што ја загрозуваат безбедноста и економијата во една или повеќе земји членки на Унијата.

Директивата за задржување податоци бараше од давателите на јавно достапни електронски комуникациски услуги или јавни комуникациски мрежи да ги задржат податоците на сообраќајот и локацијата коишто припаѓаат на поединци или правни лица. Периодот на задржување требаше да трае минимум шест месеци, а најмногу две години.

Во 2011 година, Европската комисија подготви извештај за оценка на спроведувањето на Директивата 2006/24/ЕЗ за задржување податоци[39]. Според извештајот, Комисијата беше задоволна од примената на директивата и процени дека задржувањето податоци претставува вредна алатка за правосудните системи и спроведувањето на правото. Во однос на забелешките за времетраењето на задржувањето и на предизвиканите трошоци за операторите, извештајот нагласува дека Европската Унија треба да продолжи да поставува и да ги подобрува стандардите преку заеднички правила што ќе бидат валидни за потребите на сите засегнати страни.

Сепак, на 8 април 2014 г., Големиот судски совет на **Судот на правдата на Европската Унија (ЕСП)** ја поништи Директивата бр. 2006/24/ЕЗ. И покрај тоа што Судот оцени дека директивата спроведува легитимна цел во борбата против тешкиот криминал и во заштитата на националната безбедност, утврди дека Директивата ги прекршува правото на приватен живот и правото на заштита на личните податоци на

[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. Достапно на: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-606.011%2B01%2BDOC%2BPDF%2BV0%2F%2FEN

[39] Достапно на http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF

поединците, гарантирани со членовите 7 и 8 од Повелбата на Европската Унија за основните права. Овие права беа повредени поради тоа што директивата на државните органи им обезбедуваше неселективен и масовен пристап до личните податоци на граѓаните, што беше и главната причина за нејзиното поништување. [40] Истражувањето спроведено од Агенцијата на Европската Унија за основните права покажа дека сите уставни судови кои се занимавале со ова прашање оцениле дека националните системи за задржување метаподатоци се делумно или целосно неуставни.[41]

Случајот се појави пред ЕСП како прелиминарно прашање од Врховниот суд на Ирска и Уставниот суд на Австрија. Имено, националните судови, при решавањето случаи, имаат право да реферираат правни прашања до ЕСП. Притоа, ЕСП одлучува за валидноста на правниот акт на Европската Унија, или за толкување на договори или подзаконски акти, а одлуката за конкретниот случај е оставена на националните судови. Во случајов, Врховниот суд на Ирска требаше да го реши спорот помеѓу ирската компанија „Дигитал Рајтс Ирланд“ (*Digital Rights Ireland*) и ирските власти во врска со законитоста на националните мерки за задржување податоци од електронските комуникации. Од друга страна, до Уставниот суд на Австрија претходно имаше поднесено неколку тужби од страна на голем број лица кои бараа поништување на австрискиот телекомуникациски закон со кој се транспонира Директивата за задржување на податоци во националното законодавство. Уставниот суд на Австрија го прифати гледиштето дека задржувањето влијае на голем број лица, а задржувањето на нивните податоци на подолго време создава ризик дека органите на власт ќе имаат пристап до содржината на податоците и ќе ја прекршат нивната приватност. Уставниот суд на Австрија изрази загриженост за тоа дали Директивата за задржување на податоци може да ги постигне зацртаните цели без да ги прекрши принципите на заштита на приватноста и личните податоци.

При разгледувањето на широката категорија на податоци која беше предмет на задржување, ЕСП воочи дека таквите податоци можат да овозможат да се изведат многу прецизни заклучоци во врска со приватните животи на лицата чии податоци биле задржани, како што се секојдневните навики, трајните или привремените места на живеење, дневните или други движења, активностите што се извршуваат, социјалните врски на тие луѓе и социјалното опкружување. Судот воочи дека под такви околности, и покрај тоа што не е дозволено да се задржи содржината на комуникациите, туку само метаподатоците, можно е да се загрози слободата на изразување на претплатниците или регистрираните корисници на давателите на електронски комуникациски услуги. ЕСП заклучи дека задржувањето податоци со цел да се овозможи пристап од страна на надлежните државни органи претставува обработка на податоци и со тоа влијае на две основни права од Повелбата на Европската Унија за основните права: а) правото на приватен живот гарантирано со член 7, и б) заштита на личните податоци гарантирано со член 8.

При разгледувањето на прашањето за нарушување на правото на приватност и заштита на личните податоци, ЕСП заклучил:

- обврската на давателите на електронски комуникациски услуги „сама по себе претставува попречување на правата гарантирани со член 7 од Повелбата“

[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.

• пристапот на националните власти до податоците „претставува дополнително мешање во тоа основно право“, и

• задржувањето, исто така, го крши правото на заштита на личните податоци.

Член 52 од Повелбата бара дека какви било ограничувања на остварувањето на гарантираните права мора да бидат воведени со закон и мора да се почитува суштината на тие права. Сите ограничувања се предмет на тест на пропорционалност и може да се изречат само доколку се потребни, и ги исполнат целите од општ интерес дефинирани од страна на ЕУ или потребата за заштита на правата и слободите на другите.

Европскиот суд на правдата се осврна на основната цел на Директивата за задржување на податоци, којашто треба да им помогне на земјите членки на ЕУ во борбата против сериозниот криминал и да придонесе за одржување на јавната безбедност. Судот се согласи дека борбата против меѓународниот тероризам е цел од општ интерес, па оттука потврди дека задржувањето податоци е важна алатка за националните органи во извршувањето на борбата против сериозниот криминал. Врз основа на овие согледувања, Европскиот суд на правдата донесе заклучок дека задржувањето на податоци со цел да им даде можност на националните власти да им пристапат на таквите податоци за спречување и откривање на тешки кривични дела „навистина задоволува цел од општ интерес“.

ЕСП понатаму испитуваше дали мешањето од страна на националните власти било пропорционално на целта заради која се остварува. Во оваа смисла, во согласност со судската пракса, стандардите што треба да се исполнат е тоа да биде „соодветно“ и „неопходно“, со цел да се постигнат целите. Во однос на прашањето дали задржувањето на податоци била соодветна мерка за постигнување на целите на Директивата 2006/24/ЕЗ, Европскиот суд на правдата, уважувајќи дека средствата за електронска комуникација играат витална улога во откривањето кривични дела, а во исто време и потребата на националните органи да пристапат до податоците, потврди дека задржувањето метаподатоци е „важна алатка“ и „може да се смета дека е соодветна“ за да се постигнат целите на Директивата.

Што се однесува до тестот за неопходност, и дали мешањето е ограничено само на она што е неопходно, судот даде три значајни забелешки: а) Директивата предвидува задржување на сите податоци од телекомуникацискиот сообраќај, генерирани од широк спектар на електронски начини на комуникација, вклучувајќи ги и фиксна телефонија, мобилна телефонија, интернет пристап, електронска пошта и интернет телефонија; б) опсегот на Директивата се однесува на сите претплатници и регистрирани корисници на услугите за електронска комуникација; и в) Директивата ги нарушува основните права на сите граѓани на Европската Унија. Судот констатираше дека задржувањето метаподатоци влијае не само на лица чии податоци можат да придонесат за поведување на судска постапка, туку и на оние за кои не постои трага на докази кои покажуваат дека нивното однесување може да биде поврзано со сериозен криминал. Исто така, беше забележано дека никој не е ослободен од ова правило; тоа важи дури и за оние чии комуникации се предмет на службена тајна, во согласност со националните правила. Во понатамошната дискусија за Директивата, ЕСП забележа отсуство на каква било поврзаност меѓу задржаните податоци и закана за јавната безбедност. Судот исто така истакна дека задржувањето не е ограничено само на метаподатоци на лица поврзани со одреден временски период, или на одредена

географска зона, или на група на лица кои би можеле да имаат поврзаност со сериозно кривично дело.

Покрај тоа, ЕСП разгледа дали Директивата ги содржи сите општи ограничувања на правото на националните власти за пристап до задржаните метаподатоци. Во овој поглед, ЕСП забележа недостаток на општи граници. Оттука, судот констатираше дека Директивата: а) не воспоставила ниту материјални, ниту процедурални ограничувања за пристап на надлежните државни органи до задржаните податоци, б) не го условила пристапот на националните власти до метаподатоците условено со претходна контрола извршена од страна на суд или друг независен административен орган би го ограничил пристапот до податоците и нивната употреба на она што е апсолутно неопходно, и в) не бара од земјите членки да воспостават такви ограничувања. Што се однесува до периодот на задржување, којшто трае од шест месеци до две години, ЕСП истакна дека Директивата не утврдува никакви објективни критериуми за да се утврди соодветен период на задржување „на она што е неопходно".

Врз основа на овие елементи, Судот оцени дека Директивата не воспоставила јасни и прецизни правила со коишто се регулира „степенот на мешање со основните права од член 7 и 8 од Повелбата". Затоа, беше заклучено дека Директивата „вклучува широко и особено сериозно мешање во тие основни права во правниот поредок на ЕУ, без таквото мешање да биде ограничено со одредби што ќе обезбедат дека е сведено само на она што е строго неопходно".

Во однос на безбедноста и заштитата на податоците што се задржани, ЕСП утврди дека Директивата 2006/24/ЕЗ не содржи доволно заштитни мерки, во согласност со член 8 од Повелбата, за да се обезбеди ефикасна заштита на задржаните податоци во однос на ризикот од злоупотреба и против кој било незаконски пристап и користење на податоците. Според членот 8 од Повелбата, меѓу другото, потребна е согласност на субјектот на податоците за обработка на неговите лични податоци. Судот констатираше дека Директивата 2006/24/ЕЗ не содржи правила за регулирање на заштитата и сигурноста на податоците на јасен и прецизен начин коишто соодветствуваат на: а) огромната количина на податоци чиешто задржување се бара со таа директива; б) чувствителната природа на тие податоци; и в) ризикот од незаконски пристап до тие податоци. Исто така, не се утврдени посебни обврски на земјите членки да воспостават вакви правила.

Европскиот суд на правдата, исто така, сметаше дека безбедноста и заштитата на личните податоци не може да се гарантира целосно во отсуство на надзор од страна на независен орган за заштита на личните податоци, како што се бара со член 8 од Повелбата на Европската Унија за основните права. Оттука, ЕСП заклучил дека законодавните тела на ЕУ, со усвојување на Директивата 2006/24/ЕЗ, ги надминале границите наметнати од страна на принципот на пропорционалност во однос на членовите 7, 8 и 52 од Повелбата. Како резултат на тоа, Директивата беше поништена.

Задржувањето податоци во ЕУ по поништувањето на Директивата 2006/24/ЕЗ

По поништувањето на Директивата 2006/24/ЕЗ во 2014 година од страна на Европскиот суд на правдата, Европската комисија се изјасни дека нема да работи на подготовка на нова Директива која би ја заменила поништената.[42] Европската Унија им

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

сугерираше на државите членки и релевантните европски институции да подготват соодветни измени во согласност со пресудата којашто поставува нов стандард за националните законодавства за задржување податоци[43]. При креирањето на новите регулативи, мора да се води сметка истите да бидат во согласност и со правата на приватност и заштита на лични податоци нагласени во член 15 од Директивата 2002/58/ЕЗ за е-приватност, како и со општите начела содржани во Повелбата на Европската Унија за основните права.

Во својот годишен извештај од 2017 година, Агенцијата на Европската Унија за основните права посочува дека членките на ЕУ во рамките на националното законодавство треба да избегнуваат општо и недискриминирано задржување податоци од страна на телекомуникациските оператори. Националното законодавство треба да вклучува строги проверки на пропорционалноста, како и соодветни процедурални заштитни мерки за ефективно гарантирање на правата за приватност и заштитата на личните податоци.

Европскиот супервизор за заштита на податоци (ЕСЗП) и Работната група за член 29[44] ја нагласија потребата да се избегне барањето за задржување на податоци во новата законска рамка за е-приватност, во согласност со одлуката на ЕСП.[45]

И покрај тоа што одлуката на ЕСП доведе до тоа неколку држави подетално да го разгледаат проблемот со задржувањето податоци, сепак немаше широко распространето повлекување на воспоставените системи за задржување податоци ширум Европа. Повеќето држави се обидоа на своја рака да балансираат меѓу одлуката на ЕСП и потребата за задржување на податоците за цели поврзани со државната безбедност и ефикасното гонење на криминални групи. Подолу се претставени неколку случаи од држави членки на ЕУ во однос на преземените дејствија по укинувањето на Директивата за задржување податоци, заедно со краток преглед на законските одредби за следење на содржината на комуникации и достапни статистики за следењето.

Сојузна Република Германија

Уште пред укинувањето на Директивата за задржување податоци во 2014 година, Федералниот уставен суд на Германија во 2010 година го прогласи за неважечки[46] актот за имплементација со кој беше транспонирана Директивата 2006/24/ЕЗ во националното право. Сепак, ваквата одлука беше донесена врз основа на тоа што оваа Директива не е во согласност со правата на тајност на комуникациите и информациска самоопределба, со тоа што нејзината имплементација не беше прогласена за

[43] Став на ЕУ во однос на пресудата на ЕСП за поништување на Директивата: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp220_en.pdf

[44] Скратено име за Работната група за заштита на податоци, која е воспоставена согласно членот 29 на Директивата 95/46/ЕЗ. Групата дава независни совети на Европската комисија и помага во развивањето хармонизирани политики за заштита на податоци.

[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.

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

неуставна. Во 2015 година, Министерот за правда предложи нов закон кој беше донесен со цел да се постигне компромис меѓу прашањата од државна безбедност и прекршувањето на граѓанските слободи и права. Согласно овој Закон, усвоен со големо мнозинство во Бундестагот, времетраењето на задржувањето на податоците се скрати од 6 месеци на 10 седмици, се исклучи од задржување целиот сообраќај по електронска пошта, а беше прокламирана потребата за обезбедување судски налог за предавање на задржаните податоци на државните органи. Дополнително, новите законски одредби посветуваат значително внимание на безбедноста, преку обврска за енкрипција и создавање записи за пристап до фајлови, како и овластување од минимум две овластени лица за технички пристап до податоците.

Во однос на следењето на содржината на комуникациите, во 2016 година од „Дојче Телеком“ бил обезбеден пристап до 44.238 линии[47] на барање на државните органи. Сепак, во извештајот се наведува дека операторите во Германија се должни да достават специфични податоци до Сојузната разузнавачка служба (БНД), но опсегот и бројот на вакви доставени податоци не се објавува.

Република Австрија

Австрискиот Уставен суд беше првиот национален суд кој прогласи за неважечки голем дел од Законот за задржување податоци по донесената одлука од ЕСП. Австриските оператори повеќе немаат обврска да ги задржуваат податоците и да ги доставуваат до националните власти. Сепак, на операторите им е дозволено да задржуваат податоци за сообраќајот за нивни легитимни цели, како што се фактурирање, превенција од измами и сл. Дополнително, овие податоци повторно се оставаат да бидат достапни и за јавните власти кога постојат сигурносни ризици и закани по државната безбедност.

Во Австрија, во 2016 година, од страна на „Т-мобајл Австрија“ била обезбедена содржината на разговорите од вкупно 2.183 линии[48], на барање на надлежните органи.

Република Естонија

Законодавството во Естонија коешто ги регулира заштита на приватноста и личните податоци е целосно усогласено со европските директиви во оваа сфера. Делот од Законот за електронски комуникации[49] што се однесува на задржувањето податоци се заснова на Директивата 2006/24/ЕЗ. По укинувањето на оваа директива не се направени никакви измени во законските решенија, со што операторите се должни да ги чуваат метаподатоците во рок од една година. Естонскиот инспекторат за заштита на податоци има објавено неколку водичи во коишто се претставуваат правата на граѓаните и обврските на операторите и надлежните државни органи во однос на

[47] Извештај за транспарентност на „Дојче Телеком“ за Германија. Достапен на: https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/news/germany-363566
[48] Извештај за транспарентност на „Дојче Телеком“ за Австрија. Достапен на: https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/news/austria-363540
[49] Закон за електронски комуникации на Естонија. Достапен на: https://www.riigiteataja.ee/en/eli/501042015003/consolide

надзорот и следењето на комуникациите и задржувањето податоци, но сепак овие водичи не се задолжителни.

Република Литванија

Во Законот за електронски комуникации на Литванија е транспонирана Директивата 2006/24/ЕЗ, а задржувањето на податоците се врши во најкраткиот предвиден период со поништената директива – шест месеци. Режимот на задржување податоци се однесува и на телекомуникациски и на интернет сообраќај. Во 2015 година се започнати одредени консултации во врска со потребата од промени во оваа област, но сепак, иако беа направени одредени амандмани на надлежниот закон, немаше промени во однос на задржувањето податоци. Согласно Кривичниот законик на Литванија, задржаните податоци се користат стриктно за истражување, препознавање и гонење сериозен криминал.

Република Ирска

Долго пред донесувањето на Директивата за задржување податоци во 2006 година, Ирска имаше воспоставено систем за задржување метаподатоци во времетраење од 7 години. Ваквото задржување било спроведувано без никаков надзор и контрола врз работењето на операторите. Овие одредби беа променети со усвојувањето на Директивата 2006/24/ЕЗ, со која се воведе максималниот период на задржување податоци од две години за телекомуникации и една година за интернет комуникации. Организацијата „Дигитал Рајтс Ирланд“ (*DRI*) [50] започна постапка за да се утврди уставноста на законот пред Европскиот суд на правдата. Во 2014 година, Судот пресуди дека Директивата, којашто е основа на ирското право во оваа област, ги повредува правата на граѓаните на ЕУ гарантирани во Повелбата на Унијата за основите права.

Дополнително, Врховниот суд на Ирска го покрена прашањето дали поништувањето на Директивата ги прави доказите собрани со задржување податоци недозволени. Сепак, националните власти немаат пристапено кон промена на законодавството. „Дигитал Рајтс Ирланд“ има започнато и постапка пред Уставниот суд на Ирска во однос на националниот закон за која сè уште се чека пресуда.

Република Чешка

Во Чешка, Законот за електронски комуникации пропишуваше задржување на метаподатоците во времетраење од 6 до 12 месеци. Но, Уставниот суд на Чешка во 2011 година го прогласи законот за неуставен, со образложение дека го повредува правото на приватност на граѓаните. Во јули 2012 година, беа усвоени измени на Законот за електронски комуникации со што се зацврстија техничките и организациските мерки за заштита на податоците за сообраќај и локација. Понатаму,

[50] Организацијата е посветена на одбрана на човековите права во дигиталната ера. https://www.digitalrights.ie/

безбедносните и разузнавачките служби можат да побараат пристап до метаподатоците под определени услови, единствено со дозвола од судија на Уставниот суд.

Во 2016 година, „Т-мобајл Чешка“ обезбедил пристап на надлежните државни органи до вкупно 8.492 линии.[51] Ваквиот пристап е обезбеден согласно Законот за електронски комуникации којшто ги дефинира условите за легално следење на комуникациите и задржувањето податоци.

Република Хрватска

Хрватскиот Закон за електронски комуникации[52] во член 109 одредува дека операторите имаат обврска да ги задржуваат метаподатоците во времетраење од една година. Како причини за задржувањето податоци се наведуваат: а) потребата за спроведување истраги, откривање, гонење и казнување на сериозни криминалци; и б) потребата за заштита и одбрана и зачувување на националната безбедност. И по поништувањето на Директивата за задржување податоци, законот остана на сила во Хрватска. Иако беа иницирани истражувања и анализи на состојбата од страна на Хрватската регулаторна агенција за мрежни дејности и Агенцијата за заштита на лични податоци, сепак задржувањето податоци ќе продолжи сè додека не бидат донесени законските измени.

Во Извештајот за транспарентност за 2016 година, „Хрватски Телеком“ наведува дека нема достапни информации за бројот на следени линии поради тоа што државните власти имаат директен пристап до содржината на комуникациите. Понатаму, се појаснува дека согласно законските одредби, операторите мора да обезбедат постојан и директен пристап до техничката опрема за следење на комуникациите, со што „Хрватски Телеком“ нема никакви податоци во однос на бројот на пресретнати линии.

Во однос на надзорот над работата на безбедносно - информативните агенции, Хрватска има воведено повеќестепен систем со цел да се спречат можните злоупотреби кои се возможни со следењето на комуникациите на граѓаните. Имено, хрватскиот Сабор, покрај Одборот за национална сигурност којшто е во негов состав, има формирано и Совет за граѓански надзор над безбедносно - информативните агенции. Членовите на Советот ги избира Саборот од редот на универзитетските професори од областа на безбедноста, правото, безбедноста на ИКТ системите, претставниците на граѓанските организации, адвокатите и експертите од областа.

[51] Извештај за транспарентност на „Дојче Телеком“ за Република Чешка. Достапен на: https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/news/czech-republic-363568

[52] Закон за електронски комуникации на Хрватска. Достапен на: https://www.zakon.hr/z/182/Zakon-o-elektroni%C4%8Dkim-komunikacijama

Анализа на правната рамка за заштита на приватноста и личните податоци при електронските комуникации во Македонија

Заштитата на приватноста и личните податоци при електронските комуникации во Македонија е регулирана со Уставот, Законот за заштита на личните податоци и Законот за електронските комуникации. Подолу е направен краток осврт на секој од овие правни акти.

Уставот на Република Македонија во член 17 ја гарантира слободата и неповредливоста на писмата и на сите други облици на комуникација. Само врз основа на одлука на суд, под услови и во постапка утврдена со закон, може да се отстапи од правото на неповредливост на писмата и на сите други облици на комуникација, ако тоа е неопходно заради спречување или откривање кривични дела, заради водење кривична постапка, како и заради безбедноста и одбраната на Републиката. Законот се донесува со двотретинско мнозинство гласови од вкупниот број пратеници. Членот 18 ги гарантира сигурноста и тајноста на личните податоци. На граѓаните им се гарантира заштита од повреда на личниот интегритет што произлегува од регистрирањето на информации за нив преку обработка на податоците.

Првиот **Закон за заштита на личните податоци**[53] во духот на Конвенцијата на Советот на Европа 108/81 и Директивата 95/46/ЕЗ е донесен во 2005 година. Законот за заштита на личните податоци ја уредува заштитата на личните податоци како дел од основните слободи и права на физичките лица, а особено правото на приватност. Овој закон се применува на целосно и делумно автоматизирана обработка на личните податоци и на друга обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел од збирка на лични податоци.

КЛУЧНИ ДЕФИНИЦИИ ОД ЗАКОНОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ	
личен податок	Секоја информација која се однесува на идентификувано физичко лице или физичко лице кое може да се идентификува
Обработка на личните податоци	Операција или збир на операции што се изведуваат врз лични податоци на автоматски или друг начин, како што е: собирање, евидентирање, организирање, чување, приспособување или промена, повлекување, консултирање, употреба, откривање преку пренесување, објавување или на друг начин правење достапни, изедначување, комбинирање, блокирање, бришење или уништување
Контролор на збирка на лични податоци	Физичко или правно лице, орган на државната власт или друго тело, кое ги утврдува целите и начинот на обработка на личните податоци
Корисник	Физичко или правно лице, орган на државната власт или друго тело на кое му се откриваат податоците

Заштитата на личните податоци му се гарантира на секое физичко лице, без дискриминација, вклучително и заснована врз државјанството. Како посебни категории на лични податоци коишто не смеат да се обработуваат, односно може да се обработуваат само под посебни услови во законот се утврдени: личните податоци што го откриваат расното или етничкото потекло, политичкото, верското, филозофското или друго уверување, членството во синдикална организација и податоците што се

[53] Закон за заштита на личните податоци, „Службен весник на Република Македонија“ бр.7/2005, 103/2008, 124/2010 и 135/2011.

однесуваат на здравјето на луѓето, вклучувајќи ги и генетските податоци, биометриските податоци или податоците што се однесуваат на сексуалниот живот. Ваквото дефинирање на осетливите податоци е во согласност со Општата регулатива на ЕУ за заштита на податоците.

Законот пропишува дека личните податоци се обработуваат правично и во согласност со закон; се собираат за конкретни, јасни и со закон утврдени цели и се обработуваат на начин што е во согласност со тие цели. Предвидено е и дека ќе се преземаат сите соодветни мерки за бришење или коригирање на личните податоци што се неточни или нецелосни, имајќи ги предвид целите заради коишто биле собрани или обработени. Исто така, законот предвидува чување на личните податоци не подолго од што е потребно да се исполнат целите поради коишто податоците се собрани за натамошна обработка. По истекот на рокот за чување, личните податоци може да се обработуваат само за историски, научни или статистички цели, со почитување на правото на заштита на приватноста, личниот и семејниот живот од нивна неовластена употреба и нивна анонимизација.

Законот за заштита на личните податоци пропишува дека обработката на личните податоци може да се врши: по претходно добиена согласност на субјектот на лични податоци; за извршување на договор во којшто субјектот на лични податоци е договорна страна; за исполнување на законска обврска; за заштита на животот или суштинските интереси на субјектот на лични податоци; за извршување на работи од јавен интерес или на службено овластување на контролорот или на трето лице на кое му се откриени податоците или за исполнување на легитимните интереси на контролорот, трето лице или лице на кое податоците му се откриени, освен ако слободите и правата на субјектот на лични податоци не преовладуваат над таквите интереси.

Законот за електронските комуникации (ЗЕК), [54] меѓу другото, има за цел да обезбеди заштита на правата на корисниците и доверливост на комуникациите.[55] За работите од областа на електронските комуникации, Законот ги определува како надлежни институции Министерството за информатичко општество и администрација и Агенцијата за електронски комуникации.

Законот ги обврзува операторите да преземаат соодветни технички и организациски мерки со цел соодветно да управуваат со ризиците за безбедноста на мрежите и услугите, особено за да се спречи и минимизира влијанието врз корисниците.[56] Во случај на нарушување на безбедноста на личните податоци, операторот е должен во рок од 24 часа да достави известување за нарушувањето до Агенцијата за електронските комуникации и Дирекцијата за заштита на личните податоци.[57] Ако нарушувањето на безбедноста на личните податоци може негативно да влијае на личните податоци или приватноста на претплатникот или на друго физичко лице, операторот е должен во рок од 24 часа за тоа да го извести односниот претплатник или физичкото лице освен ако Агенцијата не реши поинаку.[58]

[54] Закон за електронските комуникации, „Службен весник на Република Македонија“ број 39/2014, 188/2014 и 44/2015.
[55] Член 2 од Законот за електронските комуникации.
[56] Член 166 од Законот за електронските комуникации.
[57] Член 167 од Законот за електронските комуникации.
[58] Исто.

Законот ја регулира и доверливоста на комуникациите,[59] која се однесува на содржината на комуникациите, податоците за комуникациски сообраќај и податоците за локација и фактите и околностите за прекинот на конекцијата или за неуспешни обиди за воспоставување на конекција. Јасно се забранети сите форми на слушање, следење, чување, снимање, задржување или секој друг облик на пресретнување или надзор над комуникациите, без добиена согласност од корисниците за кои се работи. Исклучоците од ваквата забрана се однесуваат на примената на Законот за следење на комуникациите, задржувањето метаподатоци за претплатниците регулирано со Законот за електронските комуникации, техничкото чување податоци неопходно за пренос на комуникациите, како и снимањето на комуникациите и соодветните податоци за комуникациски сообраќај заради обезбедување доказ за комерцијални трансакции, но не подолго од законските рокови во коишто може да се оспори сметката или да се изврши плаќањето.[60]

Пристапот до податоците за комуникациски сообраќај, како еден вид метаподатоци, е дозволен само на овластени лица на операторот кои работат на пресметка на трошоците на претплатниците и трошоците за интерконекција, управување со комуникацискиот сообраќај, барања на потрошувачите, откривање измами, маркетинг или обезбедување услуги со додадена вредност.[61]

Податоците за локацијата на претплатниците или корисниците на електронски комуникациски услуги, како посебен вид метаподатоци, можат да се обработуваат од операторот само во случај кога се направени анонимни или врз основа на претходно добиена согласност од претплатникот или корисникот на услуги, во онаа мера и во времетраење потребно за обезбедување на услугите со додадена вредност.[62] Претплатникот или корисникот на услугите во секое време може да ја повлече својата дадена согласност за обработка на податоците за локација.[63]

Законот за електронските комуникации предвидува глоба во износ од 4% до 7% од вкупниот годишен приход на операторот на услугите за електронски комуникации, како и 1.500 до 3.000 евра за одговорното лице во операторот, доколку:[64]

- врши слушање, следење, чување, снимање, задржување или секој облик на пресретнување или надзор над комуникациите без добиена согласност од корисниците;
- чува информации или дава пристап до информации што се веќе зачувани во терминалната опрема на претплатникот или корисникот, спротивно на Законот;
- не ги избрише или не ги направи анонимни податоците за комуникациски сообраќај (освен кога се потребни за пренос на комуникациите и обезбедување доказ за комерцијални трансакции);
- обработува податоци за комуникациски сообраќај и локација спротивно на законот;
- дозволува пристап до обработката на податоците за комуникациски сообраќај и за локација на неовластени лица;
- податоците за комуникациски сообраќај не ги чува во Република Македонија;
- не ги почитува начелата за безбедност на задржаните метаподатоци;
- задржува податоци што ја откриваат содржината на комуникацијата.

[59] Член 168 од Законот за електронските комуникации.
[60] Исто.
[61] Исто.
[62] Член 171 од Законот за електронските комуникации.
[63] Исто.
[64] Член 181 од Законот за електронските комуникации.

Анализа на правната и институционална рамка за следење на комуникациите и задржување податоци во Македонија

Следењето на комуникациите и задржувањето метаподатоци при електронските комуникации во Македонија е регулирано со Законот за следење на комуникациите, Законот за кривичната постапка и Законот за електронските комуникации. Сите три закони и искуствата од нивната примена се анализирани паралелно, расчленети под неколку тематски поднаслови дадени во продолжение.

Дефинирање и опфат на следењето комуникации

Законот за следење на комуникациите[65] ги уредува условите и постапката за следење на комуникациите, начинот на постапување, чување и користење на податоците и доказите, како и контролата на законитоста на следењето на комуникациите.[66] Со овој закон, следењето комуникации е дефинирано како тајно дознавање и истовремено создавање технички запис на содржината на комуникациите, со можност да се репродуцира. Следењето може да ги опфати сите видови телефонски и други електронски комуникации како интернет протокол, говор преку интернет протокол, интернет страница и електронска пошта.[67] Вака дефинирано, следењето на комуникациите во Македонија ги опфаќа и комуникациите преку апликации за пренос на глас, видео и други содржини преку интернет (на пр. *Skype, Viber, Snapchat, WhatsApp, FaceTime*), но не го опфаќа увидот во метаподатоци за остварените електронски комуникации. Последново не е во согласност со Списокот за проверка на владеењето на правото на Венецијанската комисија, каде што е прецизирано дека и тајното собирање метаподатоци за електронските комуникации претставува следење на комуникациите.

Покрај содржината на разговорите и другите електронски комуникации, **Законот за кривичната постапка** дозволува пристап и до метаподатоците. Имено, како една од посебните истражни мерки е пропишан увидот во остварените телефонски и други електронски комуникации, што поради лошата формулација може да ги опфати и метаподатоците, но и содржината на ваквите комуникации. Ако оваа мерка треба да се однесува на метаподатоците, нејасно е каква е разликата во однос на членот 287 од истиот закон. Имено, во делот што ја регулира предистражната постапка, со овој член се определува дека на барање на јавниот обвинител, операторите на јавни комуникациски мрежи и давателите на јавни комуникациски услуги се должни да достават податоци за остварени контакти во комуникацискиот сообраќај за одредено лице.[68] Тоа претставува еден облик на метаподатоци.

[65] Закон за следење на комуникациите, „Службен весник на Република Македонија“ бр. 121/2006, 110/2008 и 116/2012.
[66] Член 1 од Законот за следење на комуникациите.
[67] Член 7 од Законот за следење на комуникациите.
[68] Член 287 од законот.

Основ за следење комуникации

Законот за следење на комуникациите дозволува следење на комуникациите за откривање и гонење на сторители на кривични дела, како и заради заштита на интересите на безбедноста и одбраната на земјата. Текстот под овој наслов се осврнува на следењето поврзано со сторителите на кривични дела, а следењето заради безбедноста и одбраната е обработено под посебен наслов подолу.

Следењето на комуникациите е утврдено како посебна истражна мерка во Законот за кривичната постапка.[69] Овие мерки се регулирани во глава XIX, каде што законот посочува дека може да се преземат посебни истражни мерки – меѓу кои е и следење и снимање на телефонските и другите електронски комуникации – кога е тоа неопходно за обезбедување на податоци и докази за водење на кривичната постапка, **коишто не можат да се соберат на друг начин**.

Со измените и дополнувањата на Законот за следење на комуникациите во 2012 г. се избриша одредбата што потесно дефинираше, заради спречување и гонење на кои кривични дела, може да се следат комуникациите.[70] Сепак, такви одредби постојат во Законот за кривичната постапка. Според овој закон, следењето комуникации може да се пропише како посебна истражна мерка во случаи во кои се сторени, се преземаат дејствија за извршување или се подготвуваат:[71]

- кривични дела за кои е пропишана казна затвор од најмалку четири години, а се подготвуваат, во тек е извршување или се извршени од страна на организирана група, банда или друго злосторничко здружение;
- кривични дела против државата и кривични дела против човечноста и меѓународното право;
- низа други тешки кривични дела, од убиство па сè до тероризам и финансирање тероризам.

Наредбата може да се однесува и спрема лице кое прима или проследува пратки од осомничениот или осомниченият користи негово комуникациско средство.[72]

Ако се споредат овие основи со избришаната одредба од Законот за следење на комуникациите, може да се заклучи дека се проширени основите за следење на комуникациите со следниве кривични дела:

- прикажување порнографски материјал на дете;
- грабнување (претходно било опфатено само грабнување малолетно лице);
- намамување на обљуба или друго полово дејствие на дете кое не наполнило 14 години;
- оштетување и неовластено навлегување во компјутерски систем (член 251, ставови 4 и 6 од Кривичниот законик; претходно било опфатено само доколку делото е сторено преку средства за електронска комуникација);
- злоупотреба на постапката за стечај;

[69] Закон за кривичната постапка, „Службен весник на Република Македонија" број 150/2010, 100/2012 и 142/2016.
[70] Беше избришан членот 8 од законот.
[71] Членови 253 и 255 од Законот за кривичната постапка.
[72] Член 255 од Законот за кривичната постапка.

- изнесување во странство на добра под привремена заштита или културно наследство или природни реткости (член 266, став 1 од Кривичниот законик; претходно се однесувало само за значајно добро или добро од особено значење за Република Македонија);
- отуѓување културно наследство од особено значење во државна сопственост.

Останува впечатокот дека е доста широк опфатот на кривични дела за кои се дозволува употреба на следењето комуникации. Според релевантна препорака на Советот на Европа, посебните истражни мерки треба да се наменети за откривање и истражување тежок криминал.[73] Според конвенција на Обединетите нации, тежок криминал е оној што според националното законодавство е казнив со затворска казна од 4 или повеќе години.[74] Сепак, меѓу гореспоменатите кривични дела за кои со законски измени е овозможено следење на комуникациите, има и такви за кои минималната пропишана казна е шест месеци затвор, а речиси во сите наведени случаи е под четири години затвор. Оттука, **потребно е да се преиспита оправданоста да се дозволува употребата на оваа инвазивна мерка за толку широк опсег на кривични дела** врз основа на анализа дали нарушувањето на приватноста е пропорционално на тежината на кривичното дело за коешто станува збор и доказите што се очекува да се соберат со посебните истражни мерки, односно следењето комуникации.

Барање за следење комуникации

Текстот под овој наслов се однесува на следењето на комуникациите, поврзано со сторителите на кривични дела, а следењето заради безбедноста и одбраната е обработено под посебен наслов подолу.

Според член 9 од Законот, барање за следење на комуникациите за откривање и гонење сторители на кривични дела до надлежниот судија поднесува надлежниот јавен обвинител по сопствена иницијатива или на предлог на Министерството за внатрешни работи, Управата за финансиска полиција или Царинската управа. Писменото барање за следење на комуникациите се поднесува до судијата на претходната постапка и, меѓу другото, треба да содржи: назив на кривичното дело; лицето или предметите врз кои ќе се примени следењето комуникации (на пример, телефонски број или адреса на електронска пошта); техничките средства што ќе се применат; сознанијата и доказите врз основа на кои се засноваат основите на сомневање и образложение за причините поради кои податоците или доказите не можат да се соберат на друг начин; времетраењето на следењето на комуникациите, како и видот на телекомуникацискиот систем, телефонскиот број или друг податок за идентификација на телекомуникацискиот приклучок.[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, достапно на https://wcd.coe.int/ViewDoc.jsp?id=849269&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.

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

[75] Член 10 од Законот за следење на комуникациите.

Загрижува што **за следење на комуникациите е доволно да се наведе само основ за сомневање – а не основано сомневање** – за можно извршување или веќе извршено кривично дело што е многу низок степен на сомневање.[76]

Наредба за следење на комуникациите

Текстот под овој наслов се однесува на следењето на комуникациите поврзано со сторителите на кривични дела, а следењето заради безбедноста и одбраната е обработено под посебен наслов подолу.

Посебната истражна мерка „следење и снимање на телефонските и другите електронски комуникации“ по образложено барање на јавниот обвинител ја определува судијата на претходната постапка со писмена наредба. Мерката за увид во остварени телефонски и други електронски комуникации ја определува јавниот обвинител со писмена наредба.[77]

Според Законот за следење на комуникациите, судијата на претходната постапка треба да одлучи за применото барање за следење на комуникациите во рок од 48 часа.[78] Ваквиот рок е прилично краток, имајќи предвид дека постојат случаи во пракса кога барањето се однесува и на над 100 лица, а би требало да содржи соодветно образложени сознанија и докази за основите на сомневање. Кусиот рок што е даден за одлука на судијата може да се оправда единствено со постоење на случаи на итност, на пример, кога треба да се спречи кривично дело, да се документира неговото извршување, да се избегне бегство на можните сторители или уништувањето докази. Сепак, за итните случаи, законот во членот 11 пропишува можност да се врши следење на комуникациите времено, врз основа на усна наредба од судија, издадена на усно барање од надлежен јавен обвинител, а којашто е валидна во рок од 48 часа. Оттука, **загрижува дали пропишаниот рок од 48 часа е доволен за судијата да може соодветно да го проучи барањето** за следење на комуникациите и да одлучи дали ќе издаде соодветна наредба, а нелогично е што за барањето за продолжување на времетраењето на мерката е утврден рок од 72 часа – што е повеќе од времето утврдено за првичното одобрување на следењето комуникации. Дополнително, со измените на Законот за следење на комуникациите во 2012 г. се пропиша дека усна наредба може да се издаде во итни случаи кога постои „опасност од предизвикување ненадоместлива штета на кривичната постапка“. Старото законско решение беше многу попрецизно и порестриктивно, бидејќи пропишуваше дека усна наредба може да се издаде само кога постои опасност од:

- предизвикување смрт или тешка повреда;
- предизвикување материјална штета на имот од големи размери;
- бегство на сторител на кривично дело за што е пропишана казна доживотен затвор.

[76] Според Законот за кривичната постапка, основи на сомневање се сознанија кои врз основа на криминалистичкото знаење и искуство може да се оценат како доказ за сторено кривично дело, додека основано сомневање е повисок степен на сомневање заснован врз прибавените докази кои упатуваат на заклучок дека определено лице сторило кривично дело.

[77] Член 256 од Законот за кривичната постапка.

[78] Член 11 од Законот за следење на комуникациите.

Оттука, **потребно е да се прецизираат порестриктивно условите во коишто е дозволено следењето комуникации да се врши врз основа на усна наредба.**

Дополнително, **за да судијата донесе информирана одлука за оправданоста на барањето за следење на комуникациите, како и да процени дали се исполнети условите за нарушување на приватноста и личните податоци, неопходно е да се воведе уште една страна во постапката што ќе го застапува интересите на лицата чии комуникации се предлага да се следат**. Оваа улога може да ја извршува панел на експерти, претставник на Дирекцијата за заштита на личните податоци или Народниот правобранител, како „застапник на јавниот интерес".[79]

Во однос на обезбедувањето налог од судските власти за следење на комуникациите, соговорниците кои порано биле дел од МВР истакнаа дека постојат случаи судската наредба да се бара ретроактивно, при што од судиите се бара да ја потпишат наредбата без дури и да знаат по кој основ овластуваат следење комуникации и врз кого. Притоа беа наведени случаи во кои без издадена судска наредба е почнато следење на комуникациите, а во моментот кога е најдена индиција за кривично дело, ретроактивно да се побара издавање наредба. Во минатото, кога постоела рачна евиденција на документацијата, се пристапувало и кон препишување на цели евидентни книги за да се покрие ретроактивноста на судските наредби, а со воведувањето електронска евиденција, наводно ваквиот процес на фалсификување на евиденцијата само се олеснил. Сомнеж во ефективноста на претходниот судски надзор на следењето комуникации создава и податокот дека досега немало случај да има одбиено барање од судовите за спроведување посебни истражни мерки.

Законот за кривичната постапка, во член 257 ја пропишува содржината на наредбата за следење на комуникациите што ја донесува судијата. Спорно е што **овој член не пропишува обврска во наредбата да се наведе органот на чие барање се наредува следење** на комуникациите. Овој елемент на наредбата беше задолжителен согласно членот 13 од Законот за следење на комуникациите, што беше избришан со измените и дополнувањата во 2012 г.

Законот пропишува, условно речено, жалбена постапка доколку судијата не се согласи со барањето за следење на комуникациите или со барање за продолжување на времетраењето. Во тој случај, по барањето треба да одлучува тричлен совет на надлежниот првостепен суд.[80] **Загрижувачки е што респективно „право на приговор" не е пропишано и за заштита на правата и интересите на лицата чии комуникации се предлага да се следат**. Имено, законот не содржи одредби со коишто ќе се овозможи на соодветен ентитет, на пример, Дирекцијата за заштита на личните податоци или Народниот правобранител, да учествува во постапката на издавање наредба за следење на комуникациите и да има можност пред друга инстанца да ја оспори основаноста на евентуално издадена наредба од судија во претходна постапка.

[79] Ваков механизам постои во Квинсленд, Австралија.
[80] Член 11-а од Законот за следење на комуникациите.

Времетраење на следењето комуникации

Со измените и дополнувањата на Законот за следење на комуникациите во 2012 г. беше избришана одредбата според која следењето на комуникациите може да трае одредено време, што, пак, наметна прашање на кој начин ќе се обезбеди следењето на комуникациите на одреден субјект да не биде постојано.[81] Иако останатите одредби на законот дефинираат временски ограничувања за следењето на комуникациите за конкретно кривично дело, сепак не постои одредба со која ќе се спречи континуирано следење нечии комуникации. Континуираното следење нечии комуникации е можно под хипотетичко оправдување дека постојано се јавуваат нови основани сомневања за некакво ново кривично дело.

Рокот содржан во барањето за следење на комуникациите е ограничен на 4 месеци и може да се продолжи за уште 4 месеци.[82] Барањето за продолжување се упатува од Министерството за внатрешни работи, Управата за финансиска полиција, или Царинската управа до јавниот обвинител, кој – доколку е согласен – го проследува до надлежниот судија.[83] За кривични дела за кои е пропишана казна затвор од најмалку четири години за кои постои основано сомневање дека се извршени од страна на организирана група, банда или друго злосторничко здружение, судијата на претходната постапка може да го продолжи овој рок за уште најмногу шест месеци.[84] Оттука, следењето не смее да надмине 14 месеци. Ваквите рокови се значително подолги од

Клучните наоди на Прибе

Групата високи експерти за системските прашања од владеење на правото, предводена од Рајнхард Прибе, во извештаите од 2015 и 2017 г. како главна причина за скандалот со прислушувањето ја наведува концентрацијата на власт во Управата за безбедност и контраразузнавање (УБК) и лошиот надзор над неа. Во извештајот од 2015 г. се наведува дека УБК делувала вон законските овластувања во име на Владата, за контрола на највисоките функционери во јавната администрација, обвинители, судии и политички опоненти со последователно мешање во независноста на судството и другите релевантни институции. Во извештајот од септември 2017 г. се наведува дека не се преземени конкретни чекори за надминување на проблемите.

Според групата експерти, само УБК има техничка способност за следење на комуникациите и при разузнавачките и при кривичните истраги. Следењето се спроведува од УБК во сопствено име и во име на Полицијата, Царинската управа и Финансиската полиција. Врз основа на членовите 175 и 176 од Законот за електронски комуникации, секој од националните телекомуникациски провајдери ѝ овозможува копирање на целокупниот сообраќај, со што УБК може директно да ги следи комуникациите – самостојно и непречено – без разлика дали е издаден судски налог или не.

[81] Извештај од јавната расправа на Националниот совет за евроинтеграции по работната верзија на Предлог-законот за изменување и дополнување на Законот за следење на комуникациите, Собрание на Република Македонија, 16.07.2012 г. Извештајот е достапен на: https://www.sobranie.mk/WBStorage/Files/JRSledenjenakomunikacii.pdf

[82] Член 260 од Законот за кривичната постапка.

[83] Член 15 од Законот за следење на комуникациите.

[84] Член 260 од Законот за кривичната постапка.

оние што беа предвидени пред измените во Законот за следење на комуникациите во 2012 г. Претходно, мерката се одобруваше во времетраење од еден месец, со можност со дополнителни барања да се продолжува за по уште еден месец секојпат, но не повеќе од вкупно времетраење од една година.

Законот за кривичната постапка пропишува дека кога ќе се постигнат целите заради коишто се определени посебните истражни мерки или ќе престанат да постојат основите заради коишто се одобрени, органот што ја издал или продолжил наредбата е должен веднаш да нареди запирање на мерките. Сепак, во пракса е можно судијата или јавниот обвинител да не дознае веднаш за изменетите околности, па **препорачливо е ваквиот услов да се вклучи меѓу задолжителните елементи на наредбата за следење на комуникациите и да го обврзува органот што треба да ја спроведе наредбата**.[85] За ова е потребно дополнување во членот 257 од Законот за кривичната постапка.

Оперативно спроведување на следењето комуникации

Според Законот за кривичната постапка, посебните истражни мерки – вклучително и следењето комуникации – се спроведуваат од јавниот обвинител или правосудната полиција под контрола на јавниот обвинител. Ова не е усогласено со законот за следење на комуникациите, ниту со праксата каде што оперативното спроведување на следењето на комуникациите е делегирано на Министерството за внатрешни работи, поточно на Управата за безбедност и контраразузнавање.

Според членот 175 од Законот за електронските комуникации операторите се должни да ги обезбедат сите неопходни технички услови за да овозможат следење на комуникациите во нивните мрежи, согласно со Законот за следење на комуникациите. Операторите се должни на сопствен трошок да обезбедат и одржуваат опрема, соодветен интерфејс и да воспостават електронски комуникациски водови за пренос до овластениот орган за следење на комуникациите. Законот ја уредува и техничката спецификација на опремата и интерфејсот за следење на комуникациите, односно за истата операторите треба да ги следат инструкциите од овластениот орган за следење на комуникациите. Операторите се обврзани да овозможат следење на комуникациите во реално време.

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

Наведеното упатува на тоа дека и во Законот за електронските комуникации од 2014 година се задржа директниот и неограничен пристап на МВР до целокупниот телекомуникациски сообраќај во Македонија. Имено, со измените и дополнувањата од 2010 година на стариот Законот за електронските комуникации,[86] се воведоа новини во начинот на следење на комуникациите. Имено, покрај обврската на операторите да обезбедат соодветна опрема и интерфејс за спроведување на мерката следење на комуникациите, се додаде и обврска дека опремата подразбира и воспоставување на телекомуникациски водови и телекомуникациска опрема за пренос до локацијата на овластениот орган за следење комуникации. Оттука, УБК може да го врши следењето без дополнителни дејства од страна на операторите, и без нивно знаење. Опремата со која располага операторот (набавена врз основа на спецификациите наложени од МВР) се користи стриктно за пренасочување на содржината на комуникациите кон УБК. Поради законската обврска за обезбедување директен пристап на МВР до комуникацијата при нарачката на опремата, самиот „Македонски Телеком“ побарал активностите за следење да се невидливи за операторот, односно операторот да не дознава кој, кога и колку се следи за да нема никаква одговорност.

Директниот пристап до содржината на комуникациите го зголемува ризикот од злоупотреби, односно случаи следењето да се врши без соодветен налог од судија. Дополнителен ризик се јавува и поради техничката можност МВР да ги пренасочи следените комуникации кон други ентитети и други локации. Соговорниците истакнаа наводи дека вакво пренасочување се врши и по безжичен пат до три други локации на МВР, што создава големи ризици за пресретнување на комуникациите од трети лица, а беа изнесени и наводи за пренасочување на следените комуникации во партиски простории.

За разлика од сегашниот директен пристап на МВР до содржината на комуникациите, до 1998 година, поради користење на друг тип опрема, за да врши следење на нечии комуникации било потребно МВР претходно да го извести соодветниот оператор и да достават судски налог врз основа на кој операторот ќе го овозможи следењето. Стариот систем овозможувал и

Прибе за реформирањето на УБК

Во извештајот на групата експерти од 2017 година е наведено дека се започнати реформски процеси преку проект со меѓународна поддршка, при што е подготвена анализа и се посочени модели за управување, спроведување и надзор над прислушувањето. Една од предложените насоки за надминување на моменталната состојба е одземање на директниот пристап на УБК до содржината на комуникациите и враќање на пренасочувањето на комуникациите во операторите, кои по судски налог ќе бидат обврзани да овозможат услови за прислушување, додека друга можна алтернатива е креирање на посебен Операциско-технички центар, кој ќе биде задолжен за следењето на комуникациите, но само доколку се процени дека ваквото ново тело би било во можност да одолее на надворешните притисоци и влијанија.

[86] Закон за изменување и дополнување на Законот за електронските комуникации („Службен весник на Република Македонија“, бр. 83/2010).

операторите да се вклучат во претходен надзор обезбедувајќи дека се исполнети законските услови за следење на комуникациите. Дополнително, со тоа постоела уште една точка во системот – надвор од МВР – во која надзорните органи можеле да извршат увид и контрола.

Во 2010 година, Уставниот суд донесе одлука со која се поништуваат спорните членови кои се однесуваат на следењето на комуникациите во Законот за електронските комуникации донесен во 2005 година.[87] Согласно оваа одлука,[88] Судот се произнесе дека одредбите во овој Закон содржат опасност од неуставно и неовластено навлегување во приватноста, и истите не се прецизни, подлежат на импровизации или интерпретации и им даваат директна сила на овластените органи за примена на мерката на следење на комуникациите без ставање на нивното овластување во цврста законска рамка. Судот оцени дека оспорените одредби од Законот не содржат доволно гаранции против евентуална злоупотреба од страна на овластениот орган со дадената техничка можност за континуирано и самостојно следење на содржината на комуникацијата, како и при прибирањето на потребните податоци во врска со остварената комуникација. Во отсуство на јасни законски одредби во врска со следењето на комуникациите, постои огромен ризик за создавање неограничена моќ, во спротивност со принципот на владеењето на правото.

И покрај ваквата одлука на Уставниот суд, Законот за електронските комуникации од 2014 година повторно овозможи Министерството за внатрешни работи да има *директен* и *неограничен* пристап до содржината на *сите* електронски комуникации на *сите* граѓани. Наспроти тоа, законското решение што беше во сила до 2010 година беше многу поповолно за заштита на приватноста, а согласно со него, операторите овозможуваа пристап до содржината на комуникациите на *одреден* корисник само врз основа на налог од надлежен суд. Во 2015 г. беше поднесена иницијатива за преиспитување на уставноста на членот 175 од Законот за електронските комуникации. Претседателот на Уставниот суд не го ставаше овој предмет на дневен ред две години, иако задолжениот судија-известител го припремил предметот, а Судот можел да се повика на претходната одлука и повторно да ја поништи спорната одредба. Уставниот суд дури на 21.06.2017 година одлучи да поведе постапка за оценување на уставноста на спомнатиот член. Одлуката на Уставниот суд беше најавено дека ќе се достави до Собранието, кое ќе има 30 дена за одговор.

Дополнително, Законот за електронски комуникации, како и Законот за следење на комуникациите не ги раздвојуваат надлежноста, прописите и техниката за следење на комуникациите при кривичните истраги, од оние од безбедносен и разузнавачки карактер – што е посочено како друг сериозен проблем во итните реформски приоритети[89].

[87] Член 4 точки 47 и 48, член 112 ставови 7 и 8, член 114 ставови 7, 8 и 9, член 115 и член 138 став 1 точки 28 и 29 од Законот за електронските комуникации („Службен весник на Република Македонија“ бр. 13/2005, 14/2007, 55/2007, 98/2008 и 83/2010).

[88] Одлука на Уставен суд, у. број 139/2010-0-1 од 15.12.2010, достапна на: http://www.ustavensud.mk/domino/WEBSUD.nsf/ffc0feee91d7bd9ac1256d280038c474/7119424dde39fdadc1257809002db948?OpenDocument

[89] Итни реформски приоритети за Македонија, јуни 2015. Достапно на: https://eeas.europa.eu/sites/eeas/files/urgent_reform_priorities_en.pdf

Владата на Република Македонија во **Планот 3-6-9**[90] ја нагласува потребата од реформа на разузнавачките и безбедносните служби со цел враќање на довербата во нив. Со овој план, Владата презеде обврска да подготви план за реализација на препораките на групата високи експерти за системските прашања од владеење на правото во врска со следењето на комуникациите, со транспарентен и инклузивен процес на консултации со сите засегнати страни. Планот предвидува и учество на органите вклучени во следењето на комуникациите на редовни седници на надлежната собраниската комисија за надзор над нивната работа, како и учество на Управата за безбедност и контраразузнавање и Агенцијата за разузнавање на редовни седници на собраниската комисија која врши надзор над нив.

Употреба на сознанијата од следењето на комуникациите

Во 2012 г. избришани беа одредбите од Законот за следење на комуникациите со кои се утврдуваше обврска за Министерството за внатрешни работи да изработува извештај до судијата во претходна постапка од секој завршен предмет за следење на комуникациите и се пропишуваше содржината на таквиот извештај.[91]

Сепак, во Законот за кривичната постапка се пропишува дека по спроведувањето на посебните истражни мерки, правосудната полиција изготвува извештај кој го доставува до јавниот обвинител.[92] Во извештајот ги наведува времето на почеток и завршување на мерката, бројот и идентитетот на лицата опфатени со мерката, дава краток опис за текот и резултатите од примената на мерката. **Потребно е ваквата одредба да се дополни за да се пропише обврска во овој извештај да се наведува и бројот на телефонска или друга корисничка линија или адреса за електронска пошта што се следеле**, особено што следењето на комуникациите може да се нареди и во однос на предмет на кривично дело (телефонска линија или адреса за електронска пошта).

Сите податоци, известувања, документи и предмети прибавени со примена на посебните истражни мерки можат да се користат како доказ во кривичната постапка.

Според членот 255 од Законот за кривичната постапка, доколку при примената на мерката бидат следени и снимени комуникации на лица кои не се опфатени со наредбата, јавниот обвинител е должен да ги издвои и да го извести судијата на претходната постапка. По предлог на јавниот обвинител, судијата на претходната постапка може да нареди од целосната документација од примената на мерката да се издвојат само делови што се однесуваат на кривичното дело за коешто е издадена наредбата. Дополнително со членот 263 од Законот за кривичната постапка, ако при спроведувањето на мерката се добијат податоци за кривично дело што не е опфатено со наредбата, мерката ќе продолжи само доколку станува збор за кривично дело за коешто се предвидени посебни истражни мерки и така собраните податоци можат да се користат како доказ во кривичната постапка. **Членовите 255 и 263 е потребно да се преиспитаат за да се осигури дека собраните податоци од следењето на**

[90] План 3-6-9 на Владата на Република Македонија, достапен на: http://vlada.mk/sites/default/files/programa/2017-2020/Plan%203-6-9%20MKD.pdf

[91] Членови 19 и 21 од Законот за следење на комуникациите.

[92] Член 258 од Законот за кривичната постапка.

комуникациите се однесуваат на намената за којашто е издадена наредбата и се собрани податоците. Имено, таа намена е собирање податоци за однапред одредени кривични дела и лица – или утврдување на лица кои користат телефонска, друга линија или мејл адреса која е предмет на кривично дело. Оттука, имплицирањето нови лица во делото, или утврдувањето нови кривични дела треба да бара повторно обновување на наредбата од судијата, а барањето за такво нешто не би требало да се заснова на снимени комуникации што ја надминуваат наредбата врз чија основа се собрани.

Според Законот за кривичната постапка, кај една од предвидените посебни истражни мерки[93] снимањето ќе се прекине ако за време на снимањето постојат показатели дека ќе се пресретнат искази што спаѓаат во основната сфера на приватниот и семејниот живот. Документацијата за таквите искази треба веднаш да се уништи.[94] Нејасно е зошто законодавецот не предвидел слична претпазливост и за посебните категории на личните податоци коишто според законот за заштита на личните податоци не смеат да се обработуваат, односно можат да се обработуваат само под посебни услови,[95] а коишто во случајов можат да се собрани со примена на мерката следење и снимање на телефонските и другите електронски комуникации.

Известување на лицата чии комуникации се следени, право на оспорување на следените комуникации, право на приговор и надомест на штета

Законот за следење на комуникациите пропишува дека лицето чија комуникација е следена има право да ја оспорува автентичноста на собраните податоци и законитоста на постапката за следење на неговите комуникации, во постапка утврдена со Законот за кривичната постапка на Република Македонија.[96] Сепак, симптоматично е што со измените и дополнувањата на законот во 2012 г. беше избришана одредбата од законот со која се забрануваше следење на комуникациите без наредба на надлежен суд.[97] Во членот 4 од законот, пак, со кој се класифицираа информациите собрани со *овластено* следење на комуникациите, беше избришан зборот „овластено“. Дополнително, Законот за кривичната постапка на Република Македонија не утврдува посебна постапка за оспорување на автентичноста на собраните податоци и законитоста на следењето на комуникациите.

[93] Следење и снимање во дом, затворен или заграден простор што му припаѓа на тој дом или деловен простор означен како приватен или во возило и влез во тие простории заради создавање на услови за следење на комуникации.

[94] Член 268 од Законот за кривичната постапка.

[95] Законот за заштита на личните податоци ги утврдува следниве посебни категории на лични податоци кои не смеат да се обработуваат, односно можат да се обработуваат само под посебни услови во законот се утврдени: личните податоци што го откриваат расното или етничкото потекло, политичкото, верското, филозофското или друго уверување, членството во синдикална организација и податоци што се однесуваат на здравјето на луѓето, вклучувајќи ги и генетските податоци, биометриските податоци или податоците што се однесуваат на сексуалниот живот.

[96] Член 6 од Законот за следење на комуникациите.

[97] Закон за изменување и дополнување на Законот за следење на комуникациите, „Службен весник на Република Македонија“ бр. 116/2012.

Во случај на судска одлука дека комуникацијата била следена спротивно на одредбите од Законот за следење на комуникациите, лицето има право на надомест на штета од државниот буџет.[98] Сепак, **не е прецизирано како овие лица ќе можат да го искористат правото за оспорување и надомест на штета кога во законот за следење на комуникациите беше избришана одредбата според којашто по донесувањето решение за спроведување истрага требаше да бидат запознаени со извештајот за следењето комуникации** изготвен од Министерството за внатрешни работи.[99] Во Законот за кривичната постапка е предвидено дека по прекинувањето на посебните истражни мерки, ако тоа не штети на постапката, по барање на засегнатото лице, јавниот обвинител ќе му ја достави писмената наредба. Како и во претходниот случај, за да засегнатите лица можат да поднесат вакво барање, треба претходно да знаат дека нивните комуникации биле следени, а законот не предвидува јасен механизам за да се случи тоа. Оттука, **неопходни се законски измени со коишто ќе се воведе обврска засегнатите лица да се известат за посебните истражни мерки по нивното прекинување**.

Заштита, чување и уништување на следените комуникации

Со измените на Законот за следење на комуникациите во 2012 г. беа избришани и заштитните мерки за чување на записите од следењето на комуникациите што вклучуваа нивно чување во запечатени обвивки кај судијата на претходна постапка и надлежниот обвинител, за чиешто отворање мора да постои судска наредба, како и записник од отворањето. Истото се однесува и на одредбите според коишто, по истекот на рокот за застареност на кривичното гонење за делото за коешто било наредено следење на комуникациите, се уништуваат записите што ги има Јавното обвинителство, како и оригиналните материјали од следењето на комуникациите што се чувале во Министерството за внатрешни работи.[100] Иако Законот за кривична постапка има одредба за уништување на записите, таа не е детално прецизирана како што беше во избришаните одредби од Законот за следење на комуникациите. Имено, според член 261 од законот за кривичната постапка, ако јавниот обвинител се откаже од кривично гонење или ако собраните податоци со посебните истражни мерки немаат значење за водење на постапката, пропишано е дека ќе се уништат под надзор на судијата, а за тоа јавниот обвинител ќе изготви записник.[101] Ако во рок од 15 месеци по завршувањето на спроведувањето на мерките не се поведе кривична постапка, сите собрани лични податоци треба да бидат избришани или уништени под надзор на судијата на претходна постапка, јавниот обвинител и претставникот на Дирекција за заштита на личните податоци, за што јавниот обвинител треба да состави записник.[102] Овие одредби не спомнуваат што ќе се случи со оригиналните материјали од следењето на комуникациите што ги собрала Управата за безбедност и

[98] Член 28 од Законот за следење на комуникациите.

[99] Закон за изменување и дополнување на Законот за следење на комуникациите, „Службен весник на Република Македонија“ бр. 116/2012.

[100] Членови 22 и 25-а од Законот за следење на комуникациите.

[101] Член 261 од законот за кривичната постапка.

[102] Член 267.

контраразузнавање. Оттука, **измените на законските одредби за чување и уништување на податоците од следењето на комуникациите значително и неразумно ја намалија заштитата на собраните податоци**.

Лицата кои на кој било начин дознале податоци што се однесуваат или произлегуваат од примената на посебните истражни мерки се должни да ги чуваат како службена тајна.[103]

Специфики на следење на комуникациите заради заштита на интересите на безбедноста и одбраната на земјата

Судот може да нареди следење на комуникациите и заради заштита на интересите на безбедноста и одбраната на земјата. Табелата долу дава преглед на главните сличности и разлики меѓу законските одредби за следењето на комуникациите по овој основ,[104] во споредба со следењето на комуникациите заради откривање и гонење сторители на кривични дела.

	Следење на комуникациите заради откривање и гонење сторители на кривични дела	**Следење на комуникациите заради заштита на интересите на безбедноста и одбраната на земјата**
Основ	Откривање и гонење сторители на кривични дела	Подготовка на кривично дело против државата, вооружените сили или против човечноста и меѓународното право, како и подготовка, поттикнување, организирање или учествување во вооружен напад против Македонија или во онеспособување на безбедносниот систем
Подносител на барање	Надлежниот јавен обвинител по сопствена иницијатива или на предлог на Министерството за внатрешни работи, Управата за финансиска полиција или Царинската управа	Јавниот обвинител на Република Македонија на предлог на министерот за внатрешни работи, министерот за одбрана или лице овластено од било кого од нив
Времетраење	До 4 месеци, со можност за повеќекратно продолжување од по најмногу 4 месеци, но не повеќе од 14 месеци збирно	До 6 месеци, со можност за продолжување, но не повеќе од 24 месеци збирно
Судија што издава наредба	Судијата на претходната постапка	Одреден судија на Врховниот суд
Рок за одлучување на судијата	48 часа, а во случаи на итност може да се издаде усна наредба која е валидна 48 часа	72 часа, а во случаи на итност 5 часа
Приговор при одбивање на барањето се упатува до	Тричлен совет на судии на надлежниот првостепен суд	Тричлен совет на судии на Врховниот суд
Приговор при прифаќање на барањето (од ентитет што ги застапува интересите на лицата)	Не е предвиден	Не е предвиден

[103] Член 264 од Законот за следење на комуникациите.

[104] Членови 29 до 34 од Законот за следење на комуникациите.

	Следење на комуникациите заради откривање и гонење сторители на кривични дела	Следење на комуникациите заради заштита на интересите на безбедноста и одбраната на земјата
Најдолг период на чување на записите	Нема ограничување	Пет години по истекот на времето определено со наредбата
Право на информирање на лицата чии комуникации се следат	Не е предвидено	Не е предвидено
Право на надомест на штета на лица чијашто комуникација била следена спротивно на одредбите на законот	Одлучува надлежниот суд за донесување на наредбата за следење на комуникациите во итна постапка, што не може да трае подолго од три месеци	Не е предвидено
Право на надомест на штета на лица чијашто комуникација била следена без да се докажат сомневањата	Не е предвидено	Не е предвидено

При спроведувањето на истражувањето, соговорниците кои порано работеле во безбедносниот систем на Република Македонија наведуваат дека во службата не се врши претходна безбедносна проценка за да се одлучи дали треба да се поведе постапка и да се побара налог за следење на комуникациите од судија.

Надзор и контрола над следењето комуникации

Надзорот над спроведувањето на посебната истражна мерка следење на комуникациите го врши петочлена собраниска комисија, составена од тројца претставници на опозицијата и двајца претставници на политичките партии на власт. Проблематично е што со законските измени во 2012 г. беше додадена одредба[105] дека комисијата донесува одлука за надзор со мнозинство гласови. **Нејасно е зошто е воопшто потребно да се пропише дека комисијата треба да донесе посебна одлука за надзор, кога истата е основана токму со таа намена.**

Дополнително, **Комисијата треба да поднесе годишен извештај до Собранието на Република Македонија во рок од два месеца по завршувањето на тековната година, но не постојат одредби со кои ќе се обезбеди дека ќе и бидат обезбедени податоци за навремено да ја исполни ваквата обврска**.[106]Јавниот обвинител на Република Македонија е должен еднаш годишно да достави извештај за посебните истражни мерки до Собранието на Република Македонија за мерките што се побарани во претходната година,[107] но не е утврден рок за ваквата обврска што би ѝ овозможил на соодветната собраниска комисија да го испочитува зацртаниот рок за сопствениот извештај. Надзорните собраниски комисии немаат пристап до никакви дополнителни податоци од службите.

Собраниската комисија за надзор на следењето на комуникациите и Комисијата за надзор над работата на разузнавачките и контраразузнавачките служби досега не можеа да остварат ефективен надзор поради **немање пристап до релевантни**

[105] Член 36-а од Законот за следење на комуникациите.
[106] Член 37 од Законот за следење на комуникациите.
[107] Член 271 од Законот за кривичната постапка.

податоци, како и поради опструкции со постојано менување на членовите од редовите на партиите од тогашната власт, што пак повлекуваше неможност за одржување седници сè до стекнување со безбедносни сертификати за новите членови. Според разговорите со поранешни членови на овие комисии, **издавањето безбедносни сертификати се одолговлекувало од МВР и по повеќе од 6 месеци**, па дури и година, со што се блокирала работата на комисиите. Беа наведени и примери на промена на членовите на комисијата од страна на партиите на власт со цел да се создаде потреба за издавање нови безбедносни сертификати, што во меѓувреме ги оневозможува седниците на комисијата. Иронично во целата ситуација е што министрите по автоматизам добиваат највисок безбедносен сертификат, а ваквиот пристап не важи за пратениците.

Увид на лице место од страна на собраниските комисии се оневозможува и со тоа што мнозинство во комисијата за надзор над Управата за безбедност и контраразузнавање и Агенцијата за разузнавање имала позицијата, а во комисијата за надзор над посебната истражна мерка следење на комуникациите имала опозицијата, но дури и во вториот случај, членовите од позицијата инсистирале дека мора да се одлучува со консензус. Дополнително на комисиите не им стојат на располагање стручни лица, а самите пратеници не се експерти по информациски технологии во областа. Дури и да им се даде можност да извршат увид, без присуство на стручни лица немаат соодветни познавања (технолошки, информатички, па дури и правни) за да го изведат увидот. Оттука, Собраниските комисии за надзор имаат само формална улога.

Контрола над спроведувањето на посебната истражна мерка следење на комуникациите врши надлежниот јавен обвинител, односно – во случај кога мерката е наредена заради заштита на интересите на безбедноста и одбраната на земјата – судијата на Врховниот суд кој ја издал таа наредба.

Согласно член 7 од Законот за електронските комуникации, пак, Агенцијата за електронски комуникации е должна да обезбеди одржување на интегритетот и безбедноста на јавните електронски комуникациски мрежи. Агенцијата е должна да спроведе постапка на надзор над операторите во врска со исполнувањето на обврските во однос на обезбедувањето неопходни технички услови за да се овозможи следење на комуникациите согласно Законот за следење на комуникациите, по барање на овластен орган. Сепак, Агенцијата за електронски комуникации не можеше да потврди или одрече дали има извршено надзор над опремата за следење на комуникациите кај операторите.

По објавувањето на политичките бомби, беше шокантен молкот на надлежните институции. Со задоцнување реагираа три институции:

- **Министерството за внатрешни работи** и тоа по назначувањето на „опозициискиот“ министер Оливер Спасовски, коешто иницираше формирање работна група составена од претставници на повеќе институции.
- **Дирекцијата за заштита на личните податоци** (ДЗЛП), којашто врз основа на „бомбите“ има извршено инспекциски надзор[108] по службена должност во Управата за безбедност и контраразузнавање, во периодот јуни–ноември 2016 година. Надзорот се однесувал на законитоста на преземените активности при обработката на личните

[108] Дирекција за заштита на личните податоци, Годишен извештај за 2016 година. Достапен на: https://dzlp.mk/sites/default/files/u4/godisen_izvestaj_dzlp_2016.pdf

податоци и нивната заштита. Во записникот за извршениот инспекциски надзор се утврдени неправилности и повреди, и тоа: недонесена документација за технички и организациски мерки за обезбедување на тајноста и заштита на обработката на личните податоци, неприменување технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци, како и невршење контроли за проверка на воспоставениот систем за заштита на личните податоци. На почетокот на 2017 година е донесено и Решение од страна на ДЗЛП во врска со спроведениот надзор. Со Решението, Министерот за внатрешни работи е задолжен да преземе конкретни дејствија и активности за отстранување на утврдените неправилности и повреди, при што е даден рок до јули 2017 година да се постапи по Решението. ДЗЛП во текот на декември 2016 година започнала со спроведување на инспекциски надзори над законитоста на преземените активности при обработката на личните податоци и нивната заштита и кај двата телекомуникациски оператори. Од спроведените надзори било констатирано дека телекомуникациските оператори имаат воспоставено електронски комуникациски водови со соодветен интерфејс за пренос до овластениот орган за следење на комуникации во нивната мрежа. Утврдено е и дека применуваат технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци од случајно или незаконско уништување, случајно губење или изменување или пак неовластено или незаконско чување обработка, пристап или откривање на неовластени лица.

- **Народниот правобранител** добил претставка од новинарка – засегнато лице кое било споменато во разговорите – па започнале постапка со барање за информации и вршење контрола во УБК, МВР и Собранието, но не добиле никакви информации. Народниот правобранител е институција која ужива најголем рејтинг и доверба од граѓаните, но сепак располага со мали капацитети (човечки ресурси), бидејќи Владата не дозволува нови вработувања и на тој начин ја попречува работата на институцијата.

Безбедност кај операторите на јавните електронски комуникациски мрежи и давателите на услуги

Отсуствуваше јавна реакција на „политичките бомби“ и од телекомуникациските оператори коишто не ги информираа своите претплатници за нарушувањето на нивната приватност и личните податоци, како и за мерките кои ги преземаат за да испитаат како дошло до таквото нарушување и како ќе ги минимизираат ризиците за да се повтори. Според „Македонски Телеком“, операторот има редовни интерни ревизии на системите од страна на „Дојче Телеком“, кој има пропишано посебни стандарди за користењето на опремата и за лицата кои имаат пристап до неа. Беше објавено дека „Маѓар Телеком“ отворил интерна истрага во врска со бомбите во мај 2014 г., три месеци по објавувањето на првите тонски снимки од прислушувањето, но не беше објавен исходот од таа истрага.[109] Вкупно 3 лица од „Телеком“ имаат пристап до опремата за следење на комуникациите, но само од аспект на нејзината функционалност и реагираат само кога од МВР има пријава дека има некаков проблем. Операторот има многу лични податоци што се чуваат за системски потреби (на пр. за потреби на фактурирање) и постојат одредени можности за нивна

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

злоупотреба и покрај добрите системи за заштита, но досега немало случај кога се открила таква злоупотреба и кога бил казнет вработен за неа.

Казнени одредби за надлежните органи за следењето комуникации

Во законот за следењето на комуникациите отсуствуваат казнени одредби за надлежните органи и одговорните лица во нив, што е необјасниво имајќи предвид дека непочитувањето на законот може да резултира со сериозни нарушувања на правата на лицата чии комуникации се следат, како и на демократијата и владеењето на правото во земјата. Фактот што во Кривичниот законик[110] се инкриминира неовластеното прислушување и тонско снимање, како и повредата на тајноста на писмата (вклучително и обезбедена електронската пошта) е недоволен за да се покријат сите можни состојби и последици од неспроведување или недоследно спроведување на одредбите од Законот за следењето на комуникациите.[111]

Задржување метаподатоци

Законот за електронските комуникации од 2014 година воведе новини во следењето на комуникациите и масовното задржување на „метаподатоци“ од корисниците. Членовите 176 и 178 воведоа обврска сите телефонски и интернет провајдери да ги задржуваат една година за сите свои корисници следниве податоци за телефонски и интернет услуги (вклучително и е-пошта): името, адресата, телефонскиот број/ИП адресата, телефонскиот уред и локацијата на лицата кои комуницираат; времето на почетокот и крајот на комуникацијата; типот на телефонска/интернет услуга. Операторите се обврзани ваквите податоци да ги задржуваат на свој трошок и по барање, да им ги достават на државните органи. Образложението беше дека метаподатоците ќе се задржуваат заради „спречување или откривање кривични дела, водење кривична постапка или поради интересите на безбедноста и одбраната“. Притоа, пристап до метаподатоците се остварува врз основа на барање, односно наредба од јавниот обвинител, и за нив не е потребна наредба од судија. Проблематично е што нашето законодавство пропишува понизок стандард за пристап до метаподатоците, во услови кога модерните мобилни телефони обезбедуваат податоци за движењето и локацијата на нивните корисници, дури и

[110] Кривичен законик, „Службен весник на Република Македонија“ број 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.

[111] Според членот 151, ако неовластено прислушување и тонско снимање се изврши од службено лице во вршење на службата или одговорно лице во правно лице, ќе се казни со казна затвор од најмалку четири години. Со оваа казна се казнува и лице вработено во правно лице на кое во рамките на работењето му е доверено спроведувањето на мерката за следењето на комуникациите. Правно лице се казнува со парична казна, а правно лице чијашто примарна дејност е давање телекомуникациски услуги се казнува со 10% од вкупниот приход од тековната година во која е сторено делото. Со членот 147 за повреда на тајноста на писма е утврдена парична казна или затвор до една година, а доколку се работи за службено лице, ќе се казни со затвор од три месеци до пет години.

подобро и поедноставно одошто со нечие физичко следење. Ваквиот пристап не е во согласност со Европската конвенција за човекови права.

Одредбите за масовно задржување податоци беа оправдани како транспонирање на Директивата 2006/24/ЕЗ, којашто беше поништена од Европскиот суд на правдата непосредно по донесувањето на новиот Закон за електронските комуникации во Македонија. По поништувањето на Директивата, во Македонија не се преземени никакви чекори кон отстранување на спорните членови што го регулираат задржувањето на податоците. Според претставник на Агенцијата за електронски комуникации, „во 2015 или 2016 г." тие доставиле до Министерството за информатичко општество и администрација предлог за измена на Законот за електронските комуникации со цел усогласување со правото на ЕУ. Сепак, претставникот на Агенцијата не можеше да потврди дали во тој нацрт-текст предложиле и укинување на обврската за задржување метаподатоци.[112]

Законот за електронските комуникации ја дефинира обврската за задржување на податоци при обезбедување на телефонски услуги преку фиксна или мобилна јавна електронска комуникациска мрежа, како и при обезбедување на пристап до интернет, електронска пошта и до телефонски услуги преку интернет. Наведени се следните податоци кои операторите се должни да ги задржуваат во времетраење од една година:

1. Податоци што се потребни за следење и идентификување на изворот на комуникацијата (повикувачкиот број; име и адреса на корисникот; доделениот кориснички код за идентификација; корисничкиот код за идентификација и телефонскиот број доделен за каква било комуникација при пристап до јавната телефонска мрежа; името и адресата на претплатникот или на регистрираниот корисник кому му била доделена адреса за интернет-протокол (ИП), кориснички код за идентификација или телефонски број за време на комуникацијата).

2. Податоците што се потребни за идентификување на дестинацијата на комуникацијата (повиканите телефонски броеви и/или бројот или броевите каде што се пренасочува повикот; името и адресата на корисникот; корисничкиот код за идентификација или телефонскиот број на примателот на телефонскиот повик преку интернет; името и адресата на корисникот и корисничкиот код за идентификација на примателот на телефонскиот повик преку интернет).

3. Податоци што се потребни за идентификување на датумот, часот и на времетраењето на комуникацијата (датумот и часот на почетокот и на крајот на комуникацијата; датумот и времето на пријавување и одјавување на пристапот до интернет врз основа на одредена временска зона, заедно со ИП-адресата; корисничкиот код за идентификација на корисникот; датумот и часот на пријавување и одјавување од услугата за електронска пошта или од телефонските услуги преку интернет, врз основа на одредена временска зона).

4. Податоци што се потребни за идентификување на типот на комуникацијата (телефонската услуга што е користена; интернет услугата што е користена).

5. Податоци што се потребни за идентификување на комуникациската опрема на корисникот или на онаа за којашто се смета дека е негова (повикувачките и повикуваните телефонски броеви; меѓународниот идентитет на мобилниот претплатник (*IMSI*) на повикувачката страна; меѓународниот идентитет на мобилниот

[112] Министерството не одговори на барањето за разговор на оваа тема.

уред (*IMEI*) на повикувачката страна; *IMSI* на повикуваната страна; *IMEI* на повикуваната страна; датумот и часот на почетното активирање на услугата и ознаката на локацијата од каде што била активирана услугата, во случај на анонимна припејд-услуга; повикувачкиот телефонски број за *dial-up* пристап; дигиталната претплатничка линија (DSL) или друга крајна точка на иницијаторот на комуникацијата).

6. Податоци што се потребни за да се идентификува локацијата на мобилната комуникациска опрема (ознаката за локацијата на почетокот на комуникацијата; податоците за идентификување на географската локација на ќелиите со упатување на нивните ознаки за локација за временскиот период за кој се задржуваат податоците за комуникацијата).

Членот 177 од Законот за електронските комуникации поставува обврска за операторите да применуваат соодветни технички и организациони мерки за заштита од случајно или незаконско уништување на метаподатоците, случајно губење или изменување, или пак неовластено или незаконско чување обработка, пристап или откривање. Понатаму, во истиот член е дефинирано дека операторот треба да применува соодветни технички и организациони мерки за податоците за да се обезбеди дека до нив можат да пристапат само овластени лица на операторот. Заштитата на овие податоци кај операторите се заснова на фактот што системот за чување на метаподатоците создава логови при секоја посета и секоја активност може да се следи (кој пристапил, кога и сл.), а постои и ограничен број лица кои имаат пристап. На прашањето дали досега е извршен надзор на примената на вакви мерки од страна на операторите, Агенцијата за електронски комуникации не можеше ниту да потврди, ниту да негира. Операторите се должни и да ги уништат метаподатоците по истекот на периодот од 12 месеци за нивно задржување, **со исклучок на оние до коишто било пристапено и биле зачувани**. Последново значи дека за метаподатоците што се чуваат кај телекомуникациските оператори, а коишто се побарани од јавниот обвинител, не постои временско ограничување за нивното чување кај операторот.

Според Јавното обвинителство, преку метаподатоците обвинителството може да ги препознае движењето и контактите на осомничените, со што може да се изведат прецизни заклучоци околу нивната вмешаност во криминал. Сепак, до денес не е направена анализа на имплементацијата на законот, оправданоста и ефикасноста на неговата примена. Не постојат статистички докази што би помогнале во поддршка на тврдењето дека значењето на метаподатоците за борбата против криминалот е голема, наспроти масовното и големо негативно влијание врз приватноста и личните податоци на сите корисници на услугите за електронски комуникации, како и негативните финансиски импликации за операторите коишто се принудени да набавуваат опрема за задржување на метаподатоците на свој трошок.[113]

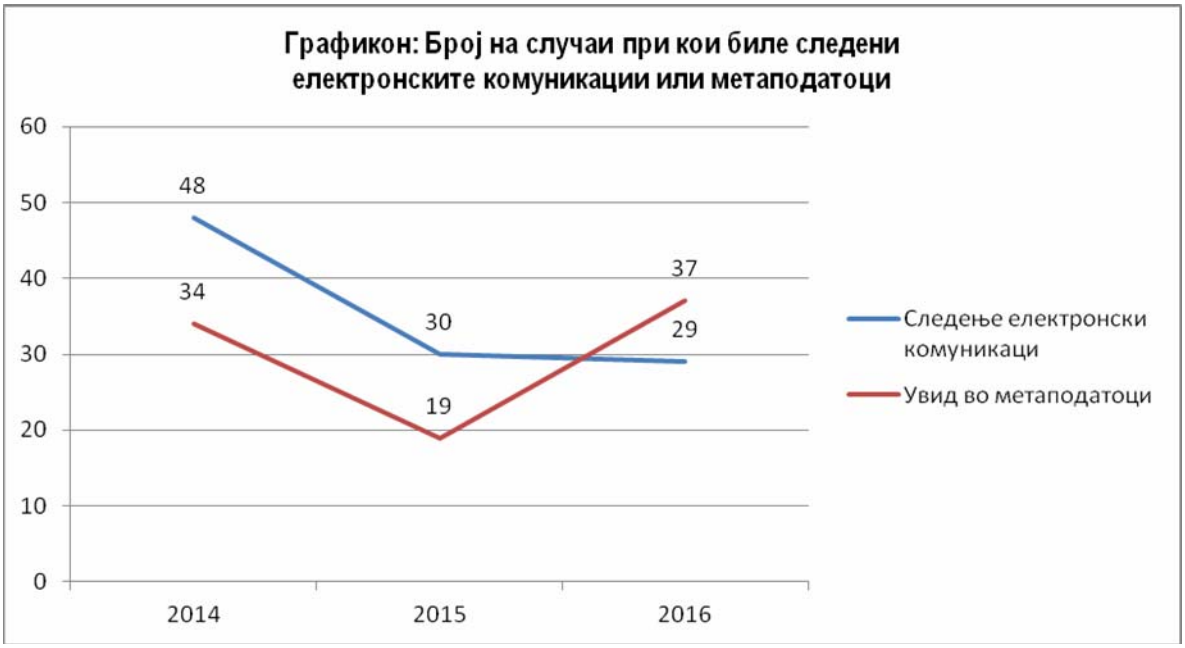
[113] Во Чешка, на пример, „Чешки Телеком“ добил средства од државата за да ја набави потребната опрема.

Анализа на извештаите на јавниот обвинител за следењето на комуникациите

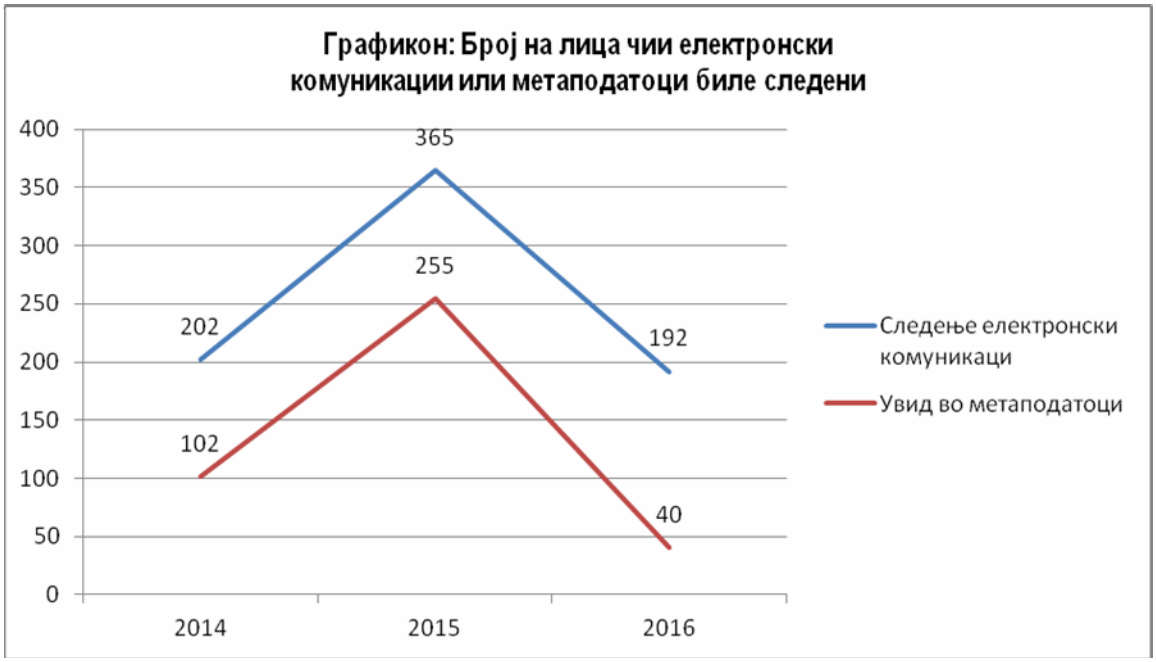
Согласно членот 271 од Законот за кривична постапка, Јавниот обвинител на Република Македонија еднаш годишно доставува извештај до Собранието на Република Македонија за примената на посебните истражни мерки во претходната календарска година. Анализата на извештаите на јавниот обвинител за следењето на комуникациите и примената на другите посебни истражни мерки за периодот 2014–2016 покажува дека Јавното обвинителство ги доставува до Собранието дури 7 месеци по истекот на годината на којашто се однесуваат – што е исклучително долг период за подготовка на извештај чијашто големина се движи од 10 до 16 страници. Извештаите не се објавуваат на веб-страницата на Јавното обвинителство, што е загрижувачко ниво на нетранспарентност. Дополнително, извештаите не ги содржат следниве елементи што се пропишани со закон:

- Ако посебната истражна мерка, односно следењето, не дале релевантни резултати за постапката, образложение за причините за тоа, диференцирано, според технички причини и други причини. Во случаите каде што следењето на електронските комуникации и метаподатоците било запрено без да се обезбедат докази за постапката, извештаите на Јавното обвинителство не нудат образложенија за причините.
- Трошоците што произлегуваат од примената на посебната истражна мерка. Извештаите за 2014 и 2015 година констатираат дека „не се произлезени трошоци за Јавното обвинителство или за судот со оглед дека Министерството за внатрешни работи директно ги спроведува овие мерки и за тоа не побарува трошоци“. Сепак, членот 271 од законот пропишува дека извештаите треба задолжително да содржат информација за трошоците од овие мерки, и притоа не ги ограничува трошоците само на оние што се настанати кај Јавното обвинителство или судовите. Неприкажувањето информации за трошоците на примената на овие мерки, ја спречува стручната јавност и пратениците во Собранието на Република Македонија да извлечат оценка за нивната ефикасност.

Во графиконот подолу се наведени податоци за периодот 2014–2016 г. содржани во ваквите извештаи, за две посебни истражни мерки: следење и снимање на телефонските и други електронски комуникации (во натамошниот текст: следење електронски комуникации) и увид во остварените телефонски и други електронски комуникации (во натамошниот текст: увид во метаподатоци за електронски комуникации).



Постојат неконзистентности во изнесените податоци во извештаите. На пример, во извештајот за 2016 е наведено дека мерката за следење електронски комуникации се вршела во 29 случаи, но при поделбата по времетраење се наведени вкупно 30 случаи, а при поделбата по исходот од постапката збирот е вкупно 31. Ако претпоставиме дека разликата кај поделбата по исходот од постапката се должи на фактот што во одредени случаи може да има повеќе од еден исход,[114] сепак не може да се утврди зошто се јавува еден случај повеќе во поделбата по времетраење на мерката, во однос на збирната бројка на декларирани случаи опфатени со оваа мерка.



[114] За различните лица опфатени со случајот.

За жал, извештаите нудат мошне оскудна анализа на изнесените бројки во нив. Во 2015 г. се јавува пад од 37% кај мерката за следење електронски комуникации и од 44% кај мерката за увид во метаподатоците. Ваквиот пад во бројот на случаи се јавува во година (2015) во која постои драстичен раст на бројот на лица (81%–150%) чии електронски комуникации или метаподатоци биле следени. Тоа се должи на 2 случаи со голем број опфатени лица во врска со терористичко загрозување на уставниот поредок и безбедноста (1 случај против 126 лица) и учество во странска војска, полиција, паравоени или параполициски формации (1 случај против 102 лица). Зголемувањето на бројот опфатени лица проследено со намалувањето на бројот на случаи, во извештајот само кусо се припишува на „фокусирање на Јавното обвинителство кон сузбивање поголеми и добро организирани криминални групи во коишто членуваат поголем број на лица“. Сепак, истата констатација се јавува и во извештајот за 2016 г., иако во таа година просечниот број на лица чии метаподатоци и електронски комуникации се следени е драстично намален на 1–7 лица по случај.

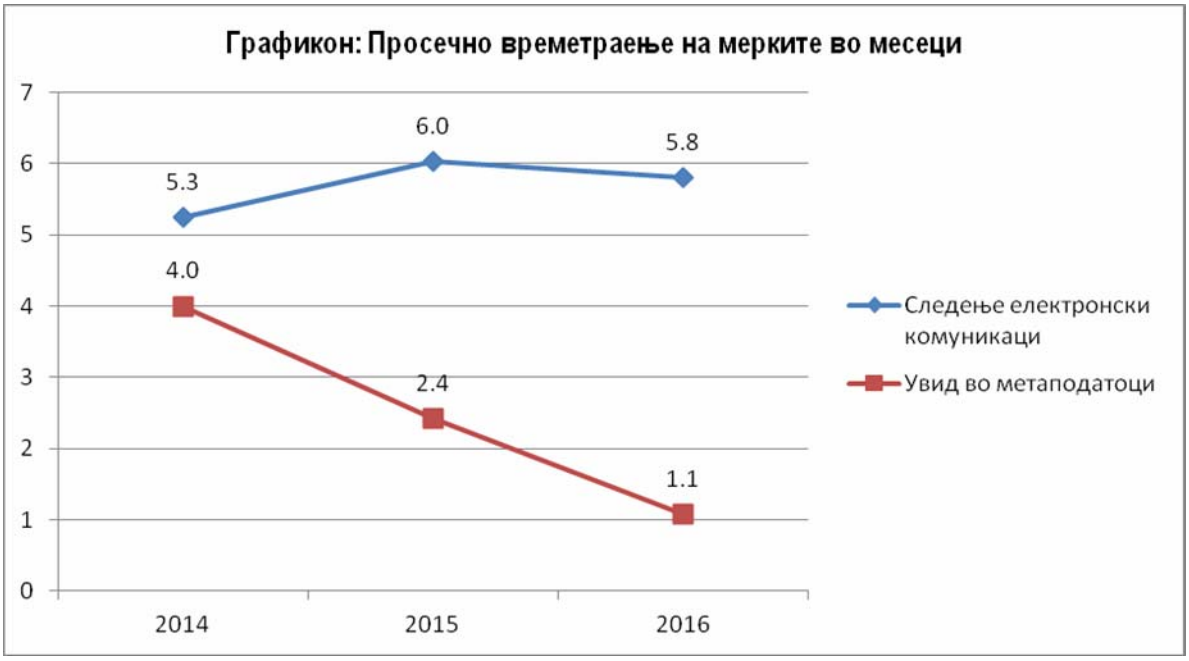
Законот за кривична постапка дефинира и можност за определување посебни истражни мерки спрема предметот на кривично дело (на пример телефонска линија или адреса за електронска пошта), во случај кога не се располага со сознание за идентитетот на сторителот на кривичното дело. Според статистиката објавена во Извештајот на Јавниот обвинител за примена на посебни истражни мерки во 2016 година, мерката „следење и снимање на телефонските и други електронски комуникации“ била применета спрема 74 предмети на кривично дело – телефонска линија којашто ја користи непознато лице во моментот додека се спроведува. Во извештаите за 2015 и 2014 година, пак, не се наведени одделни податоци за бројот на распишани посебни истражни мерки за предмети на кривично дело.

Следната табела дава преглед на најчестите сомневања за кривични дела во кои се применети двете посебни истражни мерки.

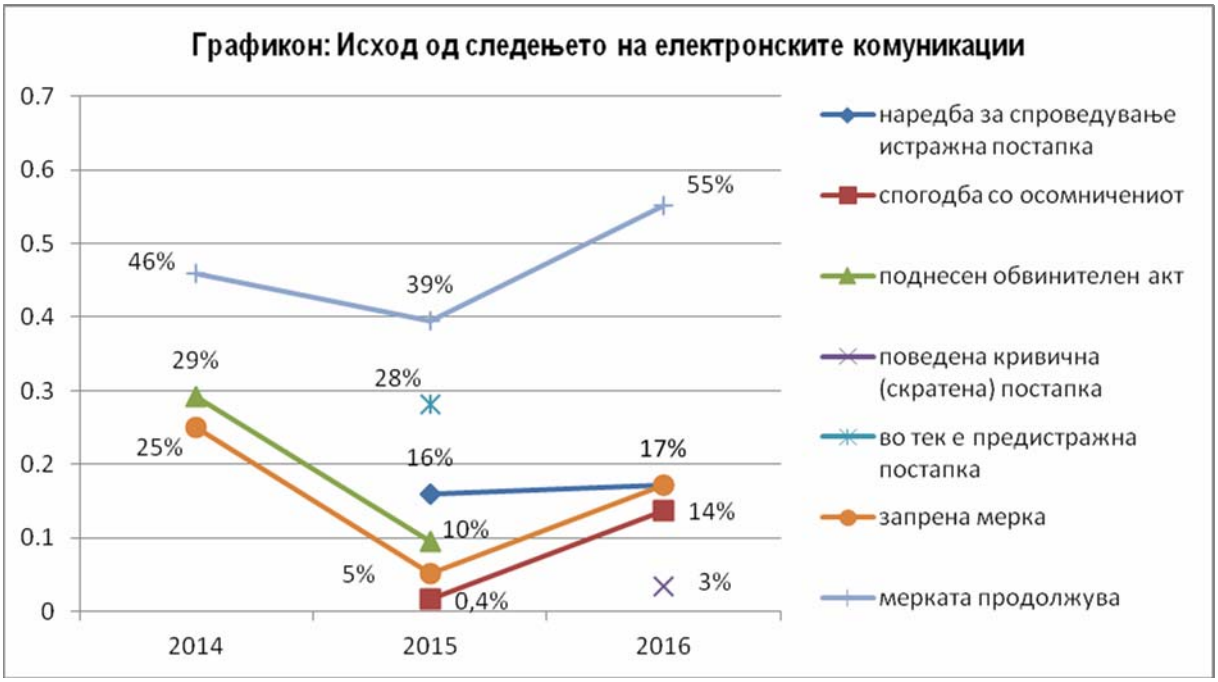
	Следење електронски комуникации	Увид во метаподатоци
2014	• Криумчарење мигранти (10 случаи) • Примање поткуп (5 случаи) • Злосторничко здружување (4 случаи)	• Неовластено производство и пуштање во промет наркотични дроги, психотропни супстанции и прекурзори (10 случаи) • Злоупотреба на службена должност и овластување (5 случаи) • Спречување на докажување (5 случаи)
2015	• Терористичко загрозување на уставниот поредок и безбедноста (1 случај против 126 лица) • Учество во странска војска, полиција, паравоени или параполициски формации (1 случај против 102 лица) • Тероризам (6 шест случаи против 36 лица)	• Терористичко загрозување на уставниот поредок и безбедноста (1 случај против 116 лица) • Учество во странска војска, полиција, паравоени или параполициски формации (1 случај против 102 лица) • Неовластено производство и пуштање во промет наркотични дроги, психотропни супстанции и прекурзори

		(8 случаи против 20 лица)
2016	• Тероризам (7 случаи) • Неовластено производство и пуштање во промет наркотични дроги, психотропни супстанции и прекурзори (6 случаи) • Учество во странска војска, полиција, паравоени или параполициски формации (2 случаи)	• Криумчарење мигранти (22 случаи) • Неовластено производство и пуштање во промет наркотични дроги, психотропни супстанции и прекурзори (9 случаи) • Злоупотреба на службената положба и овластување (2 случаи) • Организирање на група и поттикнување на извршување на делата трговија со луѓе, трговија со малолетно лице и криумчарење мигранти (2 случаи)

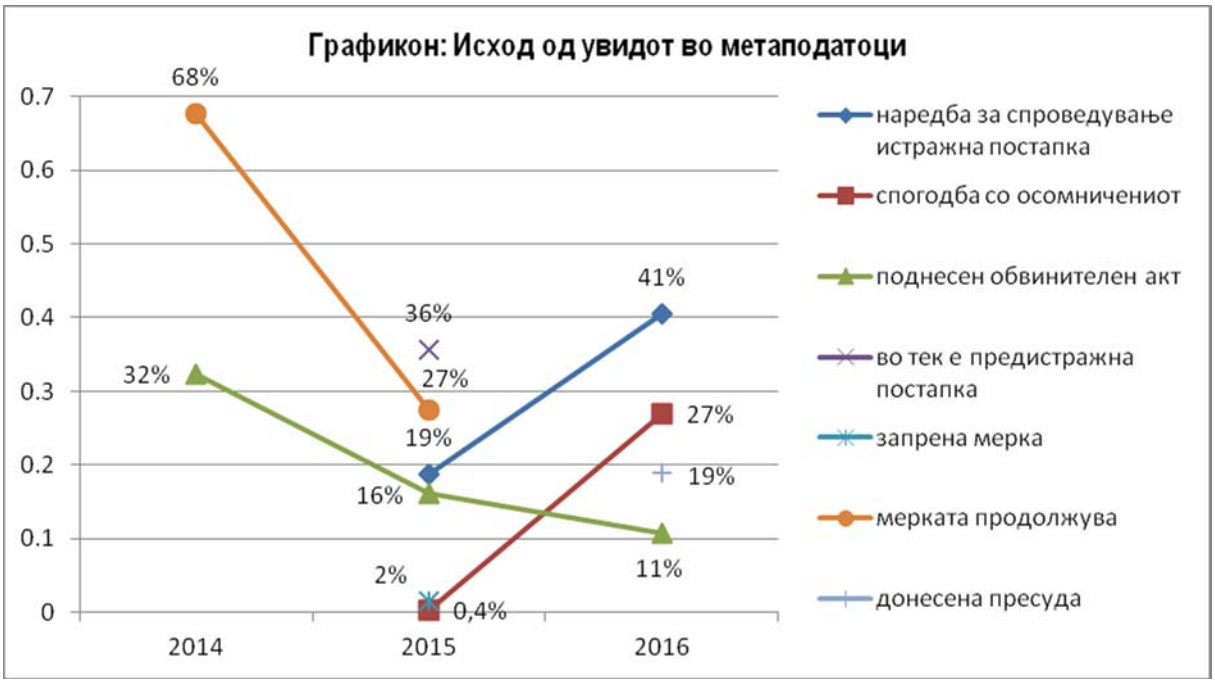
Просечното времетраење на мерката за следење електронски комуникации е 5,6 месеци, а на мерката за увид во метаподатоци е 2,5 месеци.



Дополнителна неконзистентност кај извештаите е што податоците за исходот од примената на мерката, во извештаите за 2014 и 2016 година се дадени по случаи, а во извештајот за 2015 година податоците се дадени по лица и нема податоци за исходи по случаи. Оваа и други неконзистентности ја отежнуваат споредбата на податоците од различните години, како и давањето оценка за ефективноста на мерките за следење на комуникациите и метаподатоците.



Кај мерката за увид во метаподатоци, во извештајот за 2016 година за еден случај во кој била применета мерката нема податок каков бил исходот, ниту колкаво било времетраењето на примена на мерката.



Изненадувачки е што во анализираните извештаи за трите години, само на едно место се наведува дека примената на една од двете анализирани мерки резултирала со собирање докази за 7 пресуди. Сепак, не е експлицитно наведено дали и колку од овие пресуди се осудителни, и дали истите се правосилни или не. Нејасно е дали во останатите години воопшто немало пресуди врз основа на докази собрани со двете анализирани посебни истражни мерки, или можеби само не бил следен таков показател. Отсуствуваат и примери на откриени или спречени тешки кривични дела со

примената на посебните истражни мерки, и поконкретно, со примена на следењето комуникации.

Извештаите не содржат податоци за тоа колку предлози за следење на комуникациите биле доставени до јавниот обвинител, со колку од нив обвинителот се согласил, колку сопствени иницијативи имал за следење на комуникациите, и за колку од поднесените барања била издадена наредба од судија, ниту пак индикација во колку наредби судиите целосно се согласиле со барањето, колку модифицирале (на пр. во поглед на лицата, или времетраењето), а колку отфрлиле.

Во извештаите исто така не е наведена статистика за тоа дали и колку барања имало за обезбедување метаподатоци до странски провајдери на интернет услуги, како што се *Twitter, Facebook, Gmail* и други.

Препораки

Дефинирање и опфат на следењето комуникации

• Следењето и увидот во метаподатоците за електронските комуникации да биде опфатено со дефиницијата за „следење на комуникациите“ во Законот за следење на комуникациите.

• Во законот за кривичната постапка да се прецизира разликата меѓу увидот во остварените телефонски и други електронски комуникации, како посебна истражна мерка, од обврската на операторите да доставуваат податоци до јавниот обвинител за остварените контакти во комуникацискиот сообраќај согласно членот 287 од истиот закон.

Основ за следење комуникации

• Да се преиспита оправданоста да се дозволува следење на комуникациите за толку широк опсег на кривични дела, врз основа на проценка дали нарушувањето на приватноста е пропорционално на тежината на кривичното дело за коешто станува збор и доказите што се очекува да се соберат со посебните истражни мерки, односно следењето комуникации. Едно можно решение е примената на ваквата мерка да се дозволува само за кривични дела за кои е предвидена минимална казна затвор од четири или повеќе години.

Барање за следење комуникации

• Да се воведе обврска судовите да треба да објавуваат на годишна основа колку барања добиле за следење на комуникациите, за колку лица се однесувале барањата, од кој орган се побарани, по која основа, а исто така и колку такви барања одбиле, а колку одобриле.

• Во барањето за следење на комуникациите да треба да се наведе и образложи основано сомневање за можно извршување или веќе извршено кривично дело, а не само основ за сомневање како многу низок степен на сомневање.

Наредба за следење на комуникациите

• Да се преиспита дали пропишаниот рок од 48 часа со членот 11 од Законот за кривичната постапка е доволен за судијата да може соодветно да го проучи барањето за следење на комуникациите и да одлучи дали ќе издаде соодветна наредба.

• Да се прецизираат порестриктивно условите во коишто е дозволено следење на комуникациите врз основа на усна наредба, согласно старото законско решение од Законот за следење на комуникациите. Имено, оваа можност беше дозволена само кога постои опасност од предизвикување смрт или тешка повреда, предизвикување

материјална штета на имот од големи размери, или бегство на сторител на кривично дело за коешто е пропишана казна доживотен затвор.

- За да може судијата да донесе информирана одлука за оправданоста на барањето за следење на комуникациите, како и да процени дали се исполнети условите за нарушување на приватноста и личните податоци, неопходно е да се воведе уште една страна во постапката што ќе ги застапува интересите на лицата чии комуникации се предлага да се следат. Оваа улога може да ја извршува панел на експерти, претставник на Дирекцијата за заштита на личните податоци или Народниот правобранител, како „застапник на јавниот интерес“.
- Во членот 257 од Законот за кривичната постапка, да се додаде уште еден задолжителен елемент во содржината на наредбата за следење на комуникациите што ја донесува судијата – називот на органот на чие барање се наредува следење на комуникациите.
- „Правото на приговор“ на одлуката на судијата по барањето за следење на комуникациите да не е достапно само на надлежните органи чии барања се одбиени, туку да биде применливо и за заштита на правата и интересите на лицата чии комуникации се предлага да се следат. Имено, законот за следење на комуникациите треба да се дополни со одредби со кои ќе се овозможи на соодветен ентитет, на пример Дирекцијата за заштита на личните податоци или Народниот правобранител, да учествува во постапката на издавање наредба за следење на комуникациите, и да има можност пред друга инстанца да ја оспори основаноста на евентуално издадената наредба од судија во претходна постапка.

Времетраење на следењето комуникации

- Да се преиспита оправданоста на пропишаните долги максимални рокови за следење на комуникациите (сегашниот првичен рок од максимални 4 месеци со можност за продолжување до 14 месеци, наспроти поранешните 1 месец со можност за продолжување до 12 месеци од старата верзија на Законот за следење на комуникациите).
- Да се дополни членот 257 од Законот за кривичната постапка со цел меѓу задолжителните елементи на наредбата за следење на комуникациите да се вклучи обврската органот што го спроведува следењето да ја запре мерката кога ќе се постигнат целите заради кои се определени посебните истражни мерки или ќе престанат да постојат основите заради кои се одобрени.

Оперативно спроведување на следењето комуникации

- Законски да се раздвојат надлежноста и прописите за следење на комуникациите при кривичните истраги, од оние од безбедносен и разузнавачки карактер.
- Да се оневозможи директниот пристап до содржината на комуникациите од страна на службите, односно надлежните органи претходно да треба да го известат

операторот и да достават судски налог за следење, а потоа операторот да го овозможи пристапот до комуникациите на опфатените лица.

- Да се пропише евиденција на следењето на комуникациите кај операторите, кон којашто ќе имаат пристап надзорните органи. Меѓу другото, да се евидентира кои вработени кај операторот пристапиле кон податоците за содржината на комуникациите и метаподатоците, кои вработени имаат право на пристап, и кога пристапиле. Да се практикуваат строги казни за вработените во операторите кои неовластено ќе пристапат или ќе овозможат пристап до метаподатоците или до содржината на комуникациите.
- Да се зајакне внатрешната контрола во МВР за да врши контрола и на случаи во коишто е злоупотребено овластувањето за следење на комуникациите.

Употреба на сознанијата од следењето на комуникациите

- Да се дополни членот 258 од Законот за кривичната постапка за извештајот на правосудната полиција за следењето комуникации што го доставува до јавниот обвинител, задолжително да содржи и број на телефонска или друга корисничка линија или адреса за електронска пошта (или друг идентификатор) што се следеле.
- Да се преиспитаат членовите 255 и 263 од Законот за кривичната постапка за да се осигури дека собраните податоци од следењето на комуникациите се однесуваат на намената за којашто е издадена наредбата и се собрани податоците. Имено, таа намена е собирање податоци за однапред одредени кривични дела и лица – или утврдување на лица кои користат телефонска, друга линија или мејл адреса која е предмет на кривично дело. Оттука, доколку со следењето комуникации се стекнат сознанија коишто имплицираат други лица во кривичните дела, или со коишто се утврдуваат основи за други кривични дела од оние на коишто се однесува постојната наредба за следење на комуникациите, да биде потребно издавање нова наредба од судијата за да продолжи следењето комуникации и записите од тие комуникации да можат да се користат на суд. Образложението што би се поднесувало до судијата за таквото барање за проширен опфат на мерката не би требало да се заснова на снимени комуникации што ја надминуваат наредбата врз чија основа се собрани.
- Да се предвиди претпазливост за посебните категории на лични податоци (онака како што се утврдени со Законот за заштита на личните податоци), односно при следењето комуникации да се исклучат или избришат искази поврзани со овие категории лични податоци.

Известување на лицата чии комуникации се следени, право на оспорување на следените комуникации, право на приговор и надомест на штета

- Со законски измени да се воведе обврска засегнатите лица да се известат за посебните истражни мерки по нивното прекинување. Најмалку следните информации да се достапни до лицето чии лични податоци се собрани: идентитетот на контролорот, постоењето на операцијата за собирање, како и целта на операцијата, правото да поднесе жалба и правото да побара пристап до собраните податоци, но и

да побара замрзнување и рестрикција на понатамошно обработување. Правото на пристап до овие информации да може да се дерогира само кога може да се докаже дека ќе доведе до попречување или прејудицирање на кривичното гонење, но такво дерогирање да може да направи само независно тело.

- Да се воведат делотворни правни лекови кои можат да се користуваат во случаите кога одредено лице смета дека му се прекршени правата со следење на комуникациите од страна на надлежните органи. Меѓу другото, лицата чии комуникации се следат да имаат законска можност на приговор до Дирекцијата за заштита на личните податоци за употребата на нивните лични податоци. Непрофитни организации кои дејствуваат во сферата на заштита на приватноста и личните податоци да добијат законско право да можат да поднесуваат приговори и да ги застапуваат засегнатите лица од следењето комуникации.

Заштита, чување и уништување на следените комуникации

Да се зајакнат законските одредби за безбедност на собраните податоци од следењето на комуникациите, како и за нивно уништување во случаите кога веќе не се потребни заради целта за која биле собирани. Во законот за следење на комуникациите да се пропишат многу подетални мерки за безбедност при обработката на податоците, согласно предвиденото со Директивата 2016/680 за заштита на податоци во полицијата и кривичното право. Меѓу другото, да се воведе принципот на минимизирање на податоците при следењето на комуникациите, вклучително и псевдоанонимизацијата – обработка на податоците на начин каде што личните податоци повеќе не можат да се припишат на конкретно лице без употребата на дополнителни информации што се чуваат одделно и се предмет на технички и организациски безбедносни мерки. Да се обезбеди дека при уништувањето на податоците ќе бидат уништени оригиналниот запис и сите копии во сите институции вклучени во следењето.

- Кога како резултат на неовластен пристап ќе настане повреда на собраните лични податоци од следењето на комуникациите, надлежниот орган веднаш да мора да го информира надзорниот орган за заштита на личните податоци, како и лицата чии лични податоци биле загрозени.

Специфики на следење на комуникациите заради заштита на интересите на безбедноста и одбраната на земјата

- Задолжително да се врши безбедносна проценка пред да се одлучи дали треба да се побара следење на нечии комуникации заради заштита на интересите на безбедноста и одбраната на земјата.

Надзор и контрола над следењето комуникации

- Да се донесе регулатива што ќе обезбеди ефикасно спроведување постапка за добивање безбедносен сертификат за членовите на надзорните собранискиот комисии.

Пратениците кои нема да добијат ваков сертификат во разумен рок да немаат можност да членуваат во овие комисии.

- Сите податоци за пристап кон системот на следење на комуникациите да се евидентираат.
- Да се избрише одредбата од Законот за следење на комуникациите според кој соодветната собраниска комисија треба да донесе посебна одлука за надзор. Да се обезбеди можност за ненајавен надзор да има секој член на надлежните собранискиот комисии, при што би имале пристап и до агрегирани податоци за следењето и до имињата на лицата и основите по кои се следат. Имињата да не бидат достапни за вршителите на надзорот единствено кога основот за следење е поврзан со заштита на интересите на безбедноста и одбраната на земјата.
- Собранискиите комисии да имаат на располагање стручни лица што ќе им помагаат со техничките и правните аспекти на надзорот, како и вршењето увид на лице место.
- Да се воведе и граѓанска комисија за надзор над следењето на комуникациите, што ќе ја именува Собранието од редот на експерти и претставници на граѓанското општество, врз основа на отворена, транспарентна и објективна постапка за номинирање и избор на членови.
- Надзорните тела да вршат надзор над законитоста и ефективноста на следењето комуникации, во сите негови фази: изборот на мерки за следење, собирањето податоци, но и при нивната анализа.
- Дирекцијата за заштита на личните податоци да добие надзорна улога и во однос на податоците од следењето на комуникациите од надлежните органи, и да биде задолжена за следење на примената на правото за заштита на податоците и во овие случаи.
- Извештаите на јавниот обвинител за примената на посебните истражни мерки да ги содржат сите законски пропишани податоци (вклучително и оние за трошоците и образложение во случаите кога мерките не ги дале очекуваните резултати) прикажани на конзистентен начин, како и податоци за тоа колку предлози за следење на комуникациите биле доставени до јавниот обвинител, со колку од нив обвинителот се согласил, колку сопствени иницијативи имал за следење на комуникациите, и за колку од поднесените барања била издадена наредба од судија, како и показатели во колку наредби судиите целосно се согласиле со барањето, колку модифицирале (на пр. во поглед на лицата, или времетраењето), а колку отфрлиле. Во извештаите да се наведува и статистика за тоа дали и колку барања имало за обезбедување метаподатоци до странски провајдери на интернет услуги, како што се *Twitter, Facebook, Gmail* и други, како и бројот на следените предмети на кривично дело и бројот на уништени записи од посебните истражни мерки. Извештаите да се објавуваат на веб-страницата на Јавното обвинителство најдоцна до крајот на февруари во тековната година за претходната година.
- Да се пропише обврска и за операторите на услугите за електронски комуникации да објавуваат годишни извештаи за бројот на наредби што ги добиле за следење на телефонски или други линии, и пристап до метаподатоци, за кои дела и за колку лица. Овие извештаи да бидат достапни во форма на агрегирани податоци на нивните веб-страници.

Безбедност кај операторите на јавни електронски комуникациски мрежи и давателите на услуги

• Давателите на електронски комуникациски услуги треба да преземат соодветни технички и организациски мерки за да обезбедат дека пристап до личните податоци имаат само овластени лица, да ги заштитат личните податоци од кој било незаконски или неовластен облик на обработка, и да обезбедат примена на политика за безбедност при обработката на личните податоци. Во согласност со правото на ЕУ, давателите на услуги да имаат обврска за дизајн насочен кон приватност, т.е. техничките и организациските мерки што обезбедуваат заштита на личните податоци да ги предвидат уште при дизајнот на системите, а не отпосле.

• Метаподатоците да се користат само за цели на наплата и за техничко овозможување на услугата, а кога повеќе не се потребни за овие намени, задолжително да се избришат или да се анонимизираат.

• При пристапот до метаподатоците или при обезбедувањето на содржината на комуникациите од страна на операторите за цели на законско следење на комуникациите, задолжително да се прави двојна верификација, односно пристапот да биде овозможен само преку најавување на минимум две овластени лица од операторот.

• Да се преиспита ефективноста и функционалноста на членот 167 од Законот за електронските комуникации за известување од страна на операторите на Агенцијата за електронските комуникации, Дирекцијата за заштита на личните податоци и претплатниците за нарушување на безбедноста на личните податоци.

• Надлежните органи да прават редовни контроли кај операторите за пристапот и обработката на податоците за комуникациски сообраќај и податоците за локација на претплатниците.

Казнени одредби за надлежните органи за следењето комуникации

• Во законот за следењето на комуникациите да се воведат казнени одредби за надлежните органи и одговорните лица во нив.

Задржување метаподатоци

• Да се укинат членовите 176–178 од Законот за електронски комуникации што го пропишуваат задржувањето метаподатоци поради неоправданоста од масовноста на задржувањето на ваквите податоци и поради укинување од Европскиот суд на правдата на Директивата 2006/24/ЕЗ којашто е транспонирана во овој закон.

• Да се измени Законот за следење на комуникациите во делот на дефинирање на следењето на комуникациите што треба да вклучи и следење, односно увид во метаподатоци.

• Следењето метаподатоци да се врши по барање на јавниот обвинител, но соодветната наредба за тоа да ја издава судија во претходна постапка.

Едукација

- Да се спроведе кампања за подигнување на свеста на граѓаните околу ризиците при електронските комуникации, како и нивните права за заштита на приватноста и личните податоци при комуникацијата. Според Агенцијата на ЕУ за темелни права, потребно е информирање и потсетување за поединците да бидат свесни за нивните права за заштита на податоците и достапните правни лекови[115].
- ДЗЛП да промовира подигнување на јавната свест и разбирање на ризиците, правилата, начините на заштита во однос на електронските комуникации и следењето на комуникациите; да ги советува во согласност со правото на ЕУ Собранието, обвинителството, Министерството за внатрешни работи, телекомуникациските оператори и други ентитети што имаат врска со следењето на комуникациите.
- Да се јакне стручноста и етиката кај јавните обвинители, судиите, да се обезбеди надворешна поддршка за имплементација на стандарди, како и за обука и специјализација на обвинителите и судиите во областа на следењето на комуникациите, приватноста и заштитата на личните податоци.

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

АНЕКС I. СПИСОК НА ПРЕТСТАВНИЦИ НА ИНСТИТУЦИИ И ЕКСПЕРТИ СО КОИ БЕА СПРОВЕДЕНИ ИНТЕРВЈУА[116]

- Претставник на Дирекцијата за заштита на лични податоци
- Претставник на Агенцијата за електронски комуникации
- Претставник на Вишото јавно обвинителство
- Судија на Уставниот суд на Република Македонија
- Заменик народен правобранител на Република Македонија
- Поранешен Претседател на Собранието на Република Македонија и член на собраниска комисија за надзор на следењето на комуникациите
- Поранешен министер за внатрешни работи и член на собраниска комисија за надзор на следењето на комуникациите
- Поранешен дипломат и функционер во Министерството за внатрешни работа
- Поранешен функционер во Дирекцијата за безбедност и контраразузнавање
- Претставници на „Македонски Телеком“
- Професор на Факултетот за безбедност и поранешен заменик министер за внатрешни работи
- Експерт за заштита на лични податоци и приватност
- Претставници на граѓански организации – експерти во областа

[116] При спроведувањето на интервјуата, на сите учесници им беше гарантирана нивната анонимност, па затоа во списокот се дадени само институциите што
ги претставуваат, а во некои случаи и нивните поранешни функции

АНЕКС II. БИБЛИОГРАФИЈА

- Агенцијата на Европската Унија за основните права. FRA (2015), Fundamental rights: challenges and achievements in 2014, Luxembourg, Publications Office.
- Глобално заладување – влијание на масовното следење врз меѓународните писатели, Резултати од меѓународно истражување на писатели, Американски ПЕН центар, 2015.
- Директива 2002/58/ЕЗ на Европскиот парламент и Советот од 12.07.2002, О. Ј. 2002 L 201.
- Директива 2006/24/ЕЗ за задржување податоци. Достапно на: http://eur-lex. europa.eu/LexUriServ/LexUriServ. do? uri=OJ: L: 2006: 105: 0054: 0063: EN: PDF
- Директива 2006/24/ЕЗ за задржување податоци. Достапно на http://eur-lex. europa.eu/LexUriServ/LexUriServ. do? uri=COM: 2011: 0225: FIN: en: PDF
- Директива 2016/680 за заштита на податоци во полицијата и кривичното право. Достапно на: http://eur-lex. europa.eu/legal-content/EN/TXT/? uri=CELEX%3A32016L0680
- Дирекција за заштита на личните податоци, Годишен извештај за 2016 година. Достапен на: https://dzlp. mk/sites/default/files/u4/godisen_izvestaj_dzlp_2016.pdf
- Договор за функционирањето на Европската Унија 2012/С 326/01
- Европска комисија. Изјава во однос на националните закони за задржување податоци, 16.09.2015. Достапно на: http://europa. eu/rapid/press-release_STATEMENT-15-5654_en. htm
- Европска конвенција за човекови права
- Европски дигитални права (European Digital Rights). Германскиот федерален уставен суд го отфрли законот за задржување податоци: https://edri. org/edrigramnumber8-5german-decision-data-retention-unconstitutional/
- Закон за електронски комуникации на Естонија. Достапен на: https://www. riigiteataja.ee/en/eli/501042015003/consolide
- Закон за електронски комуникации на Хрватска. Достапен на: https://www. zakon.hr/z/182/Zakon-o-elektroni%C4%8Dkim-komunikacijama
- Закон за електронските комуникации (ЗЕК), Службен Весник на Република Македонија број 39/14, 188/14 и 44/15.
- Закон за електронските комуникации, „Службен весник на Република Македонија“ број 39/2014, 188/2014 и 44/2015.
- Закон за изменување и дополнување на Законот за електронските комуникации („Службен весник на Република Македонија“, бр. 83/2010)
- Закон за изменување и дополнување на Законот за следење на комуникациите, „Службен весник на Република Македонија“ бр. 116/2012
- Закон за кривичната постапка, „Службен весник на Република Македонија” број 150/2010, 100/2012 и 142/2016
- Закон за следење на комуникациите, „Службен весник на Република Македонија“ бр. 121/2006, 110/2008 и 116/2012.
- Извештај за активностите на Специјалното јавно обвинителство за периодот од 15.09.2016 до 15.03.2017, достапен на http://www. jonsk.mk/wp-content/uploads/2017/03/6-MESECEN-IZVESTAJ. pdf;

• Извештај за активностите на Специјалното јавно обвинителство за периодот од 15.09.2015 до 15.03.2016 достапен на http://www. jonsk.mk/wp-content/uploads/2016/03/izvestaj-konecen-zaklucen. docx;

• Извештај за транспарентност на "Дојче Телеком" за Австрија. Достапен на: https://www. telekom.com/en/corporate-responsibility/data-protection-data-security/news/austria-363540

• Извештај за транспарентност на "Дојче Телеком" за Германија. Достапен на: https://www. telekom.com/en/corporate-responsibility/data-protection-data-security/news/germany-363566

• Извештај за транспарентност на "Дојче Телеком" за Република Чешка. Достапен на: https://www. telekom.com/en/corporate-responsibility/data-protection-data-security/news/czech-republic-363568

• Извештај на "Дојче Телеком" за приватност и безбедност на податоците, 2015. Достапен на: https://www. telekom.com/resource/blob/323750/a7b17936956c92c23c07f433084e21d6/dl-report-datasecurity-2015-data. pdf

• Извештај од јавната расправа на Националниот совет за евроинтеграции по работната верзија на Предлог-законот за изменување и дополнување на Законот за следење на комуникациите, Собрание на Република Македонија, 16.07.2012. Достапно на: https://www. sobranie.mk/WBStorage/Files/JRSledenjenakomunikacii. pdf

• Институт за информациско право при Универзитетот во Амстердам, Десет стандарди за надзор и транспарентност на националните разузнавачки служби, 2015.

• Итни реформски приоритети за Македонија, јуни 2015. Достапно на: https://eeas. europa.eu/sites/eeas/files/urgent_reform_priorities_en. pdf

• Како функционирала шемата за прислушување во „Пуч"?", Алфа ТВ, 26.02.2015, достапно на http://www. alfa.mk/News. aspx? id=90130.

• Канцеларија на ОН за дрога и криминал. Практики за електронско следење во истражувањето на сериозен и организиран криминал. Виена, 2009. Достапно на: https://www. unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance. pdf

• Конвенција за заштита на лица во однос на автоматската обработка на лични податоци на Совет на Европа

• Конвенција на Обединетите Нации против транснационален организиран криминал, достапно на: https://www. unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e. pdf

• Констанца ди Франческо Маеса, Рамнотежа меѓу безбедноста и заштитата на основните права – анализа на Директивата 2016/680 за заштита на податоци во полицискиот и правосудниот сектор и на Директивата 2016/681 за употребата на записите за имиња на патници (ПНР), 2016. Достапно на: 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/

• Кривичен законик, „Службен весник на Република Македонија" број 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.

- Мислење на европскиот супервизор за заштита на податоци, 22 јули 2016
- Одлука на Уставен суд, у. број 139/2010-0-1 од 15.12.2010, достапна на: http://www. ustavensud.mk/domino/WEBSUD. nsf/ffc0feee91d7bd9ac1256d280038c474/7119424dde39fdadc1257809002db948? OpenDocument
- Откритија на Едвард Сноуден. Достапно на: https://edwardsnowden. com/revelations/
- Откритија објавени на Викиликс. Достапно на: https://wikileaks. org/
- Оценка и препораки на групата високи експерти за системските прашања од владеење на правото 2017. Достапно на: https://ec. europa.eu/neighbourhood-enlargement/sites/near/files/2017.09.14_seg_report_on_systemic_rol_issues_for_publication. pdf
- План 3-6-9 на Владата на Република Македонија, достапен на: http://vlada. mk/sites/default/files/programa/2017-2020/Plan%203-6-9%20MKD. pdf
- Повелба на Европската Унија за основните права
- Повелба на Европската Унија за основните права, 2012 O. J. (C 326) 391
- Политички „бомби“, достапни на: http://vistinomer. mk/site-prislushuvani-razgovori-objaveni-od-opozitsijata-video-audio-transkripti/.
- Предлог регулатива на Европскиот Парламент и Совет во однос на почитувањето на приватноста и заштитата на личните податоци. Достапно на: http://eur-lex. europa.eu/legal-content/EN/ALL/? uri=COM: 2017: 0010: FIN.
- Препорака на Советот на Европа за користење на посебни истражни мерки, достапно на: https://wcd. coe.int/ViewDoc. jsp? id=849269&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.
- Препораки на групата високи експерти за системските прашања од владеење на правото 2015. Достапно на: https://ec. europa.eu/neighbourhood-enlargement/sites/near/files/news_corner/news/news-files/20150619_recommendations_of_the_senior_experts_group. pdf
- Пресуда на Европскиот суд на правдата. Достапна на: https://curia. europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en. pdf
- Пресуда на Европскиот суд на правдата: ECtHR, Klass et al, 6 септември 1978, пас. 41.
- Пресуда на Европскиот суд на правдата: ECtHR, Malone v. the United Kingdom, 2 август 1984, пас. 84.
- Пресуда на Европскиот суд на правдата: ECtHR, S. and Marper v. the UK, 4 декември 2008, пас. 101.
- Пресуда на Судот на правдата на Европската Унија (CJEU), Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, 9 ноември 2010, пас. 81.
- Пресуда: CJEU, Digital Rights Ireland v. Seitlinger and Others, C-293/12, 8 April 2014.
- Регулатива (ЕУ) 2016/679 на Европскиот парламент и на Советот за заштита на поединците во врска со обработката на личните податоци и слободното движење на

такви податоци (Општа регулатива за заштита на податоците), OJ L 119, 27.04.2016, достапна на: http://eur-lex. europa.eu/legal-content/EN/TXT/? uri=CELEX%3A32016R0679

- СЈО конечно влезе во Телеком“, SDK. MK, 24.04.2017, достапно на http://sdk. mk/index. php/makedonija/sjo-konechno-vleze-vo-telekom/.
- Список за проверка на владеењето на правото. Венецијанска комисија
- Став на ЕУ во однос на пресудата на ЕСП за поништување на Директивата: http://ec. europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp220_en. pdf
- Electronic Frontier Foundation и Article 19, Неопходно и пропорционално – меѓународни принципи за примена на правната рамка за човековите права при следењето комуникации, 2014.


152
166
180
193
207