МЕТАМОРФОЗИС

Фондација за интернет и општество

Проект „Слобода на Интернет“

Прелиминарен извештај за состојбите поврзани со примената на законските рамки поврзани со прислушување

Автори
Александар Николов
Душко Тодороски
Весна Радиновска

Скопје, 2018

Содржина

Вовед

Цел на овој извештај е да се даде преглед на состојбите поврзани со примената на законските рамки поврзани со прислушувањето во Република Македонија (РМ) во изминатиот и тековниот период, до 31 декември 2017 година.

Овој извештај дел од поширок извештај кој се однесува на состојбите со слободата на интернет, со фокус на слободата на изразување, приватноста и безбеденоста во дигиталниот свет, како дел од проектот „Слобода на интернет“ кој го спроведува Фондацијата „Метаморфозис“ во рамки на регионалниот проект „Интернет слобода во Источна Европа и Евроазија“ на Американска адвокатска комора (АБА РОЛИ).

Содржината на текстот е единствена одговорност на авторите и на ниту еден начин не може да се смета дека ги одразува гледиштата на Фондацијата „Метаморфозис“ и на АБА РОЛИ.

Сите материјали и извештаи од проектот се достапни на веб-локацијата на Фондацијата „Метаморфозис“ www.metamorphosis.org.mk.

Законски рамки поврзани со прислушување

Меѓународни правни рамки поврзани со областа

Во рамки на системот на ООН

Универзалната Декларација за Човековите права[1] на Организацијата на Обединетите Нации пропишува дека никој не смее да биде изложен на произволно мешање во приватниот живот, семејството, домот или преписката, ниту на напади врз честа и угледот. Секој има право на заштита од законот против вакво мешање или напад во приватноста.[2]

Меѓународниот пакт за граѓански и политички права[3], усвоен од Генералното собрание на Обединетите Нации во 1966 година, ја потврдува потребата за заштита на приватноста согласно одредбите во Универзалната декларација.[4]

Конвенцијата на Обединетите нации за заштита на детето[5] забранува арбитрарно или незаконско мешање во приватноста, семејството, домот или преписката на детето, и пропишува обврска за законска заштита од такво мешање.[6]

Извештајот на Канцеларијата на Високиот Комесар за човекови права на ООН за правото на приватност во дигиталното време[7] од 2014 г. се осврнува на потребата од заштита и промоција на правото на приватност во контекст на домашно и меѓународно следење на дигиталните комуникации и собирање на лични податоци, вклучително и на масовно ниво. По разгледувањето на извештајот, Советот за човекови права одлучи да воспостави и специјален известувач за правото на приватност, кој е задолжен да собира информации, да проучува трендови во различни држави, да идентификува можни пречки во примената на ова право и да известува за прекршувања на приватноста.

[1] Достапно на: www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf
[2] Член 12 од Декларацијата.
[3] Достапно на: http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx
[4] Член 17 од Пактот.
[5] Достапно на: http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx
[6] Член 16 од Конвенцијата.
[7] Достапно на: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

Во рамки на системот на Советот на Европа

Според Европската конвенција за човекови права[8] „секој човек има право на почитување на неговиот приватен и семеен живот, домот и преписката“. Концептите на приватен живот и преписка ги вклучуваат и телефонските и телекомуникациските податоци.[9] 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.

Конвенцијата за заштита на лица во однос на автоматската обработка на личните податоци[10] на Советот на Европа, којашто е ратификувана и од страна на Република Македонија 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. 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. 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.

Венецијанската комисија има утврдено Список за проверка на владеењето на правото[11] според кој 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.[12] Покрај тоа, потребно е да постојат делотворни правни лекови што можат да се користуваат 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.

Европскиот суд за човекови права (ЕСЧП) има мандат да испитува дали постои потреба и оправданост за вмешување на националните власти во приватниот живот или преписката на

[8] Совет на Европа. Европска конвенција за човекови права. Достапно на: http://www.echr.coe.int/Documents/Convention_ENG.pdf
[9] Подгледнете ECtHR, Klass et al, 6 септември 1978, пас. 41.
[10] Достапно на: https://rm.coe.int/1680078b37
[11] Достапно на: http://www.venice.coe.int/images/SITE%20IMAGES/Publications/Rule_of_Law_Check_List.pdf
[12] Метаподатоци се податоците за тоа со кого, кога и колку често комуницираме, како и со кои уреди и од кои локации.

граѓаните во демократско општество. Судот е надлежен да процени дали ваквото прислушување било спроведено во согласност со закон, со легитимна цел, како и дали се задржало на целта која е предвидена или било злоупотребено за други цели.

Во рамки на системот на Европската Унија (ЕУ)

Според Договорот за функционирање на Европската Унија[13], секој има право на заштита на личните податоци.

Повелбата на Европската Унија за основните права[14] 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.

Директивата[15] за обработката на личните податоци и заштитата на приватноста во електронскиот комуникациски сектор, 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.

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 телекомуникациискиот 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.

Во 2017 година, Европската комисија објави нацрт-регулатива за е-приватност[16] со која 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

[13] Договор за функционирање на Европската Унија 2012/C 326/01
[14] Повелба на Европската унија за основните права, 2012 O.J. (C 326) 391
[15] Директива 2002/58/ЕЗ на Европскиот парламент и Советот од 12.07.2002, O.J. 2002 L 201.
[16] Предлог за регулатива за е-приватност**, достапно на:** http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2017:0010:FIN.

(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.

Во 2016 година, ЕУ усвои Општа регулатива за заштита на податоците[17] (ОРЗП) и Директива 2016/680 за заштита на податоци во полицијата и кривичното право[18] – којашто се однесува на заштита на податоците поврзани со кривични дела и кривични казни. ОРЗП ќе се применува од 25 мај 2018 година.

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.

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. 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.[19] 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*.

Во оваа сфера е значајно да се спомене и фактот дека во 2014 г., Големиот судски совет на **Судот на правдата на Европската Унија (ЕСП)** ја поништи 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,[20] беше создадена со цел да овозможи метаподатоците да бидат задржани за истрага, препознавање и гонење на сериозни кривични дела во период од 6 месеци до 2 години. 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. И покрај тоа што Судот оцени дека директивата спроведува легитимна цел во борбата против тешкиот криминал и во заштитата на националната

[17] 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

[18] Директива 2016/680 на ЕУ за заштита на физичките лица во поглед на обработката на лични податоци од надлежните органи со цел превенирање, истрага, откривање и гонење на сторители на кривични дела или извршување на изречени казни и на слободно пренесување на таквите податоци, со која се укинува Рамковната одлука на Советот 2008/977/ЈНА, OJ L 119, 4.5.2016, достапно на: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680

[19] Член 4, став 1.

[20] Директива за задржување податоци.

безбедност, утврди дека Директивата ги прекршува правото на приватен живот и правото на заштита на личните податоци на поединците, гарантирани со членовите 7 и 8 од Повелбата на Европската Унија за основните права.

Усогласеност на националната регулатива со стандардите на ЕУ

Нашето законодавство е само делумно усогласено со меѓународното право во областа. Имено, фактот што телекомуникациските оператори се обврзани во реално време да прават копија од целокупниот телекомуникациски сообраќај на сите граѓани и да го пренасочуваат кон МВР, е непропорционално и неселективно нарушување на приватноста и создава непотребен ризик за заштитата на личните податоци.

Дополнително, нашата регулатива не пропишува соодветни безбедносни мерки кои би обезбедиле 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 – нешто што е наложено и со Конвенцијата за заштита на лица во однос на автоматската обработка на личните податоци на Советот на Европа.

Истото важи и за законската обврска на операторите една година да ги зачувуваат метаподатоците за сите претплатници, и на барање на јавниот обвинител да ги предадат. Дополнителен проблем во врска со задржаните метаподатоците е што истите можат да се користат од јавниот обвинител без постоење на судски наредба, што упатува дека не постојат процедурални контроли, вклучително и давање овластување од судија или независно тело за следење и користење на метаподатоците. Задржувањето на метаподатоците во нашиот систем беше воведено поради усогласување со Директива на ЕУ, која во меѓувреме беше поништена од Судот на правдата на Европската Унија поради прекршување на правото на приватен живот и правото на заштита на личните податоци на поединците, гарантирани со членовите 7 и 8 од Повелбата на Европската Унија за основните права.[21]

Оттука, нашето законодавство не е целосно усогласено и со измените на правото ЕУ во оваа сфера. Покрај спомнатиот проблемот со метаподатоците, значајно е да се потенцира дека во Македонија не е започнато усогласување со новата Директива на ЕУ за заштита на податоци во полицијата и кривичното право[22], односно нашето законодавство не ги пропишува сите механизми за заштита на личните податоци содржани во Директивата, ниту пак соодветно го ограничува собирањето на податоците 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.[23] Нашата законска регулатива недоволно детално и несоодветно го регулира уништувањето на зачуваните податоци на граѓаните од институциите, ниту пак правото на приговор или надомест на штета на оние чие комуникации биле следени.

[21] Директивата 2006/24/ЕЗ за задржување податоци.
[22] Директива 2016/680
[23] Таканаречен *принцип на минимизирање на податоците.*

Правна практика на меѓународните институции во оваа област

Европскиот суд за човекови права има донесено голем број пресуди кои се однесуваат на прекршување на членот 8 од Конвенцијата и претставуваат случаи на масовно прислушување и следење на комуникациите[24]. Праксата на судот може да се прикаже преку следните значајни случаи кои се релевантни и за Македонија:

Сабо и Виши против Унгарија

Случајот „Сабо и Виши против Унгарија“ се однесува на унгарскиот закон од 2011 година кој го уредувал антитеристичкиот надзор над комуникациите. Тужителите навеле дека унгарската легислатива за државна безбедност прави од нив потенцијална мета на неправедни и непропорционални мерки на таен надзор. Според нив, ваквите закони биле подложни на злоупотреба особено поради недостигот од судска контрола. Судот одлучил дека има повреда на членот 8 од Конвенцијата на Советот на Европа за заштита на лица во однос на автоматската обработка на личните податоци. Било прифатено дека современите форми на тероризам ги принудуваат државите да користат напредна технологија, вклучително и масовно следење на комуникациите, за да спречат потенцијални инциденти, но сепак било потенцирано дека конкретниот закон не овозможува соодветни заштитни механизми кои би спречиле злоупотреба на таквото овластување. Мерките за надзор можеле да ја опфатат буквално секоја личност во Унгарија, а техничките средства со кои располагале државните органи овозможувале лесен пристап до податоците на лица надвор од првобитниот опсег на следење. Ваквите констатации се применливи и за Македонија.

Либерти и другите против Обединетото Кралство

Тужителите, една британска и две ирски организации за граѓански слободи, навеле дека во периодот од 1990 до 1997 година нивната комуникација, вклучително и размената на доверливи информации, преку телефон, факс и електронска пошта била пресретнувана од електронски уред управуван од британското Министерство за одбрана. Нивните тужби пред националниот трибунал за следење на комуникациите, директорот на јавното обвинителство и трибуналот за истражни овластувања биле неуспешни. ЕСЧП, од друга страна, одлучил дека постои повреда на членот 8 од Конвенцијата на Советот на Европа за заштита на лица во однос на автоматската обработка на личните податоци. Судот донел одлука дека тогашното национално законодавство не обезбедува доволно јасна и соодветна заштита од злоупотреба на овластувањата и дава големи дискрециони права на властите за следење, обработка зачувување и уништување на комуникациите. И овие констатации се применливи и за Македонија.

[24] http://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

Анализа на состојбите во Македонија

Правни рамки во Република Македонија

Уставот на Република Македонија

Уставот на Република Македонија[25] 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. 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. Сепак, фактот што телекомуникациските оператори се обврзани во реално време да прават копија од целокупниот телекомуникациски сообраќај на сите граѓани и да го пренасочуваат кон МВР, го доведува во прашање почитувањето на оваа уставна одредба. Истото може да се рече и за фактот што пристап до метаподатоците за комуникациите на граѓаните може да се оствари и без судска одлука, односно само со барање на Јавното обвинителство.

Законски решенија

Првиот **Закон за заштита на личните податоци**[26] 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. 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 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.

[25] Достапно на: https://www.sobranie.mk/WBStorage/Files/UstavnaRmizmeni.pdf
[26] Закон за заштита на личните податоци, „Службен весник на Република Македонија“ бр.7/2005, 103/2008, 124/2010 и 135/2011.

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) [27] ги обврзува операторите да преземаат 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.[28]

Законот ја регулира и доверливоста на комуникациите, 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. Забранети се 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.

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.

Законот за следење на комуникациите[29] 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. 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.[30] 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

[27] Закон за електронските комуникации, „Службен весник на Република Македонија“ број 39/2014, 188/2014 и 44/2015.
[28] Член 166 од Законот за електронските комуникации.
[29] Закон за следење на комуникациите, „Службен весник на Република Македонија“ бр. 121/2006, 110/2008 и 116/2012.
[30] Член 7 од Законот за следење на комуникациите.

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.

Следењето на комуникациите е утврдено како посебна истражна мерка во **Законот за кривичната постапка**.[31] 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.** Според Законот за кривичната постапка, кај една од предвидените посебни истражни мерки[32] 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.[33]

Практиката на националните институции за заштита на правата на граѓаните

„Големото уво“

Во 2000 година, новинарите беа дел од лицата кои беа предмет на незаконско прислушување од страна на службите во склоп на скандалот „Големото уво“. Како резултат на тоа, група од 17 новинари поднесоа тужба против државата во 2001. Јавното обвинителство иницираше кривична постапка против тогашната министерка за внатрешни работи, Доста Димовска, и началникот на т.н. Петта управа во МВР, Александар Цветков – осомничени како нарачатели на прислушувањето. Постапката беше запрена, поради тоа што претседателот Борис Трајковски ги аболицираше обвинетите. Во 2006 г. Основниот суд Скопје II, донесе пресуда со која се потврди дека МВР, со помош на Македонски телекомуникации, незаконски ја прислушувала комуникацијата помеѓу седумнаесетте новинари кои според пресудата треба да добијат финансиски надомест од државата во износ од 6000 евра по човек.[34] Судот ги прифати доставените докази и ја потврди автентичноста на незаконски следените комуникации.

Во меѓувреме новинарите поднесоа тужба пред Европскиот суд за човекови права за судење во неразумен рок. Судот уважи дека времетраењето на постапката било неразумно и им определи надомест од 1850 евра по човек.

Случај „Пуч“ - пресуда за Звонко Костовски врз основа на спогодба

[31] Закон за кривичната постапка, „Службен весник на Република Македонија” број 150/2010, 100/2012 и 142/2016.

[32] 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.

[33] Член 268 од Законот за кривичната постапка.

[34] Управување со безбедносно – разузнавачките служби во Македонија, достапно на: http://www.analyticamk.org/images/stories/files/report/r01_mak.pdf

Веќе една година во Врховниот суд е заглавено барањето на Специјалната обвинителка Катица Јанева да се испита законитоста на спогодбата со која Звонко Костовски, единствениот осуден од згаснатиот случај „Пуч“, признал дело помагање во шпионажа и неовластено прислушување.[35] Признавањето резултирало со осудување на Костовски на единствена казна затвор во траење од три години за кривичните дела: неовластено прислушување, тонско снимање и шпионажа. Според пресудата, обвинетиот како службено лице во Министерството за внатрешни работи на РМ, поттикнат од Зоран Верушевски и Ѓорги Лазаревски, ги пречекорил своите службени овластувања така што ги искористил посебните уреди на МВР за прислушување и тонско снимање. Така, тој неовластено прибавувал технички записи со можност за репродукција и ги ставал на преносни носачи на податоци, а потоа содржините биле соопштувани и предавани на странска држава од страна на Зоран Верушевски. На 14 септември годинава, обвинителката Фатиме Фетаи од Специјалното јавно обвинителство[36], во Спогодбата на Обвинителството за организиран криминал со Звонко Костовски направени се процесни повреди на одредбите кои се применуваат при спогодувањето за вина. Според неа во овој случај не било утврдено кривично дело шпионажа, ниту била утврдена конкретна одговорност на непосредниот сторител на кривичното дело шпионажа, бидејќи битието на тоа дело се состои во прибавување на тајни податоци и документи, со намера да бидат предадени на странска држава, организација. Во пресудата, пак, не е наведено која е таа странска држава, ни која организација, ни лица.

„Политички бомби“ – Виктор Цветковски против СДСМ

Ослободителна пресуда донесе кривичниот совет во Кумановскиот суд, по приватна тужба на Виктор Цветковски од ГРОМ против лидерот на СДСМ Зоран Заев, СДСМ како правно лице и Мартин Костовски, претседател на општинската организација на СДСМ во Куманово, за кривично дело неовластено снимање и објавување на разговорите во т.н. бомби. Цветковски ги тужеше Заев, СДСМ и Костовски, заради неовластено снимање и објавување на разговорот меѓу него и поранешната министерка за внатрешни работи, Гордана Јанкуловска, каде се договараат за обезбедување гласови на ВМРО-ДПМНЕ меѓу двата круга на локалните избори во 2013 година во Куманово. Тој од судот бараше да се казнат тужените затоа што ја нарушиле неговата приватност, додека одбраната на Заев тврдеше дека објавувањето на снимените разговори била одлука на партијата поради повисоки државни цели, исклучиво заради откривање на криминалите на власта и политичкото пазарење на политичарите со гласовите на граѓаните во изборните процеси. Цветковски претходно покрена и иницијатива пред Специјалното јавно обвинителство, која беше отфрлена.[37]

По објавувањето на т.н. „бомби“ во 2015 г. **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 па неможеле да ја продолжат постапката.

[35] Член 316 став 4 во врска со член 24 од Кривичниот законик, како и член 151 став 1 и 4 а во врска со член 45 од Кривичниот законик

[36] https://sdk.mk/index.php/makedonija/edna-godina-zaglaveno-baraneto-na-sjo-kaj-vangelovski-vo-vrhovniot-sud-da-se-ispita-zakonitosta-na-spogodbata-za-zvonko-kostovski-edinstven-osuden-za-puch/

[37] https://sdk.mk/index.php/dopisna-mrezha/osloboditelna-presuda-za-zaev-za-objavenata-bomba-vo-kumanovo/

Дирекцијата за заштита на личните податоци (ДЗЛП), врз основа на „бомбите“ има извршено инспекциски надзор[38] 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 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 е задолжен Министерот за внатрешни работи 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.

Статистика

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. 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. 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.

Изненадувачки е што во анализираните извештаи на Јавниот обвинител 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.

[38] 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

Судска пракса од областа на заштитата на личните податоци

..

Периодични оценувања

Годишниот извештај за напредокот на ЕУ

Извештајот на Европската комисија за Македонија во 2016 година[39] истакнува дека длабоката политичка криза, која произлезе од откривањето на широко распространетото нелегално следење на комуникациите (прислушувани разговори) во 2015 година и нивната сериозна содржина, продолжи и во 2016 година. Севкупно, демократијата и владеењето на правото продолжија да се соочуваат со предизвици, особено поради заробеноста на институциите како што се судските тела, регулаторните агенции и медиумите. Според извештајот, двете комисии за надзор со кои претседава опозицијата (комисија за безбедност и контраразузнавање и комисија за следење на комуникациите) ја започнале својата работа во септември 2015 година и ја посетиле Управата за безбедност и контраразузнавање (УБК) и други служби, но не спровеле ефикасен надзор. Потенцирано е и дека јасните препораки за надзор и реформа на разузнавачките служби наведени во „Итните реформски приоритети“ не се спроведени, како и дека системот за надзор сè уште не е целосно функционален, особено во поглед на разузнавачките служби. Во октомври 2016 година се започнати и активности во однос на реформа на разузнавачкиот сектор.

Извештаите на Прибе, еден и два

Групата високи експерти за системските прашања од владеење на правото, предводена од Рајнхард Прибе, во извештаите од 2015[40] и 2017[41] 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.

Итните реформски приоритети

[39] Достапно на: https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2016/20161109_report_the_former_yugoslav_republic_of_macedonia.pdf

[40] Достапно на: https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/news_corner/news/news-files/20150619_recommendations_of_the_senior_experts_group.pdf

[41] Достапно на: https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/2017.09.14_seg_report_on_systemic_rol_issues_for_publication.pdf

Итните реформски приоритети[42] на Европската комисија од 2015 година го посочуваат следењето на комуникациите како клучен предизвик за Македонија. Итните реформски приоритети[43] се надоврзуваат на препораките на групата високи експерти предводена од Рајнхард Прибе од 2015 година и имаат за цел да дадат насока во решавање на системските слабости кои овозможија да се создаде ситуацијата која доведе до политичката криза. Како клучно законско решение кое придонесе до скандалот со прислушувањето е посочена можноста УБК да има директен пристап до содржината на комуникациите во реално време, што е содржана во членот 175 од Законот за електронските комуникации, а отстранувањето на директниот пристап е основа препорака содржана во итните реформски приоритети.

Во овој дел, документот поставува неколку приоритети кои треба да бидат исполнети:

- да се обезбеди јасно разграничување на надлежностите и прописите во врска со следењето на комуникации заради кривични истраги, од една страна, и заради безбедносни причини од друга страна;
- да се отстрани посредничката функција на УБК како „чувар“ во активностите на следење од страна на органите за спроведување на законот (полиција, царина, финансиска полиција);
- да се отстрани директниот пристап на УБК до техничка опрема што овозможува следење на комуникацискиот сигнал на телекомуникациските оператори (на пример целосно отстранување на практичната и техничка способност на УБК за директно следење на комуникациите);
- појаснување во законските одредби и во практиката дека телекомуникациските оператори активираат и пренасочуваат сигнали кон надлежните агенции за спроведување на законот (полиција, царина, финансиска полиција) или кон безбедносните агенции (УБК, Агенција за разузнавање и Воената служба за безбедност и разузнавање при Министерството за одбрана) исклучиво со претходно добиен соодветен судски налог и само за целите на законско следење на комуникациите;
- да се воведат алатки за управување со ризици за насочување и водење на сите разузнавачки операции, како и зајакната безбедност и складирање на податоци;
- да се обезбеди соодветна обука на вработените за заштита на податоците, основните права, професионалната етика и интегритетот;
- да се осигури итно и редовно заседавање на соодветните парламентарни комисии за следење на комуникациите и за безбедност и контраразузнавање, како и нивно непречено функционирање;
- да се осигури дека овие комисии функционираат во согласност со нивните законски должности за известување, како и дека се во состојба непречено да ги добијат потребните податоци, сведоштва, техничка помош и пристап, неопходни за да ги подготвуваат тие извештаи.

Годишниот извештај за човекови права на Стејт департментот

Според Извештајот на Стејт Департментот за човекови права од 2016 година[44], Владата на Република Македонија не ги почитувала забраните за арбитрарно и противзаконско вмешување во приватноста, семејството, домот и комуникацијата. Понатаму, извештајот се надоврзува и

[42] Достапно на: https://eeas.europa.eu/sites/eeas/files/urgent_reform_priorities_en.pdf
[43] Достапно на: https://eeas.europa.eu/sites/eeas/files/urgent_reform_priorities_en.pdf
[44] Достапно на: https://www.state.gov/documents/organization/265658.pdf

повикува на забелешките истакнати во извештајот на Европската Комисија за Македонија во 2016 година.

Прајваси интернешнл (Privacy International) изразува загриженост што актуелното законодавство во Македонија го олеснува масовното следење на комуникациите. Според Извештајот од 2015 година[45], отсуството на ефективен надзор и актуелниот систем на одговорност на разузнавачките служби покажуваат дека Македонија несоодветно го заштитува правото на приватност и со тоа го прекршува членот 17 од Меѓународниот пакт за граѓански и политички права (МПГПП). Врз основа на извршените набљудувања, Прајваси Интернешнл ѝ упатува неколку препораки на македонската Влада:

- Да се преземат сите неопходни мерки кои можат да обезбедат следењето на комуникациите да биде во согласност со МПГПП, вклучувајќи го и членот 17. Поконкретно, мерките треба да гарантираат дека секое прекршување на правото на приватност е во согласност со принципите на законитост, пропорционалност и неопходност, без оглед на националноста или локацијата на лицата чии комуникации се следат.
- Да се воведат гаранции дека јавните и приватните телекомуникациски и интернет провајдери ќе можат да ги прегледаат наредбите/барањата кога се побарани податоци за нивните претплатници и дека тие можат да поднесат приговор против таквите барања/наредби пред независно набљудувачко тело или пред суд.
- Да се реформира системот за надзор на следењето на комуникациите со цел да се обезбеди негова ефективност, вклучувајќи и воведување ефективно и независно надзорно тело кое би ги превенирало евентуалните злоупотреби.

Извештајот на Фридом хаус (Freedom House)[46] посочува дека веродостојните обвинувања за масовно прислушување поддржано од Владата кои се обелоденија во 2015 година предизвикаа криза која ја оневозможи нормалната политичка активност и доведе до антивладини протести.

Извештајот на Репортери без граници (Reporters without borders)[47] укажува дека масовното шпионирање на новинари претставува сериозна повреда на слободата на медиумите и на тој начин ги загрозува сите аспекти на владеење на правото. Ако Македонија навистина сака да влезе во Европската унија, според овој извештај, мора да се открие кој стои зад масовната повреда на фундаменталните права на македонските новинари и без одлагање тие лица треба да бидат изнесени на суд.

Тековни реформи

Консултации со граѓанските организации за состојбите и потребните реформи

[45] Достапно на: https://www.privacyinternational.org/sites/default/files/PI%20submission%20Macedonia.pdf
[46] Достапно на: https://freedomhouse.org/report/freedom-world/2017/macedonia
[47] Достапно на: https://rsf.org/en/news/large-scale-illegal-wiretapping-journalists-macedonia

Граѓанските организации подготвија препораки во однос на насоките за реформа на безбедносните служби на организиран и структуриран начин[48]. Препораките се во согласност со извештајот на Прибе и имаат намера да се справат со клучните ризици кои постојат за нелегално и масовно прислушување и злоупотреба на лични податоци. Иако Владата иницираше средби со граѓанските организации, сепак претставници на граѓанските организации не се вклучени во работната група за реформи во Управата за безбедност и контраразузнавање. Ваквата состојба е загрижувачка имајќи предвид дека во медиумите излегоа информации дека Владата веќе избрала модел по кој ќе се реформира системот и начините на техничко спроведување на следењето на комуникациите, без притоа да организира широк консултативен процес со сите засегнати страни. Дополнително, загрижувачки е фактот што во работната група која треба да ги реформира безбедносно-разузнавачките служби најмногу претставници имаат претставници токму на безбедносно-разузнавачкиот систем. Во групата има само еден претставник што е вон државните органи – универзитетски професор. Дополнително, трите средби со граѓанските организации[49] не се засноваа на пишан материјал за предлог-реформите кој претходно е доставен, за да може граѓанските организации да се подготват и да дадат свои коментари, ниту пак после овие средби беа дистрибуирани записници или извештаи.

Реформски планови на Владата

Владата на Република Македонија во **Планот 3-6-9**[50] 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. Владата се обврза дека во декември 2017 г. ќе предложи пакет закони за реформа на системот за следење комуникации согласно препораките на Прибе.

Според Владата, „по интензивните консултации во рамките на Министерството за внатрешни работи за моделот за реформа на разузнавачкиот и безбедносниот систем истиот е избран од страна на Владата на 12.09.2017 г.“[51] Загрижувачки е што моделот е избран без јавна консултација, нетранспарентно и само врз основа на консултации „во рамките на Министерството за внатрешни работи“ – институцијата од каде произлегуваат сите досегашни случаи на незаконско прислушување.

Во медиумите излегоа информации дека Владата формирала работна група задолжена за планирање на реформите во следењето на комуникациите, но сепак повеќе информации во

[48] Предлог на граѓанските организации за итни демократски реформи, каде посебен сегмент е посветен на контрола врз полицијата и агенциите за безбедност и (контра)разузнавање

[49] Две организирани од Владата во склоп на средбите за Планот 3-6-9, а друга од МВР.

[50] Достапно на: http://vlada.mk/sites/default/files/programa/2017-2020/Plan%203-6-9%20MKD.pdf

[51] Фактографски преглед на статусот на мерките предвидени во Планот 3-6-9. Достапен на: http://vlada.mk/sites/default/files/dokumenti/Faktografski%20pregled%20na%20statusot%20na%20implementacija%20na%20merkite%20predvideni%20vo%20Plan%203-6-9%20MK.pdf

врска со моделот по кој ќе се реорганизира функционирањето на Управата за безбедност и контраразузнавање не се достапни. Владината работна група се состои од 29 членови – претставници на МВР, УБК, други државни органи, пратеници и еден универзитетски професор, без да бидат вклучени претставници на граѓанските организации, и покрај најавите на Владата за широки консултативни процеси со сите засегнати страни при планирањето на клучните реформи во областа. Досега, не се направени никакви законски измени во согласност со препораките од извештајот на Прибе. Дополнително, Владата упати мислење до Уставниот суд дека треба да ја прекине постапката за укинување на членот 175 од Законот за електронски комуникации – кој овозможува директен пристап на УБК до содржината на комуникациите – со образложение дека таквото укинување е парцијално и не го решава проблемот, и дека истото ќе биде само еден дел од сеопфатните реформи кои Владата ќе ги преземе во идниот период. Сепак, според најавите, предложените законски измени доколку бидат прифатени од Собранието, се очекува да стапат на сила дури во ноември 2018 г. Оттука, постои ризик досегашните неуставни решенија во оваа сфера да се применуваат подолго време.

.

Заклучоци и препораки

Заклучоци

Масовното нарушување на приватноста и заштитата на личните податоци при електронските комуникации во Македонија 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.

Препораки

Со цел да се надминат воочените предизвици во следењето на комуникациите и да се подигне степенот на заштита на приватноста и личните податоци на граѓаните, ги даваме следните препораки:

- 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. Според релевантна препорака на Советот на Европа, посебните истражни мерки треба да се наменети за откривање и истражување тежок криминал.[52] Според конвенција на Обединетите нации, тежок криминал е оној што според националното законодавство е казнив со затворска казна од 4 или повеќе години.[53]
- 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.
- Законски да се раздвојат надлежноста и прописите за следење на комуникациите при кривичните истраги, од оние од безбедносен и разузнавачки карактер.
- 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 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.

[52] 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.

[53] 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

- Да се воведе и граѓанска комисија за надзор над следењето на комуникациите, којашто ќе ја именува Собранието од експерти и претставници на граѓанското општество.
- 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.