

Проект „ Унапредување,  
обликување и поддржување на  
слободите на интернет “

# АНАЛИЗА ЗА ПРАВНАТА РАМКА ЗА СЛЕДЕЊЕТО НА КОМУНИКАЦИИТЕ И НЕЈЗИНАТА ПРИМЕНА

Автор:  
Александар Николов

МЕТАМОРФОЗИС   
Фондација за интернет и општество



# ВОВЕД

Целта на оваа анализа е да даде преглед на состојбите со законските рамки поврзани со медиумите во Република Македонија во изминатиот и тековниот период. Анализата е развиена како дел од активностите на проектот „ Унапредување, обликување и поддржување на слободите на интернет“ спроведуван од Фондацијата за интернет и општество - Метаморфозис, а поддржан од Асоцијацијата за прогресивни комуникации (АРС).

Главните цели на проектот „Унапредување, обликување и поддржување на слободите на интернет“ се: унапредување на знаењето и разбирањето за состојбите поврзани со заштита на основните човекови права на интернет во Република Македонија, градење на капацитети на граѓанските организации и медиумите, олеснување на процесот на споделување на знаење и добри практики помеѓу граѓаните, граѓанските организации и медиумите.

Содржината на текстот е единствена одговорност на авторите и на ниту еден начин не може да се смета дека ги одразува гледиштата на Фондацијата за интернет и општество - Метаморфозис и на Асоцијацијата за прогресивни комуникации (АРС).

Со реформите на системот за следење на комуникациите од 2018 г., беше донесен нов **Закон за следење на комуникациите**<sup>1</sup> и беше изменет **Законот за електронските комуникации (ЗЕК)**<sup>2</sup> со што беше одземен директниот пристап на Управата за безбедност и контраразузнавање (УБК) до телекомуникацискиот сообраќај на граѓаните и нејзината улога на посредник во следењето на комуникациите – барање што беше дел и од Итните реформски приоритети<sup>3</sup> на Европската комисија од 2015 година. 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 – а ваквата поделба е во согласност со Уставот и Итните реформски приоритети.

Со **Законот за оперативно-техничка агенција**<sup>4</sup> беше воспоставен нов орган (ОТА) кој од ноември 2018 г. дејствува како посредник меѓу овластените органи за следење на комуникациите и телекомуникациските оператори со цел да се избегне концентрација на моќ во еден орган, и да се обезбеди дека следењето на комуникациите ќе биде само врз основа на закон и соодветни судски одлуки. Законот ги уредува надлежностите, раководењето со ОТА, стручниот надзор и нејзиното финансирање. Предвидено беше дел од персоналот на УБК да премине во ОТА, но не беше утврдено како ќе се спречи тоа да бидат лица кои биле претходно вклучени во злоупотребите на системот за следење на комуникациите.

Во февруари 2019 г. во собраниска процедура влезе **Предлог законот за Агенција за национална безбедност (АНБ)**, со кој е предвидено згаснување на УБК. Од јуни 2019 г., на нејзино место се предвидува да се формира Агенција за национална безбедност, која нема да биде во состав на Министерството за внатрешни работи. Агенцијата треба да собира, обработува, анализира, проценува, разменува, чува и штити податоци и информации со цел откривање и спречување на активности што се

1 Закон за следење на комуникациите, „Службен весник на Република Македонија“ бр. 71/2018.

2 Закон за електронските комуникации, „Службен весник на Република Македонија“ број 39/2014, 188/2014, 44/2015, 193/2015, 11/2018 и 21/2018.

3 Достапно на: [https://eeas.europa.eu/sites/eeas/files/urgent\\_reform\\_priorities\\_en.pdf](https://eeas.europa.eu/sites/eeas/files/urgent_reform_priorities_en.pdf)

4 „Службен весник на Република Македонија“ број 71/2018.

поврзани со безбедносни закани и ризици за националната безбедност. Агенцијата ќе врши тајно следење на телекомуникациските линии, електронските начини на комуницирање, аудиоснимање во простории и аудио, видео и фотографирање на отворени простори, увид во комуникациски метаподатоци на граѓаните како и прибирање на податоци и информации од физички и правни лица и останати релевантни страни. Предвидено е дел од персоналот на УБК да премине во АНБ, но не е утврдено како ќе се спречи тоа да бидат лица кои биле претходно вклучени во злоупотребите на системот за следење на комуникациите.

При законските измени од 2018 и 2019 г. не беше извршено усогласување со правото на ЕУ, поконкретно со Директивата на ЕУ за заштита на податоци во полицијата и кривичното право<sup>5</sup>, пресудата на Европскиот суд на правдата со која беше укината Директивата 2006/24/EЗ за задржување комуникациски податоци, како и друга релевантна пракса на Европскиот суд на правдата и Европскиот суд за човекови права. Овие извори на правото на ЕУ воопшто не беа идентификувани при спроведените проценки на влијанието на регулативата, ниту пак во образложенијата за законските иницијативи кои Владата ги достави до Собранието. Нашето законодавство не ги пропишува сите механизми за заштита на личните податоци содржани во Директивата 2016/680, не го ограничува соодветно собирањето на податоците само на она што е директно потребно и релевантно за конкретна намена<sup>6</sup>, не пропишува право на непрофитните организации што дејствуваат во интерес на поединците да поднесуваат жалби и да ги застапуваат засегнатите лица<sup>7</sup>, не воведува и обврска за известување на луѓето во случај на повреда на нивните личните податоци кои се собрани.<sup>8</sup>

Во продолжение, накратко се наведени и другите домашни правни акти кои се релевантни за следењето комуникации.

**Уставот на Република Македонија** ја гарантира слободата и неповред-

<sup>5</sup> Директива 2016/680

<sup>6</sup> Таканаречен принцип на минимизирање на податоците.

<sup>7</sup> Членови 52–55 од Директивата.

<sup>8</sup> Член 31 од Директивата.

ливоста 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.<sup>9</sup> Уставот ја гарантира и 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.<sup>10</sup>

Следењето на комуникациите е утврдено како посебна истражна мерка во **Законот за кривичната постапка**.<sup>11</sup> 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<sup>12</sup> 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.<sup>13</sup>

Слично на ова, **Законот за заштита на личните податоци**<sup>14</sup> утврдува посебни категории на лични податоци коишто не смеат да се обработуваат, односно може да се обработуваат само под посебни услови. Овој дел од законот треба да важи и за обработката на податоци при следењето комуникации, и тука се вброени: личните податоци што го откриваат

9 Амандман XIX со кој се заменува членот 17.

10 Член 18 од Уставот.

11 „Службен весник на Република Македонија“ број 150/2010, 100/2012, 142/2016 и 198/2018.

12 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.

13 Член 268 од Законот за кривичната постапка.

14 „Службен весник на Република Македонија“ бр.7/2005, 103/2008, 124/2010 и 135/2011, 43/2014, 153/2015, 99/2016 и 64/2018.

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.

**Законот за електронските комуникации (ЗЕК)**<sup>15</sup> ја регулира доверливоста на комуникациите, која се однесува и на нивната содржина, но и на податоците за комуникациски сообраќај и податоците за локација. Исклучоците од доверливоста се однесуваат на примената на Законот за следење на комуникациите, задржувањето метаподатоци за корисниците, 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. Законот ги обврзува операторите да преземаат технички и организациски мерки за соодветно управување со ризиците за безбедноста на мрежите и услугите, а особено за да се спречи и минимизира влијанието врз корисниците.<sup>16</sup>

#### **КЛУЧНИ ИЗВОРИ НА РЕЛЕВАНТНО МЕЃУНАРОДНО ПРАВО**

Универзалната декларација за човековите права на Обединетите нации;

Меѓународниот пакт за граѓански и политички права на Обединетите нации;

Европската конвенција за човекови права;

Конвенцијата за заштита на лица во однос на автоматската обработка на личните податоци на Советот на Европа;

Директивата 2016/680 за заштита на податоци во полицијата и кривичното право;

- **Праксата на Европскиот суд за човекови права и Европскиот суд на правдата во случаите со следење на комуникациите, заштита на приватноста и личните податоци.**

...7

<sup>15</sup> Закон за електронските комуникации, „Службен весник на Република Македонија“ број 39/2014, 188/2014, 44/2015, 193/2015, 11/2018 и 21/2018.

<sup>16</sup> Член 166 од Законот за електронските комуникации.





# ВИДОВИ НА ЗАКОНСКИ ДОЗВОЛЕНО СЛЕДЕЊЕ НА КОМУНИКАЦИИТЕ





# ВИДОВИ НА ЗАКОНСКИ ДОЗВОЛЕНО СЛЕДЕЊЕ НА КОМУНИКАЦИИТЕ

Законот за следење на комуникациите ги опфаќа сите видови телефонски и други електронски комуникации како интернет протокол, говор преку интернет протокол, интернет страница и електронска пошта.<sup>17</sup> Вака дефинирано, следењето на комуникациите во земјата ги опфаќа и комуникациите со интернет апликации за пренос на глас, видео и други содржини (на пр. *Skype, Viber, Snapchat, WhatsApp, FaceTime*). Законот за следење на комуникациите предвидува и можности за следење комуникации кои не се одвиваат преку телекомуникациски средства, вклучително и снимање на комуникациите во внатрешноста на објекти, или на отворен простор, како и фотографирање или видео снимање на отворен простор.

Законот за електронските комуникации, пак, ги обврзува сите телефонски и интернет провајдери да ги задржуваат една година т.н. „метаподатоци“ на сите свои корисници, односно податоците за тоа кога, со кого комуницираме, со кој облик на комуникација, со кои уреди, од кои локации, а и каде се движиме со мобилните телефонски уреди.<sup>18</sup> Метаподатоците се генерираат и без луѓето да бидат свесни за тоа, 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 и зачувува податок за локацијата каде се наоѓа мобилниот телефон и во која насока се движи неговиот корисник. Иако јавниот обвинител, Управата за безбедност и контраразузнавање и други органи<sup>19</sup> имаат право да вршат увид во нашите комуникациски

...11

<sup>17</sup> Член 4 од Законот за следење на комуникациите.

<sup>18</sup> Закон за електронските комуникации, членови 176, 178 и 181.

<sup>19</sup> Воената служба за безбедност и разузнавање и армискиот Центар за електронско извидување.

метаподатоци што ги собираат операторите, ова не е опфатено со дефиницијата за следење комуникации од Законот за следење на комуникациите.<sup>20</sup>

Последново не е во согласност со Списокот за проверка на владеењето на правото<sup>21</sup> на Венецијанската комисија, каде што е прецизирано дека и тајното собирање метаподатоци за електронските комуникации претставува следење на комуникациите. Воведувањето на одредбите за масовно задржување комуникациски метаподатоци во нашиот закон за електронски комуникации (ЗЕК) беше оправдано како транспонирање на Директивата 2006/24/ЕЗ.<sup>22</sup> Сепак, непосредно по донесувањето на новиот ЗЕК, во 2014 г. Директивата беше поништена од Европскиот суд на правдата. Судот оцени дека *масовното* задржување комуникациски метаподатоци го 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.<sup>23</sup> Државата сè уште нема преземено мерки за усогласување со правото на ЕУ во однос на задржувањето метаподатоци, и покрај фактот што во 2018 и 2019 беа иницирани и спроведени измени во релевантните закони.

## **ПРЕПОРАКИ – КАКО ДА СЕ УСОГЛАСАТ ВИДОВИТЕ НА ДОЗВОЛЕНО СЛЕДЕЊЕ НА КОМУНИКАЦИИ СО УСТАВОТ И ПРАВОТО НА ЕУ?**

- Да се укинат членовите 176 и 178 од Законот за електронските комуникации кои пропишуваат масовно задржувањето комуникациски метаподатоци за сите граѓани, 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 на конкретни лица и предмети да биде опфатено во дефиницијата за следење комуникациите во Законот за следење на комуникациите.

20 Иронично, Законот за следење комуникации не го вбројува увидот во комуникациските метаподатоци во дефиницијата за следење комуникации, но сепак го доуредува правото и начинот на остварување ваков увид.

21 Достапно на: [http://www.venice.coe.int/images/SITE%20IMAGES/Publications/Rule\\_of\\_Law\\_Check\\_List.pdf](http://www.venice.coe.int/images/SITE%20IMAGES/Publications/Rule_of_Law_Check_List.pdf)

22 Директивата 2006/24/ЕЗ за задржување податоци.

23 Здружени предмети C-293/12 и 594/12.

**ИНИЦИРАЊЕ  
И СУДСКО  
ОДОБРУВАЊЕ  
НА СЛЕДЕЊЕТО  
КОМУНИКАЦИИ**





# ИНИЦИРАЊЕ И СУДСКО ОДОБРУВАЊЕ НА СЛЕДЕЊЕТО КОМУНИКАЦИИ

Според Законот за следење на комуникациите, судот може да нареди следење на комуникациите заради откривање и гонење сторители на кривични дела или заради заштита на интересите на безбедноста и одбраната на земјата. Табелата долу дава преглед на главните сличности и разлики меѓу одредбите за следење на комуникациите по овие две основи.

...15

|              | <b>Следење на комуникациите заради откривање и гонење сторители на кривични дела</b> | <b>Следење на комуникациите заради безбедноста и одбраната</b>   |
|--------------|--|--|
| <b>Основ</b> | Откривање и гонење сторители на кривични дела  | Подготовка на кривично дело против државата, вооружените сили или против човечноста и меѓународното право; подготовка, поттикнување, организирање или учествување во вооружен напад против државата или во онеспособување на безбедносниот систем; превенирање терористичка организација, тероризам и финансирање на тероризам |

|   | Следење на комуникациите заради откривање и гонење сторители на кривични дела   | Следење на комуникациите заради безбедноста и одбраната  |
|---|---|--|
| Подносител на барање за следење комуникации | Надлежниот јавен обвинител по сопствена иницијатива или на предлог на правосудната полиција <sup>24</sup>   | Јавниот обвинител на предлог на министерот за внатрешни работи, министерот за одбрана или лице овластено од било кого од нив<br><br>За пристап до комуникациските метаподатоци на граѓаните кои ги собираат телекомуникациските оператори: Управата за безбедност и контраразузнавање, Воената служба за безбедност и разузнавање или Центарот за електронско извидување на Армијата |
| Времетраење на следењето                    | До 4 месеци, со можност за повеќекратно продолжување на барање на јавниот обвинител, од по најмногу 4–6 месеци секојпат, но не повеќе од 14 месеци збирно | До 6 месеци, со можност за продолжување, но не повеќе од 24 месеци збирно  |

<sup>24</sup> Полициските службеници во Министерството за внатрешни работи, припадниците на Управата за финансиска полиција и Царинската управа кои работат на откривањето на кривичните дела, припадниците на правосудната полиција во истражните центри на јавното обвинителство



|  | Следење на комуникациите заради откривање и гонење сторители на кривични дела  | Следење на комуникациите заради безбедноста и одбраната   |
|--|--|---|
| Судија што издава наредба за следење комуникации                 | Судијата на претходната постапка<br><br>За пристап до комуникациските метаподатоци на граѓаните, законите не бараат одобрување на барањето од суд. Јавниот обвинител го поднесува барањето директно до телекомуникацискиот оператор. | Одреден судија на Врховниот суд<br><br>За пристап до комуникациските метаподатоци на граѓаните, законите не бараат одобрување на барањето од суд. УБК и другите органи го поднесуваат барањето директно до операторот, а Јавниот обвинител ја потврдува оправданоста во рок од 48 часа. |
| Рок за одлучување на судијата по барањето за следење комуникации | 72 часа, а во случаи на итност може во рок од 12 часа да се издаде привремена писмена наредба која е валидна 48 часа   | 24 часа, а во случаи на итност веднаш може да се издаде привремена писмена наредба која е валидна 48 часа   |
| Приговор при одбивање на барањето се упатува до                  | Тричлен совет на судии на надлежниот основен суд   | Тричлен совет на судии на Врховниот суд   |

...17

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.<sup>25</sup> Според конвенција на Обединетите нации, тежок криминал е оној што според националното законодавство е казнив со затворска казна од 4 или повеќе години.<sup>26</sup> Сепак, меѓу кривичните дела за чие гонење или

<sup>25</sup> 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.

<sup>26</sup> The United Nations Convention Against Transnational Organized Crime, Article 2.

спречување е овозможено следење на комуникациите, има и такви за кои минималната пропишана казна е шест месеци затвор.

Горниот преглед открива сериозен проблем во врска со пристапот до комуникациски метаподатоци на граѓаните што телекомуникациските оператори се обврзани да ги задржуваат 12 месеци за сите корисници – истите можат да се користат од овластените органи без постоење на судска наредба. Тоа е спротивно на Амандман XIX на Уставот, со кој се заменува членот 17, според кој неповредливоста на писмото и другите облици на комуникација може да се наруши само врз основа на одлука на суд. Според списокот за проверка на владеењето на правото на Венецијанската комисија потребно е да постојат процедурални контроли и надзор, вклучително и давање овластување од судија или независно тело, дури и во случаите на следење на метаподатоците за телекомуникацискиот сообраќај на конкретна личност. Праксата на Европскиот суд за човекови права<sup>27</sup>, потврдува дека отсуството на претходно одобрување на пристапот до комуникациските метаподатоци на граѓаните – од страна на суд или независно тело – претставува прекршување на правото на приватност од членот 8 од Европската конвенција за човекови права.

Со законските измени од април 2018 г. усната наредба за следење комуникации во итни случаи – пр. кога може да има последици по кривичната постапка – е заменета со привремена писмена наредба. Сепак, новиот Закон за следење на комуникациите не пропишува попрецизни услови кои ќе демонстрираат потреба за итност. Во законско решение кое беше на сила до 2012 г., итноста беше оправдана 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.

Во новиот Закон за следење на комуникациите проширен е опфатот на овластени органи за следење на комуникациите заради заштита на интересите на безбедноста и одбраната, со додавање на Воената служба за безбедност и разузнавање. Дополнително, скратено е и онака кусо-

<sup>27</sup> Пр. *Big Brother Watch and Others v. the United Kingdom*, nos. 58170/13, 62322/14, 24960/15, ECHR 2018, Judgment of 13 September 2018, paragraph 467.

то време за судско одобрување на барањата за следење комуникации по овој основ од 24 на само 12 часа, наспроти зголемување на времето за судско одлучување кога се бара следење на комуникациите заради кривично гонење. Законот за следење на комуникациите дава право следените комуникации по основ на заштита на безбедноста и одбраната да можат да се користат и како индиции за кривично гонење<sup>28</sup> кое е неповрзано со безбедноста и одбраната. Тоа е проблематично затоа што претставува непочитување на опфатот со кој е дадена судската наредба за следење на комуникациите и ги употребува податоците за намена за која не биле собрани.

При судското одлучување по барањата за следење на комуникациите, законот за следење на комуникациите пропишал „правото на приговор“ само кога барањето нема да биде прифатено од надлежниот судија, а такво право не постои за заштита на правата и интересите на лицата чии комуникации се предлага да се следат. Фактот што не постојат податоци дека судиите отфрлиле барем едно барање за следење на комуникациите, остава простор за сомнеж дека можеби и ваквото еднострано „право на приговор“ создава притисок кај судиите да ги одобруваат сите барања.

...19

## **ПРЕПОРАКИ – КАКО ДА СЕ ПОДОБРИ ПОСТАПКАТА ЗА ИНИЦИРАЊЕ И СУДСКО ОДОБРУВАЊЕ НА СЛЕДЕЊЕТО КОМУНИКАЦИИ?**

- Да се преиспита оправданоста за 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.<sup>29</sup> Според конвенција на Обединетите нации, тежок криминал е оној што според националното законодавство е

28 Член 28.

29 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.

казнив со затворска казна од 4 или повеќе години.<sup>30</sup>

- Да се измени Законот за следењето на комуникациите и Законот за кривичната постапка за следењето и увидот во метаподатоци за електронските комуникации да се заснова на претходно издадена судска наредба во која ќе бидат наведени конкретни лица или комуникациски предмети, во согласност со Амандман XIX на Уставот, наместо сегашното решение кога масовно се собираат метаподатоците на сите граѓани, а овластените органи имаат пристап до нив без одлука на суд.
- Да се воведат 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 воведат обврска 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, и истата да биде дел од барањето кое јавниот обвинител го доставува до судијата на Врховниот суд.
- Да се јакне стручноста и етиката кај јавните обвинители и судиите во областа на следење на комуникациите, приватноста и заштитата на личните податоци; да се обезбеди надворешна поддршка за имплементација на европските стандарди во оваа сфера, вклучително и со обуки и специјализација на обвинителите и судиите.

---

30 The United Nations Convention Against Transnational Organized Crime:

# СПРОВЕДУВАЊЕ НА СЛЕДЕЊЕТО КОМУНИКАЦИИ





# СПРОВЕДУВАЊЕ НА СЛЕДЕЊЕТО КОМУНИКАЦИИ

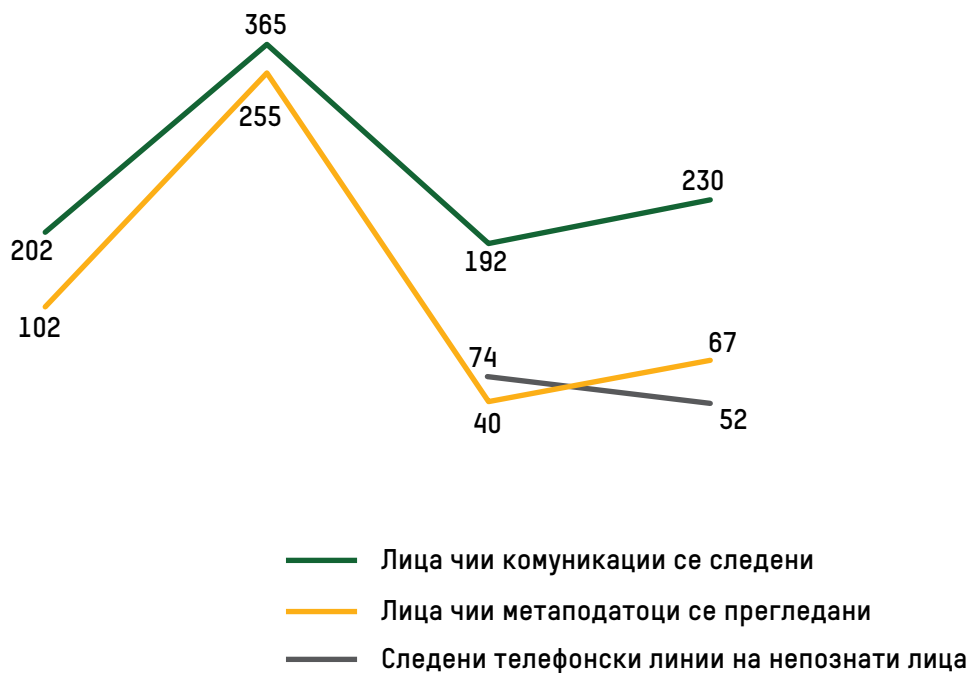
|                                      | Следење на комуникациите заради откривање и гонење сторители на кривични дела   | Следење на комуникациите заради безбедноста и одбраната   |
|--------------------------------------|---|---|
| Спроведување                         | <p>1) Со посредство на Оперативно-техничката агенција (ОТА), или</p> <p>2) Со опрема што се чува во Основното јавно обвинителство за гонење на организиран криминал и корупција (притоа, ОТА не се јавува како посредник во следењето комуникации)</p>                                      | <p>1) Со посредство на Оперативно-техничката агенција (ОТА), или</p> <p>2) Со опрема на Управата за безбедност и контраразузнавање (притоа, ОТА не се јавува како посредник во следењето комуникации)</p> |
| Најдолг период на чување на записите | До затворање на истрагата без можност за повторно отворање, а доколку се поднесе обвинение – до истекот на рокот за застареност на кривичното гонење за делото за коешто било наредено следење на комуникациите или до истекот на рокот за застареност на извршување на кривичната санкција | Три години по истекот на времето определено со наредбата, а овој рок може да започне повторно да тече во случај на „добивање нова информација“  |

Графикон 1: Случаи на кривично гонење при кои биле следени електронски комуникации или метаподатоци



24...

Графикон 2: Број на лица и телефонски линии кои биле следени поради кривично гонење





Во графиконите се наведени податоци за примена на две посебни истражни мерки во периодот 2014–2017 г.: следење и снимање на телефонските и други електронски комуникации (следење електронски комуникации) и увид во остварените телефонски и други електронски комуникации (увид во метаподатоци).<sup>31</sup> Не се достапни податоци за следењето поврзано со безбедноста и одбраната. Просечното времетраење на мерката за следење електронски комуникации бележи тренд на намалување, и во 2017 г. изнесува 4 месеци. Кај мерката за увид во метаподатоци просекот во 2017 г. е 1,5 месеци.

Законот за следење на комуникациите донесен во 2018 г. овозможува следењето комуникации да се спроведе со посредство на новата Оперативно-техничка агенција (ОТА) и телекомуникациските оператори, што го олеснува надзорот бидејќи создава повеќе точки од кои може да се добијат податоци и истите да се споредат.

Сепак, Законот овозможува следењето комуникации да се изврши и без посредство на ОТА и операторите,<sup>32</sup> со посебна опрема која не е специфицирана, па нејасно е дали ваквата формулација ги опфаќа сиот хардвер и софтвер за следење на комуникациите со кој располагаат овластените органи.<sup>33</sup> Законот за следење на комуникациите не поставува никакви услови кои треба да бидат исполнети за да се следат комуникациите без ОТА. Овој закон и Предлог-законот за агенција за национална безбедност не овозможуваат ефективен надзор над тоа чии комуникации се следени без посредство на ОТА, бидејќи не предвидуваат создавање неменливи електронски записи, како што е тоа случајот кога следењето се врши преку ОТА – кога, пак, се предвидуваат вакви записи со детален

...25

---

31 Податоците се од годишните извештаи на Јавното обвинителство за примена на посебните истражни мерки.

32 Членови 17 и 34 од Законот.

33 Според медиумски изјави, може да се однесува на пр. на IMSI catchers, т.е. опрема која најчесто се сместува во возила и која ги имитира базните станици на мобилните оператори. Опремата може да ги следи комуникациите на мобилната телефонија, но и локациите на корисниците на мобилни телефони. Спомнатата одредба може да се однесува и на други контроверзни технологии за следење, како на пр. FinFisher, со кој, според медиумски објави, земјата исто така наводно располага, а кој овозможува пристап до податоци и комуникации од мобилни телефони, компјутери, компјутерски мрежи, опрема на телекомуникациски оператори и др.

преглед за извршени активности, кој ги извршил, за кој телефонски број или IP адреса, кога почнало и кога завршило следењето. За разлика од деталниот опис на ваквите записи во однос на следењето со посредство на ОТА, Законот за следење на комуникациите и Предлог-законот за агенција за национална безбедност предвидуваат само регистар кога опремата е изнесена од просториите на Јавното обвинителство или од оние на УБК<sup>34</sup> и бројот на судската наредба, а предлог-актот за Агенција за национална безбедност утврдува дека овластените лица не смеат да бришат податоци од ваквата опрема. Бидејќи ваквата опрема е инсталирана и во возила,<sup>35</sup> дополнително се доведува во прашање можноста за ефективна контрола и надзор над нејзината употреба доколку се чува во УБК (односно идната Агенција) и само УБК/Агенцијата води евиденција за нејзината употреба.

Загрижувачки е што Законот за следењето на комуникациите и предложениот закон за Агенција за национална безбедност не ги предвидува низата мерки за безбедност на собраните податоци од Директивата 2016/680 за заштита на податоци во полицијата и кривичното право. Дополнително, Директивата<sup>36</sup> и нашиот Закон за заштита на личните податоци и утврдуваат посебни категории на лични податоци<sup>37</sup> коишто не смеат да се обработуваат, односно може да се обработуваат само под посебни услови. Овие податоци се поопшто уредени во Законот за кривичната постапка, и не важат за мерките за следење на електронските комуникации, ниту пак за следењето на комуникациите за безбедносни и одбранбени цели.

Законот за следење на комуникациите предвидува собраните комуникации да се чуваат до истекот на роковите за застареност на кривичното гонење, дури и во случаите кога е донесена ослободителна или одбивателна пресуда. Кога станува збор за следење на комуникациите

---

34 Според законските прописи, опремата наменета за следење по основ на безбедноста се чува во УБК, а онаа за следење по основ на кривично гонење се чува во Јавното обвинителство.

35 Според медиумски изјави на поранешни и сегашни функционери.

36 Но и Конвенцијата за заштита на лица во однос на автоматската обработка на личните податоци на Советот на Европа.

37 Пр. етничко потекло, политичко уверување, здравствени податоци, податоци за сексуалниот живот.

за безбедноста и одбраната на Републиката, податоците се чуваат 3 години, а овој рок може да започне повторно да тече во случај на „добивање нова информација“. Последново отстранува било какви заштита од неразумно долго или дури и неограничено чување на податоците – што од гледна точка на заштита на приватноста е неприфатливо – и ги зголемува ризиците за несоодветна употреба на овие лични податоци.<sup>38</sup>

## **ПРЕПОРАКИ – КАКО ДА СЕ ПОДОБРИ ОПЕРАТИВНОТО СПРОВЕДУВАЊЕ НА СЛЕДЕЊЕТО НА КОМУНИКАЦИИТЕ?**

- Подзаконскиот акт со спецификација и технички карактеристики на опремата за следење на комуникациите без посредство на ОТА и операторите, како и начинот на чување и ракување со оваа опрема да се утврдува со одобрение од Комисијата за надзор над работата на УБК/Агенцијата и Агенцијата за разузнавање.
- Законски да се пропише дека опремата на новопредвидената Агенција за национална безбедност со која може да се следат комуникациите без посредство на ОТА ќе се чува во друга институција, за да има уште еден ентитет што ќе има евиденција за тоа кога опремата била користена од Агенцијата.
- Согласно Итните реформски приоритети, да се обезбеди соодветна обука на вработените во ОТА и овластените органи за следење на комуникациите за заштита на податоците, основните права, професионалната етика и интегритетот.
- Во Законот за следење на комуникациите и предлог-законот за Агенција за национална безбедност да се пропишат многу подетални технички и организациски мерки за безбедност при обработката на податоци согласно предвиденото со Директивата 2016/680 за заштита на податоци во полицијата и кривичното право. Меѓу другото, законски да се воведат принципот на минимизирање на податоците при следењето на комуникациите, што подразбира законски да се ограничи 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.

...27

---

38 Член 29 од Законот.

- 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 ограничи рокот во кој може да се продолжува чувањето на податоци собрани со следење на комуникациите за потребите на безбедноста и одбраната.
- Законски да се пропише дека при уништување на податоците од следењето на комуникациите ќе бидат уништени оригиналниот запис и сите копии во сите вклучени институции и ентитети. Уништувањето на податоците да се врши и во присуство и на претставници од Дирекцијата за заштита на личните податоци и Народниот правобранител.

# НАДЗОР И КОНТРОЛА





# НАДЗОР И КОНТРОЛА

Реформите од 2018 г. го зголемија бројот на органи, покрај Собранието, кои вршат надзор над следењето на комуникациите.<sup>39</sup> Нивните сфери на надзор се прикажани во табелата долу.

| Надзорен орган                                      | Законитост | Ефективност <sup>40</sup> | Ефикасност |
|---|------------|---------------------------|------------|
| Собрание  | ✓          | ✓                         |            |
| Совет за граѓански надзор                           | ✓          |                           |            |
| Дирекција за безбедност на класифицирани информации | ✓          |                           |            |
| Дирекција за заштита на лични податоци              | ✓          |                           |            |
| Народен правобранител                               | ✓          |                           |            |

...31

Со Законот за следење на комуникациите беше допрецизиран начинот на вршење на надзорот на законитоста и ефективноста на мерките за следење на комуникациите од страна на надлежната собраниската комисија, се предвиде експертска поддршка и се намали ризикот за блокирање на нејзината работа од страна на политичките партии на власт.

<sup>39</sup> Надзорните органи вршат надзор над овластените органи, ОТА и телекомуникациските оператори, со исклучок на Советот за граѓанска контрола кој не врши надзор над операторите. ОТА пак, врши стручен надзор над операторите.

<sup>40</sup> Надзорот на ефективноста се однесува само на следењето комуникации како посебна истражна мерка, а не и на следењето за заштита на интересите на безбедноста и одбраната.

Текстот на Законот што беше објавен за јавна консултација ја овластуваше Комисијата да ги повикува раководителите на овластените органи за следење на комуникациите, ОТА и операторите заради утврдување на законитоста на нивните активности. Оваа одредба требаше да спречи повторување на минати случаи кога функционери одбиваа да дојдат на седница на Комисијата на која беа поканети, но беше избришана во верзијата што Владата ја достави до Собранието и што подоцна беше донесена – иако јакнењето на способноста на Комисијата да обезбедува сведоштва беше предвидено со Итните реформски приоритети. Во 2018 г. Комисијата беше претежно фокусирана на учество во активности за јакнење на капацитетите за надзор и запознавање со претставници на надлежните органи за следење на комуникациите.<sup>41</sup> Експертската поддршка за нејзината работа сè уште не беше обезбедена во февруари 2019 г., иако за оваа намена беше објавен оглас.<sup>42</sup> Не е познато дали Комисијата постапувала за објавениот случај од 2018 г. кога беа откриени уреди за снимање на комуникациите во Јавното обвинителство и Основниот суд Скопје 1.

И покрај тоа што имаше доволно пријавени кандидати од редот на експерти и претставници на граѓански организации, Собранието не ги назначи сите членови на Советот за граѓански надзор – поради барањата на дел од собраниските партии за повторно објавување на огласот и за постигнување правична застапеност во неговиот состав – па истиот сè уште не функционира.

Контролни тела, пак, за законитоста на спроведувањето на посебната истражна мерка – следење на комуникациите – од страна на овластените органи, операторите и ОТА се јавниот обвинител и судијата кој ја издал наредбата за следење комуникации. Тие имаат право да вршат ненајавен увид во овластените органи, ОТА и операторите, и да пристапат до сите податоци, а можат да ангажираат и технички експерти кои ќе им помагаат при контролата.

41 Годишен извештај за работата на Комисијата за надзор над спроведување на мерките за следење на комуникациите во 2018 година.

42 <https://sobranie.mk/javen-povik-za-angaziranje-na-dvajca-tehnicki-eksperti-za-postojana-poddrshka-vo-komisijata-za-nadzor-nad-sproveduvanje-na-merkite-za-sledenje-na-komunikaciite.nsp>



Предлог-законот за Агенција за национална безбедност ги предвидува истите надзорни тела како и за следењето на комуникациите, со таа разлика што во овој случај е надлежен и Државниот завод за ревизија како и собраниската Комисија за надзор на работата на УБК и на Агенцијата за разузнавање. Предлог-законот го утврдува подетално опфатот на надзорот и начинот на вршење на надзорот само од страна на Собранието, но не и од останатите надзорни тела, а недоволно се дефинирани и податоците кои Агенцијата ќе биде должна да ги доставува до нив. Значајно е што се предвидува собраниската надзорна комисија да може да го повика директорот на Агенцијата, и што се воведува внатрешна контрола во Агенцијата. Во предлог-законот е предвидено директорот да доставува годишен извештај до надлежната собраниска надзорна комисија, како и да објавува јавен извештај за работата, но не е специфицирана содржината на овие извештаи.

Согласно Законот за кривична постапка,<sup>43</sup> Јавниот обвинител доставува годишен извештај до Собранието за примената на посебните истражни мерки, вклучително и следењето на комуникациите. Анализата на извештаите за периодот 2014–2017 покажува дека Јавното обвинителство ги доставува до Собранието дури 7–9 месеци по истекот на годината на којашто се однесуваат – што е долг период за подготовка на извештај чијашто големина се движи од 10 до 16 страници. Извештаите не се објавуваат на веб-сајтот на Јавното обвинителство, што е загрижувачко ниво на нетранспарентност. Дополнително, извештаите не ги содржат следниве елементи што се пропишани со Законот за кривичната постапка, а се клучни за Собранието да може да врши надзорот на законитоста, ефективноста и ефикасноста:

- образложение за причините зошто следењето комуникации не дало релевантни резултати за постапката, односно не обезбедило докази за постапката;
- трошоците што произлегуваат од примената на посебната истражна мерка.

---

<sup>43</sup> Член 271 од Законот.

Постојат неконзистентности во изнесените податоци во извештаите. На пример, во извештајот за 2017 г. е наведено дека мерката за следење електронски комуникации се вршела во 32 случаи, но при преглед по времетраење на мерката по случаите се наведени вкупно 33 случаи. Ваква разлика се јавуваат и во извештајот за 2016 г. 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. Во извештајот пак за 2017 г., се наведуваат број на случаи и лица за кои е отпочната истражна постапка, а за останатите исходи е даден само преглед по лица, а не и по случаи. 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. Ваквите неконзистентности ја отежнуваат споредбата на податоците од различните години, како и давањето оценка за ефективноста на мерките за следење на комуникациите и метаподатоците.

Изненадувачки е што во анализираните извештаи за четирите 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 наведено дали и колку од овие пресуди се осудителни, ниту, пак, 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 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.

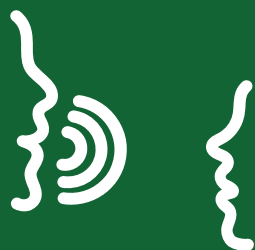
Извештаите не содржат податоци за тоа колку предлози за следење на комуникациите биле доставени до јавниот обвинител, со колку од нив обвинителот се согласил, колку сопствени иницијативи имал за следење на комуникациите, и за колку од поднесените барања била издадена наредба од судија. Во извештаите 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 – КАКО ДА СЕ ПОДОБРИ НАДЗОРОТ И КОНТРОЛАТА НА СЛЕДЕЊЕТО НА КОМУНИКАЦИИТЕ?**

- Да се предвидат подетални одредби за начинот на следење на законитоста, ефективноста и ефикасноста на следењето на комуникациите во сите негови фази: изборот на мерки, собирањето податоци, но и при нивната анализа и постапување по нив, како и финансирањето.
- Законски да се уредат податоците кои новопредвидената Агенција за национална безбедност ќе биде задолжена да ги достави на барање на надзорните тела, вклучително и индикатори за успешност, а да се дефинираат и надлежностите и правата на надзорните тела.
- За градење отчетност, транспарентност и доверба во работењето, законски да се утврдат сите информации кои треба да ги содржи годишниот извештај на Агенцијата за национална безбедност, вклучително и податоци за колку лица и предмети на комуникација е овозможен пристап, статистика колку барања за издавање судска наредба биле поднесени, колку одбиени или преиначени, статистика за евентуално преземени дисциплински мерки против лица вработени во Агенцијата поврзано со пропусти или злоупотреби при спроведување на мерки за тајно собирање на податоци, статистика за тоа колкави биле трошоците на државата и други релевантни информации. Годишниот извештај за јавноста да ги содржи истите податоци, но претставени во лесно разбирлива форма за граѓаните. Овие категории на податоци да бидат содржани и во годишниот извештај на јавниот обвинител за примена на посебните истражни мерки.
- Надлежните органи да прават редовни контроли кај операторите за пристапот и обработката на податоците за комуникациски сообраќај и податоците за локација на претплатниците.



**ИЗВЕСТУВАЊЕ  
НА ГРАЃАНИТЕ  
ЧИИ  
КОМУНИКАЦИИ  
СЕ СЛЕДЕНИ И  
ПРАВНИ ЛЕКОВИ**





# ИЗВЕСТУВАЊЕ НА ГРАЃАНИТЕ ЧИИ КОМУНИКАЦИИ СЕ СЛЕДЕНИ И ПРАВНИ ЛЕКОВИ

Во случај на судска одлука дека комуникацијата била следена спротивно на одредбите од Законот за следење на комуникациите, како и во случај на објавување на податоци собрани со следење комуникации, лицето има право на надомест на штета од државниот буџет.<sup>44</sup> Законот им дава право на граѓаните да поднесат барање до Советот за граѓанска контрола да провери дали нивниот телефонски број е или бил незаконски следен во последните три месеци. Проблематично е што ова право се ограничува само на телефонски број, а не ги вклучува и увидот во метаподатоци, или интернет сообраќајот, вклучително и разговори и пораки преку интернет. Исто така, не постојат причини зошто ваквото право да се ограничи само на последните три месеци. Дополнително, во законот за следење на комуникациите повеќе не постои одредбата според којашто по донесувањето решение за спроведување истрага граѓанинот требаше да биде запознаен со извештајот за следењето комуникации. 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 за спроведување на таквите мерки. 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. Европската конвенција за човекови права го предвидува и правото на информираност на поединецот за кого се прибираат податоци, како што е случајот и со Конвенцијата за заштита на лица во однос на автомат-

...39

<sup>44</sup> Член 28 од Законот за следење на комуникациите.

ската обработка на личните податоци на Советот на Европа. Дополнително, спротивно Директивата 2016/680, во нашиот закон не е пропишано правото на непрофитните организации да поднесуваат жалби и да ги застапуваат засегнатите лица<sup>45</sup>, ниту пак правото овластените органи за следење на комуникациите да ги известат граѓаните во случај на повреда на нивните личните податоци кои се собрани.<sup>46</sup>

### **ПРЕПОРАКИ – КАКО ДА СЕ ПОДОБРАТ ИЗВЕСТУВАЊЕТО НА ЛИЦАТА ЧИИ КОМУНИКАЦИИ БИЛЕ СЛЕДЕНИ И ПРАВНИТЕ ЛЕКОВИ КОИ ИМ СТОЈАТ НА РАСПОЛАГАЊЕ?**

- 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 прејудуцирање 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 во случаи поврзани со следењето комуникации.

---

45 Член 55 од Директивата.

46 Член 31 од Директивата.





