М-р Бојан Стојиќ[1]

БЕЗБЕДНОСЕН КОНЦЕПТ НА ОПЕРАТИВНО ТЕХНИЧКАТА АГЕНЦИЈА И ИНТЕГРИТЕТ

1.04 Стручна статија

УДК: **355.40:621.39]:340.13(497.7)**

Апстракт

Потребата од нов Закон за следење на комуникациите, произлегува директно од констатираната злоупотреба на системите за пресретнување на комуникациите нотирано во препораките на Групата високи експерти за системски прашања од владеење на правото во врска со следењето на комуникациите од 2015 година. Извештајот од истата година, укажува на монополот кој го поседува УБК, во спроведување на мерката, како и комплетно непочитување на професионализмот, етичките стандарди, човековите права, основни принципи на менаџирање со ризик, како и непознавање на сензитивноста на оперативните задачи внатре во УБК. Од самиот закон, како и препораките на Групата високи експерти за системски прашања од владеење на правото, произлегува и Оперативно техничката агенција, која треба да биде гаранцијата против злоупотребата на следењето на комуникациите, како и самостојна стриктно професионална алатка за извршување на должностите предвидени со закон.

Клучни зборови: Оперативно техничка агенција, ОТА, следење на комуникации

[1] Проектен соработник во Здружението на судии на Република Македонија

Вовед

Потребата од нов Закон за следење на комуникациите, произлегува директно од констатираната злоупотреба на системите за пресретнување на комуникациите нотирано во препораките на Групата високи експерти за системски прашања од владеење на правото во врска со следењето на комуникациите од 2015 година. Извештајот од истата година, укажува на монополот кој го поседува УБК, во спроведување на мерката, како и комплетно непочитување на професионализмот, етичките стандарди, човековите права, основни принципи на менаџирање со ризик, како и непознавање на сензитивноста на оперативните задачи внатре во УБК[2]. Исто така, слабостите на тогашните законските решенија се потенцирани и од страна на ГРЕКО и Венецијанската комисија, кои укажуваат на можна злоупотреба. Со таа цел, Министерството за внатрешни работи формира меѓуресорна работна група која има за цел да изготви нов предлог закон за следење на комуникациите кои ќе ги содржат сите препораки од двата извештаи на Групата високи експерти, и координира имплементацијата на истите според владиниот план за реформа на безбедносниот сектор.

Со донесувањето на новиот предлог закон за следење на комуникациите, се формира и самостоен државен орган во својство на правно лице, Оперативно-Техничка Агенција (ОТА), регулирана со посебен закон, која претстаува технички сервис на сите органи овластени со закон за следење на комуникациите, како за кривичните постапки така и за безбедносните потреби на државата. Со ваквото решение, сите технички системи за следење на комуникациите и физички се отстрануваат од УБК, со што се одзема монополот на службата како што е и нотирано во извештајот на Групата високи експерти од 2017 година, со што се исполнува еден од условите за спречување на понатамошна злоупотреба на истите[3].

Од клучна важност во оваа реформа е елиминирањето на секаков потенцијален вид на злоупотреба на Законот или на Агенцијата, особено од позицијата на политичка моќ.

[2] The former Yugoslav Republic of Macedonia: Recommendations of the Senior Experts' Group on systemic Rule of Law issues relating to the communications interception revealed in Spring 2015; Brussels, 2015
[3] The former Yugoslav Republic of Macedonia: Assessment and recommendations of the Senior Experts' Group on systemic Rule of Law issues 2017; Brussels, 2017

Круцијална важност исто така има и инструментот за надзор, особено врз Оперативно-техничката агенција која треба да го предводи Собранието и да биде гарант за законитоста при исполнувањето на законските обврски. Надзорот, овој пат зајакнат преку граѓанскиот сектор и Народниот правобранител, придава значајна поддршка на Собранието како најбитна институција при контролата на законитоста на следењето на комуникациите, како и работењето на ОТА. Втор момент кој е од особено значење за успехот на реформата во оваа област е сериозната и строга професионализација на кадарот што треба да го спроведе Законот.

1. Безбедносна надлежност на ОТА

1.1 Безбедносни надлежности

Надлежностите на Оперативно-техничката агенција се уредени во членот 3 од предложениот закон, согласно кој за вршење на надлежноста утврдена со одредбите од предметниот закон, Оперативно-техничката агенција, активира и создава услови за следење на комуникациите, за кривични истраги и безбедносни потреби. Овозможува пристап до средствата за собирање податоци од комуникациско-информациските системи на операторите, за органите овластени за спроведување на мерките за следење на комуникациите, остварува оперативно-техничка координација меѓу операторите и органите овластени за спроведување на мерките за следење на комуникациите. Во соработка со органите овластени за спроведување на мерките за следење на комуникациите утврдени согласно Законот за следење на комуникациите, врши надзор врз операторите. Во овие рамки, начинот на вршење на работите во надлежност на Оперативно-техничката агенција е предвидено да биде уреден со подзаконски пропис кој го донесува Директорот на Оперативно-техничката агенција. Имено, со овој член, ОТА предвидено е да биде линкот помеѓу комуникациските оператори во државата и органите овластени за спроведување на мерките за следење на комуникациите, со што би се елиминирала секоја потенцијална закана за злоупотреба на мерката како од страна на органите, исто така и од страна на комуникациските оператори. Во ова својство, комуникациските оператори исто така располагаат со одреден број надлежности кои се од суштинско значење за обезбедување на оперативноста на Агенцијата. Со цел, да се зачува интегритетот на комуникацијата,

комуникациските оператори треба да воведат на сет безбедносни мерки кои би ја гарантирале законитоста на мерката која се применува[4].

Оперативно техничката агенција, во својата надлежност, исто така мора да го гарантира интегритетот на самите апарати кои се инструментот на извршување на зададената мерка, како и интегритетот на персоналот кој ќе ги спроведува мерките. Директорот, како и органот за надзор од агенцијата, мора стриктно и прецизно да ги утврдат критериумите за одговорност и заштита на добиените податоци, и соодветни механизми за детектирање на злоупотреби. Во овој поглед, телото за надзор во агенцијата треба да биде првиот ред на одбрана и детекција на потенцијалната злоупотреба како и навремена реакција со цел да се спречи одливот на злоупотребената информација. Имено, постои голема веројатност, особено во мерките кога се применува следење на комуникации, во ситуации кога е загрозена националната безбедност, добиените податоци од пресретнатите комуникации да бидат пробиени и предадени на агенти, кои имаат задача за офанзивно дејствување во земјата. Во нашата земја, познати се случаеви на злоупотребени информации од карактер на национална безбедност, за кои се водеа и судски процеси, како на пример случајот "Шпион", каде што информации добиени со примена на посебниистражни мерки, и пресретнати комуникации, се користени за добивање на одредена финансиска цел, или политичко влијание. Ваквите компромитирани информации исто така длабоко задираат и во основните уставно загарантирани човекови права, бидејќи карактерот на нивното створување е и спротивно на законските одредби. Од тука излегува и една од целите кои агенцијата мора да ги гарантира, а тоа е апсолутниот интегритет и заштита на добиените комуникации кои се предмет на следење.

2. Безбедносна структура на ОТА

Безбедносната структура на Агенцијата е од клучен карактер за зачувување на интегритетот на истата и на пресретнатите комуникации. Потребни се неколку безбедносно

[4] Предлог Закон за Оперативно – техничка агенција, Поглавје II, Ноември 2017 година, Скопје

структурни гаранции за да се заштитат пресретнувачките капацитети на агенцијата. Инаку, тие структурни гаранции треба да бидат составени во 4 клучни области[5]:

- Физичко обезбедување (пример, зградата, собите за серверите и опремата, камери за надзор итн.)
- Техничко обезбедување (различни безбедносни софтверски решенија како фајрволи, анти-вирусни софтвери итн.)
- Обезбедувачи (лица задолжени за физичко обезбедување, различен степен на пристап, посебен тренинг итн.)
- Процедурална безбедност (различни процедурални процеси и протоколи)

Иако овие области се широки во поим, балансот помеѓу нив може да се разликува.

Имено иако, истите безбедносни гаранции мора да бидат применети и од комуникациските оператори, може да има појава каде комуникациските оператори би располагале со помал број на обезбедувачи кои би ја гарантирале безбедноста на опремата кај операторите, насоката би требало да биде фокусирана кон постриктни протоколи и процедури за пристап кон опремата. Иако, нивото на безбедност е базирано на различни фактори, и е баланс помеѓу 4 клучни области, не постои еден единствен минимален безбедносен стандард. Без разлика на поставеноста, комуникациските оператори мора да бидат задолжени да ги следат истите безбедносни стандарди како и агенцијата со цел да се зачува интегритетот на целата мерка. Сепак би требало да биде дозволено и на комуникациските оператори да воведат некои дополнителни алтернативни мерки на безбедност, со кои би се зачувал интегритетот на податоците во соработка со Агенцијата.

2.1 Интегритет на пресретнатата информација

Кога мерката за пресретнување на комуникациите е авторизирана надлежните институции со закон овластени за тоа, проверки на договорени интервали треба да бидат превземени од страна на Агенцијата и комуникациските оператори со цел да се обезбеди интегритетот и безбедноста, и доставувањето на точната комуникација. Комуникацискиот оператор мора да биде известен доколку настанат технички проблеми при спроведувањето на мерката, како и евентуална промена на пресретнувачките капацитети или достава на

[5] Home Office, “Interception of Communication” Draft Code of Practice, February 2017

пресретната комуникација. Истиот концепт, треба да биде применет и од страна на Агенцијата при известувањето на комуникацискиот оператор, кога настанува одреден технички проблем, или има промена на пресретнувачките капацитети. Агенцијата, но исто така и комуникациските оператори, треба да обезбедат гаранција дека сите пресретнувачки капацитети се во оптимална состојба за опслужување, како и гаранција дека никакви неавторизирани промени од неавторизирани лица се направени во пресретнувачките капацитети[6]. Во случаеви кога се детектирани неправилности во протоколот, а во однос на налогот за следење на комуникацијата, комуникацискиот оператор мора веднаш да ја извести Агенцијата за превземање на соодветни наредни чекори[7].

2.2 Безбедност на персоналот

Агенцијата мора точно да ги идентификува позициите и работните должности на вработениот персонал, и да обезбеди јасна диференција помеѓу персоналот со различен степен на пристап до информации, неопходен за нивното работење. Сите права и пристапи кое вработеното лице ги поседува, мора веднаш да се терминираат со престанокот на работниот однос. Истите тие права и пристапи, мора да бидат ревидирани или повлечени, во случај кога работникот го менува своето работно место во Агенцијата. Персоналот со пристап до пресретнувачката опрема, мора да бидат подложени на безбедносен скрининг. Агенцијата мора да обезбеди соодветни механизми за проверка на персоналот, кој мора да биде во согласност со постоечката легислатива. Комуникациските оператори исто така мора да извршат соодветна безбедносна обука на својот персонал кој е задолжен за исправноста и функционирањето на пресретнувачките капацитети. Сите оние лица кои имаат пристап до пресретнатите информации, или треба да изготват или прегледат извештај кој произлегува од дадена пресретната информација, мора да поседуваат соодветен безбедносен сертификат. Директорот на агенцијата, или раководната структура на агенцијата, барем еднаш годишно, мора да ги идентификуваат сите потенцијални забелешки, кои можат да доведат до промена на безбедносното ниво за пристап до информациите на одредено вработено лице. Исто така, безбедносната проверка на секој еден вработен во Агенцијата, неопходно е да биде извршена неколку пати во годината со цел да се потврди интегритетот

[6] Предлог Закон за следење на комуникациите, Ноември 2017, Скопје
[7] Home Office, “Interception of Communication” Draft Code of Practice, February 2017

на работникот, или негова потенцијална повреда. Доколку е потребно некој работник, да сподели информација околу предмет за кој се води мерка пресретнување на комуникациите, мора да се осигура дека примателот на информацијата има соодветен безбедносен сертификат за добивање на истата[8].

2.3 Обезбедување и пристап

Агенцијата мора да имплементира соодветни безбедносни проверки, со цел да се спречи неавторизиран влез во агенцијата, како и до сензитивните информации. Пристапот до просториите каде што се сместени пресретнувачките капацитети, мора да биде лимитиран само на вработени кои поседуваат содветни безбедносни сертификати и дозволи. Опремата која служи за пресретнување на комуникациите, мора соодветно да биде оддржувана како и во одредени случаеви, прилагодена на соодветни технички стандарди. При завршувањето на употребата на опремата за пресретнување на комуникациите истата мора соодветно и прописно да се уништи. Агенцијата исто така, мора да се осигура дека пристапот и регистрацијата, како и сите лозинки кои вработените ги користат за пристап до и во опремата за пресретнување на комуникациите и нејзината документација, се менаџирани стриктно во согласност со безбедносната полиса на Агенцијата. Исто така, Агенцијата мора да се осигура дека корисниците на опремата за пресретнување на комуникациите ги разбираат и признаваат нивните безбедносни обврски. Пристапот до секаква документација како и пресретнувачките капацитети мора да биде осигуран и обезбеден за сите релевантни тела за надзор, кои со закон се пропишани да вршат надзор над Агенцијата и нејзиното работење. Во случај на инцидент, Агенцијата мора да воспостави протоколи и процедури за менаџирање на инциденти во кои при негова детекција, највисокото раководство на Агенцијата мора да биде веднаш известено. Сите злоупотреби на постојната легислатива мора да бидат веднаш пријавени кај надлежниот орган за спроведување на истрага. Системите за пресретнување на комуникациите мора да овозможат собирање на дигитални докази кои подоцна би служеле на истрагата.

[8] Ibid

Bojan Stojikj, MSc[9]

SECURITY CONCEPT OF THE OPERATIONAL TECHINCAL AGENCY AND INTEGRITY

1.04 Professional Article

UDK: 355.40:621.39]:340.13(497.7)

Summary

The need for a new Law on Interception of Communications stems directly from the established abuse of the systems for interception of communications, noted in the recommendations of the Senior Expert's Group on Systemic Rule of Law Issues from 2015. The report of the same year points to the monopoly owned by the UBK in the implementation of the interception of communication measure, as well as complete disregard for professionalism, ethical standards, human rights, basic principles of risk management, as well as the lack of knowledge of the sensitivity of the operational tasks inside the UBK. From the Act itself, as well as the recommendations of the Group of Senior Experts on systemic issues of the rule of law, an Operational Technical Agency is formed, which should be the guarantee against the abuse of the communications interception measure, as well as an independent strictly professional tool for performing the duties stipulated by the law.

Key words: Operational technical agency, OTA, communication interception

[9] Project Assistant at the Macedonian Judges Association