



Ерозија на приватноста во Република Македонија

Кон Измените и дополнувањата на Законот за електронските комуникации

Правото на приватност во Република Македонија деновиве е одново доведено во прашање. Не е прв пат Владата сериозно да го ограничува правото на приватност, едно од темелните граѓански права, без притоа да отвори поширока јавна расправа за едно така значајно прашање. Со наводно „технички“ закон за електронските комуникации, во суштина, **се прави упад во најзаштитените сфери на приватноста гарантирани со меѓународните договори за човековите права и Уставот на РМ.** Имено, со предложените измени, овој Закон навлегува во сферата на казненото право, бидејќи предвидува нови овластувања за полицијата и тајните служби, надвор од досега предвидените со Законот за кривичната постапка и Законот за следење на комуникациите. Со предложените законски решенија сега и законски се воведуваат спорните методи за обработување на личните податоци, за кои може да се каже дека се несоодветни и преобемни во однос на целите заради кои се собираат и обработуваат во смисла на одредбите од член 5 став 1 алинеи 1 и 3 од Законот за заштита на личните податоци.

Имено, наместо само „усогласување на Законот за електронските комуникации во делот кој ги уредува обврските на операторите и давателите на јавни комуникациски услуги со решенијата предвидени во Законот за следење на комуникациите“ (како што се наведува во предлогот од Владата), со овој Закон се востановуваат нови можности за лесно и директно зафаќање на полицијата и тајните служби во приватноста, без притоа да се повика или направи каков било линк со *условите* и *постапките* за примена на посебните мерки од Законот за кривична постапка, Законот за следење на комуникациите или Законот за внатрешни работи, и тоа по слободна проценка на полицијата и тајните служби и без какво и да е одобрение или контрола. Не е многу јасно како со тоа, како што се правда предлагачот, „во фокусот се ставени потрошувачите, особено во делот на зајакнување на нивните права“?!

Овластен орган за следење на комуникации според предложените измени е **Министерството за внатрешни работи**, кое има постојан и директен пристап до електронските комуникациски мрежи и објектите на

операторите на јавни комуникациски мрежи и давателите на јавни комуникациски услуги (нова точка 47 на чл. 4)! Овие, пак, се должни на барање на „надлежните државни органи“ (друг орган освен МВР не се споменува, па дури ни Министерството за одбрана!?) да им ги достават податоците за сообраќај кога е тоа потребно (а тоа го ценат самите!) заради спречување или откривање на кривични дела, заради водење на кривична постапка или кога тоа го бараат интересите на безбедноста и одбраната на Република Македонија. Со тоа и основите за примена на мерките се многу пошироки од оние досега предвидени со ЗКП и ЗСК (откривање и гонење на кривични дела).

На овластениот орган (МВР) за следење на комуникации операторите на јавни комуникациски мрежи и давателите на јавни комуникациски услуги се должни да му овозможат постојан и директен пристап до своите електронски комуникациски мрежи како и **„услови за самостојно преземање на податоците за сообраќај“**.

Никаде не се споменува судот или јавното обвинителство како органи надлежни за определување и примена на мерките согласно законите, кои МВР само ги спроведува по нивно барање, односно наредба! Ваквиот пристап е спротивен на Уставот на РМ, кој во повеќе одредби многу јасно и недвосмислено изразува голема резерва, поточно недоверба, по однос на полицијата и другите органи со посебни овластувања и затоа го одредува судот како единствен орган кој може да одлучува за зафаќањето во основните права и слободи.

Според предложените измени на Законот и така слабата контролна улога на судот и јавното обвинителство станува уште помалку реална, во ситуација кога на операторите и давателите на јавни комуникациски услуги нема да мора воопшто да им се презентира налог на судот!¹

Меѓу мерките предвидени во измените на Законот за електронски комуникации во суштина се и две „нови“, т.н. *посебни* (специјални) истражни мерки кои до сега не беа изречно предвидени во нашиот ЗКП, ниту во Законот за следење на комуникациите.² Имено, мерката која се состои во

¹ Контролната улога на судот и без тоа е минимизирана со последните измени на Законот за кривичната постапка и Законот за следење на комуникациите, бидејќи посебните истражни мерки се повлекуваат во многу рана фаза од постапката без да се бараат конкретни докази за делото и сторителот, па така судот и не е во можност да оцени дали мерките се навистина оправдани, а уште помалку дали се исцрпени другите начини на откривање и докажување. Во сферата на државната безбедност, судијата во Врховниот суд, исто така, не е многу вичен да оценува дали мерките се навистина нужни и оправдани. Од друга страна, како што кај нас стојат работите, засега не постои ама баш никаква можност кој било, па ни судот, ни обвинителството, ни собраниските комисији, да извршат каква и да е реална, редовна и ефикасна контрола врз реалниот опсег на прислушувањата.

² Види: Законот за изменување и дополнување на ЗСК (Службен весник на Р.М. бр.110 од 02.09.2008 год.); Законот за изменување и дополнување на ЗКП (Службен весник на Р.М., бр. 83 од 10.07.2008 год.).

„доставување податоци за сообраќај“ односно „листинг“ за остварените контакти преку фиксен или мобилен телефон, интернет пораки или слично одамна се практикува од страна на полицијата и тајните служби, при што податоците што на овој начин се добиваат за осомничениот, неговите навики, контакти, движења и слично, откако ќе се обработат во секторот аналитика, претставуваат извонредно корисна алатка во откривањето и спречувањето кривични дела, но и за безбедносни, па и политички цели (неретко и злоупотреби). Нешто понова метода е онаа за можноста за лоцирање и следење на движењето и контактите преку мобилната телефонија или преку следењето на поврзувањето на интернет преку компјутер, модерен телефон и сл. е многу слична на мерката *тајно следење*, сега предвидена со ЗКП, но е многу поефикасна, бидејќи практично овозможува следење на движењето и контактите на осомничените за еден подолг период наназад (практично, од воведувањето на мобилната телефонија и интернетот). За државните органи, пак, ваквите мерки се голема заштеда во време и кадри, споредено со класичните методи на оперативно следење од страна на физички лица.

Главниот проблем е, се разбира, големата интрузивност на овие мерки, особено со оглед на нивното траење (поточно долгиот временски период врз којшто тие лесно може да се протегнат).

Зачудува леснотијата со која што власта се обидува овие мерки да ги прикаже како некаква површно техничко прашање. Напротив, се работи за мерки кои Европскиот суд за човековите права одамна ги има окарактеризирано како **сериозни зафаќања во правото на приватност**, кои затоа бараат ист или сличен режим како и прислушувањето и другите специјални истражни мерки, кои што кај нас сега се опфатени во ЗКП и Законот за следење на комуникации. Прв и најпознат случај во којшто е третиран т.н. „метеринг“ (листинг) е случајот *Малоне против Обединетото Кралство* од 1984 г. кога Европскиот суд за човекови права утврдил дека добивањето на детали за броевите кои биле повикувани, времето на повикот и неговото траење не биле уредени со јасни правни правила кои би се однесувале на опсегот и начинот на практикување на дискрецијата од страна на јавните власти.

Практиката, пак, на тајно следење Европскиот суд за човековите права ја окарактеризира, исто така, како мешање во приватноста гарантирана со Европската конвенција за човековите права во познатиот случај *Клас против Германија*. Оттогаш наваму судот во Стразбур постојано ја нагласува потребата националните закони да обезбедат соодветна заштита од арбитрерно и неконтролирано мешање на државата во приватноста на поединците. Не е доволно државата да донесе каква-таква регулатива за да се смета дека се задоволени барањата на човековите права. Во повеќе пресуди Европскиот суд за човековите права се осврнува врз квалитетот на националните закони коишто пред сè мора да се доволно јасни за на граѓаните да им се даде доволна индикација за

условите и околностите во кои властите се овластени да посегнат по тајно и потенцијално мешање во правата на почитување на приватниот живот и преписката (*Малоне против Обединетото Кралство, Кхан против Обединетото Кралство, Контрерас против Шпанија* и други).

Дури и кога домашниот систем има определени вградени заштитни законски механизми и тоа на различни нивоа, вклучувајќи инволвирање на независен судија, системот сè уште може да биде отворен за злоупотреби. За да се избегнат можните злоупотреби и самоволија, Европскиот суд за правата на човекот наведува дека во домашните закони мора да бидат дефинирани најмалку следните заштитни механизми: природата на казните дела за кои може да се нареди следење; дефиниција на категориите на лица чии комуникации може да се надгледуваат; максималното времетраење на таквото набљудување; процедурата која мора да се следи за анализа употреба и чување на добиените податоци; мерките на претпазливост кој што треба да се преземат доколку информацијата се соопштува на други лица и околностите во кои добиените информации можат или мораат да бидат избришани, а записите уништени (*Вебер и Саравија против Германија* од 2006 година).

Законот мора да биде изразен со таков степен на конкретност што околностите во кој тој би се применил да бидат доволно предвидливи во таа смисла што граѓаните би требало да знаат кога полицијата или други безбедносни органи би можеле да ги следат телефонските или другите приватни електронски комуникации.

Со оглед на фактот дека ризиците од арбитрерност се секогаш големи кога овластувањата на државните органи се остваруваат во тајност и поради тоа што имплементацијата на мерките за тајно следење на комуникацијата во практиката не се отворени за контрола од страна на засегнатите поединци или пошироката јавност, ќе биде спротивно на владеењето на правото ако правната дискреција доделена на извршната власт биде изразена во вид на неконтролабилна моќ.

Собирањето и архивирањето на податоците за граѓаните во врска со националната безбедност, исто така, мора да бидат во со закон утврдени граници. Во таа смисла, во законот мора да се предвидат видот на информацијата која што може да се сними; категориите на лица против кои може да се преземат мерки на следење и обработување на информациите, времето за кое податоците може да се чуваат, како и околностите во кои таквите мерки може да се преземат и на крајот, но не и најмалку важно, постапката која што мора да се почитува (*Ротару против Романија*). Ова подразбира и предвидување на реални процедури на надзор врз примената (супервизија), било во време кога наложените мерки биле во сила или подоцна.

Може да заклучиме дека мерките што сега се сака да се легализираат не ги почитуваат доследно принципите на законитост,

сразмерност и супсидијарност, како елементарна заштита од самоволие и злоупотреби. Согласно барањето за нужност и пропорционалност нагласено од страна на Европскиот суд за правата на човекот, мерките не може да се применуваат освен за најтешки кривични дела и организиран криминал. Покрај ова, мора да се обезбеди доволен, правилен и независен систем на контрола врз примената на сите мерки кои зафаќаат во приватноста на граѓаните.

Врз барањата што се повикуват на интересите на националната безбедност, пак, посебно треба да се гледа со еден здрав скептицизам. Имено, со предложените измени, безбедносните служби воопшто нема да треба пред некого да докажат дека постои директна, непосредна, конкретна и сериозна штета за државата и уставниот поредок, а не само неопределена или шпекулативна закана.

Со закон треба да се дозволи граѓаните да имаат пристап до независна институција (суд) пред кој ќе можат правно да ја оспоруваат секоја примена на овие мерки кон некое лице како и начинот на кој тоа е сторено.

Рокот за чување на необработените податоци за сообраќај е максималниот рок кој сега е предвиден како меѓународен стандард од 24 месеци (член 112, став 1), иако во повеќето земји од Европската унија најчесто е прифатен минималниот рок од 6 месеци за чување на податоците, со цел да се почитува сигурноста и тајноста на личните податоци. Покрај ова, ќе треба да се вградат и нови одредби во членот 112 од Законот со кои ќе се операционализира материјата содржана во Директивата 2006/24/ЕК на Европскиот Парламент и Советот на Европската унија за задржување на податоци добиени или обработени во врска со обезбедувањето јавно достапни електронски комуникациски услуги или јавни комуникациски мрежи.

Во Законот треба да се вградат и одредби со кои ќе се изврши усогласување со одредбите од Директивата 2009/136/ЕК на Европскиот Парламент и Советот на Европската унија со која се менува Директивата 2002/58/ЕК во врска со обработката на личните податоци и заштита на приватноста во секторот за електронски комуникации.

Транспарентност Македонија

"Ферид Бајрам" 39, 1000 Скопје Република Македонија

тел./факс: 02/ 31 21 100

www.transparentnost-mk.org.mk