УДК 343.985(497.11); 351.746.2(497.11)

CERIF: S 149

DOI: 10.51204/Anali_PFBU_25104A

Др Милана М. ПИСАРИЋ[*]

Остоја С. КАЛАБА, мастер[**]

ЗАДРЖАВАЊЕ ПОДАТАКА И КРИВИЧНИ ПОСТУПАК У СРБИЈИ[***]

Употреба информационе технологије омогућава надлежним државним органима да приликом предузимања мера и радњи ради спречавања, откривања и истраге кривичних дела те кривичног гоњења учинилаца кривичних дела обрађују податке о личности у до сада незабележеном обиму и на незамислив начин. Једна од спорних обрада је остваривање масовног, неселективног надзора електронских комуникација у виду задржавања комуникационих података, који о појединцу понекад могу да открију више и од самог садржаја комуникације. Таква обрада података представља мешање у гарантована људска права и слободе, а да то не би било и њихово кршење, морала би да буде правно уређена у складу са Уставом и међународним стандардима заштите људских права. Аутори у раду анализирају правни оквир за задржавање комуникационих података и приступ задржаним подацима за потребе кривичног поступка у Србији, посебно у светлу релевантне праксе Суда правде Европске уније и Европског суда за људска права.

Кључне речи: *Електронске комуникације. – Задржавање података. – Кривични поступак. – Заштита података о личности. – Приватност.*

---

[*] Доценткиња, Универзитет у Новом Саду – Правни факултет, Србија, *mpisaric@pf.uns.ac.rs*, ORCID iD: 0000–0001–8344–3349.

[**] Саветник у Служби Повереника за информације од јавног значаја и заштиту података о личности, докторанд, Србија, *kalaba.ostoja@gmail.com*.

[***] Поједини делови истраживања били су изложени у виду усменог саопштења на тему „Data retention and access to retained data for the purpose of criminal procedure in Serbia", на научном скупу *SSN2024: Surveillance in an Age of Crisis: the 10th Biennial Surveillance Studies Network / Surveillance & Society Conference 2024, hosted by the Institute of Criminology at the Faculty of Law and the Faculty of Law, University of Ljubljana, Slovenia*, одржаном од 28. до 31. маја 2024. године на Правном факултету Универзитета у Љубљани.

1. УВОД

Када је Едвард Сноуден открио да је *NSA* масовно прикупљала одређене метаподатке о комуникацијама, велики део света био је шокиран и изненађен. Иако је тадашњи председник Сједињених Америчких Држава (САД) у свом говору почетком 2014. године изјавио да се таквим системом не прикупљају садржај телефонских позива ни имена лица која разговарају (*Washington Post*, 2014), академска и стручна јавност је разумела и оно што није речено – да је реч о масовном прикупљању метаподатака, те да такав надзор представља задирање у приватност, а без одговарајућих, строгих критеријума за примену и без ефективне контроле од независних надзорних органа, потенцијално и кршење појединих основних људских права и слобода, те да води ка орвеловском друштву.[1] Таква „пракса" није била ни у том тренутку, а ни сада, својствена само САД – већ годинама је оправдано предмет расправе у јавном и научном дискурсу[2], (неадекватне) регулативе и последично судског преиспитивања у многим државама.

Право Европске уније (ЕУ) утицало је на правно уређење електронских комуникација у Србији, па и у погледу задржавања комуникационих података и приступа тим подацима. Усвајањем Директиве о задржавању података[3] (Директива 2006/24/*EC*) на нивоу ЕУ је створена обавеза пружалаца јавно доступних услуга електронске комуникације или јавних комуникационих мрежа да задрже одређене податке које прикупљају или обрађују у вези са тим услугама, како би се осигурало да буду доступни надлежним органима у сврху откривања и доказивања тешких кривичних дела те откривања и кривичног гоњења учинилаца тих дела. Међутим, српски законодавац није у довољној мери и на одговарајући начин испратио даљу судбину Директиве 2006/24/*EC* и прописа о задржавању података у државама чланицама, нарочито с обзиром на одлуке Суда правде ЕУ. Осим тога, нису узете у обзир ни релевантне одлуке

---

1 Више о томе Писарић (2019, 156).

2 Више о томе нпр. Rojszczak, Marcin. 2021. National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts, *European Constitutional Law Review* 17(4): 607–635 и Rojszczak, Marcin. 2021. The uncertain future of data retention laws in the EU: Is a legislative reset possible? *Computer Law & Security Review* 41, July.

3 Directive 2006/24/EC of The European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105/54 of 13/4/2006.

Европског суда за људска права (ЕСЉП), у којима је утврђено кршење права из Европске конвенције о људских правима (ЕКЉП) у вези са задржавањем података. Аутори у овом раду анализирају домаћи правни оквир задржавања података и приступа надлежних органа задржаним подацима за потребе кривичног поступка, који сагледавају посебно кроз призму одлука Суда правде ЕУ и ЕСЉП.

2. ПРАВНИ ОКВИР У СРБИЈИ

У Србији је, по узору на Директиву 2006/24/*ЕС*, задржавање података о електронским комуникацијама нормирано 2010. године усвајањем Закона о електронским комуникацијама,[4] у глави XVII „Тајност електронских комуникација, законито пресретање и задржавање података". Поједине одредбе из те главе проглашене су неуставним 2013. године Одлуком Уставног суда Републике Србије[5] (Одлука УС), а поједине су измењене следеће године.[6] Након тих интервенција, одредбе из главе XVII и даље важе, иако је 2023. године усвојен нови Закон о електронским комуникацијама[7] (ЗЕК 2023). Наиме, у чл. 180 ст. 1 ЗЕК 2023 прописано је да ступањем на снагу тог закона престаје да важи претходни Закон о електронским комуникацијама[8] (ЗЕК), а истовремено је утврђено, из необјашњивих и легислативно неоправданих разлога, да су и даље на снази поједине одредбе ЗЕК, међу којима су управо одредбе о задржавању података. Будући да је пропуштено (или избегнуто) да се у новом пропису којим се уређују електронске комуникације нормира и задржавање података, релевантне одредбе су неприродно и непрегледно остале ван органског текста системског закона. Ради свеобухватног сагледавања правног оквира задржавања података, важно је напоменути да су начелна правила садржана у неколико чланова ЗЕК и да су ближе уређена подзаконским актима (усвојеним на основу закона који је престао да важи). У наставку ћемо анализирати задржавање података и приступ задржаним подацима као два корака једног механизма.

---

4 *Службени гласник РС* 44/10.

5 Уставни суд Републике Србије, Иуз 1245/2010, 13. јун 2013, *Службени гласник РС* 60/13, 74–80.

6 Закон о изменама и допунама Закона о електронским комуникацијама, *Службени гласник РС* 62/2014.

7 *Службени гласник РС* 35/23.

8 *Службени гласник РС* 44/10, 60/13 – одлука УС, 62/14, 95/18 – др. закон и 35/23 – др. закон.

1.1. Задржавање података

1.1.1. Сврха задржавања

У чл. 128 ст. 1 изворног текста ЗЕК било је предвиђено да је оператор *дужан да задржи* податке о електронским комуникацијама за потребе спровођења истраге, откривања кривичних дела и вођења кривичног поступка, у складу са законом којим се уређује кривични поступак, те за потребе заштите националне и јавне безбедности Републике Србије, *у складу са законима којима се уређује рад служби безбедности Републике Србије и рад органа унутрашњих послова*. Део одредбе којим се упућује на те друге законе проглашен је 2013. године *неуставним* Одлуком УС.[9] Наредне године чл. 128 је *измењен*, тако што је потпуно *изостављена сврха задржавања података*. Тренутно важећи ЗЕК просто прописује дужност оператора да задржи податке о електронским комуникацијама (чл. 128 ст. 1) и да задржане податке чува 12 месеци од дана обављене комуникације (чл. 128 ст. 6), *не одређујући сврху* због које су те обавезе установљене.

1.1.2. Подаци који се задржавају

Што се тиче података у погледу којих постоје обавезе оператора, чл. 128 ст. 1 ЗЕК упућује на чл. 129 ст. 1, који утврђује *категорије података* који се задржавају *ради задовољења одређених потреба*. Одговор на питање *који се то тачно подаци задржавају* даје подзаконски акт – Правилник о захтевима за уређаје и програмску подршку за законито пресретање електронских комуникација и техничким захтевима за испуњење обавезе задржавања података о електронским комуникацијама[10] (Правилник[11]) – који у чл. 11–16 *таксативно* прописује које податке су

[9] Уставни суд (УС) је нашао да део „у складу са законом којим се уређује кривични поступак“ и део „у складу са законима којима се уређује рад служби безбедности Републике Србије и рад органа унутрашњих послова“ нису у сагласности са чл. 41 ст. 2 Устава, јер је једино суд надлежан да дозволи (одобри) одступање од Уставом зајемчене неповредивости тајности писама и других средстава комуницирања, „а не да се то право одређује у складу са законом“. Вид. Одлука УС, 79.

[10] *Службени гласник РС* 88/2015.

[11] Изворно, у чл. 129. ст. 4 ЗЕК било је прописано да ће *министарство* надлежно за телекомуникације, по прибављеном мишљењу министарства надлежног за послове правосуђа, министарства надлежног за унутрашње послове, министарства надлежног за послове одбране, Безбедносно-информативне агенције и органа надлежног за заштиту података о личности *ближе пропи-*

оператори дужни да задрже. Задржавају се подаци који су *потребни за*: 1) праћење и утврђивање *извора* комуникације,[12] 2) утврђивање *одредишта* комуникације,[13] 3) утврђивање *почетка, трајања и завршетка*

сати захтеве у вези са задржавањем података из чл. 129 ст. 1. Када је УС неуставном прогласио одредбу чл. 128 ст. 5, исто је учинио и са чл. 129 ст. 4 – чиме је нестао правни основ за подзаконско регулисање обавезе задржавања података. Међутим, такав акт је ипак усвојен. Наиме, чл. 127, којим се иначе уређује законито пресретање електронских комуникација, измењен је 2014. године тако што је у ст. 5 додато да ће министарство ближе прописати *и техничке захтеве за испуњење обавезе задржавања података* из чл. 128 и 129 закона. Правилник је усвојен управо на основу те одредбе.

[12] Сходно чл. 11 Правилника, то су следећи подаци: а) о јавно доступној телефонској услузи на фиксној локацији и јавно доступној телефонској услузи у јавној мобилној комуникационој мрежи: број са кога је иницирана комуникација; име и презиме физичког лица, односно назив правног лица и адреса претплатника или регистрованог корисника; б) о интернет приступу, електронској пошти, услузи преноса говора коришћењем интернета и других облика пакетске размене: додељени кориснички идентификатор или телефонски број за сваку комуникацију у јавној електронској комуникационој мрежи; име и презиме физичког лица, односно назив правног лица и адресу претплатника или регистрованог корисника коме је додељена *IP* адреса, корисничка идентификација или телефонски број у време комуникације; динамичка или статичка *IP* адреса додељена од провајдера услуге или провајдера приступа и корисничка идентификација претплатника или регистрованог корисника; идентификација дигиталне претплатничке линије или друге тачке извориште комуникације.

[13] Сходно чл. 12 Правилника, то су следећи подаци: а) о јавно доступној телефонској услузи на фиксној локацији и јавно доступној телефонској услузи у јавној мобилној комуникационој мрежи: одабрани број (број који је позван), а у случају додатних услуга (усмеравање, преношење комуникације и конференцијска веза) и број на који је комуникација преусмерена, односно бројеви који су укључени у конференцијску везу; име и презиме и адреса претплатника или регистрованог корисника; б) о интернет приступу, електронске поште, услузи преноса говора коришћењем интернета и другим облицима пакетске комуникације: динамичка или статичка *IP* адреса додељена од провајдера услуге или провајдера приступа и корисничка идентификација претплатника или регистрованог корисника у време комуникације; корисничка идентификација или телефонски број припадајућег саговорника услуге преноса говора коришћењем интернета; име и презиме и адреса претплатника или регистрованог корисника, као и корисничка идентификација припадајућег саговорника у комуникацији; идентификација дигиталне претплатничке линије или друге тачке одредишта комуникације; подаци о комуникацији (сходно чл. 2 ст. 1 тач. 8 то су подаци који представљају сигнализацију повезану с циљаном електронском комуникационом услугом, мрежом или другим корисником, укључујући и сигнализацију употребљену за успостављање комуникације, контролу њеног тока (нпр. комуникација прихваћена, комуникација пребачена), чија су садржина и подаци доступни операторима електронских комуникација (нпр. време трајања комуникације).

комуникације,[14] 4) утврђивање *врсте* комуникације,[15] 5) идентификацију *терминалне опреме* корисника[16] и 6) утврђивање *локације мобилне терминалне опреме корисника*.[17] Осим тога, одредбама ЗЕК је прописано да обавеза задржавања обухвата и податке о успостављеним позивима који нису одговорени, али не и податке о позивима чије успостављање није

[14] Сходно чл. 13 Правилника, то су следећи подаци: а) о јавно доступној телефонској услузи на фиксној локацији и јавно доступној телефонској услузи у јавној мобилној комуникационој мрежи: датум, време почетка, трајања и завршетка комуникације; б) о интернет приступу, електронској пошти, услузи преноса говора коришћењем интернета и других облика пакетске комуникације: датум, време пријаве и одјаве приликом коришћења приступне услуге, у оквиру одговарајуће временске зоне, као и датум и време слања и примања електронске поште и позива путем услуге преноса говора коришћењем интернета, у оквиру одговарајуће временске зоне, за услуге које пружа оператор.

[15] Сходно чл. 14 Правилника, то су следећи подаци: а) о јавно доступној телефонској услузи на фиксној локацији и јавно доступној телефонској услузи у јавној мобилној комуникационој мрежи: подаци о коришћеној телефонској услузи; б) о електронској пошти, услузи преноса говора коришћењем интернета и другим облицима пакетске комуникације: подаци о коришћеној интернет услузи.

[16] Сходно чл. 15 Правилника, то су следећи подаци: а) о јавно доступној телефонској услузи у јавној мобилној комуникационој мрежи: *IMSI* број са којег је иницирана комуникација и *IMSI* број према којем је иницирана комуникација, као и *IMEI* број средства за комуницирање са кога је иницирана комуникација и *IMEI* број према којем је иницирана комуникација; б) о припејд услузи код јавно доступне телефонске услуге на фиксној локацији и код јавно доступне телефонске услуге у јавној мобилној комуникационој мрежи: серијски број картице (за јавно доступну телефонску услугу на фиксној локацији) и серијски број припејд картице и место са кога је извршена електронска допуна, уколико је то могуће за јавно доступну телефонску услугу у јавној мобилној комуникационој мрежи; в) о припејд услузи код интернет приступа, електронској пошти, услузи преноса говора коришћењем интернета и другим облицима пакетске размене: серијски број картице; г) о јавно доступној телефонској услузи на фиксној локацији, интернет приступу, електронској пошти, услузи преноса говора коришћењем интернета и другим облицима пакетске комуникације: серијски број уређаја, *MAC* адреса, динамичка и статичка *IP* адреса додељена од провајдера услуге или приступа, у одговарајућој временској зони, други подаци који једнозначно идентификују терминални уређај корисника.

[17] У чл. 16 Правилника није одређено који се то подаци задржавају него је прописана дужност оператора да омогући техничко повезивање своје опреме са опремом надлежних државних органа употребом одговарајућег техничког интерфејса којим се омогућава пренос података о свим мобилним терминалним уређајима који су се појавили на одређеној географској, физичкој или логичкој локацији, а у складу са техничким стандардима или могућностима поједине мобилне електронске комуникационе технологије.

успело (чл. 129 ст. 2), као ни податке које оператор није произвео нити обрадио (чл. 129 ст. 5). Изричито је забрањено задржавање података који откривају садржај комуникације (чл. 129 ст. 3).

1.2. Приступ задржаним подацима

1.2.1. Сврха остваривања приступа

У изворном тексту ЗЕК није била предвиђена сврха остваривања приступа задржаним подацима, а након што је чл. 128 измењен 2014. године, важећим ЗЕК је најпре прописано да приступ задржаним подацима није допуштен без пристанка корисника, а потом је такву могућност предвиђена *као изузетак* (чл. 128 ст. 2). Наиме, приступ задржаним подацима је допуштен изузетно „на одређено време и на основу одлуке суда". При томе, одредбама ЗЕК је јасно одређена *сврха* остваривања приступа задржаним подацима, а то је неопходност вођења кривичног поступка или заштите безбедности РС, [18] док у погледу начина упућује на други закон.

Пропис којим би требало да се уреди остваривање приступа задржаним подацима када је то неопходно ради вођења кривичног поступка је Законик о кривичном поступку[19] (ЗКП). У чл. 286 („Овлашћења полиције") ЗКП прописана је *дужност полиције*, уколико постоје *основи сумње* да је извршено *кривично дело* за које се гони *по службеној дужности*, да предузме потребне мере и радње *са циљем* да се пронађе учинилац кривичног дела, да се учинилац или саучесник не сакрије или не побегне, да се открију и обезбеде трагови кривичног дела и предмети који могу послужити као доказ те да се прикупе сва обавештења која би могла бити од користи за успешно вођење кривичног поступка. Ради испуњења те дужности полиција може, *по налогу* судије за претходни поступак, а на предлог јавног тужиоца да: 1) прибави евиденцију (већ) остварене *телефонске* комуникације, 2) прибави евиденцију коришћених базних станица, 3) изврши лоцирање места „са којег се обавља комуникација" (чл. 286 ст. 3).

---

[18] У изворном тексту ЗЕК законодавац је био одредио *заштиту националне и јавне безбедности* Републике Србије као сврху задржавања података (у чл. 128 ст. 1, пре измена), док је приликом формулисања измењеног чл. 128 и одређивања сврхе приступа задржаним подацима (чл. 128 ст. 2) доследно испратио текст из чл. 41. ст. 2 Устава (у којем стоји „заштита безбедности РС").

[19] *Службени гласник РС* 72/11, 101/11, 121/12, 32/13, 45/13, 55/14, 35/19, 27/21 – одлука УС и 62/21 – одлука УС.

1.2.2. Начин остваривања приступа

Оператор је дужан да задржава податке на *начин* да им се *без одлагања* може *приступити*, односно да се без одлагања могу *доставити* на основу одлуке суда (чл. 128 ст. 7). Анализом ЗЕК и подзаконских аката може се уочити да надлежни државни органи долазе до задржаних података на два начина: а) *непосредно* – тако што *остварују приступ* просторијама, електронској комуникационој мрежи, припадајућим средствима или електронској комуникационој опреми оператора; или б) *посредно* – тако што им оператори *достављају тражене податке.*[20]

Јаснији одговор на питање шта се под тим подразумева сазнајемо из Правилника. Правилник садржи општу одредбу којом је прописано да *сви подаци* који се задржавају у складу са ЗЕК морају надлежним државним органима, *путем одговарајућег техничког интерфејса*, бити *доступни* за период од последњих 12 месеци од дана обављене комуникације, а у складу са законом (чл. 9 ст. 2 Правилника). У погледу *података о локацији*, Правилник у чл. 16 и 21 обавезује операторе да омогуће техничко повезивање своје опреме са опремом надлежних државних органа *употребом одговарајућег техничког интерфејса*, путем кога се омогућава *пренос* одређених комуникационих података.[21]

1.3. Задржавање података, приступ задржаним подацима и Устав

Приликом нормирања задржавања података није у довољној мери и на адекватан начин сагледан један важан аспект, а то је оправданост таквог мешања у гарантована људска права и слободе. Одредбама ЗЕК се начелно предвиђа, а подзаконским актима прецизно уређује задржавање великог броја података, који надлежним органима, када им приступе и обраде их, чак и када се то врши у легитимном циљу,

[20] Јасно разликовање између два режима приступа задржаним подацима произлази и из обавезе вођења евиденција (чл. 128 ст. 8 и 9 ЗЕК, чл. 10 Правилника) и обавезе стварања техничког интерфејса посредством којег се задржани подаци чине доступним надлежним органима, како се то Правилником захтева.

[21] Реч је о: а) подацима *о свим* мобилним терминалним *уређајима* који су се појавили на одређеној географској, физичкој или логичкој локацији, сходно чл. 16 ст. 1; б) подацима *о тренутној* географској, физичкој или логичкој *локацији појединачног средства* за електронску комуникацију, сходно чл. 21 ст. 1. Правилника.

омогућују доношење врло прецизних закључака о приватном животу лица чији су подаци задржани, као што су свакодневне навике, места трајних или привремених боравака, дневна или друга кретања, обављане активности, друштвени односи и друштвене средине које су лица посећивала – што све има значајан и потенцијално свеобухватан утицај на право на приватност и заштиту података о личности, као и на право на слободу изражавања и кретања.

С тим у вези, неопходно је осврнути се на *усклађеност релевантних одредаба* ЗЕК и ЗКП са *чл. 41* Устава Републике Србије[22] (Устав) којим се *гарантује неповредивост тајности* писама и других средстава комуницирања (ст. 1), [23] а *одступање* дозвољава само на одређено време и на основу одлуке суда, ако је то неопходно ради вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом (ст. 2).

У Одлуци УС је пре више од 10 година истакнуто да *уставноправна заштита обухвата* не само садржај него и *формална обележја комуникације*,[24] што значи да и одступање од неповредивости тајности података о комуникацији може бити дозвољено једино ако је у складу са Уставом.

Само по себи, свеопште масовно задржавање и чување података о свим комуникацијама свих корисника на основу ЗЕК несумњиво представља одступање од гарантоване тајности комуникација – а могло би бити дозвољено само ако би били испуњени услови који су прописани Уставом. Ипак, чини се да законодавац задржавање података не третира као одступање од уставне гаранције – не одређује сврху због које су оператори дужни да задрже и чувају податке (неопходност вођења кривичног поступка или заштите безбедности Републике Србије). Сврха задржавања података не може се изводити из сврхе остваривања приступа задржаним подацима, прописане у чл. 128 ст. 2, јер су задржавање и приступ задржаним подацима два вида одступања од гарантованих права и неопходно је посебно оправдање за сваки. Такође, навођење одређених „потреба“ због које се поједине категорије

---

22 *Службени гласник РС* 98/06, 115/21 – амандмани I–XXIX и 16/22.

23 Интересантно је приметити да и ЗЕК и ЗЕК 2023 садрже правило о тајности комуникација. Међутим, док се у глави XVII ЗЕК, у којој су одредбе о задржавању података, тајност везује само за садржај електронских комуникација (чл. 126), у ЗЕК 2023 се јасно препознаје и тајност и са њима повезаних података о саобраћају повезаних са електронским комуникацијама (чл. 160 ЗЕК 2023).

24 Одлука УС, 78.

података задржавају у чл. 129 ст. 1 није исто што и одређивање сврхе задржавања података. Осим тога, захтеви да је одступање дозвољено „на основу одлуке суда“ и „на одређено време“ нису узети у обзир када је прописана обавеза задржавања и чувања података.

Приликом нормирања приступа задржаним подацима, законодавац се у чл. 128 ст. 2 ЗЕК доследно руководио формулацијом из Устава.[25] Међутим, не би се могло рећи да ЗКП, којим би требало да се уреди одступање од гарантоване неповредивости тајности комуницирања ради вођења кривичног поступка, то чини на исправан начин, из најмање два разлога: а) одступање може бити одобрено само одлуком суда – а налог није одлука суда (ЗКП познаје три врсте одлука у кривичном поступку: наредбу, решење и пресуду – чл. 269); б) одступање је допуштено само „на одређено време“ – а у чл. 286 ст. 3 ЗКП такав захтев се не поставља.

Такође, овлашћење из чл. 286 ст. 3 ЗКП односи се на прибављање *неких од података који се задржавају*, односно само података о телефонској комуникацији, али не и о осталим видовима електронске комуникације. Сходно томе, тај члан *не би могао да се користи за остваривање приступа* свим оним категоријама и врстама података који се задржавају на основу ЗЕК и Правилника, а који нису њиме обухваћени[26] – другим речима, одредбама ЗКП се не уређује начин

[25] Могуће је да је законодавац приликом измене чл. 128 узео у обзир и аргументе из Одлуке УС. Наиме, Уставни суд је нашао да, иако је оспореном одредбом (изворног чл. 128 ст. 1) *прописана само општа обавеза* оператора да задржава податке и *одређена сврха* због које се задржавање прописује *а не и начин коришћења* задржаних података, спорно је то што се *увођење те обавезе* врши у складу са другим, одговарајућим законима, на који начин се установљава обавеза оператора *којом посредно може доћи до повреде тајности средстава комуникације* уколико се задржани подаци не користе сагласно чл. 41 ст. 2 Устава, што значи без одлуке суда и без одређивања времена у коме се они користе *већ на основу решења из наведених закона*. Уставни суд је истакао: „Услови и сврха дозвољеног одступања од тајности средстава комуницирања су утврђени Уставом и као такви не могу бити предмет законске материје, јер се начин остваривања овог права може прописати само законом.“ Одлука УС, 78.

[26] Примера ради, чл. 286 ст. 3 ЗКП се не би могао применити за прибављање податка о динамичкој или статичкој *IP* адреси додељеној од провајдера услуге или провајдера приступа, који се задржава у смислу чл. 12 Правилника, или податка о датуму, времену пријаве и одјаве приликом коришћења приступне услуге, у оквиру одговарајуће временске зоне, као и датуму и времену слања и примања електронске поште и позива путем услуге преноса говора коришћењем интернета, у оквиру одговарајуће временске зоне, за услуге које пружа оператор, који се задржава у смислу чл. 13 Правилника – чак и када би суд издао налог за прибављање таквих података.

на који се њима остварује приступ. Осим тога, захтев за достављање таквих задржаних података, који би евентуално операторима упутила полиција или јавно тужилаштво на основу општих одредаба ЗКП, био би споран са становишта уставности.

Питањем уставности одредаба о задржавању података бавио се и повереник за информације од јавног значаја и заштиту података о личности (повереник), када је пре више од десет година извршио надзор над спровођењем и извршавањем Закона о заштити података о личности[27] (ЗЗПЛ) од стране руковалаца-оператора мобилне и фиксне телефоније у Републици Србији (Извештаји повереника за 2012).[28] На основу резултата тог надзора, повереник и заштитник грађана су у 14 тачака припремили Предлог препорука за унапређење стања у овој области, за које се, узимајући у обзир анализирано у овом раду, не може са сигурношћу рећи да су до данашњег дана примењене у пуном и адекватном обиму. Слична је ситуација и са операторима електронских комуникација који пружају услуге приступа интернету и интернет услуге (Извештај повереника за 2015).

Не само да је упитна усклађеност правног оквира о задржавању и приступу задржаним подацима са Уставом него и усаглашеност с правом ЕУ и са ЕКЉП јер се не узимају у обзир стандарди заштите људских права утврђени у пракси Суда правде ЕУ и ЕСЉП.

3. СТАНДАРДИ ЗАШТИТЕ ЉУДСКИХ ПРАВА

3.1. Пракса Суда правде ЕУ

Иако је Директива 2006/24/*EC* још пре десет година стављена ван снаге јер је широко и особито тешко задирала у основна људска права, а да такво мешање није било прецизно ограничено на оно што је стро-

[27] *Службени гласник РС* 87/18.

[28] Предмет надзора је био приступ задржаним подацима о комуникацији, па је, на основу утврђених чињеница током надзора, констатовано да обрада тих података, сваког појединачно, а поготово свих заједно, и то у периоду од 12 месеци, представља озбиљно задирање у приватност грађана, те да се тиме одступа од уставне гаранције неповредивости тајности средстава комуницирања и од одредбе да су одступања дозвољена само на одређено време и на основу одлуке суда, ради вођења кривичног поступка или заштите државне безбедности.

го нужно,[29] комуникациони подаци се и даље задржавају у државама чланицама, а национални прописи и поступање надлежних органа у више држава били су предмет преиспитивања од Суда правде ЕУ.[30] Да би се утврдио став Суда Правде ЕУ о задржавању података и приступу задржаним подацима од надлежних органа у државама чланицама, анализиране су одлуке у предметима *SpaceNet AG*,[31] *Tele2 Sverige*,[32] *La Quadrature du Net*,[33] *Privacy International*[34] и *Prokuratuur*.[35]

3.1.1. Задржавање података

Суд правде ЕУ се на *сврху задржавања* података нарочито осврнуо у одлуци у предмету *SpaceNet AG*. Пре свега, када је реч о *оправданости ограничења права*, Суд је заузео став да су циљеви у првој реченици чл. 15 ст. 1 Директиве 2002/58/*ЕС*[36] наведени таксативно, следом чега законска мера донета на основу те одредбе треба делотворно и строго да одговара једном од тих циљева, а да *постојање могућих потешкоћа* да се *прецизно утврде случајеви и услови* у којима треба спровести циљано задржавање *не може да буде оправдање* за државу чланицу да пропише *опште и неселективно задржавање* података о саобраћају и локацији комуникација, *на начин да изузетак постане правило*.[37] Наиме, Суд правде ЕУ је заузео јасан став да национално законодавство које предвиђа задржавање података треба да испуњава *објективне критеријуме*, успостављајући *везу између података* који треба да

[29] CJEU, joined cases C-293/12 and C-594/12, 8 April 2014.

[30] Више о томе Podkowik, Rybski, Zubik 2021, 1608–1609.

[31] CJEU, joined cases C-793/19 and C-794/19, 27 October 2022.

[32] CJEU, joined cases C-203/15 and C-698/15, 21 December 2016.

[33] CJEU, joined cases C-511/18, C-512/18 and C-520/18, 6 October 2020.

[34] CJEU, case C-623/17, 6 October 2020.

[35] CJEU, case C-746/18, 2 March 2021.

[36] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201/37 of 12/07/2002; Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337/11, of 18/12/2009.

[37] *SpaceNet AG*, пара. 104–113.

се задрже *и циља* који се настоји постићи. Суд је нашао да из његове судске праксе произлази да, у складу с начелом пропорционалности, постоји хијерархија између тих циљева с обзиром на њихову важност и да управо *важност циља*, који се таквом мером настоји остварити, *мора бити повезана с тежином задирања* у гарантована права, које из тога произлази. Сходно томе, истакао је да је *праву ЕУ супротно* национално законодавство које *у сврху борбе против тешких кривичних дела као правило предвиђа опште и неселективно задржавање података* о саобраћају и локацији комуникације јер прекорачује оно што је строго нужно па се не може сматрати оправданим у демократском друштву. Истиче се да се кривична дела, чак ни нарочито тешка, не могу изједначити с претњом по националну безбедност. Наиме, таквим изједначавањем би се могла створити међукатегорија – између националне и јавне безбедности – како би се на другу категорију могли применити захтеви који су својствени првој[38], што није и не може бити оправдано.

Суд правде ЕУ је државама дао *јасне смернице* како да у националним прописима *уреде задржавање података на начин који није противан праву ЕУ*. Тако је у одлуци у предмету *Tele2 Sverige* државама чланицама остављена могућност да националним законима предвиде *циљано задржавање* података о саобраћају и локацији комуникације у сврху борбе против криминала, али уз постојање *одговарајућег одобрења и ефективног надзора* приликом спровођења тих мера које би вршио суд или независно тело и уз поштовање принципа *временског ограничења* и у односу на оно *што је нужно и неопходно* за *конкретно одређену и оправдану сврху*.[39] Штавише, у одлуци у предмету *La Quadrature du Net* Суд правде ЕУ је дао *смернице за поједине облике задржавања података* и заузео став да се праву ЕУ не противе одређене мере, уколико су законом прописана јасна и прецизна правила, посебно ако су испуњени

[38] *SpaceNet AG*, пара. 70–74, 92–94, 117–124.

[39] *Tele2 Sverige*, пара. 108–112, 116–125. Такође, у тој одлуци Суд правде ЕУ је изнео и став да када је реч о циљевима који могу оправдати национални пропис којим се одступа од начела поверљивости електронских комуникација, треба подсетити да, у мери у којој је, како је то утврђено у пара. 90 и 102 те пресуде, набрајање циљева у првој реченици члана 15 став 1 Директиве 2002/58 исцрпног карактера, приступ задржаним подацима мора учинковито и строго испуњавати један од тих циљева. Будући да циљ тог прописа мора бити у вези с озбиљношћу мешања у темељна права које узрокује тај приступ, из тога следи да у подручју спречавања, истраге, откривања и прогона кривичних дела само борба против тешких кривичних дела може оправдати такав приступ задржаним подацима (вид. *Tele2 Sverige*, пара. 115).

одређени *материјални и формални услови*, а нарочито да погођена лица имају на располагању *делотворне гаранције* против ризика и опасности од злоупотребе.[40]

[40] Реч је о мерама које омогућавају: а) *опште и неселективно задржавање података* о саобраћају и локацији комуникације *ради заштите националне безбедности* у ситуацијама у којима је дотична држава чланица суочена с озбиљном претњом по националну безбедност која се показала стварном и тренутном (непосредном) или предвидљивом, ако одлука којом је предвиђено задржавање података може бити предмет делотворног надзора који врши суд или независан управни орган, чија одлука има обавезујући карактер, а којом се настоји проверити да ли постоји једна од тих ситуација и да ли се поштују услови и гаранције који се морају предвидети, те ако се наведена одлука може издати само за раздобље које је временски ограничено на оно што је строго нужно, али се може продужити у случају наставка постојаности те опасности, б) *циљано задржавање података* о саобраћају и локацији *ради заштите националне безбедности, борбе против тешких кривичних дела и спречавања озбиљних претњи јавној безбедности*, које је ограничено на основу објективних и недискриминаторних критеријума, зависно од категорије дотичних лица или посредством геолокацијског критеријума, те које се одређује за раздобље чије је трајање временски ограничено на оно што је строго нужно, али се може продужити; в) *опште и неселективно задржавање IP адреса* додељених извору везе за раздобље чије је трајање временски ограничено на оно што је строго нужно, а *у сврху заштите националне безбедности, борбе против тешких кривичних дела и спречавања озбиљних претњи јавној безбедности*; г) *опште и неселективно задржавање података* о грађанском идентитету корисника електронских комуникационих средстава *у сврху заштите националне безбедности, борбе против криминала и заштите јавне безбедности*; д) *хитно задржавање података* о саобраћају и локацији комуникација у одређеном ограниченом трајању којима ти пружаоци услуга располажу *ради борбе против тешких кривичних дела и заштите националне безбедности*, на основу одлуке надлежног органа која подлеже делотворном судском надзору, поштујући границе онога што је строго нужно; ђ) *аутоматску анализу и прикупљање у стварном времену података* о саобраћају и локацији комуникације у случају да је ограничено на ситуације у којима је држава суочена с *озбиљном претњом по националну безбедност* која се показала стварном и тренутном (непосредном) или предвидљивом, ако коришћење такве анализе може бити предмет делотворног надзора који обавља суд или независан управни орган чија одлука има обавезујући карактер, а којом се настоји проверити да ли постоји ситуација која оправдава наведену меру и да ли се поштују услови и гаранције који се морају предвидети и е) *прикупљање у стварном времену техничких података* о локацији употребљене терминалне опреме, уколико је ограничено на лица у односу на која постоји оправдан и јасан разлог за сумњу да су на било који начин укључене *у терористичке активности*, и подлеже претходном надзору који обавља суд или независни управни орган, чија одлука има обавезујући карактер, како би се осигурало да се такво прикупљање у стварном времену одобри само у границама онога што је строго нужно. *La Quadrature du Net*, пара. 168, 192. Више о томе Бугарски, Писарић 2020.

3.1.2. Приступ задржаним подацима

У одлуци у предмету *Privacy International* Суд правде ЕУ је закључио да је *праву ЕУ противан* национални пропис, који државном органу омогућава да ради *заштите националне безбедности* наложи пружаоцима електронских комуникационих услуга *општи и неселективни пренос* података о саобраћају и локацији комуникације јер се тиме *прекорачују границе оног што је строго нужно* и не може се сматрати оправданим у демократском друштву. Чак и у случају конкретне угрожености националне безбедности напомиње се да се *пропис не сме ограничити само на то* да предвиди да захтев за приступ задржаним подацима одговара остварењу прописаног циља него се морају предвидети *материјални и формални услови* којима се уређује приступ подацима на основу објективних критеријума, како би се *дефинисале околности и услови* под којима надлежним органима може бити одобрен приступ. Посебно треба водити рачуна о томе да ли је успостављен однос између података чији је пренос предвиђен и претње по националну безбедност те о томе да ли постоји јасна веза између лица чијим задржаним подацима ће бити приступљено и конкретно одређеног угрожавања националне безбедности.[41] Такав захтев *тим пре важи и за омогућавање приступа задржаним подацима за потребе кривичног поступка*.

Суд правде ЕУ је у одлуци у предмету *Prokuratuur* заузео став да *само циљеви борбе против тешких кривичних дела* или спречавања озбиљних претњи по јавну безбедност могу оправдати приступ државних органа скупу података о саобраћају или локацији комуникације, који могу пружити информације о комуникацијама које је корисник извршио средством електронске комуникације или о локацији терминалне опреме којом се користи, а на основу којих је могуће извести прецизне закључке о приватном животу дотичних лица, док други чиниоци *не могу оправдати* такав приступ са циљем спречавања, истраге и откривања *кривичних дела уопште*.[42] Даље, приступ у начелу може бити одобрен, с обзиром на циљ борбе против тешког криминалитета,

---

41 *Privacy International*, пара. 74–82.

42 У том погледу, Суд правде ЕУ је навео да *чак и приступ ограниченој количини података* или приступ подацима *из кратког временског раздобља* може пружити прецизне информације о приватном животу корисника средства електронске комуникације јер количина доступних података и конкретне информације о приватном животу дотичног лица, које из њих произлазе, представљају околности које се могу оценити тек након приступа тим подацима. Међутим, одобрење суда или надлежног независног органа нужно се даје пре него што се може приступити подацима и информацијама које из њих произлазе, због чега се оцена озбиљности задирања остваривањем приступа нужно врши с обзиром на ризик који је општесвојствен категорији тражених

само у односу на податке лица за која постоји *јасна сумња* да намеравају да изврше, да врше или су извршили тешко кривично дело или да су на други начин учествовали у том делу.[43] У сврху осигурања пуног поштовања тих услова у пракси, битно је да се *пре приступа* надлежних националних органа задржаним подацима *спроведе надзор* суда или независног органа, поводом образложеног захтева у оквиру кривичног поступка. Захтев независности, који мора испунити орган задужен за обављање претходног надзора, налаже да тај орган има својство треће стране у односу на орган који захтева приступ подацима, тако да може извршити надзор објективно и непристрано и без спољашњег утицаја. Конкретно, захтев независности у кривичном поступку подразумева да тело задужено за тај претходни надзор, с једне стране, није укључено у спровођење предметне кривичне истраге и да, с друге стране, има неутралан положај у односу на странке кривичног поступка, односно да је таквог статуса да може осигурати праведну равнотежу између, с једне стране, интереса повезаних с потребама истраге у оквиру борбе против криминалитета и, с друге стране, основних права на поштовање приватног живота и заштите података о личности лица чији су подаци обухваћени приступом. Закључујући свој став, Суд правде ЕУ наводи да те критеријуме не може испуњавати јавно тужилаштво као државни орган надлежан да води истрагу и, зависно од случаја, заступа оптужбу, из чега произлази да јавно тужилаштво није у положају да извршава претходни надзор над применом мера приступа задржаним подацима.[44] Из разлога оправдане хитности, могуће је спровести и накнадни надзор, који треба да уследи у кратком временском периоду по остваривању приступа подацима.[45]

података за приватни живот дотичних лица, при чему није важно да се зна да ли су информације о приватном животу које из њих произлазе у конкретном случају осетљиве. *Prokuratuur*, пара. 35–45.

[43] Ипак, у *посебним околностима*, попут оних у којима терористичке активности представљају претњу по кључне интересе националне безбедности, одбране или јавне безбедности, приступ подацима *других лица* може се одобрити кад постоје објективни елементи који омогућавају да се закључи да ти подаци у конкретном случају могу дати стваран и недвосмислен допринос борби против таквих активности. *Prokuratuur*, пара. 49–58.

[44] *Prokuratuur*, пара. 51–59. Више о примени принципа пропорционалности и независности органа у погледу приступа задржаним подацима вид. Rovelli, Sophia. 2021. Case Prokuratuur: proportionality and the independence of authorities in data retention, *European Papers-A Journal on Law and Integration* 2021.1, 199–210.

[45] У погледу питања да ли се може непостојање претходног надзора независног органа надоместити накнадним судским надзором законитости приступа задржаним подацима, Суд правде ЕУ је истакао да накнадни надзор не

3.2. Пракса ЕСЉП

Ради испитивања усклађености домаћег правног оквира са ЕКЉП, анализиране су одлуке ЕСЉП у предметима *Ekimdzhiev and others v. Bulgaria*,[46] *Škoberne v. Slovenia*[47] и *Podchasov v. Russia*,[48] поводом представки у којима су подносиоци истицали да им је повређено право из чл. 8 ЕКЉП тиме што су пружаоци услуга задржали њихове комуникационе податке и што су надлежни орган приступили тим подацима.

3.2.1. Ekimdzhiev and others v. Bulgaria

ЕСЉП је утврдио да су, према бугарском закону, сви пружаоци комуникационих услуга дужни да *задрже* и шест месеци од окончања комуникације *чувају све* податке о претплатнику, саобраћају и локацији свих корисника, с циљем да ти подаци буду доступни различитим надлежним органима за одређене, различите сврхе. Како се од пружалаца захтева да задрже податке који се могу, појединачно или у комбинацији с другима, односити на „приватни живот", такво, законом прописано задржавање, само по себи, представља мешање у право на поштовање приватног живота и преписке, *без обзира на то да ли надлежни органи накнадно приступају задржаним подацима*.[49] При томе, такво мешање се *може приписати бугарској држави*, иако га врше приватна лица, јер су на то обавезана законом.[50] ЕСЉП је даље нашао да бугарски надлежни органи могу да *приступе* задржаним комуникационим подацима,

---

омогућава испуњење циља претходног надзора, који се састоји у спречавању да се одобри приступ предметним подацима који прекорачује границе оног што је строго нужно. *Prokuratuur*, пара. 49–58.

[46] ECtHR, *Ekimdzhiev and others v. Bulgaria* (Application no. 70078/12), January 11, 2022.

[47] ECtHR, *Škoberne v. Slovenia* (Application no. 19920/20), 15 February 2024.

[48] ECtHR, *Podchasov v. Russia* (Application no. 33696/19), 13 February 2024.

[49] *Ekimdzhiev and others v. Bulgaria*, пара. 372.

[50] *Ekimdzhiev and others v. Bulgaria*, пара. 375. Идентичан став ЕСЉП је заузео у предмету *Podchasov v. Russia* који се односио на законску обавезу пружаоца интернет комуникационих услуга да све податке о комуникацији чува годину дана, а садржај свих комуникација шест месеци и да омогући приступ тим подацима и достави их органима за спровођење закона или службама безбедности у околностима одређеним законом, заједно са информацијама неопходним за дешифровање електронских порука ако су шифроване (пара. 50–52), као и у предмету *Škoberne v. Slovenia* који се односио на обавезу пружалаца телекомуникационих услуга да податке о саобраћају и локацији који се односе на фиксну и мобилну телефонију свих корисника телекомуникационих

ако је то неопходно ради остваривања једног или више законом одређених циљева. Према мишљењу ЕСЉП, како комуникациони подаци било ког лица теоретски могу постати неопходни за једну или више тих сврха, то и подносиоци представке могу бити погођени оспореним законодавством. Због тога је ЕСЉП утврдио да *приступ надлежних органа* задржаним комуникационим подацима представља *даље мешање* у право из чл. 8 ЕКЉП. [51] Поводом *оправданости* мешања у право из чл. 8 ЕКЉП, ЕСЉП је истакао да задржавање комуникационих података од пружалаца услуга и накнадни приступ од државних органа у појединачним случајевима морају бити праћени, *mutatis mutandis*, *истим мерама заштите као и тајни надзор комуникације*.[52]

Иако бугарско законодавство прописује одређене мере заштите с циљем да надлежни органи приступају задржаним комуникационим подацима само када је то оправдано, с обзиром на то да је потребно претходно *одобрење суда*, према оцени ЕСЉП, то је ипак *испод захтеваног стандарда делотворности заштите*.[53] Када је реч о *„судбини"*

услуга задрже и чувају 14 месеци и по захтеву доставе надлежним органима за одређене сврхе спровођења закона, при чему различити органи могу приступити тим подацима (пара. 125–128).

[51] *Ekimdzhiev and others v. Bulgaria*, пара. 376.

[52] Суд је истакао да, с обзиром на технолошки и друштвени развој у последње две деценије у области електронских комуникација, комуникациони подаци могу открити велики број података о личности, те уколико их надлежни органи прибављају масовно, могу се користити за стварање интимне слике о лицу, кроз мапирање друштвених мрежа, праћење локације, праћење претраживања интернета, мапирање образаца комуникације и увид у то са ким је то лице комуницирало и када и сл. Прибављање тих података *путем масовног и општег задржавања и приступа* задржаним подацима стога може бити *једнако наметљиво као и масовно прикупљање садржаја комуникација*, због чега њихово пресретање, задржавање и коришћење од надлежних органа треба анализирати *у контексту мера заштита* које се односе на садржај комуникације. *Ekimdzhiev and others v. Bulgaria*, пара. 394–395.

[53] Суд је утврдио да се у захтевима за приступ који се подносе ван оквира већ покренутих кривичних поступака наводе основ и сврха тражења приступа задржаним подацима, као и потпуни приказ околности које показују да су подаци потребни за тачно одређену и релевантну сврху. Насупрот томе, у погледу *захтева за приступ у вези са кривичним поступком*, иако би требало да садрже информације о наводном кривичном делу у вези са којим се приступ тражи, *надлежни органи нису изричито обавезани* да у захтеву објасне зашто су ти подаци заиста потребни (само треба да садржи опис околности које су у основи захтева) нити да судији „у потпуности и искрено" открију сва питања која су релевантна за оцену основаности захтева за приступ, укључујући питања која могу „ослабити" оправданост захтева, па ни да приложе пратећи материјал – што судију може онемогућити да правилно процени да ли је захтев за приступ

задржаних података којима приступају надлежни органи, ЕСЉП је дошао до закључка да се ти подаци једноставно чувају у списима кривичног предмета, да прате његову судбину и да им може приступити свако ко има приступ самом спису, па се *не може прихватити да постоји одговарајући ниво заштите података* јер *не постоје одредбе које на адекватан начин уређују* чување, приступ, испитивање, коришћење, саопштавање и уништавање података.[54] У погледу *обавештавања лица* чијим задржаним подацима се приступило, ЕСЉП је нашао да прописано обавештавање *није у складу са утврђеном судском праксом*[55] јер је обавештење *потребно у свим случајевима*, а не само у оним у којима се подацима приступило незаконито, и то чим се може извршити без угрожавања сврхе предузете мере.[56] Даље, ЕСЉП је утврдио да ни

основан. Такође, *закон не обавезује судију*, који испитује захтеве за приступ, да у одлуци којом одобрава приступ наведе *разлоге* који објашњавају зашто је одлучио да је одобравање заиста било неопходно и сразмерно, односно да се мање инвазивним мерама није могла постићи иста сврха. *Ekimdzhiev and others v. Bulgaria*, пара. 400–407.

[54] Релевантно законодавство Бугарске предвиђа да сви комуникациони подаци *који нису коришћени за покретање кривичног поступка* морају бити уништени у року од три месеца од дана пријема од надлежних органа, а да сви подаци којима се приступило по хитном поступку морају бити одмах уништени на исти начин, уколико такав приступ није ретроспективно потврђен од надлежног судије. Насупрот томе, *такав рок није одређен* за податке којима је приступљено *а покренут је кривични поступак*. ЕСЉП је истакао да, иако се чини да је то питање покривено интерним правилима које је издао главни тужилац, та правила нису учињена доступним јавности, па је нејасно шта предвиђају. Такође, ништа не сугерише да су одредбе одговарајућег закона ради транспоновања Директиве (ЕУ) 2016/680 до сада коришћене за попуњавање те празнине. *Ekimdzhiev and others v. Bulgaria*, пара. 408–409.

[55] Иако бугарски Закон о електронским комуникацијама захтева од специјалног парламентарног одбора да *обавести* појединца у случају да се његовим задржаним комуникационим подацима *незаконито* приступило или је незаконито тражено да им се приступи, под условом да такво обавештење не би угрозило сврху због које се тим подацима приступа, ЕСЉП је нашао да такво решење није задовољавајуће.

[56] Суд је нашао да ништа не указује на то да је такво обавештење до сада учињено на основу измена и допуна закона ради транспоновања Директиве (ЕУ) 2016/680 где је амандманима предвиђена могућност појединцима да добију такве информације о задржаним и приступљеним комуникационим подацима, нити се чини да је до сада било случајева у којима су лица могла да добију информације о задржавању или приступу својим комуникационим подацима у складу са релевантним одредбама тог закона. У недостатку даљих детаља, не може се прихватити да су одредбе о заштити података у вези са задржаним комуникационим подацима ефективне у том погледу. *Ekimdzhiev and others v. Bulgaria*, пара. 416–417.

Закон о електронским комуникацијама ни Закон о кривичном поступку не предвиђају *правни лек* у вези са задржавањем или приступом комуникационим подацима.[57] Коначно, у погледу надзора над остваривањем приступа задржаним подацима, ЕСЉП је закључио да постојећи механизми нису подобни да осигурају да се овлашћења за приступ подацима не злоупотребљавају.[58]

[57] Такође, указано је на то да се, услед недостатка детаља о „стварном функционисању" система правних лекова у вези са комуникационим подацима, не може прихватити да су новоуведена правна средства, у недостатку пријављених одлука бугарских судова, тренутно заиста и делотворна и да не постоји било какав доказ да је правни лек доступан. Из тога следи да се забринутост јавности у вези са претњом злоупотребе приступа и коришћења комуникационих података од државних органа не може у довољној мери отклонити постојањем делотворних правних лекова у том погледу. Наиме, на држави је да објасни да је обезбеђена делотворност правних лекова, за које тврди да су ефикасна, и да пружена објашњења, колико год је то могуће, поткрепи конкретним примерима, што је у случају Бугарске изостало. *Ekimdzhiev and others v. Bulgaria*, пара. 376–382.

[58] Наиме, Комисија за заштиту података о личности надлежна је да надзире поступање пружалаца комуникационих услуга, али *нема изричита овлашћења у односу на државне органе* који могу приступити задржаним подацима. Осим тога, иако су, релевантним изменама и допунама законодавства ради транспоновања Директиве (ЕУ) 2016/680, ова Комисија и Инспекторат при Врховном већу судства задужени да надгледају начин на који државни органи обрађују податке о личности у сврхе спровођења закона, ништа не сугерише да су ова тела до сада користила та овлашћења у вези са задржаним комуникационим подацима. Такође, судија који одобрава приступ задржаним подацима није у позицији да обезбеди ефикасну контролу јер, иако му надлежни органи достављају извештај о спроведеној мери, *нема овлашћења* да врши надзор ни да наложи корективне мере, није овлашћен нити се од њега очекује да врши инспекцију на лицу места, а своје надзорне дужности обавља искључиво на основу извештаја надлежних органа. Осим тога, иако главно надзорно тело – *специјални парламентарни одбор* – може да надзире и пружаоце комуникационих услуга и надлежне органе и има широка овлашћења за прикупљање информација и надзор, а годишњи извештаји показују да редовно спроводи инспекције преко службеника које запошљава, недостатак се огледа у томе што његови чланови не морају бити лица са правним квалификацијама или искуством у тој области, а одбор нема овлашћења да наложи корективне мере у конкретним случајевима већ може само да изда упутства осмишљена да побољшају релевантне процедуре те ако открије неправилности, може само да скрене пажњу надлежним органима или обавести руководиоце релевантних органа и пружаоце комуникационих услуга. *Ekimdzhiev and others v. Bulgaria*, пара. 410–415.

3.2.2. Škoberne v. Slovenia

ЕСЉП је утврдио да је (измењени) Закон о електронским комуникацијама из 2004. године *одредио бројне сврхе* у које је требало да се чувају комуникациони подаци, *али није садржао* одредбе које би *ограничиле обим и примену мере* само на оно што је било неопходно за постизање тих сврха, при чему држава није показала да је други законски акт садржао такве одредбе. ЕСЉП је најпре указао на то да из постојеће судске праксе произилази да национални закон треба, као део минималних захтева, на начин који одговара одређеној мери надзора, да дефинише обим примене мере надзора и обезбеди одговарајуће процедуре за одобравање и/или преиспитивање с циљем да мера остане у границама неопходног. Наиме, требало је да минимални захтеви буду испуњени и у погледу задржавања комуникационих података, имајући у виду природу спорног мешања. С тим у вези, ЕСЉП је истакао да се недвосмисленост закона, који *као правило прописује опште и неселективно задржавање* комуникационих података, не може сматрати довољном гаранцијом његове усклађености са принципима владавине права и пропорционалности. Непостојање одредаба или механизама који би осигурали да мера буде заправо ограничена на оно што је „неопходно у демократском друштву“ за специфичне сврхе наведене у (измењеном) Закону из 2004. године, те одређивање чувања задржаних података на период од 14 месеци, учинило је такав *режим непомирљивим са обавезама државе* према чл. 8 ЕКЉП.[59]

Поткрепљујући своје наводе, ЕСЉП се позива и на праксу Суда правде ЕУ и напомиње да *режим обавезног општег и неселективног задржавања* комуникационих података у сврху борбе против тешког криминала није у складу са захтевом пропорционалности, те да чак и у контексту заштите националне безбедности, где би се задржавање комуникационих података могло наложити као општа и неселективна мера под одређеним строгим условима, такво задржавање не може бити системске природе него мора бити предмет независног надзора у конкретном случају.[60]

Разматрајући могућност употребе података прикупљених у таквом режиму задржавања, ЕСЉП је истакао да је, без обзира на то што су Суд правде ЕУ и Уставни суд Словеније режим задржавања прогласили

[59] *Škoberne v. Slovenia*, пара. 138–139.

[60] *Škoberne v. Slovenia*, пара. 140, 68.

неважећим, за оцену да ли је у конкретном случају поступање било у складу са чл. 8 ЕКЉП релевантан тренутак када су ти подаци задржани и када им се приступило (а то је било пре него што је дотични режим проглашен неважећим) и да ли је подносилац представке, у време када су задржани комуникациони подаци, уживао адекватну правну заштиту, на коју је имао право према Конвенцији – а Суд сматра да то није био случај. Даље, ЕСЉП је нагласио да, иако је приступ подацима подносиоца представке био праћен одређеним заштитним мерама (тј. судским одобрењем), заштитне мере, саме по себи, нису биле довољне да учине режим задржавања усклађеним са чл. 8 ЕКЉП.[61]

Закључујући, ЕСЉП је изнео становиште да је, без обзира на количину података, у смислу чл. 8 ЕКЉП, важно да су подаци задржани у оквиру општег и неселективног режима, за који је утврдио да је у супротности са чл. 8 ЕКЉП.[62] Другим речима, када се утврди да задржавање комуникационих података представља *кршење чл. 8 ЕКЉП* јер није испоштован захтев „квалитета закона" и/или принцип пропорционалности, *исто важи и за приступ задржаним подацима* и њихову накнадну обраду од државних органа.[63]

---

[61] *Škoberne v. Slovenia*, пара. 142–143. Штавише, ЕСЉП је приметио да је Суд правде ЕУ на сличан начин, у предметима *SpaceNet* и *Telekom Deutschland*, нашао да *национално законодавство*, које је обезбедило пуно поштовање услова утврђених путем закона којим се имплементира Директива 2006/24/*ЕС*, у вези са приступом задржаним подацима, *не може*, по својој природи, *да ограничи или чак исправи озбиљне сметње које произилазе из општег задржавања података*, при чему су задржавање и приступ таквим подацима одвојена мешања у право која *захтевају посебна оправдања*. *Škoberne v. Slovenia*, пара. 87.

[62] Суд је навео да *није* од неког посебног *значаја* то што су, осуђујући подносиоца представке, домаћи судови користили *ограничену количину* задржаних података који су се односили на (*ограничен*) *период* од месец дана јер се представка односи на читав низ података који су задржани и чувани у периоду од четрнаест месеци, а које су прибавили надлежни органи, а затим обрадили, чували и испитали за потребе предметног кривичног поступка. *Škoberne v. Slovenia*, пара. 145, 147.

[63] *Škoberne v. Slovenia*, пара. 144. У вези са тим, ЕСЉП се позвао на став који је изразио Суд правде ЕУ у предмету *An Garda Siochana*, где је Суд правде ЕУ утврдио да комуникацијски подаци не могу бити предмет општег и неселективног задржавања у сврху борбе против тешког криминала и да стога приступ таквим подацима не може бити оправдан у ту исту сврху, те сагласно томе ЕСЉП не види разлог да утврди другачије у вези са случајем подносиоца представке.

3.2.3. Podchasov v. Russia

У одлуци у том предмету ЕСЉП је, између осталог, нашао да *само постојање закона* које захтева *континуирано и аутоматско задржавање и чување* од пружалаца електронских комуникација свих података о интернет комуникацији и сродних комуникационих података, као и чување садржаја свих интернет комуникационих услуга које се користе за пренос гласовних, текстуалних, визуелних, звучних, видео или других електронских комуникација, *потенцијални приступ надлежних органа* тим подацима и обавеза Телеграма да их дешифрује, уколико су шифровани, представља изузетно *озбиљно и неприхватљиво мешање* у права подносиоца представке из чл. 8 ЕКЉП. Суд је истакао да се на тај начин фактички утиче на све кориснике интернет комуникација, нарочито у ситуацији када не постоји одређени степен сумње да су умешани у криминалне активности или активности које угрожавају националну безбедност, односно када не постоји други разлог да се верује да задржавање података може допринети борби против тешког криминала или заштити националне безбедности.[64] Тако широко прописана обавеза задржавања података, *без икаквог ограничења обима мере* у смислу територијалне или временске примене или категорија лица чији се лични подаци задржавају и чувају, озбиљно угрожава права из чл. 8 ЕКЉП.[65]

Осим тога, ЕСЉП, као посебно инвазивну, истиче *обавезу пружалаца услуга* електронских комуникација *да инсталирају опрему* која надлежним органима омогућава *директан, даљински приступ* свим задржаним подацима о интернет комуникацијама, као и садржају остварене комуникације, чиме им се омогућава да заобиђу процедуру ауторизације и приступе сачуваним задржаним комуникационим подацима и садржају остварене комуникације без претходног судског одобрења. Таква пракса је, према ставу ЕСЉП, неприхватљива,

[64] Истакнуто је да би заштита предвиђена чл. 8 ЕКЉП била неприхватљиво ослабљена када би се употреба модерних технологија у систему кривичног правосуђа дозволила по сваку цену и без пажљивог балансирања између потенцијалних користи од екстензивне употребе таквих технологија и важних интереса заштите приватног живота, односно заштите података о личности. *Podchasov v. Russia*, пара. 62.

[65] *Podchasov v. Russia*, пара. 70.

имајући у виду да захтев да се пружаоцу комуникационих услуга, пре остваривања приступа задржаним подацима, достави претходно судско одобрење представља важну заштиту од злоупотребе од надлежних органа, док непостојање таквог претходног судског одобрења у великој мери повећава степен произвољности и могућности (склоности) ка злоупотреби, чиме нису испуњени минимални захтеви за заштитним мерама.[66]

4. УСАГЛАШЕНОСТ ДОМАЋЕГ ПРАВНОГ ОКВИРА СА СТАНДАРДИМА ЗАШТИТЕ ЉУДСКИХ ПРАВА

Поједини ставови које су Суд правде ЕУ и ЕСЉП изнели у одлукама у поменутим предметима потенцијално су примењиви и на домаћи правни оквир.

[66] *Podchasov v. Russia*, пара.72–75. Важно је напоменути и то да у истој одлуци, у погледу захтева да се безбедносним службама достављају информације које су неопходне за дешифровање електронских комуникација ако су шифроване, ЕСЉП примећује да шифровање пружа снажне техничке гаранције против незаконитог приступа садржају комуникација и стога се нашироко користи као средство заштите права на поштовање приватног живота и приватности преписке на мрежи. У дигиталном добу, техничка решења за обезбеђивање и заштиту приватности електронских комуникација, укључујући мере за шифровање, доприносе обезбеђивању уживања других основних права, као што је слобода изражавања. Штавише, чини се да шифровање помаже грађанима и предузећима да се одбране од злоупотреба информационих технологија, као што су хаковање, крађа идентитета и личних података, превара и неприкладно откривање поверљивих информација. Сагласно томе, имајући у виду да би било неопходно ослабити шифровање за све како би се омогућило дешифровање комуникација заштићених *end-to-end* енкрипцијом, те да се на тај начин мере не могу ограничити на одређене појединце и да би неселективно утицале на све, укључујући и појединце који нису претња легитимном интересу владе, слабљење енкрипције стварањем *backdoor*-а очигледно би учинило технички могућим обављање рутинског, општег и неселективног надзора личних електронских комуникација, те да криминалне мреже такође могу да искористе *backdoor* и озбиљно угрозе безбедност електронских комуникација свих корисника, ЕСЉП узима у обзир опасности ограничавања шифровања које су описали многи стручњаци у тој области, па сходно свему томе закључује да законска обавеза пружаоца интернет комуникација да дешифрује *end-to-end* шифровану комуникацију представља ризик да провајдери таквих услуга ослабе механизам шифровања за све кориснике и да се постојање такве обавезе не може сматрати сразмерним легитимним циљевима којима се тежи. *Podchasov v. Russia*, пара. 76–79.

4.1. Усаглашеност са правом ЕУ

ЗЕК из 2010. усвојен је по узору на Директиву 2006/24/ *ЕС*, а поједини делови су просто преведени и интегрисани у закон, односно преузети су некритички и без потребног номотехничког прилагођавања (имајући у виду правну природу директива). У накнадним законским интервенцијама нису узети у обзир ставови Суда правде ЕУ јасно изражени у одлуци којом је поништена Директива 2006/24/*ЕС*[67] ни ставови из неколико одлука поводом националних прописа,[68] а то није учињено ни приликом доношења новог закона 2023. године.

У погледу *задржавања података*, аргументи због којих је Директива 2006/24/*ЕС* стављена *ван снаге* – јер се широко и особито тешко мешала у основна људска права, а да притом такво мешање није било прецизно ограничено на оно што је строго нужно – могу се без проблема *применити и на српски закон*.[69] Суд правде ЕУ је одредио да је *национални пропис* којим је предвиђено *опште и неселективно задржавање* свих података о саобраћају и локацији свих корисника услуга електронске комуникације *недозвољен и прекомеран* у одлуци из 2016. у предмету *Tele2 Sverige*. То је потврдио, између осталог, и у одлукама у предмету *La Quadrature du Net* из 2020. и у предмету *SpaceNet AG* из 2022. године. Аналогно томе, није тешко доћи до одговора на питање да ли је ЗЕК, који прописује обавезу општег и неселективног задржавања података о електронским комуникацијама, *без одређивања сврхе због које се подаци задржавају*, у складу са правом ЕУ. При томе, треба имати у виду да Суд правде ЕУ заузео јасан став да *задржавање и приступ* задржаним подацима представљају *одвојена мешања* у гарантована права која захтевају посебна оправдања.

С тим у вези, а у погледу приступа задржаним подацима за потребе кривичног поступка, упитно је да ли и у којој мери одредбе ЗКП испуњавају захтеве утврђене у пракси Суда правде ЕУ. Сврха остваривања приступа произлази из чл. 286 ст. 3 ЗКП, у којем стоји да је полиција овлашћена да приступи задржаним подацима „у циљу испуњења дужности из става 1. овог члана“.[70] Не би се могло рећи да

---

67 Више о томе Писарић 2019, 187–188.

68 Више о томе Mitsilegas *et al*. 2023, 182–183.

69 Вид. посебно пара. 25–29, 54–69.

70 Односно „да се пронађе учинилац кривичног дела, да се учинилац или саучесник не сакрије или не побегне, да се открију и обезбеде трагови кривичног дела и предмети који могу послужити као доказ, као и да прикупи сва обавештења која би могла бити од користи за успешно вођење кривичног по-

је том формулацијом довољно прецизно одређена сврха остваривања приступа у поједином случају јер није довољно да се просто пропише да полиција може да приступи задржаним подацима ради остваривања одређеног циља (односно дужности из чл. 286 ст. 1).[71] Наиме, иако су одредбама ЗКП прописани услови за приступ задржаним подацима: материјални („ако постоје основи сумње да је извршено кривично дело за које се гони по службеној дужности“) и формални (да је јавни тужилац поднео захтев а судија за претходни поступак налогом одобрио прикупљање података), из праксе Суда правде ЕУ недвосмислено произлази да *услови треба да се заснивају на објективним критеријумима*, којим би се ближе одредиле околности под којима надлежним органима може бити одобрен приступ у појединим случају, што је у ЗКП изостало. Што се тиче материјалног услова да постоји најнижи степен сумње да је извршено било које кривично дело за које се гони по службеној дужности, треба имати у виду да је Суд правде ЕУ заузео став да решим *општег и неселекетивног преноса* задржаних података надлежним органима, па и у сврху борбе *против тешког криминала*, није у складу са захтевом квалитета закона и/или пропорционалности – тим пре, то би важило за приступ задржаним подацима у сврху борбе против криминала уопште, како је то предвиђено ЗКП-ом. При томе, мера из чл. 286 ст. 3 ЗКП се може одредити у односу *на било које лице* (дакле, чак и у односу на лице за које не постоји никаква назнака да њихово понашање може имати везу, чак и посредну или далеку, с циљем вођења кривичног поступка), а Суд правде ЕУ је истакао да би се приступ могао одредити само у односу на податке лица за која постоји јасна сумња да су извршили тешко кривично дело, док би у погледу података других лица приступ могао да буде одобрен само под рестриктивним условима.[72] У погледу формалног услова, из праксе Суда правде ЕУ произлази да посебно треба водити рачуна о томе да ли је успостављен однос између података чији се пренос тражи и кривичног дела те да ли постоји јасна веза између лица чијим задржаним подацима ће бити приступљено и конкретног кривичног поступка,[73] што би требало да буде *образложено* и у захтеву надлежног органа за приступ и у одлуци суда којим се одобрава приступ у конкретном случају,[74] док ЗКП не поставља такав захтев ни за предлог ни за налог.

ступка“.

71 Вид. *Privacy International*, пара. 74–81.

72 Вид. *Prokuratuur*, пара. 49–58.

73 Вид. *Privacy International*, пара. 74–81.

74 Више о томе у 4.2.1.

Осим тога, чини се да Србија до сада није размотрила могућност да нормира *циљано задржавање* података и приступ тим подацима онако како се сугерише у одлукама Суда правде ЕУ, које садрже доста јасне смернице и критеријуме за што избалансиранији приступ решавању односа заштите јавног интереса и мешања у основна људска права (као што је нпр. одређено у предмету *La Quadrature du Net*).

Због свега реченог, а након анализе релевантне праксе Суда правде ЕУ не би се могло тврдити да су национални прописи у Србији усаглашени са правом ЕУ, а Србија би, као кандидат за чланство у ЕУ, требало да узме у обзир ставове и смернице утврђене у одлукама највишег суда ЕУ. Озбиљност (не)адекватности законских решења сагледава се додатно у (не)усаглашености с праксом ЕСЉП.

4.2. Усаглашеност са ЕКЉП

Полазећи од приказане праксе ЕСЉП, могло би се рећи да сви корисници услуга електронских комуникација у Србији имају *статус жртве мешања* у њихова права из чл. 8 ЕКЉП *због начина на који прописи обавезују* операторе да *задрже и чувају* велики број података о електронским комуникацијама свих својих корисника (и то без обзира на то да ли им надлежни органи накнадно приступају) и на који *уређују приступ задржаним подацима* од стране надлежних органа за потребе кривичног поступка.[75]

Даље, како сврха задржавања података у ЗЕК није одређена, па самим тим не постоје ни одредбе које би ограничиле обим и примену задржавања на оно што је неопходно за постизање сврхе, него постоји општи и неселективни режим задржавања података, могло би се закључити да је такво *задржавање у супротности са чл. 8 ЕКЉП* јер није поштован захтев „квалитета закона" и/или принцип пропорционалности. Исто важи и за *приступ задржаним подацима* и њихову накнадну обраду од надлежних државних органа за потребе кривичног поступка, како је то уређено у ЗКП.[76]

У погледу *оправданости* таквог мешања у право из чл. 8 ЕКЉП, у наставку ћемо анализирати одредбе ЗЕК, као прописа којим се уређују задржавање и приступ задржаним подацима у начелу, одредбе ЗКП,

[75] Вид. *Ekimdzhiev and others v. Bulgaria*, пара. 372, 376; *Podchasov v. Russia*, пара. 50–52; *Škoberne v. Slovenia*, пара. 125–128.

[76] Вид. *Škoberne v. Slovenia*, пара. 144.

као прописа којим се уређује приступ задржаним подацима за потребе кривичног поступка, и одредбе других прописа, у светлу става ЕСЉП да, с обзиром на значај комуникационих података, задржавање од пружалаца услуга и накнадни приступ државних органа у појединачним случајевима морају бити праћени *истим мерама заштите као и тајни надзор комуникације*.[77]

4.2.1. Захтев/одлука

У погледу *претходног одобравања приступа* задржаним подацима, као заштитне мере која би требало да обезбеди да надлежни органи приступају задржаним комуникационим подацима само када је то оправдано, поставља се питање да ли је то питање у ЗКП уређено на адекватан начин. *Одредбама ЗКП није прописано* шта би предлог јавног тужиоца, као захтев надлежног органа за одобрење приступа, односно налог судије за претходни поступак, као одлука којом се приступ одобрава, требало да садрже,[78] *не захтева се* да буду образложени уопште, а камоли да се покаже да је испуњен услов да се мање инвазивним мерама није могла постићи иста сврха. Из тога следи да процедура за овлашћивање надлежних органа да приступе задржаним комуникационим подацима не гарантује ефективно да се такав приступ одобрава само када је то заиста неопходно и пропорционално у конкретном случају.[79] Због свега тога би се могло рећи да чл. 286 ст. 3 ЗКП *не испуњава стандард квалитета закона* у погледу остваривања приступа задржаним подацима, како је то уобличено у пракси ЕСЉП.

Такође, како је ЕСЉП негативно реаговао на прописану *обавезу пружалаца* електронских комуникација *да инсталирају опрему* која надлежним органима *омогућава директан, даљински приступ задржаним подацима*, требало би се осврнути на домаће прописе. Иако из ЗЕК недвосмислено произлази да је постојање судске одлуке неопходан претходни услов за оба начина прибављања задржаних података (чл. 128

[77] Вид. *Ekimdzhiev and others v. Bulgaria*, пара. 394–395; *Podchasov v. Russia*, пара. 72; *Škoberne v. Slovenia*, пара. 119, 133–134, 137.

[78] Према постојећем законском решењу, довољно би било да захтев садржи навод да постоје основи сумње да је извршено одређено кривично дело за које се гони по службеној дужности и да приступ задржаним подацима треба остварити како би се пронашао учинилац кривичног дела, да се учинилац или саучесник не би сакрио или побегао, како би се открили и обезбедили трагови кривичног дела и предмети који могу послужити као доказ, односно да би се прикупила сва обавештења која би могла бити од користи за успешно вођење кривичног поступка.

[79] Вид. *Ekimdzhiev and others v. Bulgaria*, пара. 400–407; *Škoberne v. Slovenia*, пара. 142–143.

ст. 7), треба пажљиво размотрити обавезе оператора у вези са *техничким интерфејсом*.[80] Осим тога, иако се податак о судској одлуци, која је основ за приступ задржаним подацима, уноси у евиденције које воде оператори и надлежни органи који остварују приступ задржаним подацима (чл. 128 ст. 8 и ст. 9 ЗЕК), њихова обавеза *да као тајну чувају те евиденције*, и то у складу са Законом о тајности података[81] (ЗТП), не доприноси отклањању потенцијалне сумње да надлежни органи могу *фактички да заобиђу процедуру ауторизације* и приступе задржаним подацима директно, без претходног судског одобрења.[82]

4.2.2. Обавештавање лица

У погледу обавештавања лица на које се односе задржани подаци којима су надлежни органи приступили, ЕСЉП је истакао да је обавештење *потребно у свим случајевима*, чим се обавештавање може извршити *без угрожавања сврхе* због које је предузета мера.[83] Међутим, у Србији се *лице не обавештава* о томе да је на основу чл. 286 ст. 3 ЗКП приступљено подацима који се односе на њега,[84] али је зато предвиђено да има право да поднесе притужбу надлежном судији за претходни поступак (чл. 286 ст. 5 ЗКП).[85]

До сазнања да је приступљено задржаним подацима који се на њега односе окривљени би могао да дође посредно, остваривањем **увида у списе предмета**, али тек након саслушања (чл. 251 ст. 1 ЗКП). С тим у вези треба истаћи да би у спис предмета, осим предлога јавног тужиоца и налога судије за претходни поступак, *требало да буду укључени* и задржани подаци којима су надлежни органи приступили – иако није прописана обавеза полиције да достави извештај о прибављеним

---

[80] Оператори су у обавези са да задржане податке *учине доступним путем одговарајућег техничког интерфејса* (чл. 9 ст. 2 Правилника), односно да омогуће техничко повезивање своје опреме са опремом надлежних државних органа употребом одговарајућег *техничког интерфејса којим се омогућава пренос* одређених комуникационих података (чл. 16 и 21 Правилника).

[81] *Службени гласник РС* 104/09.

[82] Вид. *Podchasov v. Russia*, пара. 72–75.

[83] Вид. *Ekimdzhiev and others v. Bulgaria*, пара. 416–417.

[84] У ЗКП се питање обавештавања лица уређује једино у вези са посебним доказним радњама (чл. 163 ЗКП), али је упитно да ли се то чини на адекватан начин, односно у складу са праксом ЕСЉП.

[85] С тим у вези вид. 4.2.3.

подацима ни судији за претходни поступак, па ни јавном тужиоцу (утврђена је само начелна обавеза обавештавања јавног тужиоца о предузетим мерама и радњама из чл. 286 ст. 2 и 3 ЗКП).

За остваривање права лица на које се односе задржани подаци којима је приступљено за потребе кривичног поступка, па и права на обавештеност, потенцијално су релевантне одредбе садржане у *ЗЗПЛ*,[86] нарочито одредба *о праву на приступ подацима* (чл. 27) и одредба којом се *то право ограничава* (чл. 28).[87] У вези са подношењем захтева руковаоцу за остваривање права поводом обраде података о личности (чл. 27 ЗЗПЛ), поставља се питање да ли би уопште било реално очекивати да би неко лице ако нема никаква обавештења, па ни посредна сазнања о задржавању и приступу задржаним подацима који се на њега односе, из превентивних или других сличних разлога подносило такав захтев како би дошло до сазнања о томе да ли су, који и на који начин задржани подаци који се на њега односе прикупљени и обрађивани од надлежних органа за потребе кривичног поступка.[88]

4.2.3. Правно средство

Обавештавање лица на које се односе задржани подаци неопходан је предуслов за остваривање права на делотворно правно средство поводом приступа задржаним подацима за потребе кривичног поступка. С обзиром на то да лице и не зна да је према њему примењена мера из чл. 286 ст. 3 – зато што се не обавештава о томе да је остварен приступ задржаним подацима који се на њега односе – поставља се питање

[86] Нарочито одредбе којима се уређују информисање и начини остваривања права лица на које се односе подаци када обраду врше надлежни органи у посебне сврхе (чл. 21), права лица да му се одређене информације ставе на располагање или пруже (чл. 25), право на приступ подацима (чл. 27), право на брисање или ограничење обраде (чл. 32) те права да буде обавештен у вези са исправком или брисањем података и ограничењем обраде (чл. 34). Више о начину остваривања права физичких лица у вези са обрадом података о личности вид. у Калаба 2023.

[87] Та ограничења *не могу трајати заувек и неодређено* већ само у оној мери и у оном трајању док је то неопходно и сразмерно у демократском друштву у односу на поштовање основних права и легитимних интереса физичких лица чији се подаци обрађују, а органи би морали своју одлуку образложити јасним разлозима утемељеним на закону. Даље разматрање тих питања није предмет рада.

[88] Треба напоменути и то да ЗЗПЛ предвиђа два режима обраде података о личности – општи и посебни. Више о општем и посебном режиму обраде Милић, Калаба 2023.

његовог права да поднесе *притужбу надлежном судији за претходни поступак* (чл. 286 ст. 5). Ако би лице и било обавештено или би увидом у спис дошло до сазнања, може се поставити питање на које би то околности лице поднело притужбу, шта би се њом тражило и сл. Такође, упитно је да ли је притужба делотворно правно средство против налога, између осталог, и из разлога што је судија за претходни поступак коме се подноси притужба, тај који је налог и издао, а поред тога нејасно је шта би судија поводом притужбе и могао да учини. Због свега наведеног, не би се могло рећи да је ЗКП на одговарајући начин уредио право на делотворно правно средство поводом приступа задржаним подацима за потребе кривичног поступка.[89]

Поводом приступа задржаним подацима за потребе кривичног поступка, потенцијално могу бити релевантне и одредбе ЗЗПЛ којима је предвиђено да лица на које се односе подаци, када обраду врше надлежни органи у посебне сврхе,[90] могу остварити своја права и посредством повереника, у складу са његовим овлашћењима прописаним тим законом (чл. 35), да се лица на која се односе задржани подаци могу ради заштите својих права прописаних тим законом обратити притужбом поверенику (чл. 82), чија одлука подлеже контроли управног суда (чл. 83), односно тужбом суду (чл. 84). Питање колико се та правна средства могу сматрати делотворним није предмет овог рада.

4.2.4. „Судбина" задржаних података

ЕСЉП је разматрао како је уређена судбина задржаних података којима су приступили надлежни органи у ситуацији када није покренут кривични поступак и када су прикупљени подаци укључени у спис кривичног предмета.[91] Што се тиче чувања, приступа, испитивања, коришћења, саопштавања и уништавања задржаних података којима су приступили надлежни органи за потребе кривичног поступка, да би се утврдило да ли је у Србији обезбеђен одговарајући ниво заштите, треба узети у обзир неколико прописа.

---

89 Вид. *Ekimdzhiev and others v. Bulgaria*, пара. 376–382

90 О потешкоћама да се утврде субјекти који се могу сматрати надлежним органом који врши обраду података о личности у посебне сврхе вид. Милић, Калаба 2024.

91 Вид. *Ekimdzhiev and others v. Bulgaria*, пара. 408–409.

ЗЕК обавезује операторе да предузму одређене *мере заштите*, којима, између осталог, треба да се обезбеди да задржани подаци буду заштићени од случајног или недопуштеног уништења, случајног губитка или измене, неовлашћеног или незаконитог чувања, обраде, приступа или откривања – *у складу са ЗЗПЛ* (чл. 130 ст. 1 тач. 3), и *уништени* по истеку рока од 12 месеци од дана окончања комуникације (чл. 130 ст. 1 тач. 4).[92] Такође, ЗЕК обавезује операторе (не и надлежне органе коме су подаци достављени) да податке који су *сачувани и достављени надлежним органима* буду заштићени од случајног или недопуштеног уништења, случајног губитка или измене, неовлашћеног или незаконитог чувања, обраде, приступа или откривања, али тада *у складу са ЗТП*,[93] док за уништење тих података, осим што предвиђа да се на њих *не односи рок од 12 месеци*, ЗЕК не садржи правила, већ је то уређено *другим прописима*. У Србији нажалост још увек не постоји пропис којим би се на одговарајући и свеобухватан начин уредила правила о обради података о личности коју врше *правосудни органи уопште*. Мере заштите задржаних података којима је приступила *полиција* предвиђене су у Закону о евиденцијама и обради података у области унутрашњих послова[94] (Закон о евиденцијама[95]).

И док ЗКП не садржи правило о томе шта се дешава са задржаним подацима којима је приступљено а *кривични поступак није покренут* (нпр. није прописано да се уништавају у одређеном року под одређеним условима),[96] треба имати у виду да у складу са Законом о евиденцијама[97] полиција води евиденцију о приступу задржаним подацима у телекомуникационом саобраћају,[98] да ти подаци представљају

---

92 Надзор над извршењем ових обавеза врши повереник (чл. 130 ст. 3 ЗЕК).

93 Надзор над извршењем ових обавеза врши и Министарство правде, као орган надлежан за надзор над спровођењем ЗТП (чл. 130 ст. 3 ЗЕК).

94 *Службени гласник РС* 24/2018.

95 Чл. 42 који уређује евиденцију примењених оперативних и оперативно-техничких средстава, метода и радњи, прописано је да Министарство прикупља и обрађује податке у складу с прописима којима се уређује кривични поступак (ЗКП) и електронска комуникација (ЗЕК).

96 Како то чини изричитом одредбом о поступању с материјалом који је прикупљен спровођењем посебних доказних радњи (вид. чл. 163 ЗКП).

97 Чл. 42, који уређује евиденцију примењених оперативних и оперативно-техничких средстава, метода и радњи, прописује да Министарство *прикупља и обрађује податке* у складу с прописима којима се уређује кривични поступак (ЗКП) и електронска комуникација (ЗЕК).

98 Евиденција *садржи податке из наредбе* судије за претходни поступак надлежног суда на основу које се врши приступ задржаним подацима, а који *могу да се односе на*: име и презиме лица, име једног родитеља, надимак, ЈМБГ, датум,

тајне податке који се означавају у складу с прописима о тајности података и да се чувају *трајно* (чл. 42 ст. 2)[99] – дакле, без обзира на то да ли је кривични поступак покренут и какав је исход поступка. Упитно је колико је такво решење у складу не само са ЗЗПЛ него и са Директивом 2016/680, но даље разматрање тог питања није предмет нашег рада.

За судбину задржаних података којима је приступљено у случају да је **кривични поступак покренут** релевантно је правило из ЗКП по којем поједине списе предмета може разматрати, копирати или снимати *свако ко има оправдани интерес* да то чини: у току поступка (па и предистражног)[100] – ако то дозволи јавни тужилац,[101] односно суд; а након завршетка поступка – по одобрењу председника суда или службеног лица које он одреди (чл. 250 ЗКП).[102] Разматрање списа је *ограниче-*

место, општину и државу рођења, адресу пребивалишта/боравишта лица, националност, радно место, број телефона или IMEI број телефонског апарата, кориснички број, електронску адресу, врсту возила и уређаја, регистарску ознаку возила, који су обухваћени наредбом суда, односно податке потребне за праћење и утврђивање извора комуникације, утврђивање одредишта комуникације, утврђивање почетка, трајања и завршетка комуникације, утврђивање врсте комуникације, идентификацију терминалне опреме корисника, утврђивање локације мобилне терминалне опреме корисника (чл. 42 ст. 1).

[99] Иако је у чл. 42 ст. 3 и 4 тог закона прописано да Министарство *до застарелости кривичног гоњења* чува податке који се обрађују у складу са ЗКП, у склопу дужности предузимања потребних мера и радњи да се пронађе учинилац кривичног дела, да се учинилац или саучесник не сакрије или не побегне, да се открију и обезбеде трагови кривичног дела и предмети који могу послужити као доказ и прикупљања свих обавештења која би могла бити од користи за успешно вођење кривичног поступка – односно у складу с чл. 286 ЗКП, *међу којима је прибављање евиденције* из чл. 286 ст. 3–5 ЗКП – ст. 2 истог члана *посебно и на битно другачији начин* уређује рок чувања евиденције о приступу задржаним подацима (а тиме и рок чувања задржаних података који се уносе у евиденцију).

[100] С обзиром на значење израза „поступак" у смислу чл. 2 ст. 2 тач. 14) ЗКП.

[101] С тим у вези, треба нагласити да јавни тужилац приликом давања дозволе за разматрање списа или предмета, односно издавања фотокопије списа, чак и лицима која имају оправдани интерес, *води рачуна о фази у којој се налази поступак по предмету и о интересима редовног одвијања поступка* (чл. 65 Правилника о управи у јавним тужилаштвима, *Службени гласник РС* 110/2009, 87/2010, 5/2012, 54/2017, 14/2018 и 57/2019). Такође, одредбама ЗКП је прописано да се разматрање списа може решењем ускратити или условити забраном јавне употребе имена учесника у поступку, уколико би право на приватност могло да буде теже повређено (чл. 250 ст. 3 ЗКП).

[102] Списи правноснажно окончаног кривичног поступка се чувају у складу са Судским пословником (*Службени гласник РС* 110/2009, 70/2011, 19/2012, 89/2013, 96/2015, 104/2015, 113/2015, 39/2016, 56/2016, 77/2016, 16/2018, 78/2018, 43/2019, 93/2019 и 18/2022), којим се уређују начин архивирања и

но само у случају да *имају ознаку степена тајности* – међутим, за разлику од посебних доказних радњи, подаци о предлагању, одлучивању и спровођењу мере из чл. 286 ст. 3 не представљају тајне податке нити је у ЗКП изричито прописано да се предлог јавног тужиоца, налог судије за претходни поступак и извештај о прикупљеним подацима означавају ознаком степена тајности, у складу са прописима којима се уређују тајни подаци. Имајући у виду да је ЕСЉП нашао да се *не може прихватити да постоји одговарајући ниво заштите задржаних података*,[103] када се укључују и чувају у списе предмета и прате његову судбину, па им може приступити свако ко има приступ самом спису, требало би се осврнути на уређење тог питања у Србији.

4.2.5. Надзор

Што се тиче надзора над остваривањем приступа задржаним подацима, упитно је да ли и у којој мери постојећи механизам Србији може да обезбеди да се овлашћења за приступ не злоупотребљавају.

Инспекцијски надзор над применом ЗЕК и прописа којима се уређује делатност електронских комуникација обавља Министарство информисања и телекомуникација, посредством инспектора електронских комуникација (чл. 163 ЗЕК 2023).[104] Међутим, инспектор *није надлежан* да врши надзор *над остваривањем приступа надлежних органа*, тим пре ни да оцењује оправданост остваривања приступа задржаним подацима у конкретном случају. Осим тога, *надзором над извршењем обавеза* да се предузму одређене *мере заштите* задржаних података (чл. 130 ст. 3 ЗЕК) *није обухваћен* надзор над поступањем надлежних органа.

Поводом *контроле остваривања приступа* задржаним подацима *на основу евиденција* које воде оператори и надлежни органи, у погледу евиденција које се воде *на основу чл. 128 ст. 8 и 9 ЗЕК*, с обзиром на

рокови чувања архивираног предмета у кривичном поступку, рачунајући од дана правноснажности поступка, а зависно од исхода поступка (нарочито, с обзиром на врсту и висину изречене санкције).

[103] Вид. *Ekimdzhiev and others v. Bulgaria*, пара. 408–409.

[104] Инспектор је, осим овлашћења из закона којим се уређује обављање послова инспекције, овлашћен, између осталог, да проверава поступање привредног субјекта у вези са применом мера заштите података о личности и приватности (чл. 166 ст. 1 т. 6 ЗЕК 2023), те поступање оператора у вези са омогућавањем приступа задржаним подацима (чл. 166 ст. 1 т. 7 ЗЕК 2023). Уколико се у вршењу инспекцијског надзора утврде незаконитости у примени прописа, инспектор је овлашћен да наложи одређене мере.

то да се чувају као тајна, опозив тајности податка, односно документа који садржи тајни податак био би могућ само у случајевима, на начин и под условима који су прописани одредбама ЗТП. *Евиденције о захтевима за приступ задржаним подацима из чл. 130а ЗЕК*, које се једном годишње достављају поверенику, садрже само сумарни број захтева за приступ и остварених приступа – штавише, изричито је прописано да не садрже податке о личности чијим подацима се приступало (чл. 130а ст. 3 ЗЕК).[105] На тај начин је ограничена (али не и искључена) могућност повереника да врши ефективну контролу поступања оператора *у појединим случајевима*, с обзиром на овлашћења која има, првенствено *у смислу ЗЗПЛ*. Друго је питање да ли су та овлашћења адекватно прописана и да ли се могу на ефикасан начин користити у пракси.

У погледу „надзорног механизма" у оквиру ЗКП, судија за претходни поступак који је издао налог није у позицији да контролише остваривање приступа ни коришћење задржаних података којима је приступљено. Наиме, о приступу задржаним подацима полиција одмах, а најкасније у року од 24 часа након предузимања, обавештава јавног тужиоца (чл. 286 ст. 4), а не судију. При томе треба имати у виду да се, према приказаној пракси Суда правде ЕУ и ЕСЉП, јавни тужилац не може сматрати органом које испуњава услове независности који се захтевају за орган надлежан за обављање надзора над приступом задржаним подацима, с правом се може поставити питање

[105] Проблем који се односи на достављање поменутих евиденција поверенику већ неколико година је предмет анализе неколико невладиних организација која се баве тематиком приватности података, дигиталне безбедности и транспарентности рада органа власти. У својим извештајима и анализама указују на то да, осим значајног пада транспарентности извештавања оператора и надлежних органа када је реч о њиховим праксама приступа задржаним подацима, што се највише огледа у пропуштању да се доставе информације о самосталном приступу подацима, проблем представљају и видљиве разлике у извештајима. Такође, истиче се да је, како чланом 130а ЗЕК није довољно прецизно уређена садржина евиденције која се доставља поверенику, простор за произвољно тумачење те правне обавезе прилично широк и делује да зависи од добре воље или, у најбољем случају, од процедура успостављених на корпоративном нивоу конкретног пружаоца услуга електронских комуникација. Пракса би се можда променила уколико би се изменама закона или одговарајућим подзаконским актом (нпр. правилником) прописао обавезујући образац за достављање евиденције о задржаним подацима, чији би елементи морали да садрже униформне информације. Тренутне праксе оператора и надлежних органа више представљају формално испуњење обавезе него суштинску интенцију да се законом пропише механизам транспарентности задржавања података о електронским комуникацијама и приступања тим подацима. Share фондација, Преглед евиденције приступа задржаним подацима у Србији за 2020, 2018. и 2017. годину.

адекватности домаћег решења. ЗКП не захтева да се судији достави било какав извештај о остваривању приступа нити да буде обавештен о уништавању ирелевантних или бескорисних комуникационих података којима је приступљено. Што се тиче евентуалног реаговања судије поводом притужбе лица чијим подацима се приступило (у смислу чл. 286 ст. 5) нејасно је која би била његова овлашћења.

5. ЗАКЉУЧАК

У Србији су оператори обавезни да масовно задржавају и чувају 12 месеци од остварене комуникације огроман број података о свим електронским комуникацијама свих својих корисника. Обавезу масовног, неселективног задржавања и чувања задржаних података ЗЕК је прописао не оправдавајући је било каквом јасном сврхом и циљем. С друге стране, према ЗЕК, приступ је дозвољен изузетно – само „на одређено време" и „на основу одлуке суда" ако је то „неопходно" ради вођења кривичног поступка или заштите безбедности Републике Србије, а на начин предвиђен другим законом. Приступ подацима који су задржани на основу ЗЕК остварује се за потребе кривичног поступка на основу ЗКП, но тим прописом то питање није уређено на одговарајући начин.

Домаћем правном оквиру су стога упућене критике због потенцијалне неусклађености са Уставом и неусаглашености са ЕКЉП и правом ЕУ. Треба водити рачуна о томе да је Србија, као чланица Савета Европе и као кандидат за чланство у ЕУ, дужна да прописе и њихову примену усклади с правом тих међународних организација, а што до сада, чини се, није учинила у довољној мери и на одговарајући начин. Аутори у раду јасно указују на те неусаглашеностима, упућујући на релевантне одлуке Суда ЕУ и ЕСЉП.

Из праксе Суда ЕУ јасно произлази да се опште и неселективно задржавање комуникационих података, какво прописује ЗЕК, не може само по себи оправдати те да је противно праву ЕУ. У погледу приступа задржаним подацима од надлежних органа за потребе кривичног поступка, не би се могло сматрати да је правно уређење у ЗКП ограничено на оно што је строго неопходно „у демократском друштву". Због свега наведеног у раду, након анализе релевантне праксе Суда правде ЕУ, не би се могло рећи да су до сада узети у обзир ставови и смернице утврђени у одлукама највишег суда ЕУ, а било би пожељно да их законодавац размотри.

Што се тиче усаглашености домаћих прописа са ЕКЉП, из праксе ЕСЉП произлази да, с обзиром на то да прибављање комуникационих података путем масовног и општег задржавања и приступа задржаним подацима може бити једнако наметљиво као и масовно прикупљање садржаја комуникација, опште задржавање комуникационих података од пружалаца комуникационих услуга и приступ надлежних органа тим подацима у појединачним случајевима морају бити праћени, *mutatis mutandis*, истим мерама заштите као и тајни надзор комуникације. Да се пред ЕСЉП покрене поступак против Србије због кршења права из ЕКЉП у вези са задржавањем података и приступом задржаним подацима за потребе кривичног поступка, није искључено да би ЕСЉП, као у случају Словеније, нашао да постојеће одредбе, које представљају основ за задржавање и чување комуникационих података, не испуњавају услов „квалитета закона" и да не могу да ограниче „мешање" у права из члана 8 ЕКЉП на оно што је „неопходно у демократском друштву", а да су задржавање, накнадни приступ и обрада комуникационих података на основу таквог правног оквира у супротности са Конвенцијом. Такође, може се претпоставити са високим степеном вероватноће да би ЕСЉП несумњиво указао Србији, као што је то учинио и у случају Бугарске, на то да треба да изврши неопходне измене у домаћем правном оквиру како би окончала кршење права и обезбедила да њени прописи буду компатибилни са Конвенцијом.

ЛИТЕРАТУРА

[1] Бугарски, Татјана, Милана Писарић. 4/2020. Задржавање података у пракси Суда Европске Уније. *Зборник Правног факултета у Новом Саду* 54: 1231–1252.

[2] Калаба, Остоја. 2023. Обрада података о личности од стране цркава и верских заједница у праву и пракси ЕУ и Републике Србије. 867–896. *Савремено државно-црквено право*, ур. Владимир Ђурић, Далибор Ђукић. Београд – Будва: Институт за упоредно право – Митрополија црногорско-приморска СПЦ:

[3] Милић, Иван, Остоја Калаба. 2023. Савремени 'паметни' системи за регулисање саобраћаја у градовима Републике Србије – (не) усклађеност позитивноправних прописа („пази, снима се"). 253–275. *Право између идеала и стварности*, ур. Страхиња Миљковић. Косовска Митровица: Правни факултет Универзитета у Приштини са привременим седиштем у Косовској Митровици, Институт за упоредно право.

[4] Милић, Иван, Остоја Калаба. 2024. Прекршајна одговорност и казне за кршење закона о заштити података о личности. 237–267. *Динамика савременог правног поретка*, ур. Срђан Радуловић. Косовска Митровица: Правни факултет Универзитета у Приштини са привременим седиштем у Косовској Митровици – Институт за упоредно право – Институт за криминолошка и социолошка истраживања.

[5] Mitsilegas, Valsamis, Elspeth Guild, Elif Kuskonmaz, Niovi Vavoula. 1–2/2023. Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks. *European Law Journal* 29: 176–211.

[6] Писарић, Милана. 2019. *Електронски докази у кривичном поступку*. Нови Сад: Правни факултет у Новом Саду.

[7] Podkowik, Jan, Robert Rybski, Marek Zubik. 5/2021. Judicial dialogue on data retention laws: A breakthrough for European constitutional courts? *International Journal of Constitutional Law* 19: 1597–1631.

[8] Повереник за информације од јавног значаја и заштиту података о личности. 2012. Извештај о извршеном надзору над спровођењем и извршавањем Закона о заштити података о личности од стране оператора мобилне и фиксне телефоније у Републици Србији. *https://labs.rs/Documents/PoverenikovIzvestaj.pdf*, последњи приступ 9. април 2024.

[9] Повереник за информације од јавног значаја и заштиту података о личности. 2013. Извештај о спровођењу Закона о слободном приступу информацијама од јавног значаја и Закона о заштити података о личности за 2012. годину. *https://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2012/latizvestaj2012final.pdf*, последњи приступ 9. април 2024.

[10] Повереник за информације од јавног значаја и заштиту података о личности. 2015. Извештај о извршеном надзору над спровођењем и извршавањем Закона о заштити података о личности од стране оператора електронских комуникација који пружају услуге приступа интернету и интернет услуге. *https://www.poverenik.rs/sr-yu/saopstenja/2128-nuzno-je-popravljati-nivo-zastite-licnih-podataka-u-oblasti-elektronskih-komunikacija.html*, последњи приступ 9. април 2024.

[11] Share фондација. Преглед евиденције приступа задржаним подацима у Србији за 2020. годину. *https://www.sharefoundation.info/wp-content/uploads/Zadrzani-podaci-2020_izvestaj.pdf*, последњи приступ 9. април 2024.

[12] Share фондација. Преглед евиденције приступа задржаним подацима у Србији за 2018. годину. *https://www.sharefoundation.info/sr/pristup-bez-transparentnosti-praksa-zadrzavanja-podataka-u-2018/*, последњи приступ 9. априла 2024.

[13] Share fondacija. Pregled evidencije pristupa zadržanim podacima u Srbiji za 2017. godinu. *https://resursi.sharefoundation.info/sr/resource/zadrzavanje-podataka-o-komunikaciji-u-srbiji-koliko-smo-pod-nadzorom/*, последњи приступ 9. април 2024.

[14] *Washington Post*. 2014. Transcript of President Obama's Jan. 17 speech on NSA reforms. January 17. *https://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3–9556–4a4bf7bcbd84_story.html*, последњи приступ 24. децембар 2023.

Milana M. PISARIĆ, PhD

Assistant Professor, University of Novi Sad Faculty of Law, Serbia

Ostoja S. KALABA, LL.M.

Advisor at the Office of the Commissioner for Information of Public Importance and Personal Data Protection, PhD student, Serbia

DATA RETENTION AND CRIMINAL PROCEDURE IN SERBIA

Summary

The use of information technology enables state authorities to prosecute perpetrators and process personal data on an unprecedented scale and in an unimaginable way, in the course of taking measures and actions to prevent, detect and investigate criminal acts. One of the disputed processing is the nonselective mass monitoring of electronic communications in the form of retention of communication data, which, given the technological development and social importance of electronic communications, can on occasion reveal more about an individual than the content of the communication itself. This form of data processing represents interference with guaranteed human rights and freedoms, and need to be legally regulated in order to prevent their violation. The authors analyze the legal framework for retention of communication data and access to retained data for the purposes of criminal proceedings in Serbia, especially in light of the relevant practices of the CJEU and ECtHR.

Key words: *Electronic communications. – Data retention. – Criminal procedure. – Personal data protection. – Privacy*.

Article history:
Received: 10. 4. 2024.
Accepted: 29. 11. 2024.