Прегледни чланак

343.1:[061.1EU:341.645.5
doi:10.5937/zrpfns54-29964

*Др Татјана Д. Бугарски, редовни професор*
*Универзитет у Новом Саду*
*Правни факултет у Новом Саду*
*T.Bugarski@pf.uns.ac.rs*

*Др Милана М. Писарић, асистент са докторатом*
*Универзитет у Новом Саду*
*Правни факултет у Новом Саду*
*M.Pisaric@pf.uns.ac.rs*

# ЗАДРЖАВАЊЕ ПОДАТАКА У ПРАКСИ СУДА ЕВРОПСКЕ УНИЈЕ*

***Сажетак:*** *Поседовање тачних, потпуних и поузданих релевантних података о саобраћају електронске комуникације и правовремени приступ овлашћених надлежних државних органа таквим подацима је без сумње корисно средство у борби против савремених облика криминала. Из тог разлога оправдано је да се установи обавеза за пружаоце услуга електронске комуникације да за одређени временски период чувају одређене податке о комуникацијама у чијем остваривању посредују и да те податке предају на захтев овлашћених органа државе, како би их користили у легитимне сврхе. Из тога разлога је 2006. усвојена Директива о задржавању података, које су државе чланице биле дужне да пренесу у национално законодавство. Међутим, задржавање података представља ризик по основна људска права и слободе, уколико пропис који установљава ову обавезу то чини не поштујући суштину права и слобода, пре свега права на приватност и права у вези са обрадом података о личности, из ког разлога је 2014. Суд Европске уније огласио Директиву неважећом. И поред ове одлуке, државе чланице и даље регулишу обавезу задржавања података у својим националним прописима. У вези са тим, поставља се питање усклађености ових прописа са основним правима и слободама и начелима Уније. Предмет рада је анализа одлука Суда ЕУ у вези са овим питањем након поништавања Директиве о задржавању података.*

***Кључне речи****: кривични поступак, задржавање података, Европска унија, Суд ЕУ.*

* Рад је настао као резултат рада на Пројекту „Правна традиција и нови правни изазови" у 2020, чији носилац је Правни факултет у Новом Саду, Универзитет у Новом Саду.

## 1. УВОД

На нивоу Европске уније (у даљем тексту: ЕУ) је 2006. прописом, у оквиру тадашњег Првог стуба, за пружаоце услуга електронских комуникација установљена обавеза задржавања података. Наиме, Директива 2006/24/ЕЗ Европског парламента и Савета од 15. марта 2006. о задржавању података добијених или обрађених у вези са пружањем јавно доступних услуга електронских комуникација или јавних комуникацијских мрежа и о измени Директиве 2002/58/ЕЗ[1] (у даљем тексту: *Директива о задржавању података*) донета је *са циљем да се ускладе одредбе* држава чланица које се односе *на задржавање одређених података које прикупљају или обрађују пружаоци услуга*, како би се обезбедило да ти подаци *буду доступни у сврху* спречавања, откривања и доказивања и вођења кривичног поступка за *тешка кривична дела*, као што су она повезана с организованим криминалом и тероризмом, а све то уз поштовање права из члана 7 и 8 Повеље Европске уније о основним правима[2] (у даљем тексту: Повеља). Обавеза задржавања података је установљена за пружаоце јавно доступних услуга електронских комуникација или јавних комуникацијских мрежа у члану 3 ове Директиве, и то у погледу података о комуникацији[3] наведених у члану 5,[4] а ради њихове доступности надлежним органима држава чланица.[5]

---

[1] *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, 13.4.2006, p. 54–63),* https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32006L0024.

[2] *Charter of Fundamental Rights of the European Union* (*OJ C 326, 26.10.2012, p. 391–407),* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.

[3] Подаци о комуникацији деле се на податке о кориснику (*subscriber data*), податке о оствареном комуникацијском саобраћају (*traffic data*) и податке о коришћењу услуге електронске комуникације *(usage data*). М.Писарић, *Електронски докази у кривичном поступку*, Нови Сад 2019, 88.

[4] Директива се односила на задржавање података о кориснику и података о оствареном комуникацијском саобраћају. Према члану 5 ради се о подацима који су потребни за проналажење и идентификацију извора и одредишта комуникације, за утврђивање датума, времена, трајања и врсте комуникације, комуникацијске опреме корисникâ, као и за откривање локације опреме за комуникацију мобилним телефонима, те подацима о броју, који садрже име и адресу претплатника или регистрованог корисника, телефонски број с ког се позива и који се позива, као и ИП адресу за интернетске услуге. Више о томе, вид. Т. Бугарски, „Прислушкивање и задржавање телекомуникационих података", *Правни живот* 9/2011, 837-853.

[5] Више о томе, вид. Т. Бугарски, *Доказне радње у кривичном поступку*, Нови Сад 2011, стр. 63-34.

## 2. ПОНИШТАВАЊЕ ДИРЕКТИВЕ О ЗАДРЖАВАЊУ ПОДАТАКА

Суд ЕУ (у даљем тексту: Суд) је 2014. на основу члана 267 Уговора о функционисању ЕУ[6] (у даљем тексту: УФЕУ) испитивао ваљаност Директиве у јединственом поступку поводом два захтева за доношење одлуке о претходном питању[7] – ради се о предметима *C-293/12*[8] и *C-594/12*.[9] Претходно питање се у суштини односило на то *да ли је Директива усклађена с правом грађана на слободу кретања и боравка* на државном подручју држава чланица, *на поштовање приватног живота из члана 7 Повеље, на заштиту података о личности из члана 8 Повеље, те на слободу изражавања из члана 11 Повеље*.

Суд је у својој одлуци од 8. априла 2014.[10] утврдио да *обавеза задржавања података* представља *само по себи мешање у право* на поштовање приватног живота из члана 7 Повеље (при томе, приступ надлежних државних органа представља додатно мешање у ово право)[11] и у право на заштиту података о личности из члана 8 Повеље.[12] У погледу *оправданости мешања*

---

[6] *Consolidated version of the Treaty on the Functioning of the European Union (OJ C 326, 26.10.2012, p. 47–390*), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT.

[7] На основу члана 267 УФЕУ Суд ЕУ је надлежан да одлучује о претходним питањима која се тичу *тумачења* Уговорâ и *ваљаности и тумачења* аката институција, органа, канцеларија или агенција Уније. Ако се такво питање појави пред судом државе чланице (главни поступак), тај суд може, ако сматра да је одлука о том питању потребна да би могао да донесе одлуку (у главном поступку), да тражи од Суда да о томе одлучи.

[8] Захтев је упутио Врховни суд Ирске поводом поступка који се водио пред њим, између *Digital Rights Ireland Ltd* и неколико државних органа поводом законитости мера које се односе на задржавање података у вези са електронским комуникацијама.

[9] Захтев је упутио Уставни суд Аустрије поводом поступка који се водио пред њим по уставној тужби коју су поднели Влада Покрајине Корушке, као и М. Зајтлингер и 11.129 других тужилаца, у вези с усклађеношћу закона, којим се преноси Директива у домаће аустријско право, са федералним Уставним законом.

[10] *Judgment of the Court (Grand Chamber) of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Official Journal of the European Union, 10.6.2014,* https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2014.175.01.0006.01.ENG.

[11] Наиме, задржавање одређених података у директној је вези са заштитом наведених права, јер подаци омогућавају да се утврди с којим лицем је претплатник или регистровани корисник комуницирао, којим средством, када и са ког места, односно колико учестало је комуницирао са одређеним лицима током одређеног периода. Ови подаци, а нарочито уколико се посматрају заједно и доведу у међусобну везу, омогућавају доношење врло прецизних закључака о приватном животу лица на које се односе подаци, као што су свакодневне навике, места трајних или привремених боравака, дневна или друга кретања, обављане активности, друштвени односи и друштвене средине које та лица посећују.

[12] Иако се начелно захтеви за доношење одлуке о претходном питању односе на то да ли се подаци претплатника и регистрованих корисника могу задржати с обзиром на члан 7 Повеље, они се односе и на питање да ли Директива испуњава захтеве заштите података о

у ова основна права, Суд сматра да задржавање података не вређа њихов битан садржај, да одговара циљу у општем интересу (обезбеђење доступности тих података у сврху спречавања, откривања и доказивања и вођења кривичног поступка за тешка кривична дела), те да је прикладно за остварење тог циља. [13] Међутим, *доводена је у питање нужност такве мешања*.

Суд је истакао да, иако задирање у основна права има за циљ борбу против тешких кривичних дела, што је од важности за јавну безбедност, остварење тог циља *не оправдава* меру задржавања података као *нужну*. Наиме, не може се говорити да је мешање предвиђено Директивом ограничено на оно што је строго нужно, јер обавезује на задржавање *свих података у вези с саобраћајем* свих комуникација, *свим средствима* комуникације, *свих претплатника и регистрованих корисника* – другим речима целокупног становништва, без икаквог разликовања, ограничења или изузетка.[14]

---

личности који произлазе из члана 8 Повеље. Наиме, задржавање података како би се обезбедило да надлежни надлежни органи могу евентуално да им приступе на непосредан и специфичан начин има утицаја на приватан живот, а тиме и на права зајамчена у члану 7 Повеље. На такво задржавање података примењује се и члан 8 јер оно представља обраду података о личности у смислу тог члана и мора нужно да испуњава услове заштите података који произлазе из тог члана. Иако Директива не предвиђа задржавање садржаја комуникације није искључено да задржавање података може имати утицај и на слободу изражавања претплатника или регистрованих корисника комуникацијских средстава зајамчену у члану 11 Повеље.

Суд је заузео јасан став да је Директива, наметнувши задржавање података из члана 5 став 1 током одређеног временског периода и омогућивши надлежним органима да им приступају, *одступила од режима заштите права на поштовање приватног живота* успостављеног Директивама 95/46 и 2002/58, које су у погледу обраде података о личности у подручју електронских комуникација *прописале поверљивост комуникација* и *с њима повезаних података о саобраћају*, као и *обавезу да се ти подаци обришу или учине анонимним* када више нису потребни у сврху преноса комуникације, осим кад су потребни за наплаћивање и то само док траје та потреба.

[13] Суд полази од тога да у складу с чланом 52 став 1 Повеље свако ограничење при остваривању права и слобода мора бити предвиђено законом и мора поштовати суштину тих права и слобода те су, подложно начелу пропорционалности, ограничења тих права и слобода могућа само ако су потребна и ако заиста одговарају циљевима од општег интереса које признаје Унија или потреби заштите права и слобода других лица.

[14] Директива је предвидела задржавање података о комуникацији свих лица, без обзира на то што код њих не постоји никаква назнака да могу имати везу, макар посредну или далеку, с тешким кривичним делима. Директива не захтева никакав однос између података и претње јавној безбедности, и није ограничена на задржавање података из једног привременог раздобља и/или једног одређеног географског подручја и/или једнога круга лица које могу бити умешане у извршење тешког кривичног дела или на лица која могу због других разлога да допринесу спречавању, откривању или гоњењу учинилаца тешких кривичних дела. Осим тога, прописујући задржавање података током раздобља које није краће од шест месеци а не дуже од 24 месеца, а није предвиђено никакво разликовање између категорија података с обзиром на њихову евентуалну корист за остваривање циља или с обзиром на лице на које се односи.

Поред тога, Директива не предвиђа никакав *објективни критеријум који би омогућио ограничење приступа* надлежних државних органа подацима и њихове накнадне употребе.[15]

Директивом су морала бити предвиђена *јасна и прецизна правила која уређују обим и примену мере* задржавања и *пропisани минимални услови* на начин да лица чији су подаци задржани располажу довољним гаранцијама које омогућавају учинковиту заштиту њихових података од ризика злопотребе, као и од свих незаконитих приступа и коришћења тих података, а то све није учињено.

Полазећи од утврђених мањкавости, Суд је Директиву прогласио неваљаном и поништио је.

## 3. СТАВ ЕВРОПСКЕ КОМИСИЈЕ И САВЕТА ЕУ НАКОН ПОНИШТАВАЊА ДИРЕКТИВЕ

Након поништавања Директиве о задржавању података, Комисија ЕУ је у саопштењу из 2015.[16] изнела став да *је на државама чланицама да одлуче* да ли ће на националном нивоу прописати обавезу задржавања података јер је ово питање „предмет осетљиве идеолошке дебате у којој ЕУ неће више учествовати".[17] Такође, саопштено је да Комисија ЕУ неће иступити са новом иницијативом за прописивање обавезе задржавања података на нивоу ЕУ. Из тог разлога, услед непостојања наднационалног прописа, државе чланице имају пуну слободу да *одрже или успоставе нове системе задржавања података* на својој територији, *под условом да такав систем буде у складу са основним начелима права ЕУ*, као што су она предвиђена у Директиви 2002/58/ЕЗ Европског парламента и Савета од 12. јула 2002. о обради података о личности и заштити приватности у сектору електронских комуни-

---

[15] Члан 4 који уређује приступ задржаним подацима, *не прописује изричито да тај приступ и накнадно коришћење података морају бити строго ограничени у сврху с*пречавања и откривања тачно утврђених тешких кривичних дела, него је ограничен на навођење тога да свака држава чланица прописује поступак и услове који се морају испунити како би се остварио приступ задржаним подацима у складу са захтевима нужности и пропорционалности, а није предвиђен ни критеријум применом ког би се ограничио број лица овлашћених на приступ и накнадно коришћење задржаних података. Такође, приступ није подређен претходном надзору суда чија би одлука ограничавала приступ подацима и њихово коришћење само на оно што је строго нужно у сврху остваривања циља.

[16] *European Commission statement/15/5654 on national data retention laws Brussels, 16 September 2015*, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_15_5654.

[17] Вид. F. Guarascio, *EU executive plans no new data retention law*, Reuters, 12.3.2015, https://uk.reuters.com/article/us-eu-data-telecommunications/eu-executive-plans-no-new-data-retention-law-idUSKBN0M82CO20150312.

кација,[18] која је измењена Директивом 2009/136/ЕЗ Европског парламента и Савета од 25. новембра 2009.[19] (у даљем тексту: Директива о приватности и електронским комуникацијама).

У априлу 2017. Комисија је покренула поступак процене ситуације у вези са задржавањем података, чији резултат треба да помогне државама чланицама у *анализи захтева постављених у релевантној пракси* Суда након поништавања Директиве о задржавању података (нарочито у предмету *Tele2 Sverige and Watson and Others*[20]) и у *истраживању могућих решења* за обезбеђење доступности података потребних за ефикасну борбу против криминала. У вези са овим процесом, у јуну 2017. усвојени су закључци Савета ЕУ у којима се истиче да је неопхдоно да се надлежним државним органима држава чланица обезбеди доступност одређених података о електронским комуникацијама, а да постојање различитих националних правила ограничава ефикасност прекограничне сарадње и размене података између надлежних органа.[21] Из тог разлога је Савет ЕУ у октобру 2018. позвао на *осмишљавање мера које би надлежним државним органима држава чланица омогућиле олакшан приступ подацима* о комуникацији електронским средствима.[22]

На састанку Савета ЕУ у децембру 2018. приказани су *резултати поступка процене* ситуације.[23] Нарочита пажња посвећена је *концепту ограниченог задржавања података*, у оквиру ког се задржавање података прописује у погледу одређених категорија података само на оно што је нужно потребно. Такође, разматрало се *регулисање обновљивог налога за задржавање*, што значи да, иако се налог односи само на једног пружаоца услуга

---

[18] *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 2002 L 201, p. 37*), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058.

[19] *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 2009 L 337, p. 11*), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0136&from=EN.

[20] Вид. Поднаслов 4.

[21] *Conclusions of the Council of the European Union on Retention of Data for the Purpose of Fighting Crime, EUCO 8/17, 6 June 2019*, https://www.consilium.europa.eu/media/23985/22-23-euco-final-conclusions.pdf.

[22] *Conclusions of the Council of the European Union, EUCO 13/18, 18 October 2018*, https://www.consilium.europa.eu/media/36775/18-euco-final-conclusions-en.pdf.

[23] *Council document 14319/18, Data retention – State of play, 23 November 2018*, https://data.consilium.europa.eu/doc/document/ST-14319-2018-INIT/en/pdf.

електронске комуникације за одређени временски период важења, исти се може продужити колико год пута је потребно у сврху рада органа поступка.

У закључку о задржавању података за потребе борбе против општег криминала из јуна 2019. Савет ЕУ је поново указао на значај података у поседу телекомуникационих оператера и пружалаца услуга за откривање и доказивање кривичних дела а да је њихово обезбеђење од изузетне важности за рад надлежних органа.[24] Како прописивање обавезе задржавања таквих података мора да буде у складу са гарантованим основним правима и слободама, од Комисије је затражено да *прати даљи развој легислативне и судске праксе у државама чланицама, а нарочито праксу Суда*, и да одржи консултације у циљу изналажења *свеобухватног решења* за задржавање података, *укључујући и евентуални легислативни предлог на нивоу ЕУ у будућности*. Нарочито се указује на сагледавање коцепта општег, циљаног и ограниченог задржавања података (први ниво задирања у гарантована права и слободе), концепт циљаног приступа задржаним подацима (други ниво задирања у гарантована права и слободе), као и кумулативног ефекта гаранција и могућих ограничења на задржавање података у оба нивоа задирања у гарантована права и слободе, а све у циљу стварања решења које ће истовремено обезбедити заштиту права и слобода али и ефиксаност кривичног поступка.

Може се закључити да се, са поништавањем Директиве о задржавању података, на нивоу Уније макар једно време застало са намером да се пропише обавеза задржавања података о електронској комуникацији кроз усвајање наднационалног прописа – но, није искључено да се у догледно време неће појавити нови легислативни предлог у том правцу.

Чињеница да је регулисање овог питања остављено државама чланицама отворила је спорна питања, нарочито у погледу усаглашености таквих прописа (како оних којима је Директива пренесена у национално законодавтсво тако и нових прописа о задржавању података) са основним начелима права ЕУ, пре свега оних која су предвиђена у Директиви о приватности и електронској комуникацији. У тумачењу релевантних начела ЕУ, а у недостаку јасних наднационалних смерница, државе чланице се обраћају Суду.

Након поништавања Директиве о задржавању података 2014, Суд је у последњих неколико година у више предмета разматрао *однос националних прописа* о задржавању података и приступу тим подацима *са Директивом о приватности и електронским комуникацијама*, поступајући поводом захтева за доношење одлуке о претходном питању (на основу члана 267 УФЕУ).

---

[24] *Conclusions of the Council of the European Union on Retention of Data for the Purpose of Fighting Crime*, *27 May 2019 (OR. en) 9663/19*, https://data.consilium.europa.eu/doc/document/ST-9663-2019-INIT/en/pdf.

Претходна питања се односе на примену ове Директиве на националне прописе који уређују задржавање података у циљу заштите националне безбедности и борбе против криминала. Наиме, *члан 15 став 1* Директиве предвиђа да *државе могу* ради остваривања таксативно наведених циљева, међу којима су заштита националне безбедности и спречавање, откривање и доказивања кривичних дела и вођење кривичног поступка, *да усвоје прописе* који ограничавају обим одређених права гарантованих овом Директивом. У том смислу, државе могу, између осталог, да предвиде за пружаоце услуга електронских комуникација *обавезу задржавања података* за одређени временски период у сврху остваривања поменутих циљева, при чему те мере морају бити у сагласности са основним нечелима Уније. Као спорно се, дакле, поставља питање *тумачења овог члана* – односно на који начин државе могу, и поред тога што је Директива поништена 2014, да прописују обавезу задржавања података.

## 4. ПРЕСУДА У ПРЕДМЕТУ *TELE2 SVERIGE AND WATSON AND OTHERS*

Суду су 2015. упућена два захтева за доношење одлуке о претходном питању које се односе на тумачење Директиве о приватности и електронским комуникацијама (у предметима *C-203/15*[25] и *C-698/15*[26]). У првом предмету Апелациони управни суд у Стохолму је Суду упутио следећа питања: 1) Да ли је *општа обавеза задржавања података* о саобраћају комуникације која обухвата сва лица, сва средства електронске комуникације и све податке о саобраћају комуникације без икаквих разлика, ограничења или изузетака у сврху борбе против криминала [...] у *складу* са чланом 15 став 1 Директиве 2002/58, узимајући у обзир чланове 7 и 8 и члан 52 став 1 Повеље? 2) У случају негативног одговора на прво питање, да ли се прописивање обавезе задржавање може *изузетно допустити под одређеним условима*?[27] У

[25] Предмет *C-203/15* (*Tele2 Sverige AB v Post- och telestyrelsen*) односи се на спор између пружаоца услуга електронских комуникација *Tele2 Sverige AB* и шведског органа за надзор поште и телекомуникција (*Post- och telestyrelsena*), поводом *налога који је ово тело упутило пружаоцу услуга* да спроведе задржавање података о локацији својих претплатника и регистрованих корисника.

[26] Предмет *C-698/15* (*Secretary of State for the Home Department V Tom Watson, Peter Brice, Geoffrey Lewis*) односи се на спор између три држављана Уједињеног Краљевства (T*om Watson, Peter Brice, Geoffrey Lewis*) и Министра унутрашњих послова а *поводом усклађености члана* 1 Закона о задржавању података и истражним овлашћењима (*Data Retention and Investigatory Powers Act 2014: DRIPA*) *са правом Уније*

[27] Уколико (а) је приступ државних органа задржаним подацима одређен на начин описан у тачкама 19 до 36 [одлуке којом се упућује претходно питање], (б) су безбедност и

другом предмету Апелациони суд Енглеске и Велса упутио је Суду захтев за доношење одлуке о следећим питањима: 1) Да ли пресуда о поништавању Директиве о задржавању података успоставља важне захтеве права Уније примењиве на национални систем државе чланице који уређује приступ подацима задржаним у складу с националним законодавством с циљем усклађивања с члановима 7 и 8 Повеље, и 2) Да ли та пресуда проширује обим права из чланова 7 и/или 8 Повеље у односу на члан 8 ЕКЉП, како је утврђено судском праксом Европског суда за људска права?

Суд је поводом ова два предмета водио јединствен поступак, дајући тумачење члана 15 став 1 Директиве о приватности и електронским комуникацијама, у вези са члановима 7 и 8 Повеље. Питање је, дакле, било да ли је са овим чланом *у супротности* онај национални *пропис* који *у сврху борбе против криминала одређује* опште и неселективно *задржавање* свих података о саобраћају комуникација и локацији свих претплатника и регистрованих корисника у вези са свим средствима електронске комуникације, и *приступ* тако задржаним подацима, тим пре уколико се ради о пропису који *је усвојен с циљем преношења Директиве о задржавању података (а која је поништена) у национално законодавство*.

Суд је поводом ова два захтева донео одлуку 21. децембра 2016. године.[28]

У одлуци на постављена питања Суд потврдно одговара, заузимајући став да је у *супротности* са Директивом о приватности и електронским комуникацијама (са чланом 15 став 1 Директиве) онај *национални пропис*, који у *циљу борбе против криминала* одређује *опште и неселективно задржавање података* и омогућава надлежним државним органима *приступ задржаним подацима*, *уколико сврха* у оквиру борбе против криминала *није ограничена на борбу против тешких кривичних дела*, и уколико се *приступ не подвргава претходном надзору* суда или независног органа управе.

Другим речима, прописивање задржавања података о саобраћају комуникације *оправдано је* само у сврху спречавања, откривања и доказивања и вођења кривичног поступка за *тешка кривична дела*, у складу са *начелом сразмерности*. Наиме, у пресуди којом је поништена Директива о задржавању података Суд је утврдио да задржавање и чињење доступним података о саобраћају комуникације представљају нарочито озбиљно задирање у права гарантована члановима 7 и 8, при чему је одредио *критеријуме за*

---

заштита података уређени на начин описан у тачкама 38 до 43 [одлуке којом се упућује претходно питање], и (в) сви релевантни подаци морају бити задржани током шест месеци, рачунајући од дана кад је комуникација завршена, те потом избрисани, како је описано у тачки 37 [одлуке којом се упућује претходно питање].

[28] *Judgment of the Court (Grand Chamber) 21 December 2016 in Joined Cases C-203/15 and C-698/15*, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62015CJ-0203&from=EN#t-ECR_62015CJ0203_EN_01-E0001.

*оцену поштовања начела пропорционалности*, међу којима је и *тежина кривичног дела* која оправдава задржавање и приступ тим подацима. С тим у вези, поставља се питање шта се под „тешким" кривичним делом подразумева.

## 5. ПРЕСУДА У ПРЕДМЕТУ *MINISTERIO FISCAL*

Суд је „тежину" кривичног дела као критеријум који оправдава задржавање података о саобраћају комуникације и приступ тим подацима разматрао поводом захтева за доношење одлуке о претходном питању који се упутио Апелациони суд у Тарагони (у предмету *C-207/16*[29]), а ради тумачења члана 15 став 1 Директиве о приватности и електроским комуникацијама.

Суду су упућена следећа претходна питања: (1) Да ли довољна *тежина кривичног дела* као критеријум који оправдава задирање у основна права из чланова 7 и 8 Повеље може да се утврди *само на основу запрећене казне* за кривично дело поводом ког се води истрага или је поред тога нужно да се утврди и посебна штетност противправног поступања за правне интересе појединаца или заједнице?[30] (2) Ако се утврђивање тежине кривичног дела врши само на основу запрећене казне, у складу с основним начелима права Уније, која је Суд као стандард строгог надзора Директиве [2002/58] применио у пресуди о поништавању Директиве о задржавању података, *која би то била најнижа запрећена казна* – те да ли би општа одредба о најмање три године затвора била у складу с тим?

---

[29] Оштећени је полицији пријавио крађу новчаника и мобилног телефона која се догодила 16.фебруара 2015. године. Полиција је 27. фебруара 2015. истражном суду поднела захтев којим тражи да се различитим пружаоцима услуга електронске комуникација наложи да доставе бројеве телефона који су између 16. и 27. фебруара 2015. активирани кодом међународног идентитета мобилне опреме који припада украденом мобилном телефону (ИМЕИ број) и податке о идентитету власника или корисника (имена, презимена и адресе) телефонских бројева који одговарају СИМ картицама активираним овим бројем. Решењем од 5. јула 2015. истражни суд је одбио тај захтев, оценивши да мера није могла да послужи за идентификовање учиниоца кривичног дела, а при томе дајући образложење да је Законом 25/2007 предаја података које су задржали пружаоци услуга електронских комуникација могућа само кад је реч о тешким кривичним делима а дело о ком је реч није тешко кривично дело (у складу с Кривичним закоником тешка кривична дела су она за која је запрећена казна затвора од пет година или више). Јавно тужилаштво је поднело жалбу против решења Апелационом суду.

[30] Наиме, након доношења спорног решења законодавац је, доношењем Органског закона 13/2015, изменио Законик о кривичном поступку, којим су предвиђена два нова алтернативна критеријума за утврђивање степена тежине кривичног дела: материјални критеријум (који се односи на поступања која одговарају квалификацијама кривичног дела чије су радње посебна и тешка и која су нарочито штетна за правне интересе појединаца и заједнице) и формални нормативни критеријум (који се заснива на казни од најмање три године затвора).

Суд је поводом овог захтева донео одлуку 2. октобра 2018. године.[31]

У овој одлуци Суд полази од тога да су циљеви, за остварење којих је дозвољен приступ подацима тако да не представља задирање у гарантована права, такстативно наведени у члану 15 став 1 Директиве о приватности и електронским комуникацијама, што значи да приступ подацима мора да *одговара једном од постављених циљева*. При томе, *циљ* спречавања, истраге, откривања и гоњења учинилаца кривичних дела о*дноси се на сва кривична дела* а не само на тешка кривична дела. Како се у конкретном случају подаци не односе на комуникацију остварену посредством украденог мобилног телефона и као такви не омогућавају извођење прецизних закључака у вези са приватним животом одређених лица, због чега, приступ подацима не представља озбиљно задирање у гарантована права. Другим речима, приступ надлежних државних органа подацима потребних у сврху идентификовања власника СИМ картице активиране уз помоћ украденог мобилног телефона (име, презиме и адреса) подразумева мешање у њихова основна права, које, међутим, није довољно озбиљно да би се приступ таквим подацима ограничио на спречавање, откривање и доказивање и вођење кривичног поступка за *тешка кривична дела*.

И поред тумачења датог у пресудама у предметима *Tele2 Sverige and Watson and Others* и *Ministerio Fiscal,* Суду је упућено још неколико захтева за доношење одлуке о претходном питању,[32] а у вези са односом између на-

---

[31] *Judgment of the Court (Grand Chamber) 2 October 2018 in Case C-207/16*, http://curia.europa.eu/juris/document/document.jsf?text=&docid=206332&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=15767141.

[32] Захтев за доношење одлуке о сличном претходном питању упутио Врховни суд Естоније новембра 2018 (предмет *C-746/18*: *H.K. v Prokuratuur*), постављајући питање: (1) да ли *приступ државних органа подацима* на основу којих се може утврдити полазиште и одредиште, датум, време и трајање, врста комуникацијске услуге, употребљена терминална опрема, локација употребе мобилне терминалне опреме у односу на телефонску или мобилну телефонску комуникацију осумњиченог у оквиру кривичног поступка чини тако озбиљно задирање у основна права зајамчена лкановима 7,8 и 11 Повеље да се *тај приступ* у подручју спречавања, истраге, откривања и гоњења учинилаца кривичних дела *мора ограничити на борбу против тешких кривичних дела*, независно од временског периода на који се односе похрањени подаци који су доступни државним органима? (2) Ако се пође од начела сразмерности (утврђног у предмету *Ministerio Fiscal*), а количина података доступних државним органима која су наведена у првом претходном питању није велика (и у погледу врсте података и временског оквира), да ли се задирање у основна права може оправдати циљем спречавања, откривања и доказивања кривичних дела и вођења кривичног поступка, односно да ли кривична дела морају да буду сразмерно тежа што је количина података доступних државним органима већа? (3) Да ли је захтев да се приступ надлежних државних органа подацима мора подвргнути претходном надзору суда или независног органа управе (утврђеног у предмету *Tele2 Sverige and Watson and Others*) задовољен уколико надзор врши јавно тужилаштво као орган који води истрагу и који је према закону дужан да независно поступа? Међутим, Суд још увек није донео пресуду у овом предмету.

ционалних прописа о задржавању података и Директиве о приватности и електронским комуникацијама, као да су ове пресуде „разлог за бригу за државе чланице јер их депривирају инструмента неопходног за заштиту националне безбедности и борбу против криминала и тероризма, па се Суду упућују захтеви са доношење одлуке о прелиминарном питању како би се став Суда изменио".[33]

## 6. ПРЕСУДА У ПРЕДМЕТУ *PRIVACY INTERNATIONAL*

Трибунал Уједињеног Краљевства о истражним овлашћењима је упутио захтев за доношење одлуке о неколико правних питања (у предмету *C-623/17*[34]), тражећи тумачење одредаба Директиве о приватности и електронским комуникацијама у вези са задржавањем података од стране безбедносних и обавештајних служби.

У околностима у којима су способности ових служби да користе масовне податке о комуникацијама битне за заштиту националне безбедности,[35] а да пружалац електронске комуникацијске мреже није обавезан да задржи податке дуже од раздобља које захтева његово уобичајено пословање, а да податке даље задржава само држава, Трибунал је утврдио да су заштитне мере у вези с употребом масовних података од стране служби у складу са захтевима ЕКЉП. Како Трибунал сматра да налагање захтева у тачкама 119-125 пресуде у предмету *Tele2 Sverige and Watson and Others* онемогућава службе да предузимају мере у циљу заштите националне безбедности и доводи је у опасност, Суду је упутио следећа претходна питања: (1) Да ли подручје примене Директиве о приватности и електронским комуникацијама обухвата и захтев прописан смерницом министра којим се пружаоцу електронске комуникацијске мреже налаже да безбедносним и обавештајним службама државе чланице преда масовне комуникацијске податке? (2) Ако је одговор на ово питање потврдан, да ли се на такву смерницу примењују

---

[33] Вид. *Opinion of Advocate General Campos Sánchez-Bordona delivered on 15 January 2020*, http://curia.europa.eu/juris/document/document.jsf?text=&docid=222264&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=14896635.

[34] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service*.

[35] Укључујући борбу против тероризма, противобавештајне активности и сузбијање ширења нуклеарног оружја, при чему је битно обележје употребе тих података откривање претходно непознатих претњи за националну безбедност употребом нециљаних масовних техника које се темеље на обједињавању масовних комуникацијских података на једном месту (са циљем брзог утврђивања и праћења мете, као и пружања основе за акцију у ситуацији непосредне претње).

неки од захтева примењивих на задржане комуникацијске податке наведене у тачкама 119 до 125 пресуде у предмету *Tele2 Sverige and Watson and Others*, односно и неки други захтеви уз оне који су прописани ЕКЉП? Ако је то тако, на који начин и у којој мери се ти захтеви примењују, узимајући у обзир битну потребу служби да у циљу заштите националне безбедности користе масовно прикупљање и технике аутоматске обраде, односно у којој мери прописивање таквих захтева може да онемогући такве могућности, ако су оне у другим погледима усклађене с ЕКЉП?

Одговарајући на ова питања, Суд је донео пресуду 6. октобра 2020,[36] у којој је, истакао да члан 1 став 3, члан 3 и члан 15 став 1 Директиве о приватности и електронским комуникацијама треба да се тумачи на начин да је *подручјем примене* те Директиве *обухваћен национални пропис* који државном органу омогућава да налаже пружаоцима услуга електронске комуникације да ради заштите националне безбедности предају (учине доступним) безбедносним и обавештајним службама податке о саобраћају и локацији комуникације. Другим речима, *у супротности* са чланом 15 став 1 ове Директиве је национални *пропис* који *државном органу омогућава да* ради заштите националне безбедности *налаже пружаоцима услуга* електронске комуникације *да безбедносним и обавештајним службама* уопштено и неселективно *предају* (учине доступним) податке о саобраћају и локацији комуникације.

## 7. ПРЕСУДА У ПРЕДМЕТИМА *ORDRE DES BARREAUX FRANCOPHONES ET GERMANOPHONE AND OTHERS, LA QUADRATURE DU NET AND OTHERS* И *FRENCH DATA NETWORK AND OTHERS*

У августу 2018. захтев за доношење одлуке о претходном питању у вези са тумачењем Директиве о приватности и електронским комуникацијама у погледу прописивања обавезе задржавања података упутили су Уставни суд Белгије (предмет C-520/18)[37] и Државни савет Француске (предмети *C-511/18* и *C-512/18*).[38]

---

[36] *Judgment of the Court (Grand Chamber) 6 October 2020 in Case C-623/17*, http://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=14904167.

[37] *Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v Conseil des ministres*.

[38] Предмети *C-511/18* и *C-512/18* (*French Data Network (C-511/18 and C-512/18), Fédération des fournisseurs d'accès à Internet associatifs* (C-*511/18 and C-512/18), Igwan.net (C-511/18) v Premier ministre (C-511/18 and C-512/18), Garde des Sceaux, ministre de la Justice (C-511/18 and C-512/18), Ministre de l'Intérieur (C-511/18), Ministre des Armées (C-511/18*).

Након поништавања Директиве о задржавању података, у Белгији је 2016. усвојен Закон о прикупљању и задржавању података у сектору електронских комуникација који предвиђа задржавање података за потребе откривања и доказивања свих кривичних дела, те заштите националне и јавне безбедности. Пред Уставним судом Белгије покренут је поступак за испитивање уставности и усаглашености овог закона са Директивом о приватности и електронским комуникацијама, али и са Општом уредбом о заштити података,[39] па је Уставни суд упутио питање Суду у вези са усаглашеношћу националних прописа усвојених у сврху заштите националне безбедности са правом Уније.[40] Слично томе, француски Државни савет је био у недоумици да ли се прописивање *обавезе општег и неселективног задржавања података може оправдати правом на безбедност*, па је од Суда тражио отклањање ове недоумице у предмету *C-511/18*[41] и *C-512/18*[42].

---

[39] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),* OJ L *119, 4.5.2016, p. 1–88,* https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[40] Члан 23 ове Уредбе предвиђа да је националним прописом могуће ограничити права уређена Уредбом (уколико се таквим ограничењем поштује суштина права и слобода и представља нужну и сразмерну меру у демократском друштву за заштиту) за потребе, између осталог, националне безбедности, те спречавања, откривања и доказивања кривичних дела и вођења кривичног поступка, укључујући заштиту од претњи јавној безбедности. При томе, таква законска одредба треба да уреди, као минимум, сврху обраде или категорије обраде, категорије података, обим ограничења, заштитне мере за спречавање злоупотребе или незаконитог приступа или преноса, спецификацију водитеља обраде или категорије водитеља обраде, временски период чувања и заштитне мере које се могу применити узимајући у обзир природу, опсег и сврху обраде или категорије обраде, ризике за права и слободе лица, и право лица да буде обавештени о ограничењу, осим ако то може бити штетно за сврху тог ограничења.

[41] Савет је поставио следећа претходна питања: (1) Да ли *обавезу општег и неселективног задржавања података*, која се пружаоцима услуга може наложити, у смислу члана 15 став 1 Директиве о приватности и електронским комуникацијама, у контексту који укључује озбиљне и континуиране претње националној безбедности, и нарочито ризик терористичких напада, *треба сматрати задирањем које је оправдано* правом на безбедност гарантовано чланом 6 Повеље и захтевима националне безбедности, за које су одговорне саме државе чланице на основу члана 4 УФЕУ? (2) Да ли Директиву о приватности и електронским комуникацијама, у вези с Повељом, треба тумачити на начин да *допушта законске мере*, попут мера *прикупљања у стварном времену података о саобраћају комуникације и података о локацији одређених појединаца*, које иако утичу на права и обавезе пружалаца услуга електронске комуникације, *не налажу посебну обавезу задржавања података*? (3) Да ли Директиву о приватности и електронским комуникацијама, у вези с Повељом, треба тумачити на начин да су *поступци прикупљања података о успостављеној вези* правилни само ако се лице на кога се подаци односе обавести онда када те информације више не могу да угрозе истрагу коју спроводе надлежни државни органи или се такви поступци могу сматрати правилним, с обзиром на сва остала постојеће процесне гаранције, које обезбеђују делотворност правног лека?

[42] Савет је поставио следећа претходна питања: (1) Да ли се *обавеза општег и неселективног задржавања података*, која се пружаоцима услуга налаже, сходно одредбама

Одговарајући на питања из ова три захтева, Суд је у јединственом поступку донео пресуду 6. октобра 2020. године.[43] У овој одлуци утврдио је да се члан 15 став 1 Директиве о приватности и електронским комуникацијама, у вези с члановима 7, 8, 11 и 52 став 1 Повеље, тумачи на начин да су са њим *у супротности законске мере којима се предвиђа превентивно опште и неселективно задржавање података* о саобраћају и локацији комуникације.

Међутим, са овим чланом *нису у супротности законске мере* које:

– *омогућавају*, *у циљу* заштите *националне безбедности, издавање налога* пружаоцима услуга електронских комуникација *да уопштено и неселективно задржавају* податке о саобраћају и локацији комуникације, *у околностима* у којима је држава чланица *суочена с озбиљном претњом по националну безбедност,* која се показала стварном и тренутном или предвидљивом, *под условом* да *одлука* којом је предвиђен такав налог може бити *предмет делотворног надзора* од стране суда или независног органа чија одлука има обавезујуће дејство, *са циљем* да се провери да ли постоји таква околности и да ли се поштују услови и гаранције који се морају предвидети, при чему се наведени налог може издати само за период које је *временски ограничен* на оно што је строго нужно, а може се продужити у случају постојаности опасности;
– *предвиђају*, у циљу заштите *националне безбедности*, борбе *против тешких кривичних дела* и спречавања озбиљних претњи по јавну безбедност, *циљано задржавање података* о саобраћају и локацији комуникације које је *ограничено* на основу објективних и недискриминаторних *критеријума*, у зависности од категорије лица или посредством

---

члана 15 став 1 Директиве о приватности и електронским комуникацијама, нарочито с обзиром на процесне гаранције и контроле који се потом примењују на прикупљање и коришћење тих података о спајању, *може сматрати задирањем које је оправдано* правом на безбедност гарантовано чланом 6 Повеље и захтевима националне безбедности, за које су одговорне саме државе чланице на основу члана 4 УФЕУ? (2) Да ли одредбе Директиве о одређеним правним аспектима услуга информационог друштва на унутрашњем тржишту, посебно електронске трговине (тј. Директиве о електронској трговини) треба тумачити на начин да *држави омогућавају доношење националног прописа којим се лицима*, чија је делатност нуђење приступа јавним интернетским комуникацијским услугама и физичким или правним лицима које, чак и бесплатно, за стављање на располагање јавности путем јавних интернетских комуникацијских услуга, осигуравају похрањивање било које врсте сигнала, писаног текста, слика, звукова или порука, а који су добијени од прималаца тих услуга, *налаже да задрже податке који омогућавају идентификацију* сваког лица која је допринело стварању садржаја или једног од садржаја услуга које пружају, како би правосудни орган могао, по потреби, *да затражи да му се тај садржај достави* у сврху обезбеђења поштовања правила везаних за грађанску или кривичну одговорност?

[43] *Judgment of the Court (Grand Chamber) 6 October 2020 in Case C 511/18, Case C 512/18 and Case C 520/18,* http://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=14904280.

географског критеријума, *за временски период* који је ограничен на оно што је строго нужно, али се може продужити;

– предвиђају, у циљу заштите националне безбедности, борбе против *тешких* кривичних дела и спречавања озбиљних претњи по јавну безбедност, *опште и неселективно задржавање ИП адреса* додељених извору везе, за период који је временски ограничен на оно што је строго нужно;
– предвиђају, у циљу заштите националне безбедности, борбе *против свих кривичних дела* и заштите јавне безбедности, *опште и неселективно задржавање података о грађанском идентитету* корисника електронских комуникацијских средстава; и
– омогућавају, у циљу борбе против *тешких* кривичних дела и заштите националне безбедности *издавање налога* пружаоцима услуга електронских комуникација на основу одлуке надлежног органа, подложне делотворном судском надзору, да *у одређеном трајању хитно задрже податке о саобраћају и локацији којима ти пружаоци услуга располажу.*

При томе, за наведене мере морају да постоје јасна и прецизна правила која обезбеђују да задржавање података буде у складу са материјалним и процесним условима и да лица погођена мерама имају делотворне гаранције против ризика од злоупотребе.

Осим тога, тумачећи члан 15 став 1 Директиве, Суд је утврдио да му се *не противи* национални пропис који *налаже пружаоцима услуга* електронске комуникације да *користе аутоматску анализу и прикупљање у реалном времену*, између осталог, *података о саобраћају и локацији и прикупљање у реалном времену техничких података о локацији употребљене терминалне опреме*, уколико је:

– аутоматска анализа *ограничена на околности* у којима је држава чланица суочена с *озбиљном претњом по националну безбедност* која се показала стварном и тренутном или предвидљивом, *под условом* да таква анализа буде предмет делотворног *надзора* од стране суда или независног органа управе, чија одлука има обавезујуће дејство, а којом се проверава да ли постоје околности у којима је оправдана ова мера и да ли се поштују услови и гаранције који се морају предвидети,
– прикупљање података о саобраћају и локацији у реалном времену *ограничено је на лица* у односу на која постоји основан разлог за сумњу да су на било који начин укључена у терористичке активности, а прикупљање подлеже *претходном* надзору који обавља суд или независни орган управе, чија одлука има обавезујуће дејство, чим се обезбеђује да се прикупљање одобри само у границама онога што је строго нужно. У случају оправдане хитности, надзор се мора спровести у кратким роковима.

Поред тога, Суд је утврдио да се Директива о електронској трговини не примењује на подручје заштите поверљивости комуникација и физичких лица у погледу обраде података о личности у оквиру услуга информацијског друштва јер је та заштита уређена Директивом о приватности и електронским комуникацијама или Општом уредбом о заштити података. При томе, члану 23 став 1 ове Уредбе *противи се национални пропис* који *пружаоцима услуга* приступа јавним интернетским комуникацијским услугама и пружаоцима услуга похрањивања података на серверу *налаже опште и неселективно задржавање*, између осталог, података о личности у вези с тим услугама.

Такође, Суд је утврдио да национални суд не може да примењује одредбу националног права која га овлашћује да временски ограничи дејство утврђења незаконитости које мора да утврди у односу на национално законодавство које пружаоцима услуга електронске комуникације налаже између осталог, ради заштите националне безбедности и борбе против криминала, опште и неселективно задржавање података о саобраћају и локацији комуникације које је неспојиво с чланом 15 став 1 Директиве 2002/58. Наиме, овај члан налаже националном *суду* да у кривичном поступку *издвоји податке и доказе који су прибављени општим и неселективним задржавањем података* о саобраћају и локацији комуникације.

## 8. ЗАКЉУЧАК

Суд ЕУ је 2014. утврдио да *Директива о задржавању података није садржала јасна и прецизна правила* која би уредила домет оваквог мешања у основна права зајемчена у члану 7 и 8 Повеље и ограничила га на оно што је строго нужно. Из тог разлога је Суд ЕУ обавезу задржавања података предвиђену Директивом оценио као широко и нарочито тешко мешање у основна права, *па је Директиву поништио*. Ипак, није искључено да се у догледно време неће појавити нови легислативни предлог на нивоу Уније који би поново прописао обавезу задржавања података.

Од тог тренутка, услед непостојања наднационалног прописа и препуштања државама чланицама да уређују задржавање података, присутан је комплексан и шаренолик легислативни пејсаж на националном нивоу. То је довело до отварања бројних спорних питања, нарочито у погледу усаглашености таквих прописа са основним правима и слободама као и основним начелима права ЕУ. Због непостојања јасних наднационалних смерница, за помоћ у тумачењу релевантних начела ЕУ, пре свега оних која су предвиђена у Директиви о приватности и електронској комуникацији, државе чланице се обраћају Суду ЕУ.

У пресуди из 2016. у предмету *Tele2 Sverige and Watson and Others*, тумачећи члан 15 став 1 Директиве о приватности и електронским комуникацијама, који садржи овлашћење држава чланица да усвоје законске мере којима се ограничава обим одређених права и обавеза предвиђених у тој Директиви, Суд је заузео став да национални пропис који предвиђа *опште и неселективно задржавање* свих података о саобраћају комуникација и локацији свих претплатника и регистрованих корисника у вези са свим средствима електронске комуникације и *приступ* надлежних државних органа, а у сврху борбе против *опште криминала* (дакле, која сврха није ограничена на борбу против тешких кривичних дела) *није у сагласности са овом Директивом*.

Овом важном одлуком, којом се прописивање опште и недискриминаторне обавезе задржавања података не може оправдати у демократском друштву ипак нису била решена спорна питања. Због тога је пред Суд ЕУ и у наредним годинама у више предмета постављен захтев за доношење одлуке о претходном питању, односно за тумачење Директиве о приватности и електронским комуникацијама у вези са задржавањем података.

Ипак, потпунијем разјашњавању спорних питања требало би да допринесу пресуде усвојене 6. октобра 2020, у којима се *јасно одређује какво се задржавање података* (и накнадни приступ од стране надлежних државних органа) *сматра неоправданим и у супротности са правом ЕУ*. Суд је потврдио да право Уније онемогућава да национални прописи обавезују пружаоце услуга електронских комуникација на превентивно *опште и недискриминаторно задржавање података и чињење тих података доступним* на захтев надлежних државних органа *у сврху борбе против опште криминала или заштите националне безбедности*. У супротности са чланом 15 став 1 Директиве о приватности и електронским комуникацијама и чланом 23 став 1 Опште уредбе о заштити података *је онај национални пропис* који *пружаоцима услуга* електронске комуникације, приступа јавним интернетским комуникацијским услугама и пружаоцима услуга похрањивања података на серверу *налаже опште и неселективно задржавање*, између осталог, података о личности у вези с тим услугама.

Међутим, Суд је установио и одређене *изузетке*. У пресуди у предметима *C 511/18, C 512/18* и *C 520/18* Суд таксативно наводи које мере и под којим условима се могу националним прописима предвидети, на начин да не буду у супротности са основним начелима ЕУ. Са Директивом о приватности и електронским комуникацијама није у супротности пропис којим се *у циљу борбе против тешких кривичних дела* омогућава *издавање налога* пружаоцима услуга електронских комуникација којим се обавезују на:

1) *циљано задржавање података* о *саобраћају и локацији комуникације,* које је *ограничено* на основу објективних и недискриминаторних кри-

теријума (категорија лица или географско подручје), и на временски период (који је ограничен на оно што је строго нужно, али који се може продужити);

2) *опште и неселективно задржавање ИП адреса додељених извору везе,* за временски период који је ограничен на оно што је строго нужно;
3) *хитно задржавање података о саобраћају и локацији* којима ти пружаоци услуга располажу;
4) *опште и неселективно задржавање података о грађанском идентитету* корисника електронских комуникацијских средстава (при чему је ову меру могуће предвидети за сва кривична дела, невезано за тежину).

Осим тога, Директиви се не противи ни национални пропис који налаже пружаоцима услуга електронске комуникације да у сврху заштите националне безбедности под одређеним условима (а) *користе аутоматску анализу и прикупљање у реалном времену*, између осталог, *података о саобраћају и локацији* и (б) *прикупљање у реалном времену техничких података о локацији употребљене терминалне опреме.*

Након доношења ових пресуда, очекује се даље поступање националних судова који су упутили захтев Суду (Трибунал Уједињеног Краљевства о истражним овлашћењима, белгијски Уставни суд и француски Државни савет), па остаје да се види какве ће одлуке бити донете у конкретним предметима у овим државама чланицама. У сваком случају, поступање националних судова, односно усаглашавње националних прописа о задржавању података са начелима Уније, како их Суд тумачи, указаће на фактичку правну снагу става највише судске инстанце ЕУ.

## ЛИТЕРАТУРА И ИЗВОРИ

*Treaty on the Functioning of the European Union (OJ C 326, 26.10.2012, p. 47–390*), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT;

*Charter of Fundamental Rights of the European Union* (*OJ C 326, 26.10.2012, p. 391–407),* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT;

*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 2002 L 201, p. 37*), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058;

*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, 13.4.2006, p. 54–63),* https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32006L0024;

*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 2009 L 337, p. 11*), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0136&from=EN;

*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88,* https://eur-lex.europa.eu/eli/reg/2016/679/oj;

*Conclusions of the Council of the European Union on Retention of Data for the Purpose of Fighting Crime, EUCO 8/17, 6 June 2019*, https://www.consilium.europa.eu/media/23985/22-23-euco-final-conclusions.pdf;

*Conclusions of the Council of the European Union, EUCO 13/18, 18 October 2018*, https://www.consilium.europa.eu/media/36775/18-euco-final-conclusions-en.pdf;

*Council document 14319/18, Data retention – State of play, 23 November 2018*, https://data.consilium.europa.eu/doc/document/ST-14319-2018-INIT/en/pdf;

*Conclusions of the Council of the European Union on Retention of Data for the Purpose of Fighting Crime*, *27 May 2019 (OR. en) 9663/19*, https://data.consilium.europa.eu/doc/document/ST-9663-2019-INIT/en/pdf;

*European Commission statement/15/5654 on national data retention laws Brussels, 16 September 2015*, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_15_5654;

*Judgment of the Court (Grand Chamber) of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Official Journal of the European Union, 10.6.2014,* https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2014.175.01.0006.01.ENG;

*Judgment of the Court (Grand Chamber) 21 December 2016 in Joined Cases C-203/15 and C-698/15*, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62015CJ0203&from=EN#t-ECR_62015CJ0203_EN_01-E0001;

*Judgment of the Court (Grand Chamber) 2 October 2018 in Case C-207/16*, http://curia.europa.eu/juris/document/document.jsf?text=&docid=206332&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=15767141;

*Judgment of the Court (Grand Chamber) 6 October 2020 in Case C-623/17*, http://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=14904167;

*Judgment of the Court (Grand Chamber) 6 October 2020 in Case C 511/18, Case C 512/18 and Case C 520/18,* http://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=14904280;

*Opinion of Advocate General Campos Sánchez-Bordona delivered on 15 January 2020*, http://curia.europa.eu/juris/document/document.jsf?text=&docid=222264&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=14896635;

Guarascio F., *EU executive plans no new data retention law*, Reuters, 12.3.2015, https://uk.reuters.com/article/us-eu-data-telecommunications/eu-executive-plans-no-new-data-retention-law-idUSKBN0M82CO20150312;

Бугарски Т.,*Доказне радње у кривичном поступку*, Нови Сад 2011;

Бугарски Т., „Прислушкивање и задржавање телекомуникационих података", *Правни живот* 9/2011, 837-853.

Писарић М., *Електронски докази у кривичном поступку*, Нови Сад 2019.

*Tatjana D. Bugarski, Ph.D., Full Professor*
*University of Novi Sad*
*Faculty of Law Novi Sad*
*T.Bugarski@pf.uns.ac.rs*

*Milana M. Pisarić, Assistant with Ph.D.*
*University of Novi Sad*
*Faculty of Law Novi Sad*
*M.Pisaric@pf.uns.ac.rs*

## Data Retention in CJEU Case Law

***Abstract:*** *Possession of accurate, complete and reliable relevant data on electronic communications traffic and timely access of authorized competent state bodies to such data is without a doubt a useful tool in the fight against modern forms of crime. For that reason, it is justified to establish an obligation for providers of electronic communications services to keep certain data on communications for a certain period of time in the realization of which they mediate and to hand over that data at the request of authorized state bodies, in order to use them for legitimate purposes. For this reason, the Data Retention Directive was adopted in 2006, which Member States were required to transpose into national law. However, data retention poses a risk to basic human rights and freedoms, if the regulation establishing this obligation does so without respecting the essence of these rights and freedoms, especially the right to privacy and rights related to the processing of personal data, for which reason the Court of Justice of the European Union declared the Directive invalid is 2014. Despite this decision, Member States continue to regulate the obligation to retain data in their national regulations. In this regard, the question of compliance of these regulations with the fundamental rights and freedoms and principles of the Union is raised. The subject of the paper is the analysis of the case law of the Court of Justice of the EU on this issue after the annulment of the Data Retention Directive.*

***Keywords****: criminal procedure, data retention, European Union, CJEU.*

Датум пријема рада: 22.12.2020.