

UDK: 351.759:341.462.2

Biblid 1451-3188, 13 (2014)

Год XIII, бр. 49–50, стр. 519–549

Изворни научни рад

Срђан КОРАЋ<sup>1</sup>

## ЕВРОПСКИ НАДЗОРНИК ЗА ЗАШТИТУ ПОДАТАКА: ПРОТИВТЕЖА ЗАДИРАЊУ НАДНАЦИОНАЛНИХ ИНСТИТУЦИЈА У ПРИВАТНОСТ ГРАЂАНА?

### ABSTRACT

The paper discusses to what extent the European Data Protection Supervisor's control powers can effectively protect the right to privacy against the increasing securitisation of the EU policies. Being legitimised on the ground of its rather disputable value for a successful fight against organised crime and terrorism, the securitisation approach in the EU policy-making promotes the use of collecting personal data on massive scale as well as gathering of criminal evidence by intrusive techniques. The use of crime-intelligence methods undermines the safety of personal data as a substantial part of the right to privacy. The author argues that the European Data Protection Supervisor's success in pursuing the policy of "checks and balances" against the European Commission and the Council of EU is vital to ensure the protection of personal data when they are subjected to processing in various administrative procedures. The plausible benefits that may stem from the preventive role of the European Data Protection Supervisor through networking with national data protection authorities and Data Protection Officers in the EU institutions are also analysed. The author concludes that the "soft" powers of the European Data Protection Supervisor can produce some benefits in

---

<sup>1</sup> Институт за међународну политику и привреду, Београд. Рад представља део научног и истраживачког ангажовања истраживача на пројекту: „Србија у савременим међународним односима: стратешки правци развоја и учвршћивања положаја Србије у међународним интегративним процесима – спољнополитички, економски, правни и безбедносни аспекти”, који финансира Министарство за науку и просвету Републике Србије, пројекат бр. ОИ179029, а реализује се у Институту за међународну политику и привреду у периоду 2011–2015.

the long run, namely it can build the culture of data protection in EU institutions and raise awareness amongst the broader public.

*Key words:* privacy, data protection, surveillance, intelligence services, European Data Protection Supervisor, EU institutions.

## 1) ПОДАЦИ О ЛИЧНОСТИ НА УДАРУ ПОЈАЧАНЕ СЕКУРИТИЗАЦИЈЕ НАДНАЦИОНАЛНИХ ЈАВНИХ ПОЛИТИКА

Право на приватност је једно од основних људских права и угаоних каменова демократског поретка и представља једнако важну тековину грађанских револуција које су се одиграле током осамнаестог и деветнаестог века и борбе против тоталитарних поредака у двадесетом веку. Право на приватност се односи на давање могућности сваком човеку самостално и у складу са сопственим уверењима и вољом живи властити живот и у њему слободно, те да заштићен од уплива државе или јавности ради на самоостварењу и испуњењу личних потенцијала.<sup>2</sup> Подаци о личности су неодвојиви део приватности, јер је реч о сваком оном податку који се може јасно приписати конкретної особи, било непосредно именом и презименом, било посредно неким бројчаним параметром или спојем више обележја који творе идентитет те конкретне особе.<sup>3</sup> Осим имена и презимена, примери података о личности су датум рођења, фотографије особе, електронска и поштанска адреса, број фиксног и мобилног телефона, здравствени картон, подаци о коришћењу Интернета, итд. У савременом постиндустријском друштву заснованом на примени информационих и комуникационих технологија, подаци о личности су постали неизоставан део великог броја свакодневних трансакција које појединац обавља са приватним или јавним сектором – у распону од коришћења банкарских услуга до остваривања права на здравствено и социјално осигурање. Због тога данас највећи део јавности ни не доводи у питање да се подаци о личности могу прикупљати из јавности доступних извора информација – тзв. отворених извора, или на начин који не угрожава приватност. О томе сведочи анкета спроведена 2011. године у оквиру „Еврбарометра”, према чијим резултатима скоро три четвртине испитаних грађана ЕУ (74 одсто) прихвата обелодањивање података о личности као нормалан део живота, док се скоро две трећине (64 одсто) у

---

<sup>2</sup> Jack Donnelly, “Human Rights”, in: John Z. Dryzek, Bonnie Honig, and Anne Philips (eds), *Oxford Handbook of Political Theory*, Oxford University Press, Oxford, 2006, pp. 601–620.

<sup>3</sup> Andrew McDonald, “Data Protection”, in: Mark Bevir (ed.), *Encyclopedia of Governance*, First Volume, SAGE Publications, Thousand Oaks (CA), 2007, pp. 193–194.

потпуности слаже са захтевом државе да прикупља све већи број података о личности.<sup>4</sup> Од средине прве декаде двадесет првог века, читава нова грана у приватном сектору израсла је из профита стеченог на продаји готових обавештајних производа сачињених на основу информација прикупљених управо из отворених извора.<sup>5</sup> Нагли технолошки напредак на плану аутоматизације и дигитализације учинио је податке о личности подложнијим руковању и коришћењу у различите сврхе, па и оне које задиру у поље приватности појединца. Никада раније није било лакше прикупљати податке у масовним размерама за тако кратко време, нити је било могуће тако једноставно их складиштити и обрађивати. Узмимо само примере учешћа у друштвеним мрежама на Интернету, комуникације преко *Skype*-а, тзв. *cloud computing*-а и коришћења „паметних” телефона, где корисници заправо самоиницијативно и својевољно складиште податке из домена приватног живота – додуше, у уверењу да неће допасти у туђ посед. Утолико се испоставило да поштовање права на приватност није апсолутно, јер превасходно сâм појединац означава меру у којој жели да буде у додиру са осталим члановима заједнице. На другој страни постоји и општа сагласност у теорији и пракси да демократски уређена држава такође може да се умеша у приватност појединца, увек када то налаже легитимна потреба за остварењем и заштитом јавних интереса. На пример, свака држава жели да путем периодичног пописа становништва утврди различита структурална обележја људи који живе на њеној територији, како би могла да делотворније осмисли и спроводи секторске јавне политике и у крајњој линији одговори на потребе грађана. Због тога људска права треба сагледати као веома сложену и често оспоравану друштвену праксу, која настоји да уреди однос између појединца, друштва и државе у границама омеђеним суштинским вредностима операционализованим посредством неотуђивих и једнаких универзалних права.<sup>6</sup> Ова пракса покреће бескрајну расправу око тога како успоставити равнотежу између легитимне потребе јавних институција да несметано остварују виталне функције и права појединца да у што већој мери очува неповредивост личног живота. Због тога постоји општа сагласност како у правној теорији тако и у пракси националних уставних и судова опште

---

<sup>4</sup> “Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union”, 2011, [http://ec.europa.eu/public\\_opinion/archives/ebs/ebs\\_359\\_en.pdf](http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf), p. 22.

<sup>5</sup> О овом феномену погледати у: Ben Hayes, “Spying in a see through world: the ‘Open Source’ intelligence industry”, *Statewatch Journal*, vol. 20, no. 1, [www.statewatch.org/subscriber/protected/sw20n1.pdf](http://www.statewatch.org/subscriber/protected/sw20n1.pdf), pp. 16–20.

<sup>6</sup> Jack Donnelly, “Human Rights”, op. cit., pp. 601–602.

надлежности чланица ЕУ и Европског суда за људска права да је било какво мешање државе у приватност прихватљиво само уколико се одвија у складу са законом и начелима демократског поретка и ако се њиме остварује легитиман јавни интерес.<sup>7</sup> Делотворна заштита података о личности добија на значају, будући да је неодвојиви део права које сваки појединац има на неповредивост личног и породичног живота, дома и личне преписке. Стога не чуди што је право на заштиту података, поред националних устава и закона земаља чланица, зајамчено и на наднационалном нивоу власти чланом 8 Повеље о основним правима Европске уније.<sup>8</sup> Шта је то што данас у савременим демократијама највише нарушава равнотежу између оптималног спровођења јавних политика и неповредивости приватне сфере? Чини се да је то недавна појава тренда „секуритизације” јавних политика. Секуритизација означава праксу политичких одлучилаца да дефинишу неки јавни проблем и осмисле институционалан одговор тако што придају претежни значај безбедносним импликацијама тог проблема у контексту нормалног функционисања државе и друштва.<sup>9</sup> Секуритизација је делом повезана са променом у схватању садржине вредносног елемента обухваћеног концептом људске безбедности, чије су основне карактеристике универзалност, антропоцентричност, међузависност саставних елемената и нагласак на политици превенције претњи и ризика.<sup>10</sup> Нови концепт нуди проширено виђење о томе шта све може да се појави као безбедносна претња, па тако у круг „осумњичених” уводи разноврсне природне и друштвене процесе и феномене који често превазилазе националне границе. Дрastiчно

<sup>7</sup> Milon Gupta, “Privacy and data protection in the EU”, *Eurescom mess@ge*, No. 3, 2011, [www.eurescom.eu/news-and-events/eurescommessage/eurescom-messge-3-2011/privacy-and-data-protection-in-the-eu.html](http://www.eurescom.eu/news-and-events/eurescommessage/eurescom-messge-3-2011/privacy-and-data-protection-in-the-eu.html), 25/04/2014.

<sup>8</sup> “Charter of Fundamental Rights of the European Union”, Article 8, *Official Journal of the European Communities*, 2010/C 83, 30 March 2010, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:EN:PDF>, p. 10.

<sup>9</sup> Catherine Charrett, “A Critical Application of Securitization Theory: Overcoming the Normative Dilemma of Writing Security”, *ICIP Working Paper*, No. 7, December 2009, International Catalan Institute for Peace, [www20.gencat.cat/docs/icip/Continguts/Publicacions/WorkingPapers/Arxius/WP7\\_ANG.pdf](http://www20.gencat.cat/docs/icip/Continguts/Publicacions/WorkingPapers/Arxius/WP7_ANG.pdf), pp. 12–13.

<sup>10</sup> Детаљније о концепту људске безбедности видети у: “Human Development Report 1994”, UNDP, 1994, [http://hdr.undp.org/en/media/hdr\\_1994\\_en.pdf](http://hdr.undp.org/en/media/hdr_1994_en.pdf). Безбедност се најсажетије може одредити као „одсуство претњи усвојеним вредностима”, како је то учинио Арнолд Волферс (Arnold Wolfers, “National Security” as an Ambiguous Symbol”, *Political Science Quarterly*, Vol. 67, December 1952, p. 485), или као „мала вероватноћа наношења штете усвојеним вредностима”, како је претходну дефиницију преформулисао Дејвид Болдвин (David A. Baldwin, “The concept of security”, *Review of International Studies*, Vol. 23, 1997, p. 13).

ширење садржине појма безбедности појачало је вечну дилему политичких одлучилаца у погледу објективног препознавања реалних претњи по виталне вредности једног друштва, те ефикасног проналажења делотворних институционалних одговора. Ваљана анализа безбедносних претњи претпоставља разликовање између објективне и субјективне димензије безбедности и захтева опрезну процену да ли је нека претња стварна или је прецењена/потцењена у зависности од контекста осмишљавања и спровођења јавне политике и прокламованих интереса и циљева.<sup>11</sup> Концепт безбедности примењен у конкретној датости заправо никада не даје потпуно поуздан одговор на објективне друштвене околности, већ је пре производ политичких и сазнајних избора којима се одређује његова садржина.<sup>12</sup> Етимолошки гледано, идеја безбедности сама по себи подразумева да је нешто или безбедно или небезбедно, мада је у пракси немогуће постићи да нека вредност буде апсолутно безбедна од угрожавања. Како је често тешко поуздано квантитативно утврдити степен (не)безбедности неке заједнице од унутрашњих и спољних претњи, јасно је да осмишљавање и спровођење институционалних мера улази у подручје политичких контроверзи, посебно ако те мере опсегом и садржајем драстично нарушавају приватност грађана. Терористички напади са масовним жртвама извршени 2001. године на Њујорк и Вашингтон те касније на Мадрид (2004) и Лондон (2005), били су окидач за појачану секуритизацију јавних политика засновану на опажању међународног тероризма као асиметричне претње са потенцијалним огромним штетним последицама по становништво, имовину и привредне интересе у САД и другим развијеним земљама. Будући да су истраге показале да су починиоци терористичких напада имали држављанство развијених земаља у којима су напади извршени, круг особа потенцијално интересантних за обавештајне активности драматично је проширен и то на основу нетранспарентних критеријума. Приоритет борбе против међународног тероризма, те пратећих криминалних активности попут прања новца и транснационалног организованог криминала, оправдао је као неопходно масовно прикупљање и обраду података о личности и оснаживање примене обавештајних техника на сопствене грађане. Поједини теоретичари и практичари чак говоре о настанку нове обавештајне парадигме, оличене у геслу „дели”, које наглашава потребу за прослеђивањем обавештајних производа ширем кругу јавних институција укључних у

---

<sup>11</sup> Више у: Arnold Wolfers, “‘National Security’ as an Ambiguous Symbol”, *op. cit.*

<sup>12</sup> Keith Krause and Michael C. Williams, “Broadening the Agenda of Security Studies: Politics and Methods”, *Mershon International Studies Review*, Vol. 40, No. 2, October 1996, p. 234.

спровођење безбедносних политика него што је то икада раније био случај.<sup>13</sup> Додуше, обавештајне службе су и пре покретања „рата против терора” годинама брижљиво стварале обимне базе података о „сумњивим” појединцима. На пример, током прве две декаде постојања, FBI (*Federal Bureau of Investigation*, Савезни биро за истраге) је поседовао око 450,000 досијеа о наводним државним непријатељима, које су агенти потом прогонили, пребијали, масовно хапсили или депортовали.<sup>14</sup> Архиви са досијеима су временом постали још обимнији, па је тако почетком деведесетих година двадесетог века FBI поседовао рачунарску базу са досијеима преко двадесет милиона Американаца.<sup>15</sup> Логика обавештајног рада у функцији репресивне политике претпоставља тајни упад у приватност грађана који се опажају као потенцијална претња поретку, често само на нивоу сумње, а без јасних доказа. На мети широко дефинисаног обавештајног рада усмереног на откривање и процесуирање терориста и криминалаца, нашли су се најпре подаци који су доступни у оквиру тзв. отворених извора, мада уз додатно масовно пресретање електронских комуникација. Оправданост сумњи у велике размере програма праћења становништва првенствено у САД и Великој Британији недавно су потврдиле информације које су јавности процуреле након откривања скандала у британском Штабу за владине комуникације (*Government Communications Headquarters – GCHQ*), или су их доставили „инсајдери”, попут некадашњег службеника америчке Националне безбедносне агенције (*National Security Agency – NSA*) Едварда Сноудена (*Edward Snowden*).<sup>16</sup> Масовно праћење сопствених грађана тешко се може оправдати аргументом да је реч о стандардној процедури обавештајног рада усмереног на откривање и прикупљање доказа о криминалним активностима или припреми терористичких напада, те ни не чуди што америчка и британска влада нису до сада пружиле смислен одговор на откривене злоупотребе. Упркос бројним крупним злоупотребама обавештајног рада откривеним током претходних пар деценија, обавештајни

<sup>13</sup> На пример видети: Damir Črnčec, “A New Intelligence Paradigm and the European Union”, *Varstvoslovje*, Vol. 11, No. 1, 2009, pp. 150–152.

<sup>14</sup> Alexander V. Avakov, *Plato’s Dreams Realized: Surveillance and Citizens Rights from KGB to FBI*, New York, 2006, pp. 35–39.

<sup>15</sup> *Ibid.*, p. 60.

<sup>16</sup> Искрпна прича о Едварду Сноудену доступна је на: [www.theguardian.com/world/the-nsa-files](http://www.theguardian.com/world/the-nsa-files). Скандал о британском Штабу за владине комуникације видети у: “GCHQ taps fibre-optic cables for secret access to world’s communications”, *The Guardian*, online edition, 21 June 2013, [www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa](http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa), 15/04/2014.

практичари и даље одбијају да признају испреплетани утицај саме личности аналитичара, његових вредности и интереса на коначан садржај обавештајног производа.<sup>17</sup> Ипак, рад сваке јавне институције, па и обавештајних служби подложен је било ненамерним грешкама било злоупотребама будући да почива на одлучивању човека са свим његовим личним ограничењима да увек расуђује разумно и непристрасно. Утолико се пре неуверљивим чини становиште заступљено у академским разматрањима, а са разлогом популарно у обавештајном еснафу, према којем обавештајни рад схваћен првенствено као сакупљање и обрада информација сâм по себи не чини ништа нажао људима – „нико тиме није повређен [прикупљањем информација, прим. *аут*], макар не непосредно”.<sup>18</sup> Другачије речено, овако дефинисан обавештајни рад не само да нема негативан морални предзнак, већ се измешта из поља етичког просуђивања. Ипак, обавештајни рад се никако не може свести само на сакупљање и обраду различитих врста информација. Сакупљене информације служе за израду обавештајне анализе, на основу чијих се резултата одлучује о предузимању конкретних радњи које могу *посредно* да нанесу штету праћеним особама. Уколико се не обрађују поставља се питање зашто се уопште прикупљају, а нејасан је у том случају и разлог њиховог чувања. Обелодањивање редовне праксе америчке Националне безбедносне агенције да масовно пресреће електронске комуникације и размењује податке са обавештајним службама земаља чланица ЕУ, показало је да се на мети нашла и приватност грађана Уније и кредибилитет наднационалних институција у погледу способности да заштите право на приватност од продора више испреплетаних транснационалних обавештајних мрежа којима доминира администрација у Вашингтону.<sup>19</sup> Сноуденово сведочење открило је да су подаци о личности грађана Уније предмет прикупљања и обраде Националне безбедносне агенције САД, без судског налога, и то пресретањем интернет саобраћаја у

---

<sup>17</sup> Johan Eriksson and Giampiero Giacomello, “Soft n’ Wide, but Intelligent?: Reflections on Intelligence Analysis for the European Union”, paper presented at the ECPR’s 4th General Conference, Pisa, 6–8 September 2007, [www.researchgate.net/profile/Giampiero\\_Giacomello/publication/228379369\\_Soft\\_n%27Wide\\_but\\_Intelligent\\_Reflections\\_on\\_Intelligence\\_Analysis\\_for\\_the\\_European\\_Union/file/79e415137267e0a97c.pdf?origin=publication\\_detail](http://www.researchgate.net/profile/Giampiero_Giacomello/publication/228379369_Soft_n%27Wide_but_Intelligent_Reflections_on_Intelligence_Analysis_for_the_European_Union/file/79e415137267e0a97c.pdf?origin=publication_detail), p. 7.

<sup>18</sup> Michael Herman, “Ethics and Intelligence After September 2001”, in: Len V. Scott and Peter D. Jackson (eds), *Understanding Intelligence in the Twenty-First Century: Journeys in Shadows*, Routledge, London and New York, 2004, p. 180.

<sup>19</sup> Didier Bigo et al., “Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law”, *CEPS Papers in Liberty and Security in Europe*, No. 61, November 2013, Centre for European Policy Studies, pp. 19–28.

реалном времену и непосредним приступом подацима похрањеним на серверима информатичких компанија са седиштем у САД – *Microsoft, Yahoo, Google, Apple, Facebook* и *Skype*. Поред тога, могуће су штетне последице по компаније са седиштем у ЕУ у виду отицања пословних тајни ка САД, које потом могу да злоупотребе америчке компаније и тиме стекну предност на тржишту.<sup>20</sup> Посматрано са становишта изложености података о личности грађана Уније неовлашћеном обавештајном приступу, додатни проблем представља чињеница да, званично и номинално, ЕУ нема сопствену обавештајну службу која би спроводила тајне операције на терену, па ни Европски парламент на први поглед нема над чиме да спроводи надзор. Премда се ослања на обавештајни рад националних служби земаља чланица, у стварности ЕУ је током последње две декаде – без унапред усвојене стратегије и плана, односно према текућим потребама спровођења комунитарних политика – изградила мрежу од шест служби које обављају различите обавештајне функције са укупно око 1300 запослених.<sup>21</sup> Први корак је било оснивање Европола Уговором из Мастрихта, једине институције Уније са обавештајном функцијом која задовољава мерило демократског легитимитета будући да је установљена основним уговорима. Међутим, током протекле декаде основано је више агенција и тела у чијем се делокругу рада налази и обављање обавештајних задатака: Центар за обавештајну анализу (*Intelligence Analysis Center – INTCEN*), Обавештајни директорат (*Intelligence Directorate – INTDIR*), Европска агенција за руковођење оперативном сарадњом на спољним границама земаља чланица ЕУ (*European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union – Frontex*) и Сателитски центар (*Satellite Center – SATCEN*). Само су Европол и Frontex подвргнуте извесном степену парламентарне контроле, док су тела из домена Заједничке спољне и безбедносне политике и Заједничке безбедносне и одбрамбене политике (*INTCEN* и *INTDIR*) придодата Европској служби за спољно деловање (*European External Action Service – EEAS*). У оквиру генералног секретаријата Савета ЕУ као посебна организациона јединица од 2007. делује Јединствена за обавештајну анализу (*Single Intelligence Analysis Capacity – SIAC*), која обједињује поједине функције Ситуационог центра (*Joint Situation Centre – SITCEN*) и обавештајне јединице Војног штаба Уније.

<sup>20</sup> Ibid., p. 2.

<sup>21</sup> Wolf Richter, “The EU’s Out-Of-Control Intelligence Services (That Don’t Exist, Officially)”, *Zero Hedge*, webportal, 9 May 2013, [www.zerohedge.com/contributed/2013-05-09/eu%E2%80%99s-out-control-intelligence-services-don%E2%80%99t-exist-officially](http://www.zerohedge.com/contributed/2013-05-09/eu%E2%80%99s-out-control-intelligence-services-don%E2%80%99t-exist-officially), 01/04/2014.



Аргумент против њиховог увођења у основне правне акте ЕУ заснива се на тврдњи да ове службе користе само готове обавештајне производе које им проследи националне службе држава чланица. Мартин Еренхаузер (Martin Ehrenhauser), независни посланик Европског парламента из Аустрије и члан Пододбора за безбедност и одбрану, тврди да је наведени аргумент нетачан јер ове службе и ван територије Уније самостално прикупљају и анализирају обавештајне податке, те шаљу строго поверљиве извештаје наднационалним политичким одлучиоцима.<sup>22</sup> Наведени обавештајни скандали указују да постоји простор у којем може да дође до сукоба националних и наднационалних надлежности и до покретања питања правне одговорности институција Уније, тамо где њене безбедносне активности укључују коришћење и дељење података о личности прикупљених радом националних обавештајних служби. Ризик те врсте присутан је у области спровођења свеобухватне размене информација предвиђене Стратегијом ЕУ за унутрашњу безбедност (*EU Internal Security Strategy in Action*), посебно у раду Европола и INTCEN-а (у мањој мери Евројуста, Frontex-а и OLAF-а), будући да уопште не постоји механизам верификације да су подаци послати са националног на наднационални ниво прикупљени и обрађени легитимно и на законит начин.<sup>23</sup> Актуелни директор Европола Роб Вејнрајт (Rob Wainwright), у саслушању које је септембра 2013. одржао Одбор за грађанске слободе, правду и унутрашње послове Европског парламента, није пружио чврсте аргументе да ова комунитарна агенција у свом раду користи искључиво податке о личности прикупљене сагласно стандардима садржаним у националним и наднационалним прописима.<sup>24</sup> Највећи број података се размењује на билатералном нивоу, односно између националних официра за везу смештених у седишту Европола, па према тврдњи стручњака постоји велика вероватноћа да се на наднационалном нивоу размењују и обрађују подаци прикупљени на неком другом месту на споран начин.

---

<sup>22</sup> Martin Ehrenhauser, "EU Intelligence Service without Democratic Control", [www.ehrenhauser.at/archiv/lang/en/issues/secret-service/](http://www.ehrenhauser.at/archiv/lang/en/issues/secret-service/), 03/04/2014.

<sup>23</sup> "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe", COM(2010) 673 final, Communication from the Commission to the European Parliament and the Council, 22 November 2010, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF#page=2>.

<sup>24</sup> Видео снимак саслушања доступан је на: LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, 24 September 2013, European Parliament, [www.europarl.europa.eu/ep-live/en/committees/video?event=20130924-0900-COMMITTEE-LIBE,02/04/2014](http://www.europarl.europa.eu/ep-live/en/committees/video?event=20130924-0900-COMMITTEE-LIBE,02/04/2014).

Посматрано из перспективе остварења начела друштвене правде, легитимни циљ делотворне социјалне контроле криминала и тероризма прераста у контроверзно питање када се користе обавештајне интрузивне технике и методе. Чак и неvezано за злоупотребе до којих може да дође у обавештајном раду, велики број података о личности предмет је редовне обраде у свакодневном раду институција Европске уније. озбиљна штета за грађане не мора нужно да настане као производ кршења етичких стандарда у раду безбедносних служби, већ може да проистекне из пукe нетачности или застарелости податка, или његове доступности особи која није за то овлашћена. Прикупљање података о личности је често неприметно за грађане, чак и када је великих размера и тече 24 часа дневно. На то можда најбоље указује пример видео надзора, који је током последње декаде драстично увећан у јавном простору. Видео надзор по себи увек задире у приватност и у домен заштите података о личности, будући да укључује обраду података о личности јер омогућује утврђивање идентитета снимљених особа. Видео надзор носи са собом опасност од злоупотреба и несразмерног и претераног прикупљања података о личности. На пример, ризик од кршења права на приватност може да се појави када просторни и временски параметри видео надзора нису дефинисани тако да буду ограничени на заштиту конкретних безбедносних интереса, што је приметно по несразмерности употребљене техничке опреме. Проблем је у томе што опрема углавном омогућава и снимање, па се поставља питање да ли ће власник видео надзора ваљано и безбедно чувати видео запис у смислу спречавања неовлашћеног приступа и доласка у посед, колико ће га дуго чувати и да ли ће га и како уништити.<sup>25</sup> Наведени ризици додатно добијају на значају када су могући у јавним институцијама. Све институције и тела Уније из безбедносних разлога имају у службеним просторијама видео надзор, што ствара одређене импликације по право на приватност не само посетилаца, већ и запослених. Примера ради, видео надзор се може злоупотребити како би се неовлашћено прикупиле информације о томе шта наднационални службеници говоре и раде, што у крајњој линији може да доведе до повреде њихових права у погледу слободе говора, окупљања и забране дискриминације. Уколико се као безбедносно оруђе користи селективно и сразмерно, видео надзор може да делотворно заштити интересе запослених и институције Уније у којој раде а да не наруши право на приватност. Пример видео надзора само делимично указује на значај

<sup>25</sup> Опширније видети у: Невена Ружић, „Надзор над видео надзором”, *Ревизија за безбедност*, Год. V, бр. 4, 2011, стр. 267–281.

успостављања ваљаног механизма и праксе заштите података о личности грађана ЕУ и на наднационалном нивоу власти. Грађанин има право да зна да ли нека институција Уније прикупља и/или обрађује податке о његовој личности, као и која је то институција учинила са којом сврхом и коме ће обрађени подаци бити достављени.<sup>26</sup> Грађанин има и право да бесплатно провери тачност информације која је повезана са његовом личношћу, а у случају да утврди њену нетачност или непотпуност има право да затражи њено исправљање, или да је блокира у појединим околностима. Грађанин Уније има право да затражи брисање сваког податка чије коришћење је незаконито, као и да буде обавештен када неки податак о његовој личности треба по први пут да постане доступан трећој страни у рекламне сврхе. Премда наведена права не могу да се ускрате, она ипак могу да се ограниче на одређени период у следећим околностима:

- Ради превенције, спровођења истраге, откривања и процесуирања осумњичених за кривична дела, дисциплинске и административне прекршаје;
- Ради заштите важног економског или финансијског интереса државе чланице или саме Европске уније;
- Ради заштите слобода и права других грађана;
- Из разлога националне или јавне безбедности или одбране државе чланице.
- У случају примене неког од наведених ограничења, грађанин мора да буде обавештен о разлозима због којих је то учињено.<sup>27</sup>

## II) ЕВРОПСКИ НАДЗОРНИК У НАДНАЦИОНАЛНОЈ ИНСТИТУЦИОНАЛНОЈ АРХИТЕКТУРИ

Европски надзорник за заштиту података о личности (*European Data Protection Supervisor* – EDPS) је независан наднационални орган, чији се челник и његов заменик бирају заједничком одлуком Европског парламента и Савета ЕУ на мандат од пет година.<sup>28</sup> Основна сврха овог тела је да се стара

---

<sup>26</sup> “Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data”, Section 5 (Articles 13–19), *Official Journal of the European Communities*, L8, 12 January 2001, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF>.

<sup>27</sup> *Ibid.*, Article 20.

<sup>28</sup> *Ibid.*, Article 24.

да наднационалне институције доследно поштују право на заштиту података о личности, било када обрађују ту врсту података у редовном спровођењу административних процедура било при осмишљавању и развоју нових комунитарних програма и политика. Европски надзорник нема овлашћење да контролише рад органа јавне власти и приватних организација на националном нивоу власти. Европски надзорник за заштиту података о личности остварује поверену надлежност у три основна подручја.

## 1. Контролна функција

Прво поље деловања је контрола усаглашености начина обраде података о личности у наднационалним органима и телима са стандардима установљеним комунитарним прописима. Општа контролна функција спроводи се у виду периодичног праћења примене прописа у овој области и прикупљања статистичких података потребних за утврђивање репера, како би се потом поредило фактички утврђено стање са нормативном регулативом. Европски надзорник тај посао обавља у тесној сарадњи са службеницима институција Уније задуженим за заштиту података (*Data Protection Officers*). Сарадња се одвија тако што се ови службеници у оквиру делокруга сопствених надлежности старају да су руководиоци и службеници наднационалне институције у којој раде информисани о правима и обавезама које имају на плану заштите података о личности, да се комунитарни прописи у овој области примењују, те тако што уредно воде регистар спроведених обрада података и обавештавају европског надзорника о случајевима обраде са ризиком (по права грађана).<sup>29</sup> Службеници за заштиту података чине мрежу која се састаје периодично са европским надзорником и његовим сарадницима ради размене мишљења о актуелним питањима и практичним искуствима у овој области. Европски надзорник има овлашћење да истраге и инспекције спроводи самоиницијативно.<sup>30</sup> Инспекције могу бити циљане, односно када се спроводе ради утврђивања чињеница у случајевима контроле да ли је институција

<sup>29</sup> Опширније о дужностима службеника ЕУ задужених за заштиту података видети у: "Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001", European Data Protection Supervisor, November 2005, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PositionP/05-11-28\\_DPO\\_paper\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PositionP/05-11-28_DPO_paper_EN.pdf).

<sup>30</sup> "Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data", Articles 41(2), 46(c), 47(2), *op. cit.*

поступила по решењу европског надзорника, донетом по жалби оштећеног грађанина.<sup>31</sup> Инспекције могу бити и опште природе, нпр. ради процене стања поштовања комунитарних прописа о заштити података о личности. Европски надзорник најављује да ће обавити контролу и означава њен опсег, а има овлашћење да уђе у службене просторије и да неометано приступи свим информацијама и документима релевантним за сврху истраге.<sup>32</sup> Инспекције се спроводе селективно према утврђеном годишњем плану уобличеном према процени ризика од појаве кршења права на заштиту података, а водећи рачуна и о оптималном коришћењу сопствених ресурса.<sup>33</sup> На пример, као мерила ризика узимају се врсте обрађених података о личности, број жалби на процес обраде, степен усклађености са комунитарним прописима и ранијим одлукама европског надзорника. Постоји разлика између инспекцијског надзора и посете ради утврђивања усклађености (*compliance visit*). Када уочи да у некој институцији влада низак или незадовољавајући степен поштовања комунитарних прописа или је потребно јачање свести о заштити података о личности, или када нема одговарајуће међуинституционалне комуникације, европски надзорник може да дође у једнодневну посету како би личним контактом са надлежним руководиоцем издејствовао поправљање стања.<sup>34</sup> Сврха посете је да се успостави редовна комуникација између руководства посећене наднационалне институције и европског надзорника у погледу утврђивања акционог плана са конкретним обавезама и роковима њиховог испуњавања. Уколико оваква посета не уроди плодом, европски надзорник може да изврши инспекцију. Контролну функцију европски надзорник обавља и спровођењем истраге на основу жалби које појединци подносе на рад институција Уније. Сваки грађанин или наднационални службеник који сматра да је његово право на приватност података повређено радом неке институције Уније, а није успео да то разреши са институцијом у питању, може да поднесе жалбу европском надзорнику и она се третира као поверљива.<sup>35</sup> Европски

---

<sup>31</sup> “Inspections conducted by the EDPS: Policy paper”, European Data Protection Supervisor, November 2013, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2013/13-11-04\\_EDPS\\_Inspection\\_Policy\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2013/13-11-04_EDPS_Inspection_Policy_EN.pdf), pp. 4–5.

<sup>32</sup> “Inspection Guidelines”, European Data Protection Supervisor, November 2013, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2013/13-11-04\\_EDPS\\_Inspection\\_guidelines\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2013/13-11-04_EDPS_Inspection_guidelines_EN.pdf), pp. 2–3.

<sup>33</sup> *Ibid.*, p. 1.

<sup>34</sup> “Rules of Procedure”, Article 37.

<sup>35</sup> Детаљи о подношењу жалбе доступни су на: <https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Complaints>.

надзорник се у разматрању поднете жалбе води превасходно природом и тежином наведеног прекршаја права на заштиту података о личности, бројем особа чија права су угрожена прекршајем, потенцијалним општим значајем случаја по јавне интересе, као и вероватноћом да се утврди да је прекршај начињен. Због тога се истраге поводом жалби на ситне прекршаје не покрећу, као ни жалбе које су већ поднете европском омбудсману. Уколико је жалба правно основана, европски надзорник покреће истрагу, али ће се – сходно начелима сразмерности и оправданости – првенствено постарати да постигне решење проблема посредовањем између оштећеног грађанина и институције која је прекршила право на приватност. У супротном, надзорник доноси решење и прослеђује га обема странама, а оно може да садржи мере у распону од савета, преко опомене или упозорења до изрицања забране обраде података или упућивања случаја Суду правде. Као посебан вид контролне функције предвиђена је обавеза институције Уније да, у случају када жели да обради податак о личности у оквиру операције или процедуре која носи у себи ризик по слободу и права грађана обавести европског надзорника ради претходне контроле (*prior checking*).<sup>36</sup> Највећи ризик може да се појави код обраде података који се односе на процену личних психо-физичких способности, понашања и здравственог стања, кривични прогон и кажњавање, примену безбедносних мера, као и код база података које се користе у операцијама замрзавања имовине или спречавања проневере у јавним набавкама. Као што смо показали у првом делу овог рада, вероватноћа да дође до кршења комунитарних прописа велика је и код обраде биометријских података и надзора електронске комуникације. Поступак претходне контроле почиње тако што званичник институције или тела Уније задужен за заштиту података о личности упућује европском надзорнику обавештење, које се увршћује у регистар доступан јавности. Надзорник потом проверава да ли је императив заштите података о личности ваљано уграђен у структуру предузете операције или процедуре, те да – уколико је то потребно – изда мишљење у облику препорука са тачним смерницама како да институција у предузетој операцији или процедури исправно примени комунитарне прописе о заштити података. Европски надзорник прати и да ли је институција у питању ваљано применила његове препоруке и отклонила уочене мањкавости. Сврха ове врсте контроле је да се пре почетка процеса обраде података о нечијој личности спрече евентуалне грешке или злоупотребе, мада европски надзорник обавља

<sup>36</sup> “Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data”, Article 27(1), op. cit.

контролу и након почетка обраде података у случајевима када је тај процес покренут пре његовог именованја на функцију (тзв. *ex post prior check*).

## 2. Консултативна функција

Друго поље деловања је консултативни рад са наднационалним институцијама у погледу питања која задиру у област заштите података о личности или имају шире импликације по приватност. Европски надзорник даје мишљења о законодавним предлозима и коментаре на остале врсте комунитарних правних аката и предлоге комунитарних политика и програма, а на општем плану прати технолошки развој и указује на његове друштвене последице у оквиру свог домена.<sup>37</sup> Редовно објављивање мишљења о наднационалним законодавним предлозима, које се прослеђује свим заинтересованим странама и обзнањује у *Службеном гласнику ЕУ*, повезана је са обавезом Европске комисије да поднесе европском надзорнику на увид сваки предлог комунитарног прописа који има импликације по заштиту података о личности. Европски надзорник пажљиво анализира сврху, опсег и садржај предлога у контексту утицаја на обраду, чување и приступ осетљивим подацима и на уживање права на приватност, а потом издаје препоруке како унапредити предлог прописа. Мишљење европског надзорника постаје формалан део законодавног поступка, те се представља надлежном одбору Европског парламента и релевантној радној групи Савета ЕУ. На пример, европски надзорник је само у време првог мандата (2004–2009) издао скоро 50 мишљења о законодавним предлозима који су погађали материју заштите података о личности. Реч је о областима полицијског и правосудног рада, телекомуникационог саобраћаја, приватности електронске комуникације, приступа информацијама од јавног значаја и размени поверљивих података са САД. Када даје коментаре на предлоге комунитарних јавних политика и програма, европски надзорник прави озбиљну студију и на основу њених налаза даје препоруке како садржај уподобити стандардима у области заштите података о личности. Наднационалне институције имају могућност да консултују европског надзорника приликом израде административне мере или предлога интерних правила, увек када постоји ризик да због њихове сложености дође до штетних последица по делотворну заштиту података о личности.<sup>38</sup>

---

<sup>37</sup> Ibid., Article 46.

<sup>38</sup> Европски надзорник за заштиту података о личности је издао више тематски разврстаних смерница како би подстакао институције Уније да редовно консултују службу надзорника када имају дилему о питањима заштите приватности. Смернице су доступне на: <https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/Guidelines>.

Надзорник испуњава саветодавну функцију и редовним организовањем радионица намењених званичницима наднационалних институција задужених за старање о заштити података о личности, као и одржавањем редовних састанака било у оквиру мреже ових званичника било појединачно. Европски надзорник крајем сваке године објављује списак приоритета за наредну годину и законодавних предлога Европске комисије који захтевају давање формалног мишљења о усаглашености са прописима о заштити података о личности. На пример, приоритети за 2014. годину су израда нових комунитарних прописа о заштити података о личности, изградња поверења у глобални проток података, јачање дигиталне димензије економског раста, реформа финансијског сектора, пореска утаја и тајност банкарских података и даљи развој у Простору слободе, безбедности и правде.<sup>39</sup> У оквиру консултативне функције, европски надзорник може да учествује у поступцима покренутим пред Судом правде и Трибуналом за јавну службу тако што има овлашћење да судској инстанци проследи неки случај који је разматрао у оквиру делокруга своје надлежности и да се умеша у судски поступак уколико се у њему одлучује о материји из његовог домена.<sup>40</sup> Европски надзорник није у досадашњем раду проследио ниједан случај Суду правде, али је интервенисао у више судских поступака у којима се одлучивало о испреплетаности приступа информацијама од јавног значаја и заштите података о личности, правном основу за задржавање података, размени података између институција Уније и самосталности националних институција задужених за заштиту података у односу на наднационални ниво власти.<sup>41</sup>

### **3. Остваривање заштите података о личности сарадњом са другим наднационалним и националним институцијама**

Треће подручје деловања европског надзорника обухвата сарадњу са националним парњацима у земљама чланицама ради уједначавања праксе заштите података о личности у Унији и сарадњу са надзорним телима која се старају о базама података великих размера, попут Евродака (*Eurodac*), која

<sup>39</sup> “Inventory 2014: A strategic approach to legislative consultation”, European Data Protection Supervisor, 18 December 2013, Brussels, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Priorities/13-12-18\\_Inventory\\_Note\\_Priorities\\_2014\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Priorities/13-12-18_Inventory_Note_Priorities_2014_EN.pdf).

<sup>40</sup> “Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data”, Article 47(h), op. cit.

<sup>41</sup> Списак судских предмета у којима је европски надзорник интервенисао налази се на: <https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Court>.



садржи отиске прстију свих тражилаца азила. Радна група за члан 29 (*Article 29 Working Party*) служи као форум где се национални државни органи задужени за заштиту података о личности редовно састају са европским надзорником и представницима Европске комисије, како би дошли до заједничког тумачења у погледу примене комунитарних и националних прописа.<sup>42</sup> Поред уједначавања примене наднационалних прописа које се изражава у облику заједничких ставова и мишљења, Радна група за члан 29 је важна јер пружа Европској комисији општу експертизу на основу знања и праксе стечених на националном нивоу власти и даје савете о садржају комунитарних прописа из тзв. првог стуба интеграције, када год погађају право на заштиту података о личности. Састанци чланова Радне групе се одвијају и у виду подгрупа, које се баве посебним техничким питањима попут нпр. како делотворно одговорити на претње безбедности Интернета.

Део послова европског надзорника у подручју сарадње са другим институцијама одиграва се у области полицијске и правосудне сарадње када се разматра функционисање информационих система у оквиру спровођења закона. Најважнији део сарадње тиче се великих информационих база које постоје на нивоу Уније, попут база Европола и Евројуста, а посебно Евродака – система подељене надлежности који се састоји од националних јединица и средишње, наднационалне јединице. Будући да је реч о информационим системима који стално обрађују и размењују податке о личности тражилаца азила и виза, несталих особа, путника итд., ризик од појаве злоупотребе или чињења грешака је веома велики, па је неопходан чвршћи надзор и уједначеност примене комунитарних прописа – посебно имајући у виду разлике у националним законодавствима. Због тога европски надзорник организује редовне састанке са колегама из земаља чланица како би се осигурала ваљана координација наднационалне и националне надзорне функције.

### **III) „У РАЉАМА„ НАДНАЦИОНАЛНЕ МЕЂУИНСТИТУЦИОНАЛНЕ ИГРЕ ЗА НАДМОЋ: КО ТО НЕ ЖЕЛИ ДА ЗАШТИТИ ПОДАТКЕ О ЛИЧНОСТИ?**

Као што смо показали у првом делу овог рада, тренд секуритизације јавних политика легитимизован борбом против тероризма, организованог криминала и других тзв. асиметричних, „меких” безбедносних претњи, захватио је током протекле деценије и наднационални ниво власти. Масовна и некритичка

---

<sup>42</sup> У раду овог форума учествују и представници Норвешке, Исланда и Лихтенштајна.

примена специјалних истражних метода и техника преузетих из класичног обавештајног рада, откривена у више већих обавештајних скандала у значајној је мери подрила несметано уживање права на приватност грађана Уније. Тиме је угрожен традиционално релативно низак ниво поверења јавности у наднационалне институције, првенствено у рад Европске комисије коју грађани опажају стереотипно као бриселску „еврократију” потпуно отуђену од биначког тела. У прилог томе говоре и резултати „Евробарометра” од 2012. године, према којима свега мало више од половине грађана Уније (55 одсто) има поверење да наднационалне институције (на првом месту Европска комисија) ваљано прикупљају и обрађују податке о личности.<sup>43</sup> Посматрано по наднационалним институцијама појединачно, годишњи извештаји европског надзорника у раздобљу од 2009. до 2013. године сведоче да се највећи број притужби за кршење права на заштиту података тиче управо поступања руководства и службеника Европске комисије.<sup>44</sup> Кршења права грађана највише се дешавају у виду обелодањивања, заштите поверљивости, преправљања, прекомерног прикупљања, губитка, брисања или прослеђивања података о личности другим наднационалним или националним институцијама трећих земаља.<sup>45</sup> Анализа надлежности и овлашћења европског надзорника за заштиту података о личности указује да је његов положај у структури наднационалне институционалне моћи сличан положају европског омбудсмана.<sup>46</sup> Премда је европски надзорник недвосмислено независна

<sup>43</sup> “Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union”, op. cit., p. 138.

<sup>44</sup> “Annual Report 2009”, European Data Protection Supervisor, 2010, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2009/AR2009\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2009/AR2009_EN.pdf), p. 35; “Annual Report 2010”, European Data Protection Supervisor, 2011, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2010/AR2010\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2010/AR2010_EN.pdf), p. 34; “Annual Report 2011”, European Data Protection Supervisor, 2012, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2011/AR2011\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2011/AR2011_EN.pdf), p. 33; “Annual Report 2012”, European Data Protection Supervisor, 2013, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2012/AR2012\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2012/AR2012_EN.pdf), p. 35; “Annual Report 2013”, European Data Protection Supervisor, 2014, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2013/AR2013\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2013/AR2013_EN.pdf), p. 33.

<sup>45</sup> “Annual Report 2009”, op. cit., p. 36; “Annual Report 2010”, op. cit., p. 34; “Annual Report 2011”, op. cit., pp. 32–33; “Annual Report 2012”, op. cit., p. 36; “Annual Report 2013”, op. cit., p. 34.

<sup>46</sup> Анализу институционалног положаја европског омбудсмана видети у: Срђан Кораћ, „Европски омбудсман као механизам контроле рада наднационалних институција Европске уније”, *Европско законодавство*, Год. XII, бр. 45–46, 2013, стр. 108–121.

институција, делотворност његовог контролног рада ограничена је чињеницом да му на располагању стоје углавном средства тзв. меке моћи – вршење притиска, убеђивање и преговарање, а не и извршна овлашћења која омогућавају непосредно санкционисање кршења комунитарних стандарда. Упркос поседовању меке моћи, чини се да је европски надзорник у оквиру поверених надлежности успео да израсте у релативно значајну противтежу Европској комисији и Савету ЕУ. Можда се у том светлу може сагледати једна од актуелних контроверзи наднационалног политичког процеса, а то је неоправдано одлагање именовања новог европског надзорника. Мада је петогодишњи мандат садашњем надзорнику Питеру Хастинксу (Peter Hustinx) истекао још у јануару ове године, Европска комисија је до сада одбила пријаве више особа које су конкурисале за ову наднационалну функцију, уз штуро образложење дато Европском парламенту и широј јавности да су кандидати неодговарајући.<sup>47</sup> Основана је претпоставка да је продужавање статуса европског надзорника као вршиоца дужности повезано са његовим досадашњим залагањем да у што већој мери ојача институционалну моћ ове важне наднационалне бране продору у приватност. Један од стратешких циљева европског надзорника је даље унапређење надзора над наднационалним институцијама због све обимније обраде података о личности и јачање културе заштите приватности повећањем броја теренских инспекција. Такође, Хастинкс се свесрдно залагао да се одбије потписивање контроверзног Трговинског споразума против кривотворења (*Anti-Counterfeiting Trade Agreement* – АСТА), којим би практично била укинута неутралност и слобода Интернета и тиме олакшан обавештајни продор у приватност грађана Уније. Пошто се такви ставови косе са интересима трансатлантске безбедносне сарадње, не чуди што је европском надзорнику онемогућено да присуствује састанцима радних тела Савета ЕУ на којима се разматрају питања од значаја за заштиту приватности.<sup>48</sup> Спорно одсуство одлуке о именовању подстиче сумњу да Комисија и Савет ЕУ настоје да евентуално осујете или умање утицај европског надзорника као независне институције на ток реформе комунитарних прописа о заштити података о личности, односно на преговоре који се тим поводом тренутно воде унутар радних тела Савета ЕУ.

---

<sup>47</sup> Jeremy Fleming, "Pressure grows over EU data watchdog replacement", *EurActive*, 9 January 2014, [www.euractiv.com/euro-finance/commission-asked-explain-lack-da-news-532657](http://www.euractiv.com/euro-finance/commission-asked-explain-lack-da-news-532657), 12/05/2014; "Commission: No suitable candidates for European Data Protection Supervisor", *Ecommerce Europe*, 17 January 2014, [www.ecommerce-europe.eu/news/commission-no-suitable-candidates-for-european-data-protection-supervisor](http://www.ecommerce-europe.eu/news/commission-no-suitable-candidates-for-european-data-protection-supervisor), 12/05/2014.

<sup>48</sup> Nikolaj Nielsen, "EU data supervisor wants greater powers", *EU Observer*, 23 January 2013, <http://euobserver.com/justice/118811>, 10/05/2014.

Комуитарни прописи у области заштите података о личности осмишљени су средином деведесетих година минулог века, у време када је Интернет био тек у зачетку са веома уским кругом корисника, па ни механизам заштите права на приватност није био дизајниран да би делотворно одговорио на изазове са којима се данас просечан корисник рачунара свакодневно суочава.<sup>49</sup> Европски надзорник и Европски парламент су сагласни да сврха реформе Регулative 45/2001 треба да буде постизање равнотеже између несметане легитимне употребе података о личности – чији актери могу да буду грађани, компаније и јавне институције – и могућности грађана да контролишу шта се дешава са њиховим подацима – како унутар тако и ван територије ЕУ.<sup>50</sup> Такође, право на приватност мора да се ојача једнако на националном и наднационалном нивоу власти, и то већом контролом над процесом прикупљања и обраде података о личности и већим обавезама јавних институција и актера у приватном сектору. Питање над свим питањима – а на које европски надзорник стално указује – јесте како ваљано применити начело сразмерности при задирању у приватност. Сразмерност неке интрузивне мере немогуће је јасно одредити у односу на значај доказа који се на тај начин жели прибавити ради кривичног прогона осумњиченог, будући да се таква врста доказа сада третира као тајна због интереса истраге и разлога националне безбедности. Оправданост конкретне безбедносне мере мора се процењивати искључиво према њеном актуелном дејству на безбедност, а не према опаженом или претпостављеном. Одсуство уравнотежене примене начела сразмерности води ка злоупотребима у виду коришћења прикупљених података о личности праћене особе ван њихове првобитне сврхе. На пример, када се за праћену особу на основу прикупљених података утврди да није терориста, али се у исто време открије да је починила друго кривично дело, обрађени подаци не смеју да се користе као основ за покретање нове истраге. Велики проблем представља и слаба заштита података о личности на наднационалном нивоу од неовлашћеног прослеђивања

<sup>49</sup> Peter Hustinx, "A Clear Signal for Stronger EU Data Protection", *Zeitschrift für Datenschutz*, nr. 2013/7, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-06-17\\_Editorial\\_ZfD\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-06-17_Editorial_ZfD_EN.pdf), pp. 301–302; "First report on the implementation of the Data Protection Directive (95/46/EC)", European Commission, 2003, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0265&from=en>; "Why do we need an EU data protection reform?", [http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf).

<sup>50</sup> "Report on a comprehensive approach on personal data protection in the European Union", Committee on Civil Liberties, Justice and Home Affairs, European Parliament, 22 June 2011, [www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2011-0244+0+DOC+PDF+V0//EN](http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2011-0244+0+DOC+PDF+V0//EN), pp. 4–5.

приватном сектору или иностраним обавештајним службама.<sup>51</sup> На основу представљене аргументације, европски надзорник је изразио забринутост да би измењена регулатива омогућила додатна ограничења људских права, већа овлашћења Европске комисије и нове основе за изузетке од примене начела ограничења сврхе прикупљања и обраде података о личности.<sup>52</sup>

Европски надзорник има другачије виђење у погледу оптималног решења неуједначеног третмана заштите података у националним законодавствима земаља чланица, а реч је о проблему који грађани јасно препознају. Чак 90 одсто анкетираних грађана Уније сматра да је веома важно да на целој територији ЕУ право на заштиту података о личности и пратећа пракса његове заштите буду под једнаким условима.<sup>53</sup> Правне празнине у садашњој Директиви 95/46 довеле су до значајних националних разлика у тумачењу истих права и обавеза и искомпликовале уживање права на приватност. Ипак, измене Директиве 95/46 које је предложила Европска комисија не би повећале степен заштите у државама чланицама, већ би га генерално смањиле и створиле нове ризике за приватност грађана који би сада дошли кроз рад полиције и правосуђа. Стандарди предвиђени предлогом нове директиве не прате стандарде садржане у предлогу регулативе, па се као жаришне тачке појављују: одсуство правне сигурности у области даље употребе података о личности у полицијском раду и обавезе полиције да докаже сагласност обраде података коју жели да предузме са захтевима њихове ваљане заштите, слаба заштита код прослеђивања података трећим земљама и неоправдано слаба овлашћења институција задужених за заштиту података о личности. Према мишљењу европског надзорника, заменом Директиве 95/46 регулативом са непосредним дејством у државама чланицама надоместио би се застој у отклањању лоших решења садржаних у националним прописима и осигурала тешња међусобна сарадња националних институција задужених за заштиту података.<sup>54</sup> Остваривање консултативне функције европског надзорника делом је спутано покушајима Европске комисије да се он искључи из

---

<sup>51</sup> "Protection of Personal Data in Transatlantic Security Cooperation SWIFT, PNR & Co: Which Way Forward?", Public Hearing, 8 April 2010, Statewatch, [www.statewatch.org/news/2010/apr/eu-usa-pnr-hearing-8-april-10-briefing.pdf](http://www.statewatch.org/news/2010/apr/eu-usa-pnr-hearing-8-april-10-briefing.pdf), pp. 4–5.

<sup>52</sup> "Annual Report 2012", op. cit., pp. 48–49.

<sup>53</sup> "Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union", op. cit., p. 181.

<sup>54</sup> "Stronger rights for citizens and data protection authorities: Interview with Peter Hustinx on data privacy in Europe", Eurescom mess@ge, No. 3, 2011, [www.eurescom.eu/news-and-events/eurescommessage/eurescom-messge-3-2011/data-privacy-interview-peter-hustinx.html](http://www.eurescom.eu/news-and-events/eurescommessage/eurescom-messge-3-2011/data-privacy-interview-peter-hustinx.html).

наднационалног законодавног процеса. Примера ради, Комисија није консултовала европског надзорника у поступку израде техничких регулаторних прописа у области примене нове генерације безбедносних скенера (*body image scanners*) у цивилном ваздушном саобраћају, усвојене у јулу 2011. године под окриљем Регулаторног одбора за безбедност цивилног ваздухопловства (*Regulatory Committee for Civil Aviation Security*).<sup>55</sup> Премда је на први поглед реч о усвајању мера чисто техничке природе, овај пропис заправо носи са собом импликације по право на приватност и заштиту података зато што побољшана технологија скенера омогућује детаљан приказ делова тела. Реч је о веома интрузивној методи чија примена може да буде оправдана само у случајевима када није могуће користити мање интрузивне методе да би се постигао безбедносни циљ приликом редовне контроле путника у авионском превозу. Европски надзорник и Европски парламент заузели су становиште да су стандардни скенери сасвим довољни за контролу путника, па стога одлука о примени нове генерације скенера представља пример одступања од начела сразмерности и неопходности.<sup>56</sup> Искључивање европског надзорника не само да је подрило транспарентност самог поступка доношења овог прописа, него је отворило сумњу да ли су у овом случају заиста поштована начела неопходности и сразмерности. У спровођењу консултативне улоге, европски надзорник се суочава са највећим контроверзама у области контроле спољних граница Уније и јачања полицијске и правосудне сарадње. Поводом покретања поступка за усвајање предлога регулативе о успостављању Европског система за гранични надзор (*European Border Surveillance System – EUROSUR*), европски надзорник је скренуо пажњу да овај комунитарни пропис мора да садржи одредбе са јасно и исцрпно наведеним условима у којима подаци о личности могу да буду предмет обраде и размене са трећим земљама у оквиру EUROSUR-а.<sup>57</sup>

<sup>55</sup> “Commission Regulation (EU) No 720/2011 of amending Regulation (EC) No 272/2009 supplementing the common basic standards on civil aviation security as regards the phasing-in of the screening of liquids, aerosols and gels at EU airports”, *Official Journal of the European Union*, L 193, 23 July 2011, <https://www.iaa.ie/media/720-20111.pdf>; “Commission fails to refer measures on the introduction of body scanners to the European Data Protection Supervisor”, *Statewatch News Online*, October 2011, [www.statewatch.org/news/2011/oct/03edps-body-scanners.htm](http://www.statewatch.org/news/2011/oct/03edps-body-scanners.htm).

<sup>56</sup> Становиште европског надзорника по овом питању је у целости доступно на: [www.statewatch.org/news/2011/oct/eu-edps-com-body-scanner-opinion.pdf](http://www.statewatch.org/news/2011/oct/eu-edps-com-body-scanner-opinion.pdf).

<sup>57</sup> “Annual Report 2012”, op. cit., pp. 50–52; “Proposal for a Regulation of the European Parliament and of the Council Establishing the European Border Surveillance System (EUROSUR)”, European Commission, COM(2011) 873 final, 12 December 2011, [http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/eurosur\\_final.pdf](http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/eurosur_final.pdf).

Упозорење се односи и на успостављање друге генерације Шенгенског информационог система (тзв. SIS II), будући да се предвиђају већа извршна овлашћења на плану управљања биометријским подацима у контексту преноса података и да ли он обухвата њихову измену и допуну.<sup>58</sup> Иницијатива Европске комисије „Паметне границе” за стварањем ефикаснијег система за контролу спољних граница Уније не нуди довољне доказе да ће стварно да уклони садашњи спор и непоуздан систем евиденције преласка границе, па се може рећи да не оправдава трошкове и већи продор у приватност грађана.<sup>59</sup> Систем може да се поправи осигурањем доследне употребе у земљама чланицама и учењем из добре праксе. У погледу законодавног предлога Европске комисије о оснивању Агенције за спровођење закона и обуку (односно за преображај Европола), европски надзорник је упозорио на потребу за чвршћом контролом, док је за предлог стратегије ЕУ за сајбер безбедност оценио да не сме да дозволи да повећање безбедности Интернета за корисника буде оправдање за неограничени надзор и анализу података о његовој личности. Предлог стратегије не предвиђа механизам за одговарајућу заштиту података о личности, посебно не на плану размене информација између надлежних националних безбедносних служби.<sup>60</sup> Европски надзорник је скренуо пажњу Европској комисији поводом предлога директиве о замрзавању и одузимању имовине стечене криминалом и иницијативе за оснивање Европског центра за високотехнолошки криминал (*European Cybercrime Centre – EC3*), у погледу ризика за податке о личности који могу да се појаве уколико се јасно не дефинишу односи Центра са Европолом и приватним сектором.

Објективну препреку делотворној контролној функцији европског надзорника чини технолошки напредак који омогућава пресретање телекомуникационог саобраћаја у једној земљи чланици Уније од стране друге

---

<sup>58</sup> “Proposal for a Council Regulation on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II) (recast)”, COM(2012) 81 final, European Commission, 30 April 2012, [www.statewatch.org/sem/doc/assets/files/commission/COM-2012-81.pdf](http://www.statewatch.org/sem/doc/assets/files/commission/COM-2012-81.pdf).

<sup>59</sup> Ibid., p. 49.

<sup>60</sup> “Annual Report 2013”, op. cit., pp. 47–48; “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace”, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European Commission, 7 February 2013, [http://eeas.europa.eu/policies/eu-cyber-security/cybsec\\_comm\\_en.pdf](http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf).

<sup>61</sup> Tony Bunyan, “Welcome to the new world of the interception of telecommunications”, *Statewatch News Online*, May 2011, [www.statewatch.org/news/2011/may/03eu-interception.htm](http://www.statewatch.org/news/2011/may/03eu-interception.htm), 11/05/2014.

земље чланице, а без претходног одобрења прве – односно ван установљеног оквира узајамне правне помоћи.<sup>61</sup> Поред тога, обавештајна служба једне државе чланице може уз одобрење друге чланице да пресреће телекомуникациони саобраћај у трећој земљи чланици ради праћења неке особе која је њен држављанин или се привремено налази на њеној територији, али без знања и одобрења те треће државе. Са становишта надзора заштите података о личности грађана Уније веома је ризична примена тзв. система даљинске контроле (*remote control system*) и претраге рачунара на даљину (*remote computer searches*). Код првог система, пресретање телекомуникационог саобраћаја одиграва се тако што једна земља чланица шаље захтев другој чланици за коришћењем њених сателитских уређаја да би даљински активирала пренос података о праћеној особи која се налази на територији треће земље чланице. На пример, Велика Британија може да пошаље захтев Италији да употреби њену земаљску сателитску станицу како би даљински пресретала телекомуникациони саобраћај праћене особе која се налази у Шпанији. Други систем, претрага рачунара на даљину, обухвата пресретање телекомуникационог саобраћаја успостављањем приступа хард диску рачунара праћене особе, али без техничке помоћи земље чланице на чијој територији та особа борави. Савет ЕУ заступа становиште да није неопходно подношење формалног захтева предвиђеног Конвенцијом о пружању узајамне правне помоћи од 2000. године у случајевима када једна земља чланица ЕУ пресреће телекомуникације у другој чланици.<sup>62</sup> Забринутост стручне јавности изазива одлука влада највећих земаља чланица Уније, изражена и у ставовима Савета ЕУ, да у блиској будућности покрену процес стварања нормативних предуслова на националном и наднационалном нивоу за лакше прекогранично пресретање телекомуникација помоћу даљинске претраге рачунара и других уређаја за електронско складиштење података.<sup>63</sup> Европска комисија је у склопу реформе наднационалних прописа о заштити података предвидела преиспитивање садржине важећих међународних уговора о размени података о личности које је Унија склопила првенствено са САД, док ће се у свеобухватни споразум о заштити података у оквиру трансатлантске сарадње полиције и правосуђа – а који се још увек

<sup>62</sup> “Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the Republic of Austria, the Republic of Slovenia and the Kingdom of Sweden for a Directive of the European Parliament and of the Council regarding the European Investigation Order in criminal matters: Follow-up document of the meeting on 28 September 2010”, Council of the European Union, 12 October 2010, [www.statewatch.org/news/2011/may/eu-council-eio-14641-10.pdf](http://www.statewatch.org/news/2011/may/eu-council-eio-14641-10.pdf).

<sup>63</sup> Tony Bunyan, “Welcome to the new world of the interception of telecommunications”, op. cit.



налази у фази преговора – допунити неопходним заштитним механизмом.<sup>64</sup> Ипак, у погледу надзора сарадње ЕУ и САД на размени података са обавештајним потенцијалом, као нпр. централизованих података о путницима у авионском саобраћају (*Computerised Reservation Systems – CRS*), реалан проблем је то што се скоро сви водећи сервери налазе на територији САД – укључујући и главни сервер ЕУ – чиме су подаци о унутаревропском саобраћају доступни америчкој обавештајној заједници и органима гоњења посредством Министарства за унутрашњу безбедност (*Department of Homeland Security*).<sup>65</sup> Важећим споразумима склопљеним између САД и ЕУ није обухваћен веома важан сегмент који се односи на то шта америчко Министарство за унутрашњу безбедност ради са подацима који су му доступни у оквиру CRS, нити је покривен стандардни авионски саобраћај. Премда су активности у оквиру CRS-а које се одвијају на територији Уније покривене комунитарним прописима, примена овлашћења Европске комисије у погледу контроле и спровођења истраге по притужби грађана заправо је у пракси слаба, због тога што је Генерални директорат за транспорт одговоран за CRS, а Генерални директорат за правду, слободу и безбедност за збирне податке о путницима и њиховом кретању у авионском саобраћају (*Passenger Name Record – PNR*).<sup>66</sup> Тиме је делотворност надзорне функције Комисије препуштена способности два њена сектора да остваре ваљану координацију. Европски надзорник за заштиту података о личности успео је да напорним радом у области људских права недовољно познатој широј јавности, израсте у независну институцију са експертским знањем и великим личним угледом његових челника. Попут европског омбудсмана, ова млада институција својом надзорном и консултативном функцијом подупире Европски парламент у контроли рада Комисије и Савета, који су током последњих неколико година постали главни иницијатори секуритизације комунитарних јавних политика и заговорници олакшавања продора обавештајних интрузивних техника у приватност грађана Уније. Иако број позитивно решених притужби у просеку

---

<sup>64</sup> “Myth-busting: What Commission proposals on data protection DO and DON’T mean”, [http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet\\_mythbusting\\_2012\\_en.pdf](http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_mythbusting_2012_en.pdf)

<sup>65</sup> “Protection of Personal Data in Transatlantic Security Cooperation SWIFT, PNR & Co: Which Way Forward?”, *op. cit.*, p. 2.

<sup>66</sup> PNR је својеврстан досије о путнику у авионском саобраћају који настаје прикупљањем података о личности приликом резервације карте и укрцавања на лет, а служи у комерцијалне сврхе авио превозника и да би се лако утврдио итинерер путника. PNR садржи и податке попут: путничке агенције која је продала карту, начина на који је извршено плаћање, броја седишта и карактеристике пртљага. PNR се похрањује у базама података авио превозника и аеродрома са којег је путник полетео.

расте од године до године, чини се да најконтроверзније одлуке са потенцијално највећим штетним последицама за грађане Уније – превасходно у Простору правде, безбедности и слободе и надзора преласка спољних граница ЕУ – већином остају ван домашаја контролних овлашћења европског надзорника. Ограничавајући чинилац у погледу даљег унапређења контролне улоге европског надзорника могла би да буде чињеница да скоро две трећине грађана ЕУ уопште не зна да постоје посебне јавне институције задужене да се старају о несметаном уживању права на заштиту приватности у делу који се односи на податке о личности.<sup>67</sup> Једино „меко” оруђе европског надзорника које може дати резултате – додуше на дужи рок, јесте изградња културе заштите података о личности код службеника и грађана Уније. Такође, ова институција може да помогне организацијама грађанског друштва да више учествују у раду релевантних наднационалних радних група и да им приближи техничке аспекте информационалних технологија, а националним парњацима да пружи детаљне смернице о доброј пракси.<sup>68</sup>

## V) ИЗВОРИ

- “Annual Report 2009”, European Data Protection Supervisor, 2010, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2009/AR2009\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2009/AR2009_EN.pdf).
- “Annual Report 2010”, European Data Protection Supervisor, 2011, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2010/AR2010\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2010/AR2010_EN.pdf).
- “Annual Report 2011”, European Data Protection Supervisor, 2012, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2011/AR2011\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2011/AR2011_EN.pdf).
- “Annual Report 2012”, European Data Protection Supervisor, 2013, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2012/AR2012\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2012/AR2012_EN.pdf).
- “Annual Report 2013”, European Data Protection Supervisor, 2014, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2013/AR2013\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2013/AR2013_EN.pdf).

<sup>67</sup> “Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union”, op. cit., p. 174.

<sup>68</sup> “Strategy 2013–2014: Towards Excellence in Data Protection”, European Data Protection Supervisor, 2012, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/13-01-22\\_Strategy\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/13-01-22_Strategy_EN.pdf), pp. 13–14.

- Avakov, Alexander V., *Plato's Dreams Realized: Surveillance and Citizens Rights from KGB to FBI*, Algora Publishing, New York, 2006.
- Baldwin, David A., "The concept of security", *Review of International Studies*, Vol. 23, 1997.
- Bigo, Didier et al., "Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law", *CEPS Papers in Liberty and Security in Europe*, No. 61, November 2013, Centre for European Policy Studies.
- Charrett, Catherine, "A Critical Application of Securitization Theory: Overcoming the Normative Dilemma of Writing Security", *ICIP Working Paper*, No. 7, December 2009, International Catalan Institute for Peace, [www20.gencat.cat/docs/icip/Continguts/Publicacions/WorkingPapers/Arxius/WP7\\_ANG.pdf](http://www20.gencat.cat/docs/icip/Continguts/Publicacions/WorkingPapers/Arxius/WP7_ANG.pdf).
- "Charter of Fundamental Rights of the European Union", *Official Journal of the European Communities*, 2010/C 83, 30 March 2010, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:EN:PDF>.
- "Commission Regulation (EU) No 720/2011 of amending Regulation (EC) No 272/2009 supplementing the common basic standards on civil aviation security as regards the phasing-in of the screening of liquids, aerosols and gels at EU airports", *Official Journal of the European Union*, L 193, 23 July 2011, <https://www.iaa.ie/media/720-20111.pdf>.
- "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European Commission, 7 February 2013, [http://eeas.europa.eu/policies/eu-cybersecurity/cybsec\\_comm\\_en.pdf](http://eeas.europa.eu/policies/eu-cybersecurity/cybsec_comm_en.pdf).
- Črnčec, Damir, "A New Intelligence Paradigm and the European Union", *Varstvoslovje*, Vol. 11, No. 1, 2009.
- Donnelly, Jack, "Human Rights", in: John Z. Dryzek, Bonnie Honig, and Anne Philips (eds), *Oxford Handbook of Political Theory*, Oxford University Press, Oxford, 2006.
- Ehrenhauser, Martin, "EU Intelligence Service without Democratic Control", [www.ehrenhauser.at/archiv/lang/en/issues/secret-service/](http://www.ehrenhauser.at/archiv/lang/en/issues/secret-service/), 03/04/2014.
- Eriksson, Johan, and Giacomello, Giampiero, "Soft n' Wide, but Intelligent?: Reflections on Intelligence Analysis for the European Union", paper presented at the ECPR's 4th General Conference, Pisa, 6–8 September 2007, [www.researchgate.net/profile/Giampiero\\_Giacomello/publication/228379369\\_Soft\\_n%27Wide\\_but\\_Intelligent\\_Reflections\\_on\\_Intelligence\\_Analysis\\_for\\_the\\_European\\_Union/file/79e415137267e0a97c.pdf?origin=publication\\_detail](http://www.researchgate.net/profile/Giampiero_Giacomello/publication/228379369_Soft_n%27Wide_but_Intelligent_Reflections_on_Intelligence_Analysis_for_the_European_Union/file/79e415137267e0a97c.pdf?origin=publication_detail).
- "First report on the implementation of the Data Protection Directive (95/46/EC)", European Commission, 2003, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0265&from=en>.

- Hayes, Ben, “Spying in a see through world: the “Open Source” intelligence industry”, *Statewatch Journal*, vol. 20, no. 1, [www.statewatch.org/subscriber/protected/sw20n1.pdf](http://www.statewatch.org/subscriber/protected/sw20n1.pdf).
- Herman, Michael, “Ethics and Intelligence After September 2001”, in: Len V. Scott and Peter D. Jackson (eds), *Understanding Intelligence in the Twenty-First Century: Journeys in Shadows*, Routledge, London and New York, 2004.
- “Human Development Report 1994”, UNDP, 1994, [http://hdr.undp.org/en/media/hdr\\_1994\\_en.pdf](http://hdr.undp.org/en/media/hdr_1994_en.pdf).
- Hustinx, Peter, “A Clear Signal for Stronger EU Data Protection”, *Zeitschrift für Datenschutz*, nr. 2013/7, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-06-17\\_Editorial\\_ZfD\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-06-17_Editorial_ZfD_EN.pdf).
- “Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the Republic of Austria, the Republic of Slovenia and the Kingdom of Sweden for a Directive of the European Parliament and of the Council regarding the European Investigation Order in criminal matters: Follow-up document of the meeting on 28 September 2010”, Council of the European Union, 12 October 2010, [www.statewatch.org/news/2011/may/eu-council-eio-14641-10.pdf](http://www.statewatch.org/news/2011/may/eu-council-eio-14641-10.pdf).
- “Inspection Guidelines”, European Data Protection Supervisor, November 2013, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2013/13-11-04\\_EDPS\\_Inspection\\_guidelines\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2013/13-11-04_EDPS_Inspection_guidelines_EN.pdf).
- “Inspections conducted by the EDPS: Policy paper”, European Data Protection Supervisor, November 2013, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2013/13-11-04\\_EDPS\\_Inspection\\_Policy\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2013/13-11-04_EDPS_Inspection_Policy_EN.pdf).
- “Inventory 2014: A strategic approach to legislative consultation”, European Data Protection Supervisor, 18 December 2013, Brussels, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Priorities/13-12-8\\_Inventory\\_Note\\_Priorities\\_2014\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Priorities/13-12-8_Inventory_Note_Priorities_2014_EN.pdf).
- Кораћ, Срђан, „Европски омбудсман као механизам контроле рада наднационалних институција Европске уније”, *Европско законодавство*, Год. XII, бр. 45–46, 2013.
- Krause, Keith, and Williams, Michael C., “Broadening the Agenda of Security Studies: Politics and Methods”, *Mershon International Studies Review*, Vol. 40, No. 2, October 1996.
- LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, 24 September 2013, European Parliament, [www.europarl.europa.eu/ep-live/en/committees/video?event=20130924-0900-COMMITTEE-LIBE,02/04/2014](http://www.europarl.europa.eu/ep-live/en/committees/video?event=20130924-0900-COMMITTEE-LIBE,02/04/2014).
- McDonald, Andrew, “Data Protection”, in: Mark Bevir (ed.), *Encyclopedia of Governance*, First Volume, SAGE Publications, Thousand Oaks (CA), 2007.
- “Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001”, European Data Protection Supervisor, November 2005,

[https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PositionP/05-11-28\\_DPO\\_paper\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PositionP/05-11-28_DPO_paper_EN.pdf).

- “Proposal for a Council Regulation on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II) (recast)”, COM(2012) 81 final, European Commission, 30 April 2012, [www.statewatch.org/semDOC/assets/files/commission/COM-2012-81.pdf](http://www.statewatch.org/semDOC/assets/files/commission/COM-2012-81.pdf).
- “Proposal for a Regulation of the European Parliament and of the Council Establishing the European Border Surveillance System (EUROSUR)”, European Commission, COM(2011) 873 final, 12 December 2011, [http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/eurosur\\_final.pdf](http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/eurosur_final.pdf).
- “Protection of Personal Data in Transatlantic Security Cooperation SWIFT, PNR & Co: Which Way Forward?”, Public Hearing, 8 April 2010, Statewatch, [www.statewatch.org/news/2010/apr/eu-usa-pnr-hearing-8-april-10-briefing.pdf](http://www.statewatch.org/news/2010/apr/eu-usa-pnr-hearing-8-april-10-briefing.pdf).
- “Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data”, Section 5 (Articles 13–19), *Official Journal of the European Communities*, L8, 12 January 2001, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF>.
- “Report on a comprehensive approach on personal data protection in the European Union”, Committee on Civil Liberties, Justice and Home Affairs, European Parliament, 22 June 2011, [www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2011-0244+0+DOC+PDF+V0//EN](http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2011-0244+0+DOC+PDF+V0//EN).
- Ружић, Невена, „Надзор над видео надзором”, *Ревуја за безбедност*, Год. V, бр. 4, 2011.
- “Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union”, 2011, [http://ec.europa.eu/public\\_opinion/archives/ebs/ebs\\_359\\_en.pdf](http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf).
- “Strategy 2013–2014: Towards Excellence in Data Protection”, European Data Protection Supervisor, 2012, [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/13-01-22\\_Strategy\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/13-01-22_Strategy_EN.pdf).
- “The EU Internal Security Strategy in Action: Five steps towards a more secure Europe”, COM(2010) 673 final, Communication from the Commission to the European Parliament and the Council, 22 November 2010, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF#page=2>.
- “Why do we need an EU data protection reform?”, [http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf).
- Wolfers, Arnold, “‘National Security’ as an Ambiguous Symbol”, *Political Science Quarterly*, Vol. 67, December 1952.

## VI) ЗНАЧАЈ ЗА РЕПУБЛИКУ СРБИЈУ

Средства „меке моћи” којима располаже европски надзорник за заштиту података о личности у виду консултативне улоге којом подстиче националне власти да унапређују старање о праву на приватност, значајна је превасходно за транзиционе земље попут Србије. Наша земља је одобравањем статуса кандидата за чланство у ЕУ ушла у фазу са интензивнијом уградњом и већим инсистирањем на доследној примени комунитарних прописа и стандарда. Судаћи према досадашњим скромним донетима транзиционе реформе на плану делотворне заштите људских и грађанских права, велика је вероватноћа да ће осигурање ваљане заштите података о личности напредовати веома спорим кораком. Основни разлог је тај што се право на заштиту података о личности налази у групи људских права која нису у довољној мери препозната у Србији – како међу грађанима, тако и унутар политичке елите. Известан напредак је забележен током прошле године, када су грађани Србије право на заштиту података о личности користили у далеко већој мери него претходних година. О томе сведочи повећање броја предмета које је разматрао повереник за информације и заштиту података о личности за 55 одсто у 2013. у односу на 2012. годину, док је у истом периоду издато скоро шест пута више упозорења.<sup>69</sup> Због тога је добра вест да је републички повереник за информације од јавног значаја и заштиту података о личности добио прошле године статус посматрача у раније помињаној Радној групи за члан 29. Реч је о радном телу Уније у оквиру којег европски надзорник за заштиту података у значајној мери остварује саветодавне надлежности, па је за очекивати да ће редовно учешће нашег представника у размени мишљења и добре праксе додатно појаснити тумачење појединих сложених аспеката проблематике података о личности.

Успостављање сарадње са европским надзорником утолико би могло да помогне поверенику у преношењу експертизе из развијених земаља и са наднационалног нивоа, што би – у споју са сарадњом са домаћим организацијама грађанског друштва, могло да поспеши вршење притиска на актуелну власт да у овом мандату изради и усвоји неопходан правни оквир у области електронских комуникација и обраде личних података.

<sup>69</sup> „Извештај о спровођењу закона о слободном приступу информацијама од јавног значаја и закона о заштити података о личности за 2013. годину”, Повереник за информације од јавног значаја и заштиту података о личности Републике Србије, март 2014, [www.poverenik.org.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2013/gizvestaj2013lat.pdf](http://www.poverenik.org.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2013/gizvestaj2013lat.pdf), стр. 39.

Ипак, мало је вероватно да ће европски надзорник чак и снажним залагањем код Европске комисије успети да утиче на актуелну владу да после три године закашњења донесе Акциони план за спровођење Стратегије заштите података о личности, а после пет година доцње уредбу о заштити нарочито осетљивих података. Остаје да се види и да ли ће влада покренути питање одговорности носилаца правосудних функција који скоро да уопште не поступају по кривичним пријавама за повреду права на податке о личности, како би коначно створила претпоставке за делотворну судску заштиту.