САНУ
СРПСКА АКАДЕМИЈА
НАУКА И УМЕТНОСТИ

Приватност у дигиталном добу:
илузија или национални изазов

5. октобар 2017.

Математички институт
Српске академије
наука и уметности

Privacy in the Digital Age:
Illusion or a National Challenge

October 5, 2017

ПРИВАТНОСТ У ДИГИТАЛНОМ ДОБУ: ИЛУЗИЈА ИЛИ НАЦИОНАЛНИ ИЗАЗОВ

Privacy in the Digital Age: Illusion or a National Challenge

ПРОГРАМ И САЖЕЦИ ИЗЛАГАЊА

Организатори:
Српска академија наука и уметности и Математички институт САНУ

5. октобар 2017. године од 10:00 до 16:00
Свечана сала САНУ, Кнез Михаилова 35/II

ПРИВАТНОСТ У ДИГИТАЛНОМ ДОБУ: ИЛУЗИЈА ИЛИ НАЦИОНАЛНИ ИЗАЗОВ

Privacy in the Digital Age: Illusion or a National Challenge

ПРОГРАМ И САЖЕЦИ ИЗЛАГАЊА

Организатори:
Српска академија наука и уметности и Математички институт САНУ

5. октобар 2017. године од 10:00 до 16:00
Свечана сала САНУ, Кнез Михаилова 35/II

ОРГАНИЗАЦИОНИ ОДБОР:

академик Зоран Петровић,
Институт за физику у Београду,
Секретар одељења техничких наука САНУ (копредседавајући)

др Миодраг Михаљевић,
заменик директора Математичког института САНУ (копредседавајући)

академик Небојша Радуновић,
Медицински факултет Универзитета у Београду,
Одељење медицинских наука САНУ

проф. Милан Божић,
Математички факултет Универзитета у Београду,
председник надзорног одбора ТЕЛЕКОМА СРБИЈА

др Зоран Огњановић,
директор Математичког института САНУ

САЖЕТАК О СКУПУ

Безбедност, поверење и приватност су опште препознати као кључни атрибути који омогућују да све добробити које доноси дигитални простор не постану и отворена врата за злонамерне активности које могу да доведу до катастрофалних последица. Приватност све више постаје један од доминантних захтева а време за систематску бригу о заштити приватности у дигиталном домену већ је наступило, те уколико се решавању проблема не приступи данас, већ сутра би могли да се суочимо са изузетно озбиљним последицама.

Основни циљеви скупа укључују поруке упућене најширој јавности о:

- проблемима приватности у сајбер простору и националној димензији овог проблема који дотиче све грађане зато што је приватност препозната као једно од основних људских права, а заштита приватности (и информациона безбедност) императив у дигиталном домену;
- могућим правцима стратегије наше земље у очувању како приватности појединаца, тако и чувању државних и националних интереса у условима где се деловање у сајбер простору јавља као присутни и значајни фактор реализације државних политика;
- нашим капацитетима да нудимо решења на националном нивоу и учествујемо у решавању проблема на међународном нивоу.

Скуп треба да допринесе и следећем:

- процесу решавања проблема приватности у дигиталном простору зарад добробити грађана Србије;
- стимулисању научне заједнице Србије да решава проблеме који су истовремено:
  (1) унутар светских академских приоритета,
  (2) помажу решавању проблема свакодневног живота и
  (3) имају потенцијал за развој пословних активности у националним и међународним оквирима.

Приватност јесте право и потреба сваког појединца, али појединац сам не може адекватно да заштити своју приватност зато што су простори угрожавања приватности и у различитим инфраструктурним системима у дигиталном (сајбер) простору (телекомуникациони, здравствено--медицински, системи државних органа или пословни системи), који су ван директне контроле појединца а могу бити исходиште за угрожавање грађана. Зато је један од задатака државе да даје оквир за остваривање приватности својих грађана кроз стварање и подршку институцијама које треба да доприносе заштити приватности у сајбер простору.

ПРОГРАМ

10:00–11:15 **Уводна сесија**

- **Уводна реч** – академик Зоран Петровић, секретар Одељења техничких наука
- **Отварање скупа** – академик Зоран Поповић, потпредседник САНУ
- **Најављена подршка скупу и кратка обраћања**:

  Татјана Матић, државни секретар, у име Расима Љајића, потпредседника Владе и министра трговине, туризма и телекомуникација

  Златибор Лончар, министар здравља

  Владан Вукосављевић, министар културе и информисања

  проф. Виктор Недовић, помоћник министра, у име Младена Шарчевића, министра просвете, науке и технолошког развоја

  проф. Милан Божић, председник Надзорног одбора Телекома Србија

  Предраг Ћулибрк, генерални директор Телекома Србија

  академик Небојша Радуновић, Медицински факултет Универзитета у Београду

  др Зоран Огњановић, директор Математичког института САНУ
- **Циљеви и садржај скупа**, др Миодраг Михаљевић, Математички институт САНУ

11:15–11:30 Пауза

11:30–12:30 **Историјска основа и математичко-технолошки приступ приватности**

Приватност као историјска категорија, проф. Смиља Марјановић-Душанић, Филозофски факултет Универзитета у Београду

Приказ остварења Математичког института САНУ у домену дигиталне приватности/безбедности и илустративни примери, др Миодраг Михаљевић, Математички институт САНУ

Математички методи и заштита приватности, проф. Силвиа Гхилезан, др Зоран Огњановић и Милан Тодоровић, Математички институт САНУ

12:30–12:45 Пауза

12:45–14:15 **Приватност и инфраструктурни системи у Србији**

Приватност података из угла Телекома Србија, Милан Симић, извршни директор Телекома Србија

Проблеми приватности у здравствено-медицинским системима, проф. Андрија Богдановић, Клинички центар Србије и Медицински факултет Универзитета у Београду

Проблеми приватности у напредним електро-енергетским системима, проф. Слободан Вукосавић, Електротехнички факултет Универзитета у Београду, дописни члан САНУ

Изазови заштите приватности: Искуства МУП-а Републике Србије у борби против високотехнолошког криминала, Саша Живановић, начелник Одељења за борбу против високотехнолошког криминала МУП-а Републике Србије

Капацитет Републике Србије да гарантује приватност грађана у дигиталном добу, др Ђорђе Кривокапић, Факултет организационих наука Универзитета у Београду

14:15–16:00 **Закључне напомене и дискусиони коктел**

Предлог и образложење закључака скупа, др Миодраг Михаљевић, Математички институт САНУ

- **Дискусиони коктел у Клубу САНУ**

САЖЕЦИ ИЗЛАГАЊА

Приватност као историјска категорија

Privacy as a Historical Category

Проучавање приватности као историјске категорије ослања се на научну традицију која у средиште прошлости ставља појединца – „малог човека". Упоредо са развојем оваквих историографских интересовања, пратимо континуирано теоријско трагање за успостављањем адекватних аналитичких категорија као неопходних инструмената за приступање проблему. То је посебно сложен задатак с обзиром на чињеницу да се данас, на овом пољу, умногоме сусрећемо са парадоксалном ситуацијом. С једне стране, придаје се све већи значај бризи о заштити права на приватност грађана, а са друге, деловање друштвених мрежа показује да се истовремено са појачаном бригом о заштити информација приватног карактера, јавно показује спремност модерног човека, непознатог до нашег доба, да открива и са неограниченим бројем људи дели појединости које се односе на његов лични живот. Феномен приватности неопходно је дакле сагледати на концептуалној равни. Теоријски оквири истраживања приватности постављени у досадашњим проучавањима теме подразумевају сложен методолошки приступ, омеђен појмовима приватног и јавног. Независно од исправности методске сумње у сврсисходност супротстављања двеју сфера, у свести данашњег човека ови појмови доживљавају се као међусобно супротстављени. Посматрани као историјске категорије, они мењају свој садржај зависно од епохе, простора и друштвеног статуса људи које посматрамо.

На плану развоја идеје приватности, промене до којих је у Европи дошло током 18. века успоставиле су могућност јавног деловања појединца и уобличење новог концепта „појединачне" приватности – индивидуалног и колективног приватног идентитета, суштински различитог у односу на преовлађујуће античке, средњовековне, па и ренесансне моделе. Дијахроно посматрано, историја појма приватног живота у основи се

подудара са историјом демократизације која указује на дуг пут који је прешло схватање приватности: од негативног значења које је *res privata* носило у старим епохама, утемељеног у доживљају појединца као бића које се у пуној мери остварује тек у политичком деловању, на агори или у јавној улози грађанина, приватно већ од 18. века постаје синоним за срећу, добијајући породични и просторни смисао.

Модерно схватање приватности пресудно је везано за појаву индивидуалности. У том смислу оно је блиско повезано са процесима модернизације европског друштва које је најавила филозофија раног просветитељства. На теоријском плану, ови се процеси препознају као скуп промена које постепено настају у индустријским друштвима, а огледају се у порасту значаја капитала, у уобличавању националног идентитета, у увођењу редовног школовања, у секуларизацији етичких норми и порасту значаја грађанина као појединца у друштву. Посматрање историјско-социолошког оквира феномена приватности обележено је свешћу о наглим и коренитим променама које је савремено доба унело у ову сферу живота, посебно у време двадесетих и шездесетих година 20. века. Појам приватног живота постепено се изједначава са правом на лични живот појединца, по правилу освојеним у процесима еманципације од породичног окружења. Данас тешко можемо говорити о јединственом концепту приватности, јер су укинути неки од традиционалних образаца на којима је почивало схватање индивидуе и њеног односа према себи, породици и друштву у целини. Са отварањем нових поља комуникације у дигитално доба, истовремено је прихваћен и измењен доживљај права на лични живот и на различите изборе – од освојених радних и демократских слобода и права грађанина, до права на избор сопственог пола, сексуалне оријентације и слободе вероисповести. Међутим, промене у схватању приватности нису само резултат општих трендова одређене епохе, већ остају суштински зависне и од спорих токова карактеристичних за процесе дугог трајања, укорењених у социјалном и културном кругу којима појединац припада.

СМИЉА МАРЈАНОВИЋ-ДУШАНИЋ

Рођена у Београду 1963. године, где је завршила школовање и дипломирала 1986. године на Одељењу за историју Филозофског факултета у Београду. На катедри за средњовековну историју се запослила као асистент 1987. године, где је магистирала, докторирала (1996. године) и прошла сва звања до избора у редовног професора 2007. године. Редовни је професор Филозофског факултета у Београду; шеф катедре за Општу историју средњег века и помоћне историјске науке.Уредник је неколико књига: Приватни живот у српским земљама средњег века (са Даницом Поповић), Београд 2004; *Remanier, métaphraser: fonctions et techniques de la réécriture dans le monde byzantin* (avec B. Flusin), Belgrade 2011; *Proceedings of the 23rd International Congress of Byzantine Studies*, Belgrade 2016. Аутор већег броја научних студија и књига: Владарске инсигније и државна симболика у Србији од 13. до 15. века, Београд 1994; Владарска идеологија Немањића, Београд 1997; Свети краљ, Београд 2007. *Daily Life in Medieval Serbia* (with M. Popović and D. Popović), Belgrade 2016; Свето *и* пропадљиво. Тело *у* српској хагиографској књижевности, Београд 2017; *L'écriture et la sainteté dans la Serbie médiévale.* Étude *d'hagiographie*, Paris 2017 (у штампи). Предавала на више универзитета и високих школа као гост-професор/директор студија: École Nationale des Chartes (2009); École Pratique des Hautes Etudes (2012); Université de Paris 1 Sorbonne, (2014); Université Paris 4 Sorbonne (2015). Уредник је историјске библиотеке „Полис" у издавачком предузећу Клио из Београда (од 1997. године). Члан је асоцијација: *Chercheur associé de Labex RESMED (Religion et société dans le monde Méditerranéen)*; *Comité International des Sciences Historiques: Commission Internationale de Diplomatique (membre de commission)*; *Centre de recherche d'histoire et civilisation de Byzance (membre associé):UMR 8167 Orient-Méditerranée (Laboratoire)*; *UFR 09 – Histoire: Institut de Recherches sur Byzance, l'Islam et la Méditerranée au Moyen Âge (IRBIMMA) – (membre associé)*.

Приказ остварења Математичког института САНУ у домену дигиталне приватности/безбедности и илустративни примери

An Overview of the Achievements at Mathematical Institute of SASA Relevant for Cyber Security/Privacy and Illustrative Examples

Математички институт САНУ (МИ САНУ) има више од 20 година дугу традицију основних истраживања и реализације техничких решења из области релевантних за приватност и безбедност у данашњем дигиталном (сајбер) простору. У последњој декади прошлог века МИ САНУ је препознао значај и изузетност долазећег интереса за криптологију и информациону безбедност, и данас је међународно препознат као водећа академска национална и регионална институција у области. Посебна пажња је посвећена криптологији, научној дисциплини која даје основне технике за изградњу механизама информационе безбедности неопходних за остваривање приватности и сигурности у дигиталном простору.

Ово излагање показује наше капацитетете да нудимо решења на националном нивоу и учествујемо у решавању проблема на међународном нивоу – даје се сумарни приказ остварених резултата унутар пројеката МИ САНУ и информативно приказују неки илустративни резултати.

Циљ овог излагања је да укаже на постојање суштински битних знања за остваривање приватности и безбедности у дигиталном простору и да покаже да и наша средина значајно доприноси овим знањима како би дилема "илузија" или „изазов" превагнула ка охрабрујућем: приватност у дигиталном добу не мора да буде илузија али јесте изазов.

Достигнућа у МИ САНУ у доменима од интереса за безбедност и приватност у сајбер простору остварена су у оквирима: (а) пројеката националних основних истраживања, интегрисаних интердисциплинарних истраживања и технолошког истраживања; (б) међународних истраживачких пројеката; (в) посебно уговорених истраживачко-развојних пројеката. У наведеним оквирима остварено је више стотина резултата уобличених у

више од 400 публикација и техничких решења у доменима криптологије и информационе безбедности укључујући и: (а) више од 100 радова у еминентним међународним часописима (*IEEE*, *IET*, *Springer*, *Elsevier*, и други реномирани издавачи) од којих је око 30% у IEEE часописима; (б) више од 10 поглавља у међународним монографијама; (в) више од 70 радова у зборницима еминентних годишњих међународних конференција (IEEE, IACR...) и више од 30 предавања по позиву; (г) више од 10 међународно признатих патената и техничких решења; (д) више од 30 национално признатих техничких решења за успостављање напредне дигиталне сигурности у инфраструктурним и специјализованим информационо-комуникационим системима (Телеком Србија, банке, државне институције...). Мера међународне препознатљивости и признатости наведених резултата је и више од 5000 цитата у међународним изворима (цитати у часописима, књигама и зборницима, патентним базама и докторским дисертацијама). Додатно признање значаја реултата постигнутих у МИ САНУ су учешћа по позиву у више од 10 међународних пројеката (пројекти ЕУ, Јапана, САД, Сингапура, Индије) међу којима се по трајању и обиму заједничких реултата посебно истиче сарадња са Јапаном, а такође и више десетина предавања по позиву на еминентним универзитетима, институтима и научним скуповима.

Као илустрација остварених резултата, ово предавање указује на достигнућа МИ САНУ која истовремено обезбеђују и функционалну ефикасност и адекватну сигурност у одређеним сценаријима евалуације сигурности основних саставних компонената механизама за безбедност и приватност. Механизми заштите производе допунско оптерећење система и оно треба да буде минимизирано да се не би угрожавала основна функционалност. Са друге стране, истиче се да је суштински битан услов да би заштитни механизми имали жељену сигурност, да основне технике на којима се базирају буду доказиво сигурне у што ширем сценарију могућих напада. Сагласно наведеном, приказују се неки реултати из области дизајна/конструкција и евалуације криптографске сигурности техника заснованих на здруживању елемената традиционалне криптологије и теорије кодова за корекцију грешака ради остваривања доказиве сигурности и ниског допунског оптерећења система због примене механизама за потребе остваривања дигиталне приватности и сигурности. Приказује се приступ за ојачавање криптографске сигурности компактних алгоритама шифровања (енкрипције) ниске имплементационе сложености применом резултата о кодовима за канале са синхронизационим грешкама и елемената теорије информација.

МИОДРАГ МИХАЉЕВИЋ

Миодраг Ј. Михаљевић је докторирао 1990. године, за научног саветника изабран је 1999. године, а за гостујућег редовног професора на *The University of Tokyo* 2014. године. Ради у Математичком институту САНУ од 1998. године као руководилац пројеката, а од 2015. године и као заменик директора. Реализовао је више од 15 пројеката основних истраживања, технолошког развоја, посебно уговорених и међународних пројеката који су резултовали у више од 250 његових јавних и интерних/класификованих публикација. Објавио је више од 70 радова у часописима и међународним монографијама од чега више од 50 радова у часописима са респективним импакт фактором. Листа његових референци садржи и 6 међународно признатих патената, више од 60 радова штампаних у зборницима међународних конференција и више од 30 међународно или национално признатих техничких решења. Његови радови су цитирани више од 2500 пута у међународним публикацијама, а одржао је више од 20 предавања по позиву из истакнутих институција. Реализовао је интензивну међународну сарадњу са Јапаном, САД, ЕУ, Индијом и Сингапуром. М. Михаљевић је добитник Награде САНУ 2013. године за десетогодишња остварења у области криптологије и информационе безбедности, а 2014. године изабран је за члана *Academia Europaea* са седиштем у Лондону.

Математички методи и заштита приватности

Mathematical Methods and Privacy Protection

Ово је доба силовитог развоја информационих технологија са брзом појавом нових дисциплина и њиховом применом у свим сегментима живота и друштва. Приватност је један од најбитнијих проблема који се везују за информационе технологије. Појам приватности за свакога има различито значење. Током XX века, у коме је технолошки развој убрзао доступност и коришћење информација, неминовно је дошло до појаве нових појмова приватности. Тако постоје филозофски, правни, друштвени и технички аспекти појма приватности. У основи, приватност је способност и могућност контроле како приступа подацима, тако и коме се те информације преносе.

Доба у коме живимо се може назвати информацијско доба. Различите активности које су раније биле приватне данас остављају **дигитални траг**, на основу кога се о појединцу може сазнати о његовим интересовањима, особинама, веровањима, али и о личним подацима који могу бити број телефона, адресе становања, па чак и медицински подаци. Данас се свакодневно користе електронска пошта, различити сервиси порука (*SMS*, *Skype*, *Viber*, итд), друштвене мреже (*Facebook*, *Twitter*), различити претраживачи (*Google*, *Bing*) ради налажења одговора на свакодневна али и осетљива питања, као и електронске услуге (*Booking*, *Amazon*, *eBay*) ради куповине. Коришћење оваквих услуга доводи до свесног или несвесног стварања дигиталног трага код појединаца, комерцијалних ентитета али и државних институција.

Поред коришћења наведених услуга, данас је свеприсутна парадигма **Интернет ствари**. Замисао ове парадигме је коришћење великог броја сензора, најчешће помоћу бежичне мреже, како би се прикупљали различити подаци попут температуре, потрошње електричне енергије, али и различитих медицинских информација које се прикупљају од пацијe-

ната. Важност приватности медицинских података је јасна сама по себи, док често на први поглед, приватност података попут потрошње електричне енергије делује небитно. Међутим, лако се може замислити случај где је овај податак веома битан. Ако би се приватност тих података нарушила, на основу њих би се могло предвидети када су људи у објекту а када ван њега, што би могло да доведе до тога да се лакше планира пљачка објекта.

Рачунарство у облаку (*cloud*) је још једна свеприсутна парадигма, која представља рачунарску инфраструктуру која омогућава сталан приступ дељеном скупу ресурса (складиште, услуге, апликације) преко мреже, а најчешће преко интернета. Код рачунарства у облаку, подаци корисника које он обрађује (на пример *Google docs*) или само складишти (*Dropbox*), се налазе на неком удаљеном рачунару који најчешће није у власништву корисника. У оваквом сценарију је питање приватности још значајније, поготово што подаци о којима се ради могу бити веома осетљиви, јер остали корисници облака могу бити злонамерни и угрозити приватност података на њему. Међутим, нису само корисници ти који могу да угрозе приватност. Сами пружаоци услуга облака могу бити злонамерни, или макар радознали, па могу приступити подацима својих корисника.

Све наведене парадигме и активности имају једну заједничку особину, а то је да се подаци (дигитални траг или кориснички подаци) складиште на страни пружаоца услуга на трајан начин, тако да постају практично неизбрисиви. Када се узме у обзир и то да већ постоје развијене методе за обраду велике количине података, уз помоћ којих је могуће пронаћи различите осетљиве информације, јасно је да је проблем приватности актуелан и да ће то бити и у будућности.

Математички модели и формални методи су постали основни алати у рачунарству за равој поузданог софтвера и хардвера. Нове парадигме информационих технологија такође захтевају поузданост коју једино математички модели могу да обезбеде.

Основни правци примене математичких модела у заштити приватности су:

- рачунски модели за приватност засновани на рачунским моделима за дистрибуиране и конкурентне системе;
- формални методи за приватност, базирани на логичким основама, типским системима и верификацији;
- диференцијална приватност и вероватносни методи закључивања;
- криптографски методи за приватност;

- примена у друштвеним мрежама, базама података, медицинским подацима, мрежама података (*linked data*);
- отворени подаци (*open data*);
- правни аспекти приватности у информационим системима.

Сложеност проблематике захтева мултидисциплинарне тимове математичара, информатичара, правника, социолога и психолога. Неопходно је подстицати математичка и интердисциплинарна истраживања у Србији која су релевантна за заштиту приватности јер ће то бити један од највећих изазова савременог друштва.

СИЛВИА ГИЛЕЗАН

Проф. др Силвиа Гилезан је редовни професор Факултета техничких наука, Универзитета у Новом Саду и стални је сарадник Математичког института САНУ. У неколико наврата имала је гостујућу позицију на *École Normale Superieure de Lyon*, Француска; *Radboud University*, Холандија; *University of Torino*, Италија и *McGill University*, Канада. Предаје на сва три нивоа високог образовања у земљи и иностранству. Научни рад и експертиза проф. Гилезан је у разним областима математичке логике са применама у рачунарству, као што су теоријско рачунарство, теорија типова и интерактивни доказивачи, теорија конкурентних система и математичка лингвистика. Најновија истраживачка интересовања су усмерена ка формалним методама за заштиту приватности у великим системима. Својим професионалним ангажовањем развила је сталну међународну сарадњу са истакнутим истраживачким центрима на свим континентима. Руководилац је и координатор успешно реализованих националних и међународних научних и образовних пројеката (*FP*, *COST*, *Erasmus*, *Tempus*, билатералних). Посебну пажњу посвећује раду са младим истраживачима, као и одржавању сарадње са нашим истраживачима који живе и раде у иностранству. Успешно је председавала и организовала неколико међународних конференција, међу којима су *TLCA 2011*, *RTA 2011* и *TYPES 2016*. Члан је програм-

ских одбора престижних међународних конференција, рецензент за већи број међународних часописа и конференција, члан је докторских комисија у иностранству, уредник зборника и часописа и евалуатор међународних пројеката. Велики број иностраних и домаћих коаутора сведочи о међународној репутацији проф. Гилезан. Богати опус научних резултата проф. Гилезан је представљен у бројним радовима који су објављени у водећим међународним часописима и саопштени на престижним конференцијама у целом свету. Као гостујући предавач борави и предаје на универзитетима широм Европе, САД, Канаде, Кине и Јапана. Одликована је орденом *Chevalier de l'Order des Palmes Académiques* Републике Француске.

Приватност података из угла Телекома Србије
Data privacy from the perspective of Telekom Srbija

Информације покрећу савремени свет *(data holds value)*. Велике промене које са собом доноси дигитална трансформација довеле су до неравномерног развоја различитих аспеката управљања информацијама. С једне стране модерна култура подразумева да су информације доступне свима, с друге стране постоји потреба да информације буду адекватно заштићене. Ово за последицу има нејасан концепт приватности у дигиталном свету. Бројне су дилеме и отворена питања када је тема приватност у доба Интернета. Од тога, да ли приватност на Интернету уопште постоји, и да ли кажемо због приватности оног тренутка када негде на интернету оставимо своје податке? До тога, шта уопште значи приватност у време друштвених мрежа и Интернета?

Одговори на сва ова питања зависе од контекста у којем се приватност посматра и, наравно, од свести корисника и њихове перцепције приватности. Често се поставља питање да ли корисници уопште желе приватност и колико им је она битна? Корисници желе све: и врхунску услугу и приватност. Они истовремено хоће да деле своје садржаје што широј публици, али и да приступ буде ограничен и подаци заштићени. Иако су забринути за безбедност својих података и свесни колика је њихова вредност, корисници се не труде у довољној мери да заштите своје податке или бар њихово понашање то не показује.

Регулатори су последњих година учинили значајан напор да „уведу ред“ у област заштите приватности података. Свакако највећи утицај на глобалном нивоу има усвајање ЕУ директиве из 2016, тзв. GDPR која потврђује право свих на заштиту личних података. Принципи заштите приватности података су једноставни: подаци се морају прикупљати и обрађивати само на законит начин и у легитимне сврхе. Они који прикупљају/обрађују податке морају да их штите. Међутим, одговорност за заштиту података није само на операторима већ је заједничка и

подељена између државе (регулатора), корисника и компанија које обрађују личне податке. Права мера приватности лежи негде између законских/регулаторних захтева, очекивања корисника и могућности оператора.

Приватност података представља изазов за телекомуникационе компаније. Окружење у коме послују *telco* оператори је глобално, динамично и без јасних граница. Нови трендови *(Mobility*, *Social Networking*, *Cloud Computing*, *IoT…)* додатно „компликују" ситуацију уносећи нове ризике. *Cyber* ризици и ризици који угрожавају имиџ компаније постају све доминантнији. Дигитални свет брзо расте – све више информација се генерише, размењује и чува на разним уређајима, па све више приватних и осетљивих информација постаје лако доступно. Истовремено се одвија велика конвергенција технологија. Све ово уз константан притисак са тржишта тера телекомуникационе операторе да улазе на тржиште ICT сервиса и постају ICT компаније. С друге стране технолошки напредак не прати и напредак безбедносне свести корисника, па неминовно расту и ризици по безбедност информација.

Телекомуникационе компаније су посредници у свакој трансакцији и предуслов за сваку модерну комуникацију, па су сходно томе велика и очекивања од модерних телекомуникационих/ICT компанија. Задаци који се постављају пред њих су бројни и неретко супротстављени: заштитити податке и истовремено обезбедити врхунско корисничко искуство, задовољити очекивања корисника, испунити законске и регулаторне захтеве, изборити се на тржишту и бити изнад конкуренције. Константан је притисак да се нови сервиси испоруче у кратком року, док су системи све комплекснији са бројним интеграцијама и нејасним границама. Све ово за последицу има промену безбедносног модела. Граница *(perimeter)* заштите информације се померила и није више везана за објекте. Концепт физичких безбедносних зона, као начина за заштиту вредних информација, у доба паметних телефона, таблета, *cloud*-а, друштвених мрежа, IoT, итд. постаје, не само застарео већ и бесмислен. **Подаци и дигитални идентитет корисника дефинишу нове границе заштите (нови периметар). Садашње стање захтева тзв.** *Data centric* модел за заштиту информација који фокус ставља управо на информације и њихову вредност, стварајући предуслове за очување приватности информација.

Телеком Србија као и остале ICT компаније мора да одговори на ове изазове. Информације су имовина која има критичну вредност за

компанију и сходно томе треба да буду адекватно заштићене. Приступ у заштити информација мора бити системски, зато што безбедност информација није нешто што се једноставно купује са полице, већ нешто на чему се ради сваког дана. Прихваћени стандарди представљају најбоље путоказе у развоју IT безбедности и заштити приватности. Телеком Србија је имплементирао систем за управљање безбедношћу информација *(*ISMS*)*, како би заштитио информације које прикупља, обрађује, преноси и чува. ISMS је пројектован према захтевима које прописују опште-прихваћени међународни стандарди из ове области. IT/ICT услуге које пружа Телеком Србија су из 2012. године и сертификоване су да задовољавају захтеве стандарда ISO 27001.

Заштита информација и критичних ресурса у Телекому Србије обавља се кроз примену организационих и техничких мера. Примењене мере заштите информација следе најбољу светску праксу за ту област, али уважавају посебност окружења у ком су имплементиране. Иницијативе и будуће активности Телекома Србије у контексту заштите приватности података крећу се у више праваца:

- усклађеност са регулативом, стандардима и најбољом светском праксом из области приватности;
- побољшање управљања информацијама кроз систематски приступ заснован на управљању ризиком;
- додатно унапређење контроле и заштите приступа апликацијама како би се обезбедила приватност;
- дизајн и имплементација мера којима се обезбеђује адекватна заштита информација у целом њиховом животном циклусу, од њиховог креирања до уништења;
- набавка и имплементација система заштите на свим инфраструктурним нивоима како би се подаци корисника и њихова приватност заштитила од све већег броја и све напреднијих *cyber* претњи;
- унапређење свести запослених и корисника услуга Телекома Србије о приватности података и заштити информација;
- континуирано надгледање и унапређење безбедносног стања компаније кроз програме едукације и сертификације запослених, унапређење процеса и инвестиције у нове технологије.

Честа је погрешна перцепција корисника да су искључиво телекомуникационе компаније одговорне за заштиту приватности података,

иако у доста случајева оне уопште нису присутне на апликативном нивоу већ само обезбеђују инфраструктуру за функционисање сервиса. Подизање свести има кључну улогу у побољшању разумевања јавности о проблемима везаним за приватност података и релевантним мерама за ублажавање ризика по њих.

МИЛАН СИМИЋ

Рођен је у Београду 1977. Дипломирао је на Елетротехничком факултету Универзитета у Београду: Завршио је *MBA (Master of Business Administration)* студије на *University of Sheffield*. Професионално искуство стицао је у компанијама *UVTC Sweden*, *Timepiece Portugal* и *Agena* Београд на различитим позицијама везаним за OSS/BSS платформе. Као независни консултант учествовао у ИТ пројектима у више земаља Северне и Латинске Америке и ЕУ. Учествовао у имплементацији *OSS/BSS* платформи током пуштања у рад *m:tel CG*. Извршни је директор за ИТ подршку и ICT сервисе одговоран за планирање, развој и управљање ИТ инфраструктуром, платформама и ICT сервисима. Пре ове позиције био је директор Функције за ИТ као и Сектора за ИТ развој и интеграције у Телеком Србија а.д. Био је члан Надзорног одбора Телеком Српска а.д. Бања Лука до 2010. када је постављен за члана Ревизорског одбора ћерке компаније. Члан је управног одбора *mts Banke*. Ожењен, отац Зоје и Војина.

Пробеми приватности у здравствено-медицинским системима

Privacy issues in health information systems

Право на приватност у медицини је изузетно стара и врло важна тема у односу болесника и његовог лекара као и болесника и здравственог система. Током времена, многе дискусије и етичке дилеме, довеле су до јасних ставова да су за све податке који се односе на здравље, односно болест, потребне сагласности самог болесника или његовог старатеља (често у писаној форми). Такође, формирани су јасни принципи да се неки подаци о здрављу појединца могу достављати регистрима или користити за анализу (и публикацију) само ако не откривају идентитет самог болесника. Редовни клинички рад лекара и медицинског особља стога је усмерен на непосредну заштиту података о личности, његовој болести и приступу одговарајућим медицинским документима, а ради што боље заштите приватности. Увођење различитих обавезних или стручних регистара, обавеза пријављивања болести и специфичних болесника су и пре модерне технологије увек имале и питање заштите приватности болесника као и доступност односно отвореност приступа подацима о њиховој болести. Због тога су начела заштите приватности ушла у бројне међународне документе као и одговарајуће прописе широм света којих се медицинска струка универзално придржава.

Увођење електронских система у здравствене установе у Србији кроз одговарајуће програме за вођење медицинске документације (*ZIS*, *INFOMEDIS*, *HELIANT* и други) који су у првом тренутку били намењени олакшавању процеса документовања у раду са болесницима, а касније су проширени кроз интеракцију са системима за фактурисање, евиденцију о лековима, формирање терапијских листа и друго, отворило је и нека нова питања везана за приватност и заштиту података о самим болесницима. Нехотично или намерно нарушавање приватности унутар ових система омогућава да се много лакше добију подаци о великом броју људи, како болесника тако и запослених у здравственом систему, чиме се отварају

и питања озбиљних злоупотреба (од "сензационалних вести" до крађе идентитета). Постојећи здравствени информациони системи су у оквиру своје заштите увели многе модерне мере заштите, почев од стандардне комбинације корисничких имена и лозинки, преко приступа кроз VPN конекције и токен енкрипције, до приступа преко дефинисаних IP адреса рачунара у заштићеним, одвојеним болничким мрежама и доменима унутар дефинисаних јединица здравствених установа, уз развој мера непосредне физичке и криптографске заштите приступа серверима система. Ови електронски системи су значајно унапредили вођење неопходне медицинске документације како за лежеће тако и за амбулантне болеснике и омогућили једноставније генерисање бројних података и извештаја почев од медицинских извештаја и отпусних листа до фактура, лагер листа, требовања лекова, резулата бројних испитивања унутар болница. Са друге стране, потреба идентификације болесника унутар тих система је остала отворено место за нарушавање приватности имајући у виду да се у наведеним извештајима често наводе подаци као што су датум рођења, адреса, ЈМБГ, ЛБО итд.

Неопходност формирања већег степена интеграције, могућност међусобне размене података између ових болничких система као и формирање система електронских упута, увело је у здравствени систем и интегрисани здравствени информатички систем, ИЗИС, који се налази у "облаку" Телекома Србија. Електронска комуникација корисника са свим овим системима се реализује кроз уобичајене енкриптоване интернет комуникације (најчешће 128-битни кључеви), са тиме да је приступ корисника преко уобичајених форми имена и лозинке (не дужим од 64 бита). Ту се јављају проблеми заштите укупних ресурса од директних упада и претраживања доступних података јер и даље је "човек" најслабија карика (име и лозинка се поједностављују, уносе у мобилне телефоне или записују на папир...) чиме се омогућава неовлашћен приступ уколико то неко заиста жели да искористи. За разлику од болничких система који су затворени и везани радом са одговарајућим ресурсима установа, овакав систем као што је ИЗИС доступан је преко генералних интернет конекција и свих различитих уређаја (рачунари, таблети, телефони...) чиме се намећу додатни пробеми приступа и заштите корисника приликом приступа. Поред тога, поставља се и питање "власништва" над самим програмима, над приступима кроз "задње улазе", контроле ресурса који се користе за "облак", јер је недавно преношење права приступа другим компанијама (*outsourcing*) довело до великог скандала у Шведској.

У земљама са већим искуством, најчешће се приступ корисницима преко "отворених" интернет веза омогућава уз коришћење додатних мера сигурности као што су RDF картице, USB или слични токен уређаји који омогућавају двоструку ауторизацију корисника. Поред тога, наведени уређаји често садрже и закључане сертификате неопходне за ауторизацију електронског потписа чиме се верификују документи које су саставили и одобрили корисници.

Посебан изазов за здравствене информатичке системе код нас, биће увођење "електронског картона болесника" који ће бити везан за здравствену картицу. Овај "картон" би требало да обухвати податке о претходним и актуелним обољењима, њиховој терапији, као и податке о томе где се могу добити детаљније информације о тим болестима (рецимо линкови ка архивираним медицинским документима). Оворено је питање, да ли такав картон треба да се нађе на здравственој картици (чип) или ће се наћи у неком "облаку" или на неком специјализованом серверу нпр. Министарства здравља. Поред тога, увођење и проширивање здравственог система приватним установама и приватним комерцијалним осигурањима у будућности, отвориће и питање како ће онда подаци из оваквог картона бити доступни, ко ће издавати картице (једнообразни систем идентификације осигурања) и како ће се дефинисати ко, како и када има приступ тим подацима?

У овом тренутку, можемо да кажемо да увођење нових технологија, као и развој "безпапирне" е-документације, представља значајан напредак у модернизацији нашег здравственог система. Тренутне могућности су више ограничене ресурсима него идејама, али ће ови системи све више улазити у наше здравствене установе и у редовни рад. Стога, заштита приватности болесника, њихових медицинских података, намеће потребу да здравствени радници буду не само обучени корисници, већ и да активно учествују у развоју информатичких решења. Такође, развој ових система треба да омогући и несметан приступ неперсонализованим подацима који могу бити од значаја за анализе терапијске ефикасности самог медицинског система или да дају друге одговарајуће податке о том систему, почев од потрошње лекова или других ресурса до формирања детаљних извештаја за надлежне органе у електронском облику. Боља идентификација корисника, увођење рецимо USB токена са додатним сертификатима уз већ постојеће име и лозинку, примена електронског потписа на документима, идентификација болесника у здравственом систему не преко матичног броја већ преко здравственог

броја идентификације (ЛБО или сличан), у великој мери ће омогућити боље искоришћење постојећих ресурса и допринети већој сигурности болесника у реалном свету информација.

Захваљујем се др Драгани Грбић на корисним сугестијама и значајним коментарима у вези са медицинским електронским системима, као и инжињеру Душану Ерићу на подршци у схватању широке функционалности доступних програма.

АНДРИЈА БОГДАНОВИЋ

Андрија Богдановић је ванредни професор интерне медицине и хематологије на Медицинском факултету у Београду. Стално је запослен на Клиници за хематологију Клиничког центра Србије, који је наставна база Факултета и највећа референтна установа у земљи, а и шире, за испитивање и лечење болести крви. Као шеф одсека за високоспецијализовану хематолошку дијагностику, непосредно је задужен за комплетну дијагностику хематолошких обољења а на првом месту малигних болести крви. Његове области стручног и научног интересовања обухватају хематолошку лабораторијску дијагностику и молекуларне поремећаје у малигним болестима крви. Посебно се бави хроничним болестима костне сржи као што су хронична мијелоидна леукемија, мијелопролиферативне неоплазме и мијелодиспластични синдром. Као експерт из области хроничне мијелоидне леукемије члан је саветодавног тела међународне CML фондације (ICMLF), непрофитне организације која има циљ да се бори против ове болести у свету; члан је радне групе за хроничну мијелоидну леукемију Европске Мреже за леукемије (ELN). Као наставник Медицинског факултета у Београду активно учествује у свим облицима додипломске и последипломске наставе из области интерне медицине и хематологије, као и у настави на енглеском језику на Медицинском факултету. Члан је координационог тела за енглеску наставу факултета. Аутор је 75 радова из области клиничке и лабораторијске хематологије и молекуларне медицине у вези са болестима крви.

Проблеми приватности у напредним електроенергетским системима

Safety Considerations for Smart Grid

Савремени електроенергетски системи се све више ослањају на дистрибуирану производњу електричне енергије, где се користе извори релативно мале снаге, повезани на мрежу преко даљински управљивих уређаја енергетске електронике. Поред тога, све већи број потрошача је повезан на мрежу преко уређаја енергетске електронике који мрежни напон прилагођава потребама потрошача, и који се могу даљински контролисати. Нестална природа електрана на ветар и соларних електрана ствара проблеме у уједначавању производње и потрошње електричне енергије. Зато је потребно користити системе за акумулацију електричне енергије, способне да преузму вишкове и да их пласирају у интервалима када потрошња премаши производњу, као и такозвану виртуелну акумулацију у виду V2G система или другачијег. Ефикасан рад система са контролисаним изворима, потрошачима и акумулацијом тражи увођење информационих технологија да би се омогућиле напредне енергетске трансакције, брзо и флексибилно уговарање и аутоматизована трговина енергијом. Применом информационих технологија остварује се корист произвођачу и потрошачу, али и самом електроенергетском систему чије се перформансе значајно побољшавају. Ослањање на информационе технологије отвара значајне могућности, али представља и безбедносни ризик. Злонамерни хакерски напади могу проузроковати огромне штете, тако да је потребно предвидети примерене мере заштите. Наведена област још увек није консолидована, тако да постоји простор за пласман решења створених у Србији.

СЛОБОДАН Н. ВУКОСАВИЋ

Слободан Н. Вукосавић је рођен 27. јануара 1962. године. Дипломирао је 1985, магистрирао 1987, а докторирао 1989. године на Електротехничком факултету Универзитета у Београду. Прво запослење налази у Институту «Никола Тесла». У истраживачком центру компаније *Emerson-Electric* у Сент Луису развија **оригинална решења релуктантних мотора и 1988. патентира** решења за електронско управљање синхроним моторима. Од 1991. године учествује у формирању истраживачког центра компаније *Vickers* за развој управљачких система индустријских робота и преузима руковођење истраживачким тимом. Од 2000. године сарађује са компанијом MOOG и развија алгоритме и уређаје за управљање производним ћелијама у аутомобилској индустрији. У настави на Електротехничком факултету Универзитета у Београду сарађује од 1993. године. У звање редовног професора изабран је 2003. године. Сарађивао је са *North-Eastern универзитетом* у Бостону, где је 2003. године изабран за придруженог професора, са *Imperial* колеџом у Лондону, као и са *Liverpool John Moores* универзитетом. Држао је наставу и радио на формирању наставног кадра на факултетима у Бањалуци, Сарајеву и Новом Саду. Област његовог научног рада укључује енергетску електронику, електричне машине, дигитално управљање у енергетици и индустријску роботику. Формирао је две научноистраживачке лабораторије у којима је реализовано 13 међународних и 20 националних пројеката. Публиковао је уџбенике и монографије на српском, енглеском и кинеском језику. Његови научни радови су цитирани више од 1900 пута. Члан је уређивачког одбора три међународна часописа, члан програмског одбора међународних конференција и аутор већег броја радова по позиву. Радио је као консултант за водеће светске компаније и добио Теслину награду за врхунска инжењерска достигнућа као и друге награде. За дописног члана Српске академије наука и уметности изабран је 2015. године.

Изазови заштите приватности: искуства министарства унутрашњих послова Републике Србије у борби против високотехнолошког криминала

On the chalenges of cyber privacy: experiences of the ministry of interior of the Republic of Serbia in the fight against high-tehnology crime

Број корисника интернета у свету на дан 30. Јуна 2017. Године износи 3.885.567.619, Што представља 51,7% популације човечанства, и указује на динамични развој савремених технологија, њихову свакодневну примену у свим областима друштвеног живота, као и велику флексибилност и прилагодљивост новим техничко-технолошким решењима појединаца и криминалних група које се баве неким обликом високотехнолошког криминала. Висок ризик овог нарастајућег криминалног феномена проистиче из флексибилности ове врсте криминала, његове иновативности и неограничености, због чега све више угрожава основна људска права и све већа је претња привредном и финансијском пословању. Иако не захтева велика финансијска улагања, висока софистицираност овог облика криминала, као и могућност високе информатичке заштите учинилаца, чини га мање ризичним од откривања у поређењу са другим облицима криминала, а причињену штету и остварену добит је веома тешко одредити, а процена је да се активностима криминалних група које се баве високотехнолошким криминалом на годишњем нивоу светској економији причини штета од преко 400 милијарди америчких долара. За разлику од већине других организованих и тешких облика криминала, који захтевају одређену организацију и координацију криминалних активности на интернационалном нивоу, софистицираност високотехнолошког криминала и висока друштвена опасност проистичу из немогућности разликовања глобалног од националног, појединачног од групног или организованог, што додатно отежава његово откривање. Стога су и познати облици и модуси из-

вршења кривичних дела високотехнолошког криминала на глобалном нивоу, углавном препознати и у Републици Србији. Један од друштвено најопаснијих облика високотехнолошког криминала препознатих у Републици Србији, јесте сексуална експлоатација деце и малолетних лица, као посебно рањиве категорије, у порнографске сврхе. Поред тога, заступљени су и различити облици рачунарских превара на штету физичких и правних лица које се врше на различите начине, уз технике социјалног инжењеринга и крађу и злоупотребу идентитета. Погодности Интернета, пре свега могућност да делују скривено и анонимно, неретко кроз коришћење рањивости нултог дана (*zero day vulnerability*) све чешће користе и организоване криминалне групе приликом вршења финансијског сајбер криминала, где циљани (*spear phishing*) напади у последње време нису усмерени само на мултинационалне и велике корпорације, већ су мете напада постале мала и средња предузећа са мањим бројем рачунара који им превасходно служе за обављање услуге електронског банкарства и електронске трговине. Такође, велики удео у данашњем сајбер криминалу представља и инфекција злонамерним програмом тј. *ransomware* инфекција која кодира практично све корисничке податке на рачунару и тражи откуп у криптовалутама за одговарајући кључ како би се декодирали подаци. Феномен финансијског сајбер криминала не може се сматрати новом појавом али, за разлику од претходних времена, финансијски сајбер криминал преузима доминантну појаву у сајбер простору и јавља се као последица све веће присутности и употребе информационих и комуникационих технологија (ИКТ). Свакако да уплив финансијских институција, нарочито банкарског сектора, кроз пословање правних субјеката и експанзија електронске трговине, честе међународне трансакције, различитост правних система, комплексност информационо комуникационих мрежа, доступнст аутоматизованих алата за извршење кривичних дела високотехнолошког криминала или тзв. *crimware* сервиса, као и осталих фактора мотивишу сајбер криминалце да појединачно или кроз организоване криминалне групе врше кривична дела. Високотехнолошки криминал не може се елиминисати у потпуности, али се морају направити процедуре од ризика како да се управља инцидентима. Модификација и пролиферација злонамерног софтвера, коришћење илегалних мрежа дизајнираних да украду податке и новац биће све присутније. Правовремено упознавање са новим претњама и заштитом од истих, представља кључни фактор у проактивном дејству високотехнолошком криминалу, а једини адекватни

одговор супротстављању овој врсти криминала представља јавно-приватно партнерство, уз обавезно присуство академских институција са владиним сектором.

САША ЖИВАНОВИЋ

Саша Живановић је рођен 19.03.1963. године у Тузли, БиХ, где је 1988. године дипломирао на Технолошком факултету, Универзитета у Тузли. У Министарству унутрашњих послова Републике Србије радни однос је засновао 1992. године на пословима сузбијања привредног криминала, а од 2007. године налази се на функцији начелника Одељења за борбу против високотехнолошког криминала у Служби за борбу против организованог криминала. Такође, на Криминалистичко-полицијској академији од 2014. године именован је за наставника вештина на катедри за Полицијску информатику. Током свог рада успешно је похађао на десетине сертификованих обука и тренинга на тему сузбијања финансијског, високотехнолошког криминала и повреде права интелектуалне својине, међу којима су најзначајнији ”Cyber Crime Train the Trainer” у организацији INTERPOL-a, ”High Tech Crime Management Course” у организацији *Skills for Justice*, а уназад неколико година експерт је Организације за европску безбедност и сарадњу за борбу против сајбер криминала. Аутор је више стручних радова из области високотехнолошког криминала и заштите права интелектуалне својине који су публиковани у Републици Србији и иностранству. Учесник је многобројних домаћих и иностраних конференција и семинара на тему високотехнолошког криминала и заштите права интелектуалне својине, где осим својих стручних вештина и знања, посебан акценат ставља на проактивни приступ у борби против високотехнолошког криминала и заштити права интелектуалне својине кроз јачање јавно-приватног партнерства и сарадњу са академским институцијама. За свој досадашњи рад више пута је награђиван како у земљи тако и иностранству, а у 2011. години ванредно је унапређен у звање главног полицијског саветника у Министарству унутрашњих послова.

Капацитет Републике Србије да гарантује приватност грађана у дигиталном добу

Capacity of Republic of Serbia to Provide Cyber Privacy of the Citizens In Digital Era

Технологије су омогућиле практично свакодневну производњу неслућених количина података, приликом чак и најбаналнијих активности у дигиталном окружењу. Уз остале иновације 4. индустријске револуције, настала је економија података, низ нових бизнис модела заснованих на трговини и обради података. Као неопходни ресурс за новоуспостављене производне процесе намећу се управо подаци о личности, већ прослављена нафта 21. века. Ови подаци су дигитални трагови нашег укрштања са реалношћу, које успостављена инфраструктура и методи вештачке интелигенције могу преточити у предикције, знања која разоткривају најсензитивније аспекте наше приватности и личности.

У покушају да регулише питање приватности и поверљивости, већина држава доживљава дубоку кризу суверенитета. Глобална мрежа насељена са преко 3.5 милијарди људских бића и много већим бројем паметних уређаја са сваког краја земаљске кугле, не познаје државне границе. Центар моћи новоствореног система економије података су корпорације које физички немају присуство на територији већине држава (Фејсбук, Гугл, Амазон, Епл). Спонтаност и експлозивност технолошких иновација у друштвеном окружењу додатно отежава примену успостављених механизама и природно слаби поверење и ефикасност правне заштите.

Република Србија се у свему уклапа у ову слику, што се може приказати на једном примеру. Од 100 најпосећенијих сајтова у Србији, 60% не поседује директну везу са Србијом, док само на 40% сајтова Србија може успоставити неку врсту надлежности над лицем које је власник домена, лицем које управља веб страницом, хостинг компанијом на чијим

серверима се веб страница налази или самим серверима који садржај чине доступним. Даљом анализом 60 сајтова који немају успостављене везе са Србијом по описаним критеријумима, две трећине (41 од 60) не поседује никакву додатну везу са Србијом, док се за једну трећину (19 од 60) може рећи да поседује неку врсту пословног присуства на домаћој територији (сајт је доступан на српском, постоји регистрован .РС домен поред главног домена, постоје партнери на српској територији, итд). У односу на ову трећину, Република Србија би могла да успостави одређен степен надлежности, али би за спровођење својих одлука вероватно била принуђена да користи инструменте међународне сарадње. У погледу 40% сајтова који ни по једном критеријуму не поседују везу са Србијом, а међу којима се налазе платформе које прикупљају највеће количине података о личности, било какво регулисање и спровођење домаћих политика зависило би искључиво од кооперације мреже међународних партнера. Ограничење домета националне власти додатно потврђује да за сада нисмо имали нити један успешан случај успостављања судске надлежности над интернет корпорацијама које су објективно у различитим позицијама укључене у угрожавање личних права на дневном нивоу.

Чак и када би имали сво неопходно знање и ресурсе да осмислимо и успоставимо национални нормативни систем заштите приватности, услед врло ограничене власти држава није изгледно да би били у могућности да га успешно применимо у дигиталном окружењу. Интернет корпорације немају успостављене односе са нашим владама, не плаћају порез, не запошљавају и немају представника на нашој територији. Чак је и у питањима сарадње по кривично-правним предметима сарадња ограничена и често преко посредника.

До успостављана нових правила можда може доћи договором између држава и корпорација, посебним споразумима или директним односима попут недавног успостављања амбасадора Данске у Сан Франциску задуженог за технолошке компаније. Ипак, тешко је веровати да би ови преговори омогућили заштиту приватности на жељеном нивоу узимајући у обзир преговарачку позицију националних држава.

Од маја 2018. године на снагу ће ступити европска Општа уредба о заштити података о личности од које се очекује да ће имати далекосежне последице на регулисање обраде података о личности. Уколико се покаже да су очекивања од овог регулаторног механизма основана, као једна од мера којима се може постићи унапређење стања заштите приватности

у дигиталном окружењу је заговарање да обавезе интернет компанија према европским грађанима важе и према грађанима Републике Србије.

ЂОРЂЕ КРИВОКАПИЋ

Др Ђорђе Кривокапић дипломирао је на Правном факултету Универзитета у Београду а мастер студије је завршио на Правном факултету Универзитета у Питсбургу (САД). Докторске студије Правног факултета Универзитета у Београду окончао је 2016. године одбраном докторске дисертације на тему «Сукоб закона и надлежности који произлази из повреде репутације путем Интернета» пред међународном комисијом. Од 2009. године запослен је на Факултету организационих наука Универзитета у Београду, најпре као сарадник у настави и асистент, а у октобру 2017. године ће ступити у наставничко звање доцента. Његово радно ангажовање се одвија у оквиру Катедре за организацију пословних система. Пре ангажовања на Факултету организационих наука Универзитета у Београду радио је као адвокатски приправник у адвокатској канцеларији. Лето 2010. и 2012. године провео је усавршавајући се и припремајући докторску дисертацију у оквиру Беркман центра за Интернет и друштво Правног факултета Универзитета Харвард. Од 2012. године укључен је у рад *SHARE* фондације у оквиру које као програмски директор води тим интердисциплинарних истраживача у више десетина пројеката. *SHARE* фондација промовише слободу изражавања на Интернету, информациону приватност, дигиталну безбедност и слободан приступ знању кроз истраживања, креирање јавних политика, заговарање регулаторних реформи, стратешко парничење, надзор над радом надлежних органа, мониторинг Интернет слобода и дигиталних права, правну и техничку подршку организацијама које омогућавају слободан приступ знању. Од јуна 2017. године др Кривокапић је као представник европских организација изабран за члана Управног одбора Савета цивилног друштва за информационо друштво (CSISAC) при Комитету да дигиталну економију (CDEP) Организације за економску сарадњу и развој (OECD).