NEWSIMR&D

Funded by Science Fund of the Republic of Serbia

02

WP Report

WP Leader: Prof. Dr. Mladen Milošević

Review and analysis of the legal framework for countering new security risks in the Republic of Serbia

Supported by:
Science Fund
of the Republic of Serbia

NEWSIMR&D

ИЗВЕШТАЈ 1[1]

Преглед и анализа правног оквира за супротстављање новим безбедосним ризицима у Републици Србији

Безбедност сајбер простора

Зависност савременог друштва од информационих и комуникационих технологија изнедрила је и нове ризике који се у великој мери разликују од оних који су постојали у прошлости. Безбедносни ризици који се испољавају у сајбер свету су веома хетерогени и крећу се од вршења кривичних дела на штету појединаца и правних лица преко или уз помоћ рачунарских система и мрежа до сајбер операција којима се угрожава безбедност држава и међународних организација кроз спровођење аката тероризма или чак агресије.

Међународноправни аспекти

Актуелно је и питање о могућим правним квалификацијама чина сајбер ратовања, будући да је велико питање може ли се и под којим условима одређен скуп сајбер операција подвести под дефиницију агресије усвојену у Резолуцији Уједињених нација, или је оправдано и довољно карактерисати га као кривично дело кажњиво по одредбама националних законодавстава. Пракса је показала да напади у виртуелном простору, наоко неприметни, могу у реалном, физичком свету резултовати људским жртвама и материјалним разарањима, што је отворило и питање могу ли се сајбер операције посматрати као еквивалентне употреби силе.

Први пут је агресија дефинисана као кривично дело - злочин против мира, у члану 6. Статута Међународног војног трибунала у Нирнбергу. Она се одређује као: "планирање, припремање, започињање или вођење агресорског рата или рата којим се крше међународни уговори, споразуми или гарантије, или учествовање у неком заједничком плану или завери за извршење ма ког од горе наведених дела" (Вучинић, 2013). За суђење због кривично дела против мира је био надлежан и Токијски трибунал. Од тада, међутим, нико није био осуђен за злочин против мира.

Агресорски рат је и пре суђења у Нирнбергу био забрањен Бријан-Келоговим пактом из 1928. године, мада тим пактом није била уведена потпуна забрана сваког рата. То ће се десити тек усвајањем Повеље УН која допушта искључиво одбрамбени рат и принудне мере самих Уједињених нација. Спречавање силе у односима између држава једно је од основних начела УН, а посебно се овим питањима баве чланови 1, 2, 33 и 39 Повеље УН. Резолуције Генералне скупштине Уједињених нација бр. 3314 из 1974. године пружа критеријуме за дефинисање агресије а наведени су и конкретни акти који се сматрају агресорским по слову резолуције.

[1] Извештај сачињен на основу објављених научних и стручних радова учесника на пројекту. Извештај садржи изабране делове тих радова.

Мелцер (Melzer) разматра питање jus ad bellum код сајбер операција анализирајући појам силе из Повеље УН.Она не пружа правну дефиницију силе, па се садржај овог појма одређује сходно духу и смислу Повеље и међународном обичајном праву (Melzer, 2011). Аутор истиче да је теорија недвосмислена у оцени да сајбер операције чији се ефекти огледају у смрти и рањавању људи или физичком уништењу објеката могу сматрати употребом силе у међународним односима, иако се сила у Повељи схвата на рестриктиван начин у односу на стандардно значење те речи.. У прилог његовом мишљењу говори и саветодавно мишљење Међународног суда правде (International Court of Justice, Legality of the Threat or Use of Nuclear Weapons, advisory opinion, 1996) у ком се исиче да се "било која употреба силе, без обзира на коришћено средство/оружје", може сматрати силом у овом смислу. И Шмит (Schmitt) говори да се сајбер операције могу сматрати употребом силе када доводе до последица упоредивих са резултатима примене кинетичког, нуклеарног, хемијског или биолошког оружја (Schmitt, 1999).

Проблем, међутим, настаје код сајбер операција које не резултују непосредно људским жртвама и материјалним разарањима, али остављају друге озбиљне последице, попут масовног DDoS напада на одређене системе угрожене државе (Melzer, 2011).

Други проблем лежи у чињеници да је појам оружаног напада из члана 51 Повеље ужи од појма силе из члана 2. Да би држава стекла право на индивидуалну или колективну самоодбрануу, потребно је да дође до оружаног напада на њу. Иако се поменуте сајбер операције могу сматрати употебом силе, посебно када доводе до ефеката упоредивих са кинетичким, нуклеарним, хемијским или биолошким ратовањем, недостају поуздани ослонци за доношење недвосмисленог закључка у вези изједначавања сајбер напада са оружаним нападом.

Интересантан покушај разрешења бројних недоумица је учињен од стране НАТО, када је окупљена група истакнутих правних експерата, са задатком да проучи и одговори на најважнија питања о могућности употребе правила међународног права на сајбер ратовање. Овај пројекат је резултовао издавањем Приручника о применљивости међународног права на сајбер ратовање (Tallinn Manual on the International Law Applicable to Cyber Warfare). Правило 13 Приручника јасно одређује да сајбер операција која би довела до смрти или повреда људи, треба да се сматра као оружани напад без обзира што није употребљено оружје у конвенционалном смслу. У истом смеру иде и Правило 11, које дефинише употребу силе у смислу сајбер ратовања. Дефиниција сајбер напада, дата у Правилу 30, доследно изражава исту идеју: „сајбер напад је офанзивна или дефанзивна сајбер операција за коју се основано може сматрати да ће довести до смрти или рањавања лица или уништавања или оштећења објеката" (Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013).

Коначно, и поред постојећих покушаја теоретичара и издавања правно необавезујућих докумената попут овог Приручника, далеко смо од јединственог одређења правног статуса сајбер операција у смислу међународног ратног и хуманитарног права, те можемо закључити да је међународноправна димензија сајбер безбедности суштински недовољно развијена, као и да обилује нејасноћама и различитим тумачењима.

Кривичноправна димензија (материјалноправни и процесноправни аспекти борбе против високотехнолошког/сајбер криминала)

Правна регулатива сајбер простора у Републици Србији није адекватна и потпуна, а безбедносни изазови у виртуелном свету непрестано расту и трансформишу се. Правни оквир сајбер безбедности обухвата прописе којима се регулишу надлежности органа за управљање безбедносним ризицима у информационо-комуникационим системима и сузбијање радњи којима се функционисање ових система угрожава или нарушава, као и норме о техникама, методама и процедурама заштите, координацији између чинилаца заштите, њиховој одговорности и надзору над применом законских овлашћења и обавеза. Осим њих, нормативни оквир обухвата и норме којима се регулише заштита од високотехнолошког криминала и других противправних претњи у сајбер простору. Овде спадају прописане превентивне и репресивне мере, те материјалне и процесне норме, првенствено у сфери казненог законодавства. У наведеном смислу, правни оквир сајбер безбедности је сачињен од одредаба различитих закона, којима је безбедност информационо-комуникационих система примаран или секундаран предмет регулисања.

Дела којима се нарушава или угрожава функционисање ИКТ система, као и интегритет, доступност, аутентичност и тајност рачунарских података, санкционишу се кривичноправним одредбама, чиме се кривично право показује као инструмент заштите сајбер безбедности. Са аспекта сајбер безбедности, ипак, кривично право, као ultima ratio и инструмент који најчешће служи post festum када је до нарушавања или угрожавња већ дошло, има ограничен превентивни значај. Уколико кривично право остварује извесне генералне и специјалне превентивне ефекте у односу на сајбер криминал, у домену сајбер претњи по одбрану и националну безбедност, реална превентивна моћ кривичноправних одредби је релативно мала.

Проблем супротстављања високотехнолошком криминалу има материјалноправну и процесноправну димензију, те је српски законодавац, вођен обавезама преузетим усвајањем и ратификацијом међународних конвенција, последњих деценију и по значајно изменио законски кривичноправни оквир у овој области. Србија је потписала и ратификовала Конвенцију о високотехнолошком криминалу, коју је Савет Европе усвојио 2001. године, као и њен Додатни протокол (Закон о потврђивању Конвенције о високотехнолошком криминалу, 2009; Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система, 2009). Још 2003. године, српско кривично законодавство је измењено тако да инкриминише и кривична дела против безбедности рачунарских података (Закон о изменама и допунама Кривичног закона Републике Србије, 2003). Занимљиво је да српски законодавац, инкриминишући понашања сходно начелима Конвенције, санкционише све основне облике високотехнолошких кривичних дела осим оних везаних за пресретање комуникације. Ово остаје као очигледан недостатак актуелног решења домаћег кривичног материјалног законодавства (Стојановић, 2012).

Пре доношења те конвенције, у периоду од 1989. до 2000. године, усвојен је низ инструмената међународног права у области криминалитета везаног за компјутере (Препорука Савета Евро- пе о криминалитету везаном за компјутере, 1989; Резолуција Уједињених нација о компјутерском криминалитету, 1990; Резолуција Међународног удружења за кривично право везана за компјуте- рски криминалитет, 1992; Директива Европске уније о електронском пословању из 2000. године, и др.), али је неспорно да је

тек њено ступање на снагу означило прекретницу у борби против ове савремене и сложене форме криминалног деловања (Стојановић, Делић, 2015: 283).

Иако се уочава извесна временска дискрепанца између ратификације Конвенције и мењања домаћег кривичног законодавства, наша држава је углавном на адекватан начин испунила обавезе преузете усвајањем овог међународноправног акта. Кривични законик Србије из 2005. године (КЗ, 2005) задржао је посебну главу (Глава 27) под називом „Кривична дела против безбедности рачунарских података“ уз одређене измене у односу на одредбе пре- тходно важећег кривичног закона.

Ипак, вреди нагласити да је појам високотехнолошког криминала у нашем законодавству шири од опсега кривичних дела против безбедности рачунарских података. Према члану 2 став 1 Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала ова врста криминалитета обухвата вршење кривичних дела код који се као „објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику“ (Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, 2005). Изменама и допунама закона из 2009. године прецизирана су кривична дела за чије се откривање, гоњење и суђење примењују одредбе овог прописа, чиме је, барем у законском смислу, етаблирано значење термина високотехнолошки криминал (члан 3 Закона о организацији и надлежности др- жавних органа за борбу против високотехнолошког криминала).

Члан 3 Закона о ВТК одређује да надлежност за откривање, гоњење и суђење припадају специјализованим одељењима полиције, тужилаштва и суда у случају следећих кривичних дела:

• против безбедности рачунарских података (глава 27 КЗ-а) – по правилу, од- носно без додатних услова;

• против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије – уз додатни услов: да се могу сматрати високотехнолошким криминалом имајући у виду начин извршења и коришћена средства (сходно члану 2 став 1 Закона о ВТК);

• против интелектуалне својине, имовине, привреде и правног саобраћаја – уз два услова:

1. да број примерака ауторских дела прелази 2.000 (овај услов се односи на кривична дела против интелектуалне својине, попут повреде проналазачког права или неовлашћеног искоришћавања ауторског дела или предмета сродног права) или да настала материјална штета прелази износ од 1.000.000 динара и 2. да се могу сматрати високотехнолошким криминалом имајући у виду начин извршења и коришћена средства (сходно члану 2 став 1 Закона о ВТК).

Кривична дела која не потпадају под посредне дефиниције из чл. 2 и 3 Закона о ВТК, не могу се сматрати високотехнолошким криминалом у Републици Србији.

Материјалноправни апсекти

У глави 27 Кривичног законика се налазе следеће инкриминације (чл. 298−304а КЗ): оштећење рачунарских података и програма (члан 298); рачунарска саботажа (члан 299); прављење и уношење рачунарских вируса (члан 300); рачунарска превара (члан 301); неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (члан 302); спречавање и ограничавање приступа јавној рачунарској мрежи (члан 303); неовлашћено коришћење рачунара или рачунарске мреже (члан 304); прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података (члан 304а). Последња наведена инкриминација представља врсту припремне радње уздигнуте на ниво радње извршења. Знајући значај превенције и степен друштвене опасности високотехнолошог криминала, законодавац се одлучио за кривичноправну репресију .

Имајући у виду појавне облике сајбер криминалитета нарочито је важно анализирати кривична дела преваре и рачунарске преваре. Кривично дело рачунарске преваре уведено је поменутим изменама и допунама из 2003. године и у готово истоветном облику је опстало до данас. Законски опис из члана 186г Кривичног закона Србије (КЗС, 1977) практично је истоветан са оним из члана 301 Кривичног законика (КЗ, 2005) осим разлике у новчаним износима штете који чине квалификаторне околности (тежи и најтежи облик кривичног дела).

Дело из члана 301 КЗ има основни, два квалификована и привилеговани облик. Биће основног облика кривичног дела садр- жи радњу и последицу, а имплицитно су садржани средство извр- шења и објекат радње као објективна обележја, док субјективни супстрат дела чине умишљај и одговарајућа намера. Постојање намере као субјективног обележја одређује да је дело могуће учинити једино са директним умишљајем, док је евентуални умишљај искључен.

Радња основног облика састоји се у предузимању делатности (комисивних или омисивних) којима се прикривају или лажно приказују подаци. Законодавац експлицитно наводи две радње – уношење нетачног податка и избегавање да се унесе тачан пода- так, али додаје и широку формулацију „или на други начин лажно прикаже или прикрије податак“, што представља правни стандард и омогућава релативно екстензивно тумачење.

Последица кривичног дела састоји се у утицању на резул- тат процеса електронске обраде и преноса података. Делатности извршиоца треба да доведу до одређене промене у аутоматској обради и преносу која се испољава у произвођењу другачијег резул- тата обраде у односу на очекивани, то јест резултат који би насту- пио да су унети параметри били аутентични. За постојање дела се захтева и наступање имовинске штете по другог, што представља за нијансу другачију формулацију у односу на кривично дело пре- варе из члана 208 КЗ („и тиме га наведе да овај на штету своје или туђе имовине нешто учини или не учини“).

Овде се може поставити питање да ли имовинска штета представља објективни услов инкриминације или је, заједно са утицањем на резултат електронске обраде и преноса података, по- следица кривичног дела. У првом случају имовинска штета не би морала да буде обухваћена умишљајем учиниоца, те ово предс- тавља и важно фактичко питање. С обзиром да је рачунарска пре- вара специјалан случај преваре, питање треба решавати уз узима- ње у обзир законског описа дела из члана 208 КЗ.

Према мишљењу заступљеном у литератури, код кривич- ног дела преваре штета по имовину другог треба заиста да насту- пи како би дело било довршено (Стојановић, 2012; Ђорђевић, 2014; Стојановић, Делић, 2015). На основу тога закључујемо да би и формулацију законодавца код кривичног дела рачунарске преваре било исправно тумачити тако да наступање имовинске штете представља последицу кривичног дела, те је њено наступање нужно да би се дело сматрало свршеним, а умишљај учиниоца мора да обухвати и свест о наступању имовинске штете.

Дакле, кривично дело рачунарске преваре је довршено када се предузимањем радње оствари такав утицај на резултат електронске обраде и преноса података да услед њега наступи имовинска штета по другог.

Овде се основано поставља питање разликовања објективних обележја рачунарске преваре од основног облика дела из члана 208 КЗ. Код „класичног“ кривичног дела преваре извршилац лажним приказивањем или прикривањем чињеница пасивног субјекта доводи или одржава у заблуди и тиме га наводи да нешто учини или не учини на штету своје или туђе имовине. Дакле, пасивни субјект је истовремено и предмет радње, то јест објект кри- вичног дела.

С друге стране, биће кривичног дела рачунарске преваре конструисано је тако да пасивни субјект није у потпуности подударан са предметом радње, јер се радња врши у оквиру рачунарске обраде података, а последица наступа како на самом процесу обраде и преноса података тако и на имовини пасивног субјекта. Радња се првенствено предузима на рачунару или рачунарској мрежи, а имовина пасивног субјекта бива оштећена због промењеног резултата процеса електронске обраде и преноса података ко- ји се одвија у оквиру система или мреже.

Ипак, у пракси се разликовање та два кривична дела може показати као тешко. Примера ради, кривично дело преваре може се извршити посредством фалсификоване исправе или лажног представљања, па исто тако и коришћењем рачунара. Питање је да ли се рачунарском преваром може назвати сваки случај преваре у ком се као средство извршења користе рачунари, рачунарски системи или мреже.

Нама се чини да је одговор негативан. Наиме, рачунарска превара свакако подразумева да су рачунари или рачунарске мреже средство извршења кривичног дела и то обележје је неспорно. Међутим, суштинска разлика у односу на дело из члана 208 КЗ јесте то што се рачунари или рачунарске мреже, односно свака аутоматизована електронска обрада или пренос података, појављују и као објект радње, а не само као средство извршења. Суштински, кривично дело преваре би постојало када би се као средство извршења користио рачунар, под условом да предмет радње није било утицање на електронску обраду и пренос података већ стварање погрешне представе код оштећеног услед које он нешто предузима на штету своје или туђе имовине.

У том смислу, слање мејлова који би садржали превару познату као „нигеријска“ (један од најпознатијих видова фишинга) услед којих би потенцијална жртва била наведена да себи нанесе имовинску штету због лажних чињеница изнетих у тексту елек- тронске поруке које су је навеле да поступи противно својим ма- теријалним интересима, представљало би кривично дело из члана

208 КЗ, без обзира што је изведено уз помоћ рачунара и рачунарске мреже. Треба имати у виду да ширина појма „високотехнолошки криминал“ омогућава да се и то дело открива, гони и суди сходно Закону о организацији и надлежности државних органа за бо- рбу против високотехнолошког криминала (члан 3 Закона), али оно свакако остаје квалификовано као дело преваре, а не рачунарске преваре.

Тако, можемо закључити да бројне интернет преваре често не могу да се квалификују као рачунарске преваре, већ сходно од- редби члана 208 КЗ, јер не постоји засебно кривично дело интернет преваре, различито од дела из члана 301 и дела из члана 208 КЗ (Вилић, 2016; Мирић, 2018).

Рачунарска превара постојала би у случају да извршилац успе да утиче на аутоматску обраду података тако да она пружи лажан резултат. Уколико бисмо отварањем интернет везе (линка) дошли на лажну страницу банке, изабрали опцију за плаћање преко интернет мреже и тиме уплатили новац на рачун на који нисмо желели, јер су подаци о трансакцији измењени, онда би била реч о рачунарској превари (традиционални начин извршења фишинга).

Вреди напоменути да је кривично дело преваре уз коришћење информационо-комуникационих технологија, имајући у виду хетерогене појавне облике, могуће подвести и под друге пра- вне квалификације, које такође представљају специјалне случајеве преваре, али их је законодавац уздигао на ранг посебних кривичних дела. Ту мислимо на кривична дела: превара у обављању привредне делатности (члан 223 КЗ); превара у осигурању (члан 223а КЗ) и превара у служби (члан 363 КЗ). Свако од наведених криви- чних дела може се извести тако да средство извршења буду информационо-комуникационе технологије, тако да, феноменолош- ки гледано, коришћење информационо-комуникационих технологија за вршење преварних радњи може да задобије различите кривичноправне облике, односно правне квалификације.

Посебно треба размотрити и могућност да правно лице буде извршилац неког од кривичних дела преваре (општег из 208 или наведених посебних случајева преваре, укључујући рачунарску). Међутим, примена Закона о одговорности правних лица за кривична дела у Србији (Закон о одговорности правних лица за кривична дела, 2008) од његовог доношења до данас је била изузетно ретка. Основ одговорности правног лица за кривично дело могао би бити испуњен приликом предузимања радње неког од наведених кривичних дела, јер је лако замисливо да се радња врши у склопу обављања послова одговорног лица уз постојање на- мере да се противправна имовинска корист стекне, макар и дели- мично, и за правно лице (Милошевић, 2012; Милошевић, 2012а; Милошевић, Симовић, 2018).

Субјективни елемент кривичног дела рачунарске преваре осим директног умишљаја, који подразумева свест и вољу о свим законским обележјима кривичног дела, обухвата и намеру да се „себи или другом стекне противправна имовинска корист“ (члан 301 КЗ). Привилеговани облик дела постоји када учинилац има искључиву намеру да другоме нанесе имовинску штету. Ту, дакле, извршилац тежи да другог оштети, а не и да себи или неком трећем лицу прибави имовинску корист. У том случају дело је довршено без обзира на то да ли је штета наступила или не, јер је она део субјективног елемента овог облика кривичног дела, а не и његово објективно обележје (Стојановић, 2012).

Тежи и најтежи облик се од основног облика не разликују по субјективном елементу, већ по објективном обележју – тежини последице, односно висини имовинске штете која је наступила. Код тежег облика износ штете треба да пређе 450.000 динара, док код најтежег он износи преко 1.500.000 динара.

Код основног облика запрећена је новчана казна или затвор до три године, код првог тежег облика казна је од једне до осам година затвора, док је код најтежег облика она прописана у распону од две до десет година. Лакши облик кривичног дела се кажњава новчаном казном или затвором до шест месеци (Мандић, Путник, Милошевић, 2017).

Из перспективе нових безбедносних ризика, занимљиво је размотрити и могућности за кривичноправно регулисање злоупотребе малициозних кодова, пре свега ренсомвера. Од 2016. године ренсомвер-напади изазивају велику забринутост не само кор- поративног менаџмента већ и влада држава. Разлог лежи у томе што ови напади про- узрокују велике финансијске губитке са једне стране док, са друге, могу онемогућити функционисање здравствених установа и тиме, посредно, ускратити могућност лечења пацијената. Од почетка пандемије вируса SARS-CoV-2, здравствене установе широм Америке и Европе суочавају се, паралелно, и са пандемијом ренсомвер-напада.

Напади овог типа, уколико циљају на ИКТ системе од посебног значаја, представљају озбиљан изазов не само за национално законодавство већ и за доносиоце политичких одлука и креаторе националних безбедносних политика. ИКТ систе- ми од посебног значаја су системи који се користе у обављању послова у органима јавне власти, за обраду података о личности и у обављању делатности од општег интереса (члан 6 Закона о информационој безбедности).

Ови системи се у англосаксонском говорном подручју уобичајено називају критичном информационом инфраструктуром која представља једну од посебно осетљивих критичних инфраструктура државе. Појам критичне инфраструктуре се може одредити на различите начине. Члан 4 став 1 српског Закона о критичној инфраструктури гласи: „Критична инфраструктура су системи, мреже, објекти или њихови делови, чији прекид функционисања или прекид испоруке роба односно услуга може имати озбиљне последице на националну безбедност, здравље и животе људи, имовину, животну средину, безбедност грађана, економску стабилност, односно угрозити функционисање Републике Србије“. Дакле, наш законодавац сматра критичним оне „системе, мреже, објекте или њихове делове“ чије функционисање у битној мери утиче на остваривање виталних државних или друштвених циљева и интереса (бе- збедност, привреда, живот, здравље, животна средина, имовина).

Савремено теоријско одређење појма критичне инфраструктуре односи се на имовину која укључује физичке и рачунарске системе који су од есенцијалног значаја за обезбеђивање економске и политичке стабилности земље (Radvanovsky & McDougall,2010). У суштини, оне представљају оквир међузависних мрежа и система који обу- хватају одређене индустрије, институције (укључујући људе и процедуре) и капацитете за дистрибуцију који пружају поуздан проток производа и услуга који су неопходни за одбрамбену и економску сигурност земље, неометано функционисање власти на свим нивоима, као и друштва у целини (Rakić, 2015, str. 10). Критичне инфраструктуре обухватају здравствене системе, енергетске системе, телекомуникације, саобраћај, воду, храну, банкарске системе и финансије, цивилну

администрацију, укључујући и владини приватни сектор, али нису искључиво на њих ограничене (Radvanovsky & McDougall, 2010). Ниједна подела критичних инфраструктура није апсолутна и углавном је заснована на проценама стручњака и/или доносиоца политичких одлука одређене државе.

Кривичноправни аспект је веома занимљив. Прављење рачунарског вируса уз намеру његовог уношења у туђ рачунар или рачунарску мрежу, инкриминисано је чланом 300 КЗ-а. Запрећена је новчана казна алтернативно са затвором од шест месеци. Уколико учинилац унесе рачунарски вирус и проузрокује штету, остварен је квалификовани облик, прописан ставом 2 овог члана, за који је прописана новчана казна или затвор до две године. Законом је прописана обавезна мера безбедности, којом се одузимају уређаји и средства на- мењени за или настали извршењем кривичног дела.

Члан 112 став 20 КЗ одређује значење појма рачунарског вируса, описујући га као врсту рачунарског програма (или другог скупа налога, односно наредби) који одликује тенденција самоумножавања и деловања на друге програме и податке. Вирус делује на друге рачунарске програме и податке тако што им се придодаје и мења начин на који они функционишу.

Основни облик показује намеру законодавца да реагује у раној фази, јер је прављење рачунарског вируса уз дату намеру, по својој суштини, само припремна радња. С обзиром на то да је припремање кривичног дела начелно некажњиво, зако- нодавац је прописивањем основног облика омогућио примену кривичних санкција и за припремне радње, које су овим добиле карактер радње кривичног дела.

Тежи облик је, по природи ствари, основни облик, који је законодавац „вештач- ки“ трансформисао у квалификовани, јер је припремну радњу прогласио за основни облик дела. Овде се основано може поставити питање оправданости постојања облика из става 1, након што је ЗИД КЗ из 2009. године увео кривично дело из члана 304а. Тим кривичним делом, уз прецизирање и допуне учињене доношењем ЗИД КЗ из

2016. године, инкриминишу се различите припремне радње за извршење кривичних дела против безбедности рачунарских података. Уз евентуално додатно прецизирање одредби члана 304а, потреба за постојањем основног облика из садашњег члана 300 став 1 би потпуно нестала, што би било оправдано и са становишта законодавне технике.

У вези садашње регулативе, поставља се још питања. Наиме, јасно је да ако неко направи рачунарски вирус а затим га унесе у туђ рачунар или мрежу, чини само дело из става 2. Међутим, дело из става 2 је последично, што значи да је свршено када наступи штета (Stojanović & Delić, 2020). У случају да је рачунарски вирус унет а штета изостала, реч је о покушају, који је некажњив по општим одредбама.

Дакле, само прављење рачунарског вируса у намери стављања у туђ рачунар или мрежу је кажњиво, док би уношење вируса без наношења штета било некажњиво. Ово је очигледна нелогичност, која је последица чињенице да је припремна радња кажњива, а покушај „правог“ дела некажњив. Припремне радње би требало да се кажњавају када се припрема теже кривично дело, а ово дело је у категорији лакших, што и доводи до спорних решења.

Занимљиво је да ово кривично дело нема више квалификованих облика. Уколико би се de lege ferenda приступило изменама ове главе КЗ-а, требало би раз- мотрити брисање члана 300 става 1 (уз његово јасно „припајање“ члану 304а) и до- давање тежих облика, који би се односили на извршење дела из садашњег става 2 (који би постао став 1) уз одређене квалификаторне околности. Те околности би могле да буду: наношење имовинске штете у одређеном износу; привремени или потпуни застој или поремећаји у раду (ако је пасивни субјект орган/организација).

Пре даљег разматрања de lege ferenda пак потребно је одговорити на питање: да ли се злоупотребе малициозних кодова у виду ренсомвер-напада могу квалифико- вати искључиво по овом члану КЗ-а или у обзир долазе и друге кривичноправне квалификације?

У том смислу, ваља испитати могућност да се радња злоупотребе ренсомвера подведе под кривично дело уцене из члана 215 КЗ-а. Уцена постоји уколико учинилац, у намери стицања противправне имовинске користи за себе или другог, прети да ће против пасивног субјекта „или њему блиског лица открити нешто што би њиховој части или угледу шкодило“. Према томе, употреба ренсомвер-кода, би, хипотетички, могла да представља кривично дело уцене само у случајевима када се оштећени уцењује откривањем „заробљених“ података, чијим обелодањивањем може да се нашкоди части или угледу. То, ипак, код ренсомвер-напада углавном није случај, те већински неће бити основа да се дело квалификује по члану 215 КЗ-а.

Међутим, могуће су и ситуације у којима учинилац зароби рачунарске подат- ке и уцењује жртву њиховим откривањем (нпр. стекне контролу над рачунарским системом и оствари приступ фотографијама, чијим откривањем би наудио угледу пасивног субјекта). Тада би се дело квалификовало као уцена. С обзиром на то да је уцена изведена помоћу уношења рачунарског вируса, поставило би се и питање стицаја дела из чл. 215 и 300 КЗ-а. У теорији и судској пракси се слично питање по- стављало у вези односа кривичних дела преваре и фалсификовања исправе. У вези са тим делима заузет је став да ако је фалсификовање исправе био једини начин да се изведе превара, стицај је привидан (Stojanović & Perić, 2011, str. 153). Такво стано- виште је оправдано у овом случају, али једино уколико је заиста била реч о једином могућем начину извршења уцене. У свим осталим ситуацијама, постојао би реални стицај, посебно имајући у виду да је реч о кривичним делима са врло различитим заштитним објектима.

Дакле, поједини случајеви злоупотребе ренсомвер-кодова могу да се квалифи- кују као кривично дело уцене. Међутим, ти случајеви су релативно ретки и остаје проблем подвођења осталих друштвено опасних радњи изведених употребом мали- циозних кодова под одговарајућу кривичноправну квалификацију.

Кривично дело принуде, из члана 135 КЗ-а, постоји ако се друго лице, употребом силе или претње, принуди на одређено чињење, нечињење или трпљење. Поступање код ренсомвер-напада се поклапа са законским описом основног облика овог дела, јер се жртви упућује претња и иста је принуђена на чињење или нечињење. Ипак, покушај основног облика овог кривичног дела је некажњив, јер је запрећена казна затвора до три године.

Такође, поставља се питање да ли је овде присутан стицај са кривичним делом из члана 300 или је он привидан (Delić, 2021; Vuković, 2021; Stojanović, 2018). Закључак је исти као код уцене. У већини случајева овде ће бити реч о реалном стицају два кривична дела. Уосталом, законодавац није без разлога инкриминисао уношење ра- чунарских вируса у туђ рачунар или рачунарску мрежу, већ је имао у виду посебну друштвену опасност ових радњи. Стога не би било оправдано „багателисати“ дело из члана 300 његовим свођењем на начин извршења другог кривичног дела.

На крају, али никако најмање важно, остаје да се размотри могућност правне квалификације рансомвер-напада као изнуде (члан 214 КЗ-а). Изнуда, као имовинско кривично дело, представља специјалан случај принуде и од ње се разликује по субјек- тивном елементу (намера стицања противправне имовинске користи) и последици (пасивни субјект је принуђен да нешто учини или не учини на штету своје или туђе имовине). Имајући у виду да учиниоци који користе рансомвер-вирус по правилу имају лукративне (имовинске) мотиве, јасно је да би далеко већи број ових напада могао да се квалификује као изнуда. Принуда би била исправна квалификација само у ситуацијама када учинилац није имао намеру стицања противправне имовинске користи. Проблем стицаја треба решавати на исти начин као код излагања о уцени и принуди. С обзиром на запрећену казну за кривично дело из члана 214 КЗ-а, овде би покушај био кажњив.

Имајући све наведено у виду, сматрамо да би већину појавних облика злоупот- ребе рансомвер-малвера требало квалификовати као стицај кривичних дела изнуде и прављења и уношења рачунарских вируса. Тамо где не би постојала намера стицања противправне имовинске користи нити би се последица огледала у имовинској штети, радило би се о стицају принуде и дела из члана 300, док би у најређим случајевима претње обелодањивањем података постојао стицај уцене и прављења и уношења рачунарских вируса.

Процесни аспекти борбе против високотехнолошког криминала

Пуна имплементација Конвенције је захтевала даљу законску реформу. Важан корак у том смеру представљало је усвајање Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала (Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, 2005) којим се прецизира круг кривичних дела на која се закон примењује. Ипак, остаје питање да ли је адекватно и практично решење којим се ограничава круг кривичних дела која се, уз испуњење осталих услова, сматрају делима високотехнолошког криминалитета. Можда би функционалније било решење које дозвољава поступање јавног тужилаштва посебне надлежности у свим случајевима где се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, без обзира да ли спадају у неку од поменутих глава Кривичног законика. Ова примедба се може ублажити констатацијом да су наведене групе кривичних дела свакако веома обухватно одређене те да се код њих најчешће и може јавити дело са елементима високотехнолошког криминала.

Овим законом уведене су и посебне организационе целине у надлежним тужилаштвима и судовима (Више јавно тужилаштво и Виши суд) с тим да ове одредбе ни данас нису имплементиране у потпуности. У оквиру министарства задуженог за унутрашње послове формирана је, по одредбама овог закона, служба за борбу против

високотехнолошког криминала, која је смештена у оквире Управе криминалистичке полиције. Министарство надлежно за послове правосуђа добило је задатак да обезбеди средства и услове за рад новообразованих одељења.

Важно место у броби против високотехнолошког криминала заузима Законик о кривичном поступку (Законик о кривичном поступку, 2011), јер уређује правила кривичног поступка у ком се утврђује и одговорност учинилаца дела високотехнолошког криминала. Борба против ове врсте криминала је зависна од квалитета и прагматичности примењених процесних решења. Откривање, кривично гоњење и суђење за дела високотехнолошког криминала имају бројне специфичности, које препознају упоредна права (Урошевић et al., 2012: 37). Посебно вреди поменути одредбе које се односе на спровођење посебних доказних радњи у случају откривања, разјашњавања и доказивања кривичних дела високотехнолошког криминала. Посебне доказне радње могу се одредити према лицу за које постоје основи сумње да је учинило кривично дело из члана 162. Законика о кривичном поступку, а на други начин се не могу прикупити докази за кривично гоњење или би њихово прикупљање било знатно отежан. Изузетно, мере се могу одредити и према лицу за које постоје основи сумње да припрема неко од кривичних дела из става 1. овог члана, а околности случаја указују да се на други начин кривично дело не би могло открити, спречити или доказати или би то изазвало несразмерне тешкоће или велику опасност. Тачка 1. става 1 овог члана експлицитно дозвољава примену посебних радњи доказивања уколико је реч о случају у ком поступа јавно тужилаштво посебне надлежности, где спаде и одељење за високотехнолошки криминал, а став 3. члана 162 предвиђа да се мера из члана 166 Законика о кривичном поступку – тајни надзор комуникације, може применити и за кривична дела: неовлашћено искоришћавање ауторског дела или предмета сродног права, оштећење рачунарских података и програма, рачунарска саботажа, рачунарска превара и неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података.

Иако се било која од законом предвиђених посебних мера доказивања може применити на случајеве у којима поступа јавно тужилаштво надлежно за високотехнолошки криминал, две мере се издавајау по значају за област сајбер безбедности. Прва је тајни надзор комуникације.

На образложени предлог јавног тужиоца суд може одредити надзор и снимање комуникације која се обавља путем телефона или других техничких средстава или надзор електронске или друге адресе осумњиченог и заплену писама и других пошиљки. Ова мера (тајни надзор комуникације) може се одредити у трајању од три месеца, а због неопходности даљег прикупљања доказа се може продужити највише за три месеца, с тим да у случају високотехнолошког криминала и других кривичних дела у којима поступају јавна тужилаштва посебне надлежнсости, ова мера може бити продужена још највише два пута по три месеца. Наредбу о одређивању тајног надзора комуникације спроводе полиција, Безбедносно-информативна агенција или Војнобезбедносна агенција. Према члану 168 Законика о кривичном поступку поштанска, телеграфска и друга предузећа, друштва и лица регистрована за преношење информација, су задужена да надлежном органу који спроводи меру омогуће спровођење надзора и снимања комуникације и да, уз потврду пријема, предају писма и друге пошиљке. Једноставним тумачењем долазимо до закључка да се наведена мера

односи и на интернет провајдере, јер електронску пошту можемо сврстати под екстензивну формулацију друге пошиљке.

Друга посебна радња доказивања која је од нарочитог значаја за ову област је рачунарско претраживање података. На образложени предлог јавног тужиоца судија за претходни поступак може одредити рачунарско претраживање већ обрађених личних и других података и њихово поређење са подацима који се односе на осумњиченог и кривично дело, под законом предвиђеним условима. Ову меру извршава полиција, Безбедносно-информативна агенција, Војнобезбедносна агенција, царинске, пореске или друге службе или други државни орган, односно правно лице које на основу закона врши јавна овлашћења.

Поменута одступања од начела заштите приватности и тајности комуникација, су неопходна ради остваривања циљева у борби против друштвено опасних понашања и принципијелно нису спорна. Ипак, недоумице о њиховом спровођењу и начину примене законских овлашћења су честа у стручној јавности Она, међутим, нису значајна само због борбе против високотехнолошког криминала, већ су важан аспект сајбер безбедности уопште, јер могу довести до злоупотреба везаних за кршење основних људских и мањинских права гарантованих Уставом и међународним уговорима. Законик о кривичном поступку, пак, није једини пропис који омогућава примену специјалних техника и посебних мера и процедура. Оне се могу имплементирати и на основу Закона о Безбедносно-информативној агенцији (Закона о Безбедносно-информативној агенцији , 2002; у даљем тексту: Закон о БИА) и Закона о Војнобезбедносној агенцији и Војнообавештајној агенцији (Закона о Војнобезбедносној агенцији и Војнообавештајној агенцији, 2009; у даљем тексту: Закона о ВБА и ВОА). Ови закони су се, од доношења до данас, мењали како би се ускладили са појединим уставним начелима и стандардима заштите људских права ал ии концептуалним решењима Законика о кривичном поступку. Њих ћемо, без обзира што су битни и из призме заштите од високотехнолошког криминала, првенствено разматрати из аспекта опште сајбер безбедности.

Закон о БИА, је предвиђао да директор Агенције може, ако је то потребно из разлога безбедности Републике Србије, својим решењем, а на основу претходне одлуке суда, одредити да се према одређеним физичким и правним лицима предузму одређене мере којима се одступа од начела неповредивости тајне писама и других средстава општења, у поступку утврђеном законом. Ова неодређена и недовољно јасна и прецизна одредба је измењена 2014. године. Њена непрецизност и подложност дискреционој одлуци извршне власти се понајвише очитује у чињеници да нису дати никакви ближи критеријуми којима би се одредио круг физичких и правних лица према којима се мере могу одредити, нити су специфициране врста и природа мера и поступака.

Важећа одредба експлицитније одређује да су посебне мере којима се одступа од неповредивости тајне писама и других средстава општења: тајни надзор и снимање комуникације без обзира на облик и техничка средства преко којих се обавља или надзор електронске или друге адресе, тајни надзор и снимање комуникације на јавним местима и местима којима је приступ ограничен или у просторијама, статистички електронски надзор комуникације и информационих система у циљу прибављања података о комуникацији или локацији коришћене мобилне терминалне опреме и

рачунарско претраживање већ обрађених личних и других података и њихово упоређивање са подацима који су прикупљени применом претходно наведених мера. Садашње решење је свакако усаглашеније са Законником о кривичном поступку, а у делу у ком се помиње статистички електронски надзор, можда за нијансу и прецизније.

Иако је стручна јавност на то упозоравала још од 2002. године, чл. 13, 14 и 15 Закона о БИА су проглашени неуставним тек 26. децембра 2013. године (Одлука Уставног суда РС, бр. предмета ИУз-252/2002). Члан 14 Закона о БИА прописује да се посебне мере могу одредити према лицу, групи или организацији за коју постоје основи сумње да предузима или припрема радње усмерене против безбедности Републике Србије, а околности случаја указују да се на други начин те радње не би могле открити, спречити или доказати или би то изазвало несразмерне тешкоће или велику опасност. Приликом одлучивања о одређивању и трајању посебних мера нарочито се узима у обзир да ли би се исти резултат могао постићи на начин којим се мање ограничавају права грађана, у обиму неопходном да се сврха ограничавања задовољи у демократском друштву (члан 14 став 2). Примену посебне мере предлаже директор агенције, а о њој одлучује суд, и то председник Вишег суда у Београду, односно судија којег он одреди међу судијама који су распоређени у Посебно одељење тог суда за које је законом одређено да поступа у предметима кривичних дела организованог криминала, корупције и других посебно тешких кривичних дела; у року од 48 часова од подношења предлога, што говори да је поштовано начело хитности у прописивању временских оквира. У случају да суд одбије предлог директора агенције, тј. донесе негативно решење, жалба се подноси Апелационом суду у Београду. О жалби одлучује веће састављено од троје судија Посебног одељења овог суда, за које је законом одређено да поступа у предметима кривичних дела организованог криминала, корупције и других посебно тешких кривичних дела, у року од 48 часова од часа изјављивања жалбе.

Члан 15б регулише поступање у случају да се установи потреба за допуном или проширењем примене мере, у ком у истоветним роковима одлучује надлежни суд. Чланом 15в је прописано да уколико приликом примене посебних мера прикупљен материјал о кривичном делу у односу на које се могу одредити посебне доказне радње, такав материјал се доставља надлежном јавном тужилаштву, где се даље поступа сходно правилима која уређују кривични поступак. Овде у пракси свакако остаје питање који су случајеви угожавања безбедности државе који не испуњавају услове за постојање бића неког од кривичних дела, те где је граница између случајева у којима поступа искључиво БИА и оних где се укључује тужилаштво. Чланом 15г реулисана је тајност података у случају одређивања посебних мера.

Оваквом регулативом посебних мера је начелно поштован уставни принцип по ком једино суд, на основу закона, може одобрити одступање од начела неповредивости писма и друге комуникације. Одговарајуће одредбе Закона о ВБА и ВОА су својевремено успешно оспорене пред Уставним судом Србије из наведеног разлога, а касније су мењане како би се прилагодиле уставним принципима. Закон предвиђа да је Војнобезбедносна агенција овлашћена да податке прикупља (осим на стандардни начин прописан у члану 7) и применом посебних поступака и мера. Посебни поступци и мере су: оперативни продор у организације, групе и институције; тајно прибављање и откуп података и докумената; тајни увид у евиденције података; тајно праћење и надзор лица на отвореном простору и јавним местима уз коришћење техничких средстава; тајни

електронски надзор телекомуникација и информационих система ради прикупљања задржаних података о телекомуникационим саобраћају, без увида у њихов садржај; тајно снимање и документовање разговора на отвореном и у затвореном простору уз коришћење техничких средстава; тајни надзор садржине писама и других средстава комуницирања, укључујући и тајни електронски надзор садржаја телекомуникација и информационих система и тајни надзор и снимање унутрашњости објеката, затворених простора и предмета. До измена закона из 2013. године, директор ВБА је могао да изда налог за примену мере тајног електронског надзора без одобрења суда (чл. 13. ст. 1. у вези са чл. 12. ст. 1. тач. 6) и чл. 16. ст. 2. Закона о ВБА и ВОА). Уставни суд Србије је 1. јуна 2012. године ову законску одредбу прогласио неуставном (Одлука Уставног суда РС, ИУз -1218/2010, од 19.04.2012. године, објављена у Службеном гласнику РС, бр. 88/09). Проблем је што чл. 41 Устава јемчи неповредивост тајности писама и других средстава комуницирања, а одступање се дозвољава само на одређено време и на основу одлуке суда, ако је неопходно ради вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом, што је истакнуто у иницијативу за оцену уставности, а Уставни суд прихватио као правно ваљан аргумент. У образложењу одлуке се истицало и позивање на члан 8 Европске конвенције о људским правима, која гарантује право на приватност, као и праксу Европског суда за људска права (Клас и други против Немачке, бр 5029/71(1978); Малоне против Уједињеног Краљевства, бр. 8691/79 (1984); Копланд против Уједињеног Краљевства, бр. 62617/00 (2007)).

Значајно је да се у одлуци Уставног суда истиче шта обухвата појам средства комуникације, сходно пракси Европског суда за људска права: „....не само непосредан садржај комуникација, већ и податке о томе ко је и са ким остварио комуникацију, или је то покушао, у које време, колико дуго је одређени разговор трајао, колико учестало (фреквентно) је комуникација кроз преписку, разговоре или упућене поруке остваривана у одређеном периоду времена и са којих локација је вршена".

На неуставност ове одредбе је упозоравала стручна јавност, а она је констатована и у годишњем извештају Европске комисије о напретку Србије из октобра 2012. године, где је подвучено како је потребно да Србија разјасни и прецизира законски оквир за праћење и надзор комуникација од стране служби безбедности. Директор (или лице које он овласти) је сада овлашћен за предлагање али не и одлучивање о примени мере. Посебан поступак или мера се предузима на основу образложене одлуке надлежног вишег суда. Надлежан је виши суд у седишту апелационог суда чијем подручју се припрема или је предузета радња чије је откривање, праћење и онемогућавање у надлежности ВБА. Председник Вишег суда одређује судије овлашћене за доношење одлуке.

Осим кривичноправних прописа, који се претежно баве превенцијом и репресијом у погледу заштите од високотехнолошког криминала, и закона у области регулативе рада служжби безбедности, важну улогу у изградњи правног оквира сајбер безбедности имају закони и пратећа подзаконска регулатива у области заштите података. Најважније врсте података, чије прикупљање, обрада и заштита представљају законску обавезу су су: тајни подаци; подаци о личности; информације од јавног значаја; пословне тајне и професионалне тајне (Закон о тајности података, 2009; Закон о заштити података о личности, 2009; Закон о заштити пословне тајне, 2011; Закон о слободном приступу

информацијама од јавног значаја, 2004). Имајући у виду степен зависности савременог друштва од информационих технологија и чињеницу да се подаци све чешће чувају, приказују и преносе управо у електронском облику, прописи којима се регулишу њихово прикупљање, обрада и заштита имају велики значај за област сајбер безбедности. О њима ћемо писати у другом поглављу Извештаја.

Безбедност информација

Информациона безбедност

Велики значај у овој области имају прописи којима се регулишу основи информационог система Републике Србије и друга питања о вези примене информационо-комуникационих технологија у свакодневном животу (Закон о информационом систему Републике Србије (Службени гласник РС, бр. 12/96); Закон о дигиталној имовини (Службени гласник РС, број 153/20); Закон о ауторским и сродним правима (Службени гласник РС, бр. 104/09, 99/11, 119/12 и 29/16); Закон о електронским комуникацијама (Службени гласник РС, бр. 44/10, 60/13 и 62/14, 95/18); Закон о електронским медијима (Сл. гласник РС бр. 83/14, 6/16 - др. закон, 129/21), Закон о електронском потпису (Службени гласник РС, бр. 135/04);

Ипак, основни нормативни ослонац сајбер безбедности представљају одредбе којима се успоставља систем ране детекције и успешне превенције сајбер напада, уз додељивање јасних овлашћења и обавеза надлежним субјектима. Према томе, основу сајбер безбедности треба да чини пропис који успоставља темељ борбе против претњи у сајбер простору. Овим прописима се дефинишу и основе заштите података употребом информационо-комуникационих технологија (ИКТ), а стварају се и основе система превенције високотехнолошког криминала, барем када је реч о тежим облицима ове криминалне форме, тј. о вршењу високотехнолошких кривичних дела која за стварну последицу имају или могу имати повреду или угрожавање компоненти система националне безбедности.

У Србији је то Закон о информационој безбедности, донет 2016. године. Члановима 14 и 15. Закона прописано је успостављање Националног ЦЕРТ-а и одређене су његове надлежности, а сам начин вршења послове из надлежности Националног ЦЕРТ-а би требало да буде уређен посебним подзаконским актом. Предуслов за доношење тог општег правног акта и касније функционисање националног ЦЕРТ-а је дефинисање техничких, организационих и правних стандарда и процедура за обављање послове ЦЕРТ-а који су прописани чланом 15 овог Закона. Национални ЦЕРТ у складу са законским одредбама, требало би да прикупља и размењује информације о ризицима за безбедност ИКТ система, као и догађајима који угрожавају безбедност информационо-комуникационих система (ИКТ) и у вези тога обавештава, упозорава и саветује лица која управљају ИКТ системима у Републици Србији, као и јавност.

Ризици у области обраде и заштите података

Прикупљање, обрада, анализа, оцена и заштита информација и података, као и слободан јавни приступ одређеним подацима, представљају изазовну и комплексну материју за законодавно уређивање. У позитивном праву Републике Србије на снази је више закона који непосредно регулишу ову материју, уз низ подзаконских аката и

других прописа који се, посредно и/или делимично, баве питањима од значаја за област заштите података. Важну улогу имају и поједини акти међународног права.

Како год да се кроз историју називао и представљао, податак је био један од важних извора друштвене моћи. Познавање одређених чињеница, идеја и концепата који другима нису доступни, увек је пружало компаративну предност у различитим сферама живота. Такође, чување одређених информацију у тајности, тако да су доступне само ограниченом кругу субјеката, одувек је један од предуслова личне или колективне безбедности и сигурности.

Савремено доба, а посебно неслућен развој информационо-комуникационих технологија, доноси велике изазове на овом пољу. Могућности које пружа дигитална обрада података, њихова доступност и невероватна брзина преноса и дељења, створиле су ризике по људска права, имовинску и личну сигурност грађана, пословање корпорација па и саму националну и међународну безбедност. Речју, лакоћа, једноставност и комфор које је нам је пружио сајбер простор имају и „цену“ – изгледа високу.

Подаци у електронском облику неретко постају мета ловаца на незаконите профите. Они се купују, продају и на друге начине злоупотребљавају зарад стицања противправне имовинске користи. Такође, подаци се користе ради уцене, осветничке порнографије, увреде и клевете исл. Изложеност ризицима у сајбер простору очигледно је већа него у физичком свету, јер су подаци у физичком облику мање доступни, теже преносиви и компликованији за компромитацију. Наравно, обе форме представљања чињеница (дигитални и физички облик) заслужују и потребују правну заштиту, што је утицало на законодавце широм планете али и међународне организације да се позабаве овом проблематиком. Развој информационо-комуникационих технологија несумњиво је утицао на увођење нормативних новитета.

Подаци се могу класификовати на различите начине. Уколико као критеријум узмемо отвореност податка према јавности, можемо их класификовати на: отворене, податке о личности укључујући и личне тајне као и посебно осетљиве информације о личности, пословне тајне, професионалне тајне, тајне податке и информације од јавног значаја. (Мандић, Путник, Милошевић, 2017; Milošević, 2021). Наведена подела узима у обзир и правни оквир у Републици Србији, односно разврстава их сагласно законској уређености њиховог прикупљања, обраде, преноса и заштите. Полазећи од ње, представићемо казненоправи оквир заштите: тајних података; пословне и професионалне тајне; података о личности.

Казненоправна заштита тајних података у РС је уређена Законом о тајности података („Сл. гласник РС“, број 104/09; даље: ЗТП) и Кривичним закоником („Сл. гласник Републике Србије, бр. 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19; даље: КЗ). ЗТП је први домаћи закон који систематски уређује област одређивања, означавања, размене, чувања, обраде и заштите тајних података. (Матић, 2012; Лазић, 2017). Иако се према тајним подацима примењују посебно строге мере заштите, они су изложени различитим ризицима и претњама, посебно у доба високих технологија. (Маркагић, 2018).

Казнене одредбе ЗТП уводе кривичноправну и прекршајну заштиту. Члан 98 ЗТП прописује када постоји кривично дело против тајности података (иако законодавац не даје назив овом кривичном делу). (Ковачевић, Милошевић, 2022: 98). Кривично дело, у основном облику, је у чл. 98 ст. 1 ЗТП формулисано на следећи начин: „ко непозваном лицу саопшти, преда или учини доступним податке или документа који су му поверени или до којих је на други начин дошао или прибавља податке или документа, а који представљају тајне податке са ознаком тајности интерно или поверљиво, одређене према овом закону, казниће се затвором од три месеца до три године“.

Тежи облици су прописани у ст. 2 до 4. Облик из ст. 2 је присутан уколико је предмет извршења кривичног дела податак означен степеном тајности „строго поверљиво“ (запрећена казна од шест месеци до пет година затвора), док ст. 3 санкционише одавање податке класификованог као „државна тајна“ (од једне до десет година затвора). Ст. 4 уводи квалификовани облик који постоји ако је присутна једна од три предвиђене околности: користољубље, намера објављивања или коришћења тајних података у иностранству и извршење дела за време ратног или ванредног стања. Прописана казна зависи од степена тајности податка који представља предмет извршења, односно да ли је квалификаторна околност наступила при вршењу дела из ст. 1, 2 или 3. (Ковачевић, Милошевић, 2022: 98, 99). У најтежем случају, односно ако је при извршењу дела из чл. 98 ст. 3 наступила једна од три наведене околности, запрећена је казна од пет до петнаест година затвора. Ставом 5 овог члана је прописан и нехатни облик одавања тајног податка. Запрећена казна и овде зависи од степена тајности.

Ипак, још пре доношења ЗТП, постојала је кривичноправна заштита тајних података, у оквиру главног кривичног законодавства. КЗ прописује неколико кривичних дела којима се штите тајни подаци, али уз значајне терминолошке и суштинске разлике. Реч је кривичним делима: одавање државне тајне (чл. 316 КЗ); одавање војне тајне (члан 415 КЗ) и одавање службене тајне (чл. 369 КЗ). Ова дела, осим основних, имају и допунске облике (квалификоване и привилеговане). (Милошевић, 2022; Милошевић, 2022а).

Овде, међутим, настаје озбиљан проблем који се огледа у неусаглашености прописа. Члан 321 ст. 3 КЗс прописује казну од најмање десет година затвора или доживотни затвор уколико су дела из чл. 314 до 319 КЗ учињена за време ратног или ванредног стања или оружаног сукоба. Али чл. 316 ст. 3 предвиђа казну од три до петнаест година затвора за идентично понашање (одавање државне тајне током ратног или ванредног стања односно оружаног сукоба). Који од два прописана распоне казне важи? По кривичноправним принципима, важио би блажи распон казне, али је заиста тешко разумети зашто законодавац једноставно не отклони ову неусаглашеност. (Милошевић, 2010; Ковачевић, Милошевић, 2022). Имајући у виду да и чл. 98 ст. 3 прописује трећи распон казне за садржински исто понашање, проблем постаје још озбиљнији (иако се у овом случају може бранити став да оодредбе ЗТП важе само за податке који су категорисани по одредбама тог закона, док КЗ важи за „старе“ податке).

Осим кривичноправне, законодавац прописује и прекршајну одговорност за неправилно поступање са тајним подацима. Чл. 99 ст. 1 тач. 1 до 17 ЗТП прописује прекршајне санкције за одговорно лице у органу јавне власти. Прописана новчана казна

је између 5.000 и 50.000 динара. Прекршаји из наведених тачки обухватају разноврсне радње извршења, попут: преношења овлашћења за одређивање тајног податка на треће лице; неправилно означавање податка или документа степеном тајности (иако нису испуњени услови); означавање податка неодговарајућим степеном тајности; доношење одлуке од одређивању степена тајности без образложења; неопозивање тајности податка након: истека законског рока, наступања датума или догађаја после кога престаје тајност податка, доношења решења Повереника за информације од јавног значаја и заштиту података о личности или одлуке надлежног суда о опозиву тајности; непрописивање општих и посебних мера заштите података у складу са одређеним степеном тајности, као и пропуштање да се оне организују и надзиру; неспровођење периодичне процене тајности податка; неорганизовање унутрашње контроле над заштитом тајних података; невођење евиденције о издатим сертификатима за приступ тајном податку, итд.

Према чл. 100 ЗТП исти распон новчане казне је прописан за руковаоца тајним подацима који не предузима мере заштите таних података у складу са чл. 34 истог закона. Према том члану, руковалац је дужан да: „предузима мере заштите тајних података и омогућава корисницима непосредан приступ тајним подацима, издаје копију документа који садржи тајни податак, води евиденцију корисника и стара се о размени тајних података“. (ЗТП, чл. 34).

Казненоправна заштита пословне тајне је предвиђена одредбама КЗ и Закона о заштити пословне тајне („Сл. гласник РС“, број 53/21; даље: ЗЗПТ). За разлику од тајних података, код пословне тајне је јасно разграничено да се кривичноправна заштита обезбеђује одредбама КЗ, док су прекршајна и привреднопреступна у оквирима посебног закона (ЗЗПТ). Пословна тајна је податак од великог значаја у савременој тржишној привреди, заснованој на иновацијама, истраживању и технолошком развоју. (Jovičić, 2018; Милошевић, 2022).

Важан међународни извор права у овој области је Директива 2016/943 Европског парламента и Савета од 8. јуна 2016. године, о заштити неоткривених знања и искуства те пословних информација (пословне тајне) од незаконитог прибављања, употребе и откривања, Службени лист ЕУ Л бр. 157/1. На глобалном плану значајан је тзв. ТРИПС споразум. (Споразум о трговинским аспектима права интелектуалне својине (The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Светска трговинска организација, 1994 (ступио на снагу 1995. године). Текст доступан на: https://www.zis.gov.rs/upload/documents/pdf_sr/pdf/trips.pdf (приступљено 31.05.2022. године). У РС је до 2021. године важио закон истог назива (Закон о заштити пословне тајне, „Сл. гласник РС“, број 72/11), али је потреба за хармонизацијом са Директивом ЕУ условила доношење новог закона.

Кривично дело одавања пословне тајне је прописано одредбама чл. 240 КЗ. Основни облик (чл. 240 ст. 1 КЗ) постоји када извршилац непозваном лицу неовлашћено саопшти, преда или учини доступним податке који представљају пословну тајну, као и уколико прикупља такве податке у намери да их преда непозваном лицу. Запрећена је казна затвора од шест месеци до пет година затвора.

Важан недостатак формулације основног облик, како се наводи у литератури, је што њоме нису обухваћене радње незаконитог прибављања пословне тајне од стране трећег

лица. Инкриминисано је одавање пословне тајне, које учини њен законити држалац, тако што је открије непозваном лицу. Али, ако би непозвано лице само прибавило пословну тајну, и то на незаконит начин, он се не би могло сматрати извршиоцем овог кривичног дела, већ би сносило само грађанскоправну и прекршајну (у појединим случајевим привреднопреступну) одговорност. (Милошевић, 2022: 130, 131; Miloševi ć, 2021a: 60; Пресуда Основног суда у Нишу, К 65/14 од 23.04.2014. године).

Тежи облик (чл. 240 ст. 2 КЗ) постоји уколико је дело учињено из користољубља или у погледу нарочито поверљивих података. Предвиђена је казна од две до десет година затвора уз новчану казну (кумулативно). Законодавац је предвидео, објективно гледајући, веома строгу казну за квалификовани облик одавања пословне тајне. Иначе, и у погледу тежег облика се може упутити једна критика. Није јасно, наиме, зашто законодавац није као квалификаторну околност предвидео ситуацију у којој учинилац одаје пословну тајну ради њеног коришћења у иностранству (тзв. индустријска шпијунажа). Ово решење је било присутно у ранијем кривичном законодавству. (Милошевић, 2022: 133; Срзентић и др., 1986: 459, 460).

Привилеговани облик постоји у случају одавања пословне тајне из свесног или несвесног нехата. Запрећена је казна до три године затвора. Овај облик је значајан и због превенције криминалног понашања у сфери заштите конкуренције и пословне тајне, као и ради јачања корпоративне безбедносне културе и свести. (Мандић, Путник, Милошевић, 2017; Miloševi ć, 2021a).

Прекршајна и привреднопреступна одговорност је регулисана одредбама ЗЗПТ. Члан 21 ЗЗПТ прилично широком формулацијом прописује јединствену радњу извршења прекршаја и привредног преступа против пословне тајне. Да ли ће извршилац одговарати за привредни преступ или прекршај зависи од његовог правног статуса и субјективитета – уколико је реч о одговорном лицу у правном лицу или самом правном лицу, дело се квалификује као привредни преступ; у случају да је обележја остварило физичко лице или предузетник, у питању је прекршај. Прописана је и мера обавезног одузимања, односно уништења предмета извршења привредног преступа или прекршаја (ЗЗПТ, чл. 1 ст. 5).

Радња је прописана одредбом чл. 21 ст. 1 ЗЗПТ и гласи: „Казниће се за привредни преступ новчаном казном у износу од 100.000 до 3.000.000 динара правно лице које у складу са чланом 4. овог закона незаконито прибави, користи или открије пословну тајну“. Ст. 2 до 4 прецизирају субјекте дела и тип казненог деликта: ст. 2 одређује привреднопреступну новчану казну од 50.000 до 200.000 динара за одговорно лице у правном лицу; ст. 3 прописује прекршајну новчану казну за предузетника у износу од 50.000 до 500.000 динара; док ст. 4 садржи запрећену прекршајну казну за физичко лице у износу од 20.000 до 150.000 динара.

Казненоправна заштита података о личности изгледа овако. Подаци о личности су постали важан предмет правне заштите последњих година. (Prlja, 2018: 89-90; Дилигенски и ост., 2018). Од великог значаја за развој ове материје било је доношење чувеног GDPR – Опште уредбе ЕУ о заштити података о личности (Општа Уредба (ЕУ) 2016/679 Европског парламента и Савета од 27. априла 2016. године о заштити физичких лица у односу на обраду података о личности, и о слободном кретању таквих података и о стављању Директиве 95/46/ЕЗ ван снаге; даље: Општа уредба ЕУ). Она је

заменила Директиву ЕУ из 1995. године. (Директива ЕУ о заштити грађана у вези са обрадом података о личности и о слободном кретању таквих података 1995/46).

Казненоправна заштита података о личности је уведена одредбама КЗ и Закона о заштити података о личности („Сл. гласник РС“, број 87/18; даље: ЗЗПЛ), који је донет по угледу на Општу уредбу ЕУ. Пре доношења овог закона, важио је претходни, истог назива (Закон о заштити података о личности, „Сл. гласник РС“, бр. 97/08, 104/09, 68/12 и 107/12) , али је потреба за усаглашавањем са европском регулативом довела до законодавних промена. Почнимо, ипак, од кривичноправне заштите.

У КЗ се налази више кривичних дела чија је предмет извршења податак о личности, иако се законски назив само једне инкриминације непосредно односи на ову материју (чл. 146 КЗ – неовлашћено прикупљање личних података). У литератури се истиче: „Анализа кривичноправних норми којима се штити право на заштиту података о личности треба да обухвати сва релевантна кривична дела, чијом радњом извршења може бити примарно повређено ово право. Осим дела из члана 146, то су и: неовлашћено откривање тајне (члан 141); прогањање (члан 138а став 1 тачка 3), повреда тајности писма (члан 142); неовлашћено прислушкивање и снимање (члан 143); неовлашћено фотографисање (члан 144) и неовлашћено објављивање и приказивање туђег списа, поретрета и снимка (члан 145); па и кривично дело изношења личних и породичних прилика (члан 172), а можда и друга“. (Милошевић, 2021: 117).

Уско посматрано, једино кривично дело које се по називу и садржину у потпуности односи на материју заштите података о личности је неовлашћено прикупљање података о личности. Основни облик дела је присутан када се подаци о личности који се прикупљају и обрађују на основу закона неовлашћено прибаве, саопште другим или употребе у сврху за коју нису намењени (КЗ. Чл. 146 ст. 1). Чл. 146 ст. 2 одређује да је кривично дело и када учинилац противно закону прибавља личне податке или користи незаконито прикупљене податке. За оба облика је прописана казна до једне године затвора алтернативно са новчаном казном. (Делић, 2021; Стојановић, 2018).

Гоњење се предузима по приватној тужби, што указује да је кривичноправна заштита личних података секундарна. (Милошевић, 2021: 119). Једино се квалификовани облик из става 3, за који је запрећена новчана казна или затвор до три године, гони по службеној дужности.

Прекршајна заштита је обезбеђена одредбама ЗЗПЛ. Слично као и код пословне тајне, мада у мањој мери, јавља се проблем разграничења радње прекршаја и радње кривичног дела. Казнене одредбе су смештене у оквире члана 95 ЗЗПТ. Ставом 1 је прописан низ алтернативних радњи за чије извршење одговарају руковаоци и обрађивачи у зависности од својства: за правна лица запрећена је казна од 50.000 до 2.000.000 динара; за предузетнике од 20.000 до 500.000 динара (чл. 95 ст. 4 ЗЗПЛ); за физичко лице, односно одговорно лице у правном лицу, државном органу, органу територијалне аутономије и јединици локалне самоуправе, представништву или пословној јединици страног правног лица од 5.000 до 150.000 динара (чл. 95 ст. 5 ЗЗПЛ).

Законодавац набраја чак 32 алтернативне радње извршења прекршаја у ставу 1. Међу тим радњама се налазе и оне које се у претежном делу, па чак и у потпуности

преклапају са радњом кривичног дела (нпр. ако руковалац или обрађивач обрађује податке у другу сврху; уколико обрађује податке о личности без сагласности лица на које се подаци односе, а није у могућности да предочи да је лице на које се подаци односе дало пристанак за обраду својих података; обрађује податке о личности у сврхе архивирања у јавном интересу, у сврхе научног или историјског истраживања или у статистичке сврхе супротно члану 92 ЗЗПЛ; врши пренос података о личности у друге земље и међународне организације супротно закону).

Чл. 95 ст. 2 ЗЗПЛ прописује други (лакши) облик прекршаја, за који је прописана фиксна новчана казна од 100.000 динара за руковаоца односно обрађивача у својству правног лица (казна за предузетника је 50.000 динара, а за одговорна лица у правим лицима и органима јавне власти 20.000 динара). Прописано је 6 алтернативних радњи извршења, међу којима су: када руковалац (обрађивач) не одреди свог представника у Републици Србији; или не води прописане евиденције о обради или не бележи радње обраде; не објави контакт податке лица за заштиту података о личности и не достави их Поверенику; не упозна примаоца са посебним условима за обраду података о личности прописним законом и његовом обавезом испуњења тих услова.

Посебан облик прекршаја је прописан у чл. 95 ст. 3. Радња овог прекршаја је остварена када учинилац не чува као професионалну тајну податке о личности које је сазнао током обављања послова. Извршилац може да буде физичко лице, а прописана је новчана казна од 5.000 до 150.000 динара. Ипак, овде се поставља питање судара са одговорношћу за кривично дело неовлашћеног откривања тајне из чл. 141 КЗ, посебно у светлу процесног правила ne bis in idem. (Милошевић, 2021: 132; Zupančič, 2011; Ivičević-Karas, Kos, 2012). Код дела из чл. 141 КЗ се као извршилац, осим адвоката и лекара, помиње и друго лице које је сазнало за тајну у вршењу свог позива. Дакле, предмет заштите је у оба случаја професионална тајна, а извршиоци могу да постану лица која су задужена за испуњавање законских обавеза руковаоца и обрађивача података о личности.

Списак изабраних прописа и препоручена литература

Закон о тајности података („Сл. гласник РС“, број 104/09)

Уредба о ближим критеријумима за одређивање степена тајности "ДРЖАВНА ТАЈНА" и "СТРОГО ПОВЕРЉИВО" (Сл. гласник РС бр. 46/13)

Уредба о ближим критеријумима за одређивање степена тајности "ПОВЕРЉИВО" и "ИНТЕРНО" у Безбедносно-информативној агенцији (Сл. гласник РС бр. 70/13)

Уредба о ближим критеријумима за одређивање степена тајности "ПОВЕРЉИВО" и "ИНТЕРНО" у Канцеларији Савета за националну безбедност и заштиту тајних података (Сл. гласник РС бр. 86/13)

Уредба о ближим критеријумима за одређивање степена тајности "ПОВЕРЉИВО" и "ИНТЕРНО" у Министарству одбране (Сл. гласник РС бр. 66/14)

Уредба о ближим критеријумима за одређивање степена тајности "ПОВЕРЉИВО" и "ИНТЕРНО" у Министарству унутрашњих послова (Сл. гласник РС бр. 105/13)

Уредба о ближим критеријумима за одређивање степена тајности "ПОВЕРЉИВО" и "ИНТЕРНО" у органима јавне власти (Сл. гласник РС бр. 79/14)

Уредба о начину и поступку означавања тајности података, односно докумената (Сл. гласник РС бр. 8/11)

Уредба о обрасцима безбедносних упитника (Сл. гласник РС бр. 30/10)

Уредба о посебним мерама физичко-техничке заштите тајних података (Сл. гласник РС бр. 97/11)

Уредба о посебним мерама надзора над поступањем са тајним подацима (Сл. гласник РС бр. 90/11)

Уредба о посебним мерама заштите тајних података које се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа (Сл. гласник РС бр. 63/13)

Уредба о посебним мерама заштите тајних података у информационо-телекомуникационим системима (Сл. гласник РС бр. 53/11)

Уредба о садржини, облику и начину достављања сертификата за приступ тајним подацима (Сл. гласник РС бр. 54/10)

Уредба о садржини, облику и начину вођења евиденција за приступ тајним подацима (Сл. гласник РС, број 89/10).

Закон о заштити пословне тајне („Сл. гласник РС“, број 53/21).

Директива 2016/943 Европског парламента и Савета од 8. јуна 2016. године, о заштити неоткривених знања и искуства те пословних информација (пословне тајне) од незаконитог прибављања, употребе и откривања, Службени лист ЕУ Л бр. 157/1

Споразум о трговинским аспектима права интелектуалне својине (The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Светска трговинска организација, 1994 (ступио на снагу 1995. године). Текст доступан на: https://www.zis.gov.rs/upload/documents/pdf_sr/pdf/trips.pdf (приступљено 31.05.2021. године).

Закон о заштити података о личности („Сл. гласник РС“, број 87/18)

Закон о евиденцијама и обради података у области унутрашњих послова (Сл. гласник РС бр. 24/18)

Правилник о обрасцу и начину вођења евиденције лица за заштиту података о личности (Сл. гласник РС бр. 40/19)

Правилник о обрасцу и начину вођења интерне евиденције о повредама Закона о заштити података о личности и мерама које се у вршењу инспекцијског надзора предузимају (Сл. гласник РС бр. 40/19)

Правилник о обрасцу обавештења о повреди података о личности и начину обавештавања Повереника за информације од јавног значаја и заштиту података о личности о повреди података о личности (Сл. гласник РС бр. 40/19)

Правилник о обрасцу притужбе (Сл. гласник РС бр. 40/19)

Одлука о Листи држава, делова њихових територија или једног или више сектора одређених делатности у тим државама и међународних организација у којима се сматра да је обезбеђен примерени ниво заштите података о личности (Сл. гласник РС бр. 55/19)

Одлука о листи врста радњи обраде података о личности за које се мора извршити процена утицаја на заштиту података о личности и тражити мишљење Повереника за информације од јавног значаја и заштиту података о личности (Сл. гласник РС бр. 45/19, 112/20)

Одлука о утврђивању Стандардних уговорних клаузула (Сл. гласник РС бр. 5/20)

Директива ЕУ о заштити грађана у вези са обрадом података о личности и о слободном кретању таквих података 1995/46

Општа Уредба (ЕУ) 2016/679 Европског парламента и Савета од 27. априла 2016. године о зашти-ти физичких лица у односу на обраду података о личности, и о слободном кретању таквих података и о стављању Директиве 95/46/ЕЗ ван снаге.

Закон о слободном приступу информацијама од јавног значаја („Сл. гласник РС“, бр. 120/04, 54/07, 104/09, 36/10, 105/21)

Закон о информационој безбедности (Сл. гласник РС, бр. 6/16, 94/17, 77/19)

Уредба о безбедности и заштити деце при коришћењу информационо-комуникационих технологија (Сл. гласник РС бр. 13/20)

Уредба о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја (Сл. гласник РС бр. 94/16)

Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја (Сл. гласник РС бр. 94/16)

Уредба о криптобезбедности и заштити од компромитујућег електромагнетног зрачења (Сл. гласник РС бр. 57/19)

Уредба о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја (Сл. гласник РС бр. 11/20)

Уредба о утврђивању Листе делатности у областима у којима се обављају делатности од општег интереса и у којима се користе информационо-комуникациони системи од посебног значаја (Сл. гласник РС бр. 94/19)

Правилник о подацима које садржи евиденција оператора информационо-комуникационих система од посебног значаја (Сл. гласник РС бр. 9/20)

Правилник о садржају, начину уписа и вођења евиденције посебних центара за превенцију безбедносних ризика у информационо-комуникационим системима (Сл. гласник РС бр. 37/20)

Правилник о врсти, форми и начину достављања статистичких података о инцидентима у информационо-комуникационим системима од посебног значаја (Сл. гласник РС бр. 76/20)

Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, Службени гласник Републике Србије бр. 61/05, 104/09.

Закон о потврђивању Конвенције о високотехнолошком криминалу, Службени гласник Републике Србије број 19/09

Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкрими- нацију дела расистичке и ксенофобичне природе извршених преко рачунарских система, Службени гласник Републике Србије број 19/09.

Закон о одговорности правних лица за кривична дела, Службени гласник Републике Србије, број 97/08.

Кривични законик Републике Србије, Службени гласник РС бр. 85/2005, 88/2005 – испр., 107/2005 – испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 , 94/16, 35/19.

Законик о кривичном поступку, Сл. гласник РС, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021

Закон о ауторским и сродним правима (Службени гласник РС, бр. 104/09, 99/11, 119/12 и 29/16)

Закон о Безбедносно-информативној агенцији, (Сл. гласник РС", бр. 42/2002, 111/2009, 65/2014 - одлука УС и 66/2014)

Закон о војнобезбедносној агенцијији и војнообавештајној агенцији (Сл. гласник РС", бр. 88/2009, 55/2012 - одлука УС и 17/2013)

Закон о електронским комуникацијама (Службени гласник РС, бр. 44/10, 60/13 и 62/14)

Закон о електронском потпису (Службени гласник РС, бр. 135/04)

Закон о информационом систему Републике Србије (Службени гласник РС, бр. 12/96)

Bing, C. (2021). Exclusive: U.S. to give ransomware hacks similar priority as terrorism. Available at: https://www.reuters.com/technology/exclusive-us-give-ransom- ware-hacks-similar-priority-terrorism-official-says-2021-06-03/

Bischoff, P. (2021). Ransomware attacks on US healthcare organizations cost $20.8bn in 2020. Available at: https://www.comparitech.com/blog/information-security/ran- somware-attacks-hospitals-data/

Collier, R. (2017). NHS ransomware attack spreads worldwide. Canadian Medical Association Journal, 189(22), 786-787

Coveware. (2021). Available at: https://www.coveware.com/ransomware-blog

Davis, J. (2020). UPDATE: The 10 Biggest Healthcare Data Breaches of 2020. Available at: https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020

Đorđević, Đ. (2014). Criminal Law – a Special Part, 3rd edition. Beograd: Kriminalističko-policijska akademija [In Serbian]

Fruhlinger, J. (2020). Ransomware explained: How it works and how to remove it. Available at: https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works- and-how-to-remove-it.html

Global Economic Crisis (2013). Available at: https://www.sciencedirect.com/topics/economics-econometrics-and-finance/global-economic-crisisВилић, В. (2016). Повреда права на приватност злоупотребом друштвених мрежа као облик компјутерског криминалитета, докторска дисертација. Правни факултет Универзитета у Нишу, Ниш.

Ђорђевић, Ђ. (2014). Кривично право – посебни део. Криминалистичко-полицијска академија, Београд.

Janczewski, L., Colarik, A. (2008). Cyber Warfare and Cyber Terrorism. Hershey, New York.

Knowem (2019). https://knowem.com, доступан 15. 5. 2019.

Kovačević, A., Putnik, N. & Tošković, O. (2020). Factors Related to Cyber Security Behaviour. IEEE Access, 8, 125140-125148. doi: 10.1109/ACCESS.2020.3007867

Мандић, Г., Путник, Н., Милошевић, М. (2017). Заштита података и социјални инжењеринг – правни, организациони и безбедносни аспекти. Универзитет у Београду - Фа- култет безбедности, Београд.

Mathew, T. (2004). Ethical Hacking and Countermeasures [EC-Council Exam 312-50] — Student Courseware. OSB Pub- lisher, International Council of Electronic Commerce Consul- tants, New York.

Милошевић, М. (2012). Одговорност правних лица за кривична дела, докторска дисертација. Правни факултет Универзитета у Београду, Београд.

Милошевић, М. (2012а). Кривична одговорност правних лица у англоамеричком праву. Страни правни живот, 56(2): 230–251.

Милошевић, М., Симовић, И. (2018). Појам одговорног лица у Закону о одговорности правних лица за кривична дела. У: Кривично законодавство и функционисање правне државе, међународна научно-стручна конференција, стр. 365–382. Требиње, 20. и 21. 04. 2018. године, Министарство правде Републике Српске, Српско удружење за кривичноправну теорију и праксу, Град Требиње.

Милошевић, М. (2022). Кривично право – посебни део: изабране инкриминације за студије наука безбедности. Београд: Универзитет у Бео раду-Факултет безбедности.

Мирић, Ф. (2018). Интернет превара као облик компјутер- ског криминалитета. Зборник радова Правног факултета у Нишу, 57(80), 531–542.

Phishing without borders, or why you need to update your router (2019)https://www.kaspersky.com/blog/hacked-routers- dns hijacking/26802/?utm_source=facebook&utm_medium=social&utm_campaign=rs_hacked-routers-dns hijacking_ma0111_organic&utm_content=sm-post&utm_term=rs_facebook_organic_ma0111_sm- post_social_hacked-routers-dns-

hijacking, доступан 14. 5. 2019.

Путник, Н., Милошевић, М. (2016). Смернице за израду по- литике безбедности информационо-комуникационих ресурса и њихових корисника у образовно-васпитном систему“. У зборнику (приредили: Бранислава Поповић Ћитић, Ми- лан Липовац): Безбедност у образовно-васпитним устано- вама: основна начела, принципи, протоколи, процедуре и средства. стр. 97–116. Факултет безбедности, Београд.

Путник, Н., Милошевић, М., & Цветковић, В. (2022). Рансомвер као претња безбедности - друштвени и кривичноправни аспекти. Социолошки преглед, 56(1), 328-353. DOI: https://doi.org/10.5937/socpreg56-36845.

Rittinghouse, J., Hancock, W. (2003). Cybersecurity Operations Handbook. Elsevier, Burlington.

Shinder, D. L. (2002). Scene of the Cybercrime: Computer Forensics Handbook. Syngress Publishing, Inc., Rockland.

Skoudis, E. (2002). Counter Hack: A Step-By-Step Guide to Computer Attacks and Effective Defenses. Prentice Hall, New Jersey.

Стојановић, З. (2012). Коментар Кривичног законика. Службени гласник, Београд.

Стојановић, З., Делић, Н. (2015). Кривично право – посебни део, Правна књига, Краљево.

Findface (2019). https://findface.ru, доступан 19. 5. 2019.

How cybercriminals harvest information for spear phishing (2019). https://www.kaspersky.com/blog/spearphishers-infor- mation/25589, доступан 18. 5. 2019.

Šta je DNS i koji je najbrži DNS? (2018). https://balkanandroid.com/sta-je-dns-i-koji-je-najbrzi-dns, дос- тупан 14. 5. 2019.

Beran, T. N., Li, Q. (2005). Cyber-harassment: A study of a new method for an old behavior. Journal of Educational Computing Research, 32(3), 265-277.

Вучинић З. (2001). Међународно ратно и хуманитарно право. Београд: Војноиздавачки завод.

Gross, E. F., Juvonen, J., Gable, S. L. (2002). Internet use and well-being in adolescence. Journal of Social Issues, 58(1), 75-90.

Милошевић, М., Путник, Н. (2014). Проблем правне (не)регулисаности конфликата у кибер простору, Трећи програм, ISSN 0564-7010, свеска бр. 162 (2/2014)

Младеновић, Д. (2012). Међународни аспект сајбер ратовања. Београд: Медија центар „Одбрана“.

Melzer, N. (2011). Cyberwarfare and International Law. UN UNIDIR .

National Crime Prevention Council (2006). Cyberbullying. http://www.ncpc.org/cyberbullying

Одлука Уставног суда РС, ИУз -1218/2010, од 19.04.2012. године, објављена у Службеном гласнику РС, бр. 88/09.

Одлука Уставног суда РС, ИУз -252/2002, од 26. децембра 2013. године, објављена у Службеном гласнику РС, бр. 65/2014.

Путник, Н. (2009). Сајбер простор и безбедносни изазови. Београд: Факултет безбедности.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. The Journal of Child Psychology and Psychiatry and Allied Disciplines, 49(4), 376-385.

Стратегија развоја информационог друштва у Републици Србији до 2020. године, Службени гласник Републике Србије број 51/2010

Tallinn Manual on the International Law Applicable to Cyber Warfare, Michael N. Schmitt (Ed.). Cambridge, New York: Cambridge University Press, 2013.

Урошевић, В., Ивановић, З., Уљанов, С. (2012). Мач у world wide web-у. Београд: Eternal mix,

Ризици од катастрофа

Најважнији пропис у области смањења ризика од катастрофа и управљања ванредним ситуацијама је Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама (Сл. гласник РС бр. 87/18). Доношењем овог закона престао је да важи Закон о ванредним ситуацијама (Сл. гласник РС бр. 111/2009, 92/2011 и 93/2012). Систем смањења ризика од катастрофа и управљања ванредним ситуацијама је од посебног интереса за Републику Србију и представља део система националне безбедности, па је значај овог прописа изразито велики, посебно имајући у виду да се савремени свет суочава са катастрофама изазваним елементарним непогодама, техничко-технолошким несрећама, ратним разарањима и терористичким нападима, због чега се у литератури истиче да ће 21. век, по свему судећи, бити ера терористичких напада и природних катастрофа.

Овим законом уређују се:

- смањење ризика од катастрофа, превенција и јачање отпорности и спремности појединаца и заједнице за реаговање на последице катастрофа, заштита и спасавања људи, материјалних, културних и других добара
- права и обавезе грађана, удружења, правних лица, органа јединица локалне самоуправе, аутономних покрајина и Републике Србије,
- управљање ванредним ситуацијама

- функционисање цивилне заштите, рано упозоравање, обавештавање и узбуњивање
- међународна сарадња, инспекцијски надзор и друга питања од значаја за организовање и функционисање система смањења ризика од катастрофа и управљања ванредним ситуацијама.

Закон дефинише најважније појмове у области смањења ризика од катастрофа и управљања ванредним ситуацијама. Елементарна непогода је појава хидролошког, метеоролошког, геолошког или биолошког порекла, проузрокована деловањем природних сила као што су земљотрес, поплава, бујица, олуја, јака киша, атмосферска пражњења, град, суша, одроњавања или клизања земљишта, снежни наноси и лавина, екстремне температуре ваздуха, нагомилавања леда на водотоку, пандемија, епидемија заразних болести, епидемија сточних заразних болести и појава штеточина и друге природне појаве већих размера које могу да угрозе безбедност, живот и здравље већег броја људи, материјална и културна добра или животну средину у већем обиму.

Техничко-технолошка несрећа је изненадни и неконтролисани догађај или низ догађаја који је измакао контроли приликом управљања одређеним средствима за рад и приликом поступања са опасним материјама у производњи, употреби, транспорту, промету, преради, складиштењу и одлагању, као што су пожар, експлозија, хаварија, саобраћајни удес у друмском, речном, железничком и ваздушном саобраћају, удес у рудницима и тунелима, застој рада жичара за транспорт људи, рушење брана, хаварија на електроенергетским, нафтним и гасним постројењима, акциденти при руковању радиоактивним и нуклеарним материјама, тешко загађење земљишта, воде и ваздуха, последице ратног разарања и тероризма, а чије последице могу да угрозе безбедност, живот и здравље већег броја људи, материјална и културна добра или животну средину у већем обиму.

Катастрофа представља елементарну непогоду или техничко-технолошку несрећу чије последице угрожавају безбедност, живот и здравље већег броја људи, материјална и културна добра или животну средину у већем обиму, а чији настанак или последице није могуће спречити или отклонити редовним деловањем надлежних органа и служби. Дакле, катастрофа се од осталих елеменатрних непогода и несрећа разликује по степену могућности надлежних органа и служби да настнак или последице држе под контролом, тако да катастрофа наступа онда када настанак или последице непогода или несрећа није могуће у потпуности спречити (попут поплава у Србији 2014. године, разорних земљотреса, одрона, клизишта и ерозија, великих епидемија, последица великих терористичких аката итд.).

Ванредна ситуација је стање које настаје проглашењем од надлежног органа када су ризици и претње или настале последице по становништво, животну средину и материјална и културна добра таквог обима и интензитета да њихов настанак или последице није могуће спречити или отклонити редовним деловањем надлежних органа и служби, због чега је за њихово ублажавање и отклањање неопходно употребити посебне мере, снаге и средства уз појачан режим рада.

Иако су дефиниције ванредне ситуације и катастрофа веома сличне, треба уочити да је ванредна ситуација првенствено правно стање, које се проглашава од стране надлежног

органа, када ризике, претње или последице катастрофа или елементарних непогода није могуће контролисати. Дакле, наступање катастрофе је чињеница (попут избијања неконтролисасних шумских пожара, на пример) која постоји независно од проглашавања ванредне ситуације. Ванредна ситуација је правно стање којим се активира посебан режим рада надлежних органа и додељују им се одређена овлашћења и обавезе у циљу отклањања или умањења последица елеменатрних и других непогода, укључујући и катастрофе.

Ванредна ситуација се проглашава одмах по сазнању за непосредну опасност од њеног наступања. Ванредна ситуација може бити проглашена и након њеног наступања, ако се непосредна опасност од наступања ванредне ситуације није могла предвидети или ако због других околности није могла бити проглашена одмах после сазнања за непосредну опасност од њеног наступања. Ванредна ситуација се укида престанком опасности, односно престанком потребе за спровођењем мера заштите и спасавања од катастрофа.

Ванредну ситуацију проглашава и укида:

1) за територију Републике Србије - Влада, на предлог Републичког штаба за ванредне ситуације;

2) за територију аутономне покрајине - извршни орган аутономне покрајине, на предлог покрајинског штаба за ванредне ситуације;

3) за територију дела града или града - градоначелник, на предлог градског штаба за ванредне ситуације;

4) за територију градске општине - председник градске општине, на предлог штаба за ванредне ситуације градске општине;

5) за територију дела општине или општине - председник општине, на предлог општинског штаба за ванредне ситуације.

Ванредна ситуација за територију аутономне покрајине се проглашава када постоји непосредна опасност која ће захватити, или је већ захватила најмање две јединице локалне самоуправе са територије надлежности, а процена је таква да ће се опасност или њене последице ширити и да су капацитети аутономне покрајине довољни за спречавање, отклањање, односно ублажавање последица.

Ванредна ситуација за територију Републике Србије проглашава се када постоји непосредна опасност која ће захватити, или је већ захватила најмање две јединице локалне самоуправе, а процена је таква да ће се опасност или њене последице ширити и да се сви капацитети Републике Србије морају ангажовати за спречавање, отклањање, односно ублажавање последице.

Смањење ризика од катастрофа и управљање ванредним ситуацијама је комплексан и вишеслојан задатак, који не може бити предмет рада и надлежности једног државног органа, већ захтева комплементарно учешће низа државних и недржавних актера. Сви актери система смањења ризика од катастрофа и управљања ванредним ситуацијама се називају субјекти система заштите и спасавања.

Државни субјекти система заштите и спасавања имају шира овлашћења и веће обавезе у односу на недржавне актере. Влада Републике Србије обезбеђује изградњу, развој и

планско повезивање делова система и задатака у јединствену целину, усмерава и усклађује рад органа државне управе на спровођењу мера и активности смањења ризика од катастрофа и управљања ванредним ситуацијама и доноси акте у складу са законом, што јој даје улогу централног стратешког координатора система. Ипак, водећу улогу у оперативном и тактичком смислу има Министарство унутрашњих послова, коме закон поверава најважније и најтеже задатке у области заштите и спасавања и одређује га као чворишну тачку система. У склопу МУП-а формиран је Сектор за ванредне ситуације, као посебна организациона јединица, првенствено задужена за област смањења ризика од катастрофа и управљање ванредним ситуацијама. Формирање јединствене службе за ванредне ситуације у оквиру МУП-а РС одобрено је на седници Владе Републике Србије у марту 2009. године.

У оквиру Сектора налазе се организационе јединице задужене за поједине послове и задатаке у систему заштите и спасавања - Управа за превентивну заштиту, Управа за ватрогасно-спасилачке јединице и цивилну заштиту, Управа за управљање ризиком и подручне управе и одељења, која имају нецентралну (локалну) надлежност, на нивоу градова и/или општина (управе су у Београду, Новом Саду, Нишу и Крагујевцу, а у осталим градовима и општинама ове организационе јединице носе назив одељења). Укупно, Сектор располаже са 4 подручне управе и 23 подручна одељења.

Осим МУП-а, важну улогу у систему заштите и спасавања има и Министарство одбране. У условима када друге снаге и средства система нису довољне за заштиту и спасавање људи, материјалних и других добара од последица катастрофа, на захтев Републичког штаба за ванредне ситуације, Министарство одбране обезбеђује учешће својих организационих јединица, команди, јединица и установа Војске Србије за пружање помоћи у заштити и спасавању, у складу са законом, осим у ратном и ванредном стању.

Остала министарства и органи државне управе правовремено извештавају МУП о уоченим појавама и проблемима од значаја за ову област, као и о подацима од значаја за процену постојећих ризика, о појави нових ризика и претњи и о другим чињеницама; планирају, организују и обезбеђују функционисање своје делатности у ванредним ситуацијама; учествују у изради Стратегије, Националног плана смањења ризика од катастрофа, Плана заштите и спасавања Републике Србије и других планских и програмских докумената; учествују у изради Процене ризика од катастрофа Републике Србије и врше друге послове у складу са законом.

Веома битна улога поверена је и локалним/нецентралним органима власти. Аутономна покрајина, између осталог, доноси акт о организацији и функционисању цивилне заштите на терисвојој територији ии обезбеђује њено спровођење; планира и обезбеђује буџетска средства намењена за смањење ризика од катастрофа и управљање ванредним ситуацијама; образује покрајински штаб за ванредне ситуације и врши бројне друге послове у овој области.

Јединице локалне самоуправе (градови и општине) имају бројне задатке и послове, међу којима су следећи: доносе акт о организацији и функционисању цивилне заштите на својој територији; израђују и доносе процену ризика, локални план смањења ризика од катастрофа, план заштите и спасавања и екстерни план заштите од великог удеса уколико се на територији налази СЕВЕСО комплекс вишег реда; образују штаб за

ванредне ситуације; одређују субјекте од посебног значаја за заштиту и спасавање јединице локалне самоуправе на предлог надлежног штаба; планирају и обезбеђују буџетска средства намењена за смањење ризика од катастрофа и управљање ванредним ситуацијама; образују јединице цивилне заштите, итд.

И недржавни актери имају улоге и задатке у систему смањења ризика од катастрофа. Свако привредно друштво и друго правно лице дужно је да, у оквиру своје делатности предузима све мере превенције и смањења ризика, као и да се одазове захтеву надлежног штаба и узме учешће у спровођењу мера заштите и спасавања. Нарочито је важна улога специфичних привредних друштава и других правних лица које закон назива субјектима од посебног значаја за заштиту и спасавање. Субјекти од посебног значаја за заштиту и спасавање су привредна друштва и друга правна лица која се баве делатношћу из области: телекомуникација, рударства и енергетике, транспорта, метеорологије, хидрологије, сеизмологије, заштите од јонизујућег зрачења и нуклеарне сигурности, заштите животне средине, водопривреде, шумарства и пољопривреде, здравства, збрињавања лица, ветерине, комуналне делатности, грађевинарства, угоститељства, и други који располажу ресурсима за смањење ризика од катастрофа. Субјекте од посебног значаја за заштиту и спасавање Републике Србије, одређује Влада на предлог МУП-а, док за покрајински и локални ниво то чине њихови одговарајући органи.

У оквиру своје редовне делатности хуманитарне организације и удружења учествују у припреми и спровођењу задатака заштите и спасавања и пружања помоћи становништву погођеном последицама катастрофа. Високошколске установе и друге организације које се баве научно-истраживачким радом ангажују се у спровођењу задатака заштите и спасавања и смањења ризика од катастрофа кроз учешће у штабовима, стручно-оперативним тимовима и оперативним штабовима

Као субјекти од посебног значаја, Црвени крст Србије, Горска служба спасавања и Ватрогасни савез Србије, помажу надлежним државним органима у обављању послова из своје надлежности, а у складу са јавним овлашћењима и својим програмским активностима.

И грађани имају права и дужности у систему смањења ризика од катастрофа. Грађани су дужни:

1) да се оспособљавају за заштиту и спасавање и да предузимају мере за личну и узајамну заштиту;

2) да прихвате распоред у јединице цивилне заштите и да се одазову у случају мобилизације тих јединица;

3) да се одазову позиву надлежног штаба за ванредне ситуације ради учешћа у акцијама заштите и спасавања;

4) да о настанку опасности без одлагања обавесте оперативни центар;

5) да спроводе прописане и наређене мере заштите и спасавања.

У извршавању задатака заштите и спасавања дужни су да учествују сви способни грађани, укључујући и стране држављане и лица без држављанства која у складу са

законом имају одобрење за привремени боравак или стално настањење у Републици Србији, старости од 18 до 60 година (изузетно, закон ослобађа ове обавезе поједине грађане, попут трудница и мајки са децом до десет година старости и самохраних родитеља односно старатеља са децом до 15 година старости; особа са инвалидитетом, као и лица која брину о особама са инвалидитетом и лица која се старају и живе у истом домаћинству са старијим особама које нису способне да се брину саме о себи).

Законски систем лиценцирања у области процене ризика и планирања заштите и спасавања од елементарних непогода и других несрећа

Закон уводи обавезу израде аката чији је циљ процена и смањење ризика од катастрофа и планирање заштите и спасавања у ванредним ситуацијама и великим удесима. Ове акте су дужни да израде Република Србија, органи управе, аутономне покрајине и локалне самоуправе, привредена друштва и друга правна лица, како би се повећала спремност свих субјеката система за превенцију и реаговање у ванредним ситуацијама и створили основи за ефикасно и економично управљање ризицима од катастрофа.

Проценом ризика од катастрофа идентификују се врста, карактер и порекло појединих ризика од наступања катастрофа, степен угрожености, фактори који их узрокују или увећавају степен могуће опасности, последице које могу наступити по живот и здравље људи, животну средину, материјална и културна добра, обављање јавних служби и привредних делатности, као и друге претпоставке од значаја за одвијање уобичајених животних, економских и социјалних активности. Планом смањења ризика од катастрофа утврђују се конкретне превентивне, организационе, техничке, финансијске, нормативне, надзорне, едукативне и друге мере и активности које су надлежни државни органи и други субјекти, на основу процене појединих ризика, дужни да предузму у будућем периоду у циљу смањења ризика од катастрофа и ублажавања њихових последица.

Планом заштите и спасавања се планирају мере и активности за спречавање и умањење последица катастрофа, снаге и средства субјеката система смањења ризика од катастрофа и управљања ванредним ситуацијама, њихово организовано и координирано ангажовање и деловање у ванредним ситуацијама у циљу заштите и спасавања људи, материјалних и културних добара и обезбеђења основних услова за живот.

Процену ризика од катастрофа и план заштите и спасавања израђују привредна друштва односно друга правна лица која имају овлашћење за израду процене ризика од катастрофа и плана заштите и спасавања и имају у сталном радном односу запослена најмање три лица која поседују лиценцу за израду процене ризика од катастрофа и плана заштите и спасавања. Овлашћење за израду процене ризика од катастрофа и плана заштите и спасавања и лиценцу за израду процене ризика од катастрофа и плана заштите и спасавања издаје МУП.

Лиценца за израду процене ризика од катастрофа и плана заштите и спасавања издаће се лицу које има:

1) најмање високу стручну спрему и стечених 240 ЕСП бодова (мастер-академске, специјалистичке академске, специјалистичке струковне, односно основне академске студије у трајању од најмање четири године);

2) завршену обуку за израду процене ризика и планова заштите и спасавања и

3) положен посебан стручни испит за израду процене ризика и плана заштите и спасавања.

Рок важења овлашћења за израду процене ризика од катастрофа и плана заштите и спасавања и лиценце за израду процене ризика од катастрофа и плана заштите и спасавања је пет година. Министарство ће одузети овлашћење за израду процене ризика од катастрофа и плана заштите и спасавања привредном друштву, односно другом правном лицу ако се инспекцијским надзором утврди да не испуњава услове предвиђене законом. МУП води евиденцију о издатим овлашћењима за израду процене ризика од катастрофа и плана заштите и спасавања и лиценцама за израду процене ризика од катастрофа и плана заштите и спасавања.

И поред постојања солидног броја лиценцираних правних лица за пружање услуга процене ризика од катастрофа и израду плана заштите и спасавања, испитивање експерата је показало да је евидентно како је изузетно мали проценат од укупног броја обвезника израдио ове документе. Поставља се питање и да ли је потребно појачати инспекцијски надзор и доследније примењивати санкције за непоступање по законским нормама. С обзиром да су ови акти замишљени као плански основ за супротстављање ризицима од катастрофа, а да је од доношења првог закона којим је обавеза њихове израде уведена прошло више од једне деценије, може се закључити да импалементација прописа није на одговарајућем нивоу.

Интервјуисани експерт (Мср Филип Стојановић, лиценцирани проценитељ ризика са вишегодишњим искуством у области) додаје: „Један од највећих проблема система процене ризика је што се не примењује адекватно. Основна идеја процењивања ризика на свим нивоима, од републике, преко аутономне покрајине, градова и општина, па све до привредних друштава је да се креира регистар ризика, како би се на адекватан начин управљало идентификованим ризицима, односно како би се последице умањиле. У пракси ипак постоје знатне неусаглашености, јер процењени ризици нису комплементарни. Тако на пример, ако је неко привредно друштво израдило процену ризика и план заштите и спасавања, у тим документима се неретко дешава да нису препознати ризици територије на којој се то привредно друштво налази, јер локална самоуправа није урадила процену. Или је процес обрнут - локална самоуправа је израдила процену и план, али документ није доступан и не постоје информације о ризицима, те се процена која се ради за привредно друштво на тој територији разликује у односу на идентификоване ризике локалне самоуправе на којој послује привредно друштво. Самим тим се основна идеја се тешко остварује. Када је реч о самој методологији, иако није идеална, пружа могућности да се ризици реално сагледају и процене. Ипак, оно што се може издвојити као један од проблема јесте изједначавање последица по живот и здравље људи према степену последице. То значи, да се у методологија не прави разлика у штети уколико долази до смртног исхода, лакших телесних повреда или евакуације људи. Другим речима, ако је у пожару страдало петоро особа, односно у земљотресу је тих петоро евакуисано, не постоји разлика у „штети“ по ову штићену вредност. Оно се у пракси појављује као највећи проблем је недоследно тумачење одредби Упутства о методологији, односно поступка издавања сагласности надлежног органа. Оно што је за једну управу, односно одељење СВС-а

обавезно, код других се уопште не захтева. Док једни и даље захтевају штампање, увезивање јемственником и печатирање, други су у потпуности дигитализовали процес и сл. То само ствара додатну конфузију израђивача и немогућност остваривања континуитета праксе. Такође бих поменуо да нису у довољној мери заживеле обуке именованих повереника и заменика повереника цивилне заштите“.

Он додаје и да „пролонгирање израде Националног плана заштите и спасавања отежава израду ефикасних Планова заштите и спасавања за субјекте од посебног значаја за заштиту и спасавања, који би требало да имају одређени задатак. Непостојање националног плана прави нормативни вакуум, јер се већ три године израђују само делови плана за ове субјекте, односно издају се сагласности на делове израђеног плана. То не би био проблем да је у међувремену усвојен План. Међутим, у пракси ми имамо случај да након три године, када се поново раде акта, долазимо у исту ситуацију – да израдимо део плана. Наручиоци посла, односно они који тај план треба оперативно да користе (субјекти од посебног значаја за заштиту и спасавање) видео овај процес као неозбиљан, док је на израђивачима да чекају усвајање националног плана и додељивање задатка субјектима, како би испунили своје уговорне обавезе и допунили планове, односно како би се издала сагласност на цео план. Ово је само пример како је систем додатно бирократизован и успорен, док би требало да буде оперативан, резилијентан и прилагодљив“.

Из разговора са експертима је утврђено како озбиљан проблем представља непостојање одговарајуће безбедносне културе међу грађанима, посебно међу младима. Школски програми и садржаји нису прилагођени потреби изградње безбедносне свести и културе у области личне и колективне заштите грађана.

Списак изабраних прописа и препоручена литература

Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама (Сл. гласник РС бр. 87/18)

Уредба о јединицама цивилне заштите, намени, задацима, мобилизацији и начину употребе (Сл. гласник РС бр. 84/20)

Уредба о обавезама субјеката система смањења ризика од катастрофа и управљања ванредним ситуацијама у поступку израде Регистра ризика од катастрофа, начину израде Регистра ризика од катастрофа и уносу података (Сл. гласник РС бр. 122/20)

Уредба о садржају и начину израде плана смањења ризика од катастрофа (Сл. гласник РС бр. 21/20)

Уредба о садржају, начину израде и обавезама субјеката у вези са израдом процене ризика од катастрофа и планова заштите и спасавања (Сл. гласник РС бр. 102/20)

Уредба о саставу, начину и организацији рада штабова за ванредне ситуације (Сл. гласник РС бр. 27/20)

Уредба о висини и начину остваривања права на једнократну новчану помоћ (Сл. гласник РС бр. 84/20)

Правилник о критеријумима за избор кандидата за полазнике курса за Основну обуку припадника ватрогасно-спасилачких јединица (Сл. гласник РС бр. 12/19, 14/20, 49/21, 27/22)

Правилник о начину израде и садржају Плана заштите од удеса (Сл. гласник РС бр. 41/19)

Правилник о начину обучавања, оспособљавања, наставним плановима и програмима субјеката и снага система смањења ризика од катастрофа и управљања ванредним ситуацијама (Сл. гласник РС бр. 128/20)

Правилник о начину вођења Регистра привредних друштава и правних лица која рукују опасним супстанцама (Сл. гласник РС бр. 34/19)

Правилник о организацији и начину рада ватрогасно-спасилачких јединица (Сл. гласник РС бр. 66/21)

Правилник о организационо-техничким условима које морају испуњавати правна лица за добијање овлашћења за израду плана заштите од удеса (Сл. гласник РС бр. 9/19)

Правилник о организационо-техничким условима које морају испуњавати правна лица за добијање овлашћења за израду процене ризика од катастрофа и плана заштите и спасавања (Сл. гласник РС бр. 9/19, 116/20 - УС)

Правилник о раду повереника и заменика повереника цивилне заштите и критеријумима за њихово именовање (Сл. гласник РС бр. 102/20)

Правилник о садржини, начину успостављања и одржавања регистра ризика од катастрофа (Сл. гласник РС бр. 78/19)

Правилник о стручном испиту за израду процене ризика од катастрофа и плана заштите и спасавања (Сл. гласник РС бр. 20/19)

Правилник о униформи и ознакама цивилне заштите, ознакама функција и специјалности и личној карти припадника цивилне заштите (Сл. гласник РС бр. 32/20, 83/20)

Правилник о условима које морају испуњавати правна лица за издавање овлашћења за организовање и спровођење обуке за полагање посебног стручног испита за израду процене ризика од катастрофа и плана заштите и спасавања, начину израде и садржају плана (Сл. гласник РС бр. 13/19)

Правилник о врсти и количини опасних супстанци на основу којих се сачињава План заштите од удеса (Сл. гласник РС бр. 34/19)

Ризици од појединих форми криминалитета

Кривичноправна заштита од политичког криминалитета

Кривична дела политичког криминалитета су, највећим делом, смештена у Главу 28 Кривичног законика Републике Србије (Службени гласник Републике Србије, бр.85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19; даље: КЗ), која носи

назив „кривична дела против уставног уређења и безбедности Републике Србије". Почнимо, ипак, од вероватно јединог кривичног дела које је уперено ка политичким добрима у ужем смислу, а није (више) у оквиру овог поглавља КЗ-а.

Кривично дело тероризма је, након законодавних измена (ЗИД КЗ из 2012. године) премештено у Главу 34 („кривична дела против човечности и других добара заштићених међународним правом"). Тачније, укинуто је некадашње кривично дело међународног тероризма, док је инкриминација под називом„Тероризам" премештена у члан 391, који је до тада носио назив „међународни тероризам" (Стојановић 2010; Стојановић и Коларић 2020). Елементи међународног тероризма утиснути су и у измењен законски опис кривичног дела тероризма, који обухвата радње уперене против домаће и стране државе, као и међународне организације (Стојановић 2018; Делић 2021; Мрвић-Петровић 2019).

Имајући у виду да се терористички напади најчешће изводе према цивилним метама, односно насумично одабраним жртвама, да им је циљ изазивање страха, панике, нереда и несигурности међу грађанима, као и да је деловање терористичпких организација често међународно, па чак и глобално, законодавац је ово кривично дело оправдано сврстао међу инкриминације чији је заштитни објекат човечност (Милошевић 2009; Мрвић-Петровић 2019; Делић 2021; Бодрожић 2015).

У вези са овом инкриминацијом осврнућемо се на три важне чињенице. Прва је да је законодавац, доношењем ЗИД КЗ из 2012. године, начинио озбиљан пропуст. Наиме, припремање тероризма је било кажњиво на основу одредбе члана 320 КЗ-а (члан у ком је била прописана кажњивост припремања низа кривичних дела из Главе 28 КЗ-а).

Коначно, дела сродна тероризму, која суштински представљају елементе терористичке активности, прописана су чл. 391а, 391б, 391в и 391г, 393 и 393а КЗ. Међу њима се посебно издваја веома широка и флексибилна законска формулација кривичног дела из члана 391а, која инкриминише јавно изношење или проношење идеја којима се посредно или непосредно позива на вршење дела из члана 391. Ова инкриминација је оправдано унета у домаће кривично законодавство, и поред недовољне прецизности појединих појмова (нпр. појма идеје). (Бановић 2019: 360–361). Иако је законодавчева интенција усаглашавање са међународноправним актима, судска пракса треба да буде изузетно пажљива приликом примене ове „каучук" норме. Практично, овде се кажњава и „неодређено проношење идеја, које посредно подстичу на извршење таквог акта". (Вуковић 2019: 156). Тек ће правилна примена права показати пуну оправданост уношења овог кривичног дела у домаће законодавство. У досадашњој пракси присутна је само једна правноснажна пресуда за кривично дело из члана 391а, па свакако треба бити опрезан приликом доношења закључака (Бановић 2019: 356).

Вреди поменути и да је код кривичног дела из чл. 391б додат став 3 (ЗИД КЗ из 2019. године), који постоји ако учинилац, у намери извршења дела из члана 391 „отпутује у иностранство ради припреме, обучавања, планирања или учествовања у извршењу тог дела" (члан 391, ст. 3 КЗ). Увођење овог облика кривичног дела везано је за испуњавање међународноправних обавеза и представља израз тренда да се круг кажњивих припремних радњи код појединих кривичних дела све више шири, уз упитне

криминалнополитичке аргументе. У литератури се оправдано упозорава да постоје веома јаки, чак и претежни аргументи против увођења ове инкриминације (Вуковић 2019: 170).

Кривична дела из Главе 28 су релативно разноврсна, а повезује их заштитни објекат. У овом приказу нећемо се бавити делима која се односе на заштиту тајних података (одавање државне тајне и шпијунажа), као ни изазивањем расне, националне и верске мржње, већ ћемо се фокусирати на политичка дела у ужем смислу. Из истог разлога нећемо представити ни диверзију и саботажу, иако је реч о делима која су политичког карактера, јер се она, по правилу, изводе у односу на друге (делом споредне) елементе система националне безбедности, а не виталне елементе чију заштиту овде представљамо.

Ово је, иначе, једина група кривичних дела код којих је једним чланом (члан 320) прописана кажњивост припремних радњи за већи број инкриминација (додуше, не за сва дела из ове главе). Члан 319 прописује удруживање ради противуставне делатности као засебно кривично дело. Квалификовани облици низа кривичних дела из ове главе прописани су чланом 321 (тежи: ако је дело довело до смрти једног или више лица, тешког насиља, великих разарања, или је произвело угрожавање безбедности, односно економске и војне моћи земље; и најтежи облици: умишљајно лишавање живота једног или више лица или вршење дела током рата, оружаног сукоба или ванредног стања).

Кривично дело угрожавања независности постоји када учинилац, поступајући супротно Уставу, покуша да доведе Србију у „положај потчињености или зависности према некој другој држави" (члан 305). Предвиђена је казна од три до петнаест година затвора. Дело се сматра довршеним самим покушајем, због изузетне друштвене опасности и чињенице да би у случају довршавања кривичног дела учиниоца било немогуће казнити, барем док траје успостављено противправно стање. У вези са овом инкриминацијом истакли бисмо да је циљ законодавца био да се уведе кривичноправна заштита од разноликих облика напада на независност земље. Осим радњи које би се испољавале у примени силе или претње, овде долазе у обзир и различите политичке радње којима се, уз кршење Устава, држава покушава потчинити страној сили. Наравно, овако широка криминална зона оставља простор и за извесне злоупотребе, посебно у смислу коришћења кривичног законодавства за обрачун са политичким противницима, због чега треба бити веома обазрив приликом примене права.

Треба имати у виду да међународни и регионални политички процеси, чланство у интернационалним организацијама и закључивање билатералних и мултилатералних споразума којима се држава добровољно одриче појединих овлашћења или пристаје да мења унутрашње уређење не представљају радњу овог кривичног дела, јер није реч о противуставним радњама, већ дозвољеној политичкој активности у светлу савремене глобалне политике. Ипак, и овде је могуће прећи границу криминалне зоне, али је питање веома осетљиво и у великој мери зависи од дискреционе оцене.

Ко „потпише или призна капитулацију или прихвати или призна окупацију Србије или појединог њеног дела" (члан 306) чини кривично дело признавања капитулације или окупације, за које је запрећена казна од најмање десет година затвора.

Чини се да инкриминација из члана 306 временом губи на значају, посебно имајући у виду да су у политичкој пракси готово непостојеће ситуације у којима се формално признаје капитулација или окупација. Чешће решење је да се оне фактички спроводе кроз различите правне форме мировних споразума. Наравно, законска формулација се може и екстензивније тумачити, тако да обухвати и радње фактичког признавања капитулације или окупације, без обзира на форму у којој су учињене.

Капитулацију треба схватити у ширем смислу, не само као класичну војну капитулацију, већ као сваку одлуку/споразум о престанку пружања отпора (Чејовић 2008: 776). Ово дело, по законском опису, може да изврши сваки грађанин, али фактички извршилац је само лице које је у позицији да призна капитулацију или окупацију у име државе. У литератури је присутан став да се ово дело може извршити и нечињењем (Стојановић 2018: 835). Покушај отцепљења дела државне територије или припајања дела територије другој држави употребом силе или другог противуставног начина представља кривично дело угрожавања територијалне целине из члана 307 КЗ-а. Радња је алтернативно прописана и може се манифестовати на један од два начина: покушај отцепљења дела државне територије или његовог припајања другој суверености држави. Покушај се, због изразите друштвене опасности, сматра довршеним делом. Довршено дело је, по природи ствари, такође кажњиво.

Напад на уставно уређење постоји када учинилац употребом силе или претњом да ће применити силу покуша да промени уставно уређење или сврге највише државне органе. Запрећена је казна од три до петнаест година затвора. У домаћој теорији истиче се да је ово кривично дело еквивалент велеиздаји у упоредним законодавствима. Оно представља напад на унутрашњу безбедност. (Стојановић и Перић 2011: 258). Радња је алтернативно постављена, тако да ће дело постојати у случају остварења било које од њих. Могуће је и да учинилац изврши обе радње, што ће представљати отежавајућу околност приликом одмеравања казне. (Вуковић 2021). Законски опис обухвата и начин извршења – употребу силе или претњу употребом исте. Некадашње законодавство (све до измена и допуна кривичног законодавства из 1990. године) садржало је инкриминацију много ширег опсега. По њој, ово кривично дело је постојало ако лице предузме било коју радњу уперену ка промени уставног уређења уз постојање одговарајућег субјективног елемента (намере). Тако широк законски опис није примерен демократским земљама, нити савременом кривичном праву, заснованом на начелу легалитета и легитимитета. Садашња инкриминација је у складу са упоредноправним стандардима и не одступа од кривичноправних принципа. Дакле, по важећој одредби, радња постоји само ако је примењена сила или је њоме пређено. Уз тај начин извршења, дело ће постојати ако (Милошевић 2010):

1. Извршилац покуша да промени уставно уређење. Радња треба да буде уперена ка најзначајнијим елементима уставног уређења (Мрвић-Петровић 2019: 350; Чејовић 2008).

2. Извршилац покуша да сврге највише државне органе. Највиши државни органи су утврђени Уставом Србије (председник, Влада, Народна скупштина, Врховни касациони суд, Уставни суд).

Занимљиво је да се ово дело сматра свршеним ако учинилац покуша да га изврши. Покушај се сматра довршеним делом због посебне друштвене опасности ове

радње, као и чињенице да ће, уколико дело и буде свршено, бити отежано или онемогућено санкционисање извршиоца (ако, примера ради, успе да сврги власт или промени уставно уређење). Наравно, довршена радња је такође кривично дело и исто може бити предмет кривичног поступка чим се стекну услови за кажњавање учиниоца (Симовић-Хибер 2007).

Кривично дело позивања на насилну промену уставног уређења постоји када лице позива или подстиче да се силом промени уставно уређење или свргну највиши државни органи или њихови представници, уз намеру угрожавања уставног уређења или безбедности Републике. Предвиђена је казна од шест месеци до пет година затвора. Ово дело се у нашем ранијем законодавству називало непријатељска пропаганда (Стојановић и Перић 2005: 31).

Основни облик овог кривичног дела наликује радњи подстрекавања на кривично дело напад на уставно уређење. Међутим, када се позива неодређен број лица на извршење дела, неће бити реч о саучесништву у кривичном делу (Вуковић 2021, Стојановић и Делић 2019). Знајући да су ове радње изузетно друштвено опасне, законодавац их је прописао као засебно кривично дело. Практично, овде је реч о пропагандном деловању (Ђорђевић и Коларић 2020, 203). Позивање представља изазивање одлуке код другог, док је подстицање управљено на учвршћивање већ постојеће одлуке (Стојановић, Перић, 2005: 32).

Позивање или подстицање не мора да буде успело. За постојање дела, као што је утврђено у судској пракси, није важно да ли је пропагандно деловање лица остварило ефекат, нити да ли је он уопште могао да буде остварен (Чејовић 2008:779). Радња може да се изврши на било који подесан начин – непосредним разговором, упућивањем писаних, аудио или видео-материјала, објављивањем постова на друштвеним мрежама или другим интернет платформама, наступом у телевизијским или радио-емисијама, слањем писама и других пошиљака итд. Облик кривице је директни умишљај, а тражи се и утврђивање намере угрожавања уставног уређења и безбедности.

Тежи облик, за који је запрећена казна од једне до осам година, постоји када је дело учињено уз помоћ из иностранства. Помоћ из иностранства може пружити друга држава, организација, један или више грађана стране земље, а испољава се у било којој делатности којом се доприноси извршавању кривичног дела (Ђорђевић и Коларић: 203–204).

Привилеговани облик је присутан када учинилац, са намером растурања, израђује или умножава материјал који позива на вршење дела из става 1 овог члана, или „пребацује на територију Србије такав материјал или држи већу количину тог материјала у намери да га он или неко други растура”. Запрећена је казна од три месеца до три године затвора. Убиство представника највиших државних органа постоји када је представник ових органа умишљајно лишен живота, под условом да је учинилац поступао са намером угрожавања уставног уређења и безбедности Републике. То значи да, ако, на пример, представника највишег органа убије комшија због препирке око паркирања аутомобила, дело ће се квалификовати као обично (евентуално тешко) убиство, а не као ово кривично дело. Умишљај не може да буде евентуални, јер се захтева утврђивање намере (Ђорђевић и Коларић 2020; Чејовић 2008). Учинилац лишава живота представника највиших државних органа из политичких побуда и

његово дело је првенствено управљено ка угрожавању уставног поретка и националне безбедности. То је додатни разлог за издвајање овог кривичног дела. За разлику од тешког убиства, код ког је заштитни објекат живот и тело, овде је фокус на уставном уређењу и безбедности државе јер учинилац првенствено тежи ка угрожавању државе, а лишавање живота високог званичника је средство за остварење тог циља.

Пасивни субјект овог кривичног дела могу да буду само лица која, у време извршења кривичног дела, обнашају функције у највишим државним органима. То су:

1. председник Републике;

2. народни посланик;

3. председник и члан Владе;

4. судија највишег суда;

5. судија Уставног суда;

6. републички јавни тужилац.

Интересантно је да законодавац користи термин „судија највишег суда" уместо конкретног „судија Врховног касационог суда". Разлог је то што и судови, са променама Устава и закона, могу да мењају називе (тако је некадашњи Врховни суд постао Врховни касациони, а после последњих уставних промена враћа се назив Врховни). Законодавац није очекивао да ће се мењати назив републичког тужиоца, али са уставним променама из 2022. године и овај назив одлази у историју и замењује се са термином врховни јавни тужилац. Живот је увек маштовитији од законодавца, као што каже стара изрека. Прописана казна за убиство представника највиших државних органа је најмање десет година или доживотни затвор. У случају осуде постоји могућност условног отпуста, за разлику од помињаних облика тешког убиства, што је врло упитно решење, јер се не може убедљиво аргументовати да је ово дело мање друштвено опасно од тих облика тешког убиства. Квалификовани облици дела не постоје, што је логично с обзиром на то да је за његово извршење могућа најтежа казна у домаћем законодавству, те прављење квалификованих облика не би имало смисла. Кривично дело из члана 311 чини лице које учествује у оружаној побуни управљеној на „угрожавање уставног уређења, безбедности или територијалне целине Србије" (члан 311 став 1). Прописана је казна од три до петнест година затвора. Законодавац не прецизира шта обухвата појам оружане побуне, нити која је врста учешћа довољна за постојање кривичног дела (Стојановић и Перић 2011:261–262).

Полазећи од логичког и језичког тумачења можемо да закључимо како оружана побуна обухвата супротстављање законитим властима у виду побуне групе грађана која носи оружје, користи га или прети његовом употребом, са циљем да угрози безбедност, територијални интегритет или уставни поредак државе. Није прецизирано колико грађана мора да учествује у побуни да би постојало ово кривично дело, чак ни оквирно. Ипак, сам термин „оружана побуна" указује да не може бити реч о малом броју лица, већ да се о побуни може говорити када је реч о масовнијем учешћу грађана. Такође, не мора сваки учесник у побуни да буде наоружан. Довољно је да лице учествује у групи у којој има наоружаних лица и свестан је да иста могу да употребе оружје, те својим учешћем потпомаже остварење циљева побуњене групе (Стојановић 2018; Делић 2021).

Није до краја разјашњено ни питање која се врста учешћа сматра довољном, али лице својим радњама свакако мора да покаже како није пуки посматрач или симпатизер акција групе, већ неко ко конкретно доприноси побуни својим радњама (нпр. учествовао је у групи која је реметила јавни ред и мир, онемогућавала рад државних установа и узнемиравала грађане, све у циљу промене уставног уређења земље, при чему није носио оружје али је све време био физички присутан и кретао се заједно са осталим члановима групе, односно својим телом доприносио извођењу акције тако што је блокирао улаз у државну установу, викао и претио, гађао каменицама итд.). Субјективни елемент је директни умишљај, што закључујемо на темељу законског описа који захтева да је побуна „управљена" на одређене политичке циљеве. (Стојановић 2018). Тежи облик дела предвиђен је у ставу 2 истог члана. Квалификовани облик се од основног разликује само по улози коју извршилац обавља у оружаној побуни. Основни облик дела је учествовање у побуни, док тежи облик постоји када је лице у улози организатора побуне (Ђорђевић и Коларић 2020: 207). Организатор координира, планира и припрема акције побуњене групе, издаје наређења и усмерава активности. Кривично дело повреде територијалног суверенитета постоји када учинилац, „кршећи правила међународног права, продре на територију Србије" (члан 318). Предвиђена је казна затвора од једне до осам година.

Радња дела састоји се из противправног продирања на суверену државну територију Србије. Додуше, израз територијални суверенитет је помало необичан, али је реч о терминолошкој, а не суштинској замерци. Противправно продирање је оно које је супротно правилима међународног права. Оно се може учинити различитим средствима (нпр. ваздухопловом или неким средством речног или копненог превоза) (Чејовић 2008, 797) : Продирање је, по природи ствари, насилна радња. У том смислу поставља се питање разликовања овог дела и инкриминације из члана 350 (недозвољен прелаз државне границе и кријумчарење људи). Дело из члана 350 постоји када неко пређе или покуша да пређе границу без дозволе, и то наоружан или употребом насиља. Свакако да дело из члана 318 подразумева много већи интензитет и другачију врсту насиља у односу на дело из члана 350.

За постојање повреде територијалног суверенитета потребно је да дошло до напада на територијални интегритет, било да је он релативно малог (нпр. тако што се војним ваздухопловом без дозволе пређе гранична линија Републике Србије), већег (рецимо, када наоружана група или организација пређе границу како би запосела део територије или преотела одређени објекат), или веома великог обима (попут агресивног атака трупа друге државе / међународне организације).

Члан 8 Устава одређује да је територија Србије јединствена и недељива (Устав Републике Србије, 2006). Границе су неповредиве, а њихова промена се, према члану 8 став 2 Устава, врши по поступку предвиђеном за измену устава. Продирање на територију Србије подразумева недозвољен продор преко државне границе, односно граничне линије.

Према члану 3 тачка 1 Закона о граничној контроли, „државна граница је замишљена вертикална раван која се граничном линијом простире по Земљиној површини и одваја простор Републике Србије, његов копнени део, унутрашње воде, ваздушни простор и простор испод површине земље од простора суседних држава. У смислу граничних провера под државном границом сматрају се и подручја граничних прелаза на аеродромима и пристаништима преко којих се одвија међународни саобраћај" (Закон о граничној контроли 2018). Гранична линија је „обележена или замишљена линија којом се на Земљиној површини протеже државна граница" (члан 3 тачка 4 Закона о граничној контроли).

Облик кривице је умишљај (евентуални или директни). Законодавац не тражи утврђивање посебне намере. Довољно је да је учинилац био свестан да продире на територију Србије, па је то и хтео или је барем на то пристао. Ако је учинилац поступао из нехата (нпр. због спољашњих околности које су га навеле да залута, односно погреши пут), ово кривично дело неће постојати.

Организовани криминал, тероризам и екстремизам – стратешки и нормативни приступ

Проблематика која се тиче сузбијања екстремизма, организованог криминала, као и других облика нарушавања националне безбедности у научној публицистици представља готово бескрајну инспирацију за бројна истраживања, као и за прегледне студије. Међутим, таква академска проучавања неретко остају на нивоу прегледних радова, без јасних препорука или даљих предлога за побољшање система процене ризика. Сложеност система међународних односа и процеси који се, чини се, све брже и интензивније испољавају и остављају корените промене на начине на које модерна друштва функционишу, утиче и на нешто радикалније одговоре које државне власти креирају у жељи да умање њихове негативне последице.

Основу законског оквира борбе против организованог криминала, тероризма и екстремизма чини табеларно приказани скуп прописа:

Закони и други прописи Републике Србије у области организованог криминала, тероризма и екстремизма

01 Кривични законик
02 Законик о кривичном поступку
03 Закон о организацији и надлежности државних органа у сузбијању организованог криминала, тероризма и корупције
03-01 Уредба о евидентирању имовног стања лица која врше функцију, односно обављају послове и задатке у посебним организационим јединицама из Закона о организацији и надлежности државних органа у сузбијању организованог криминала
03-02 Правилник о организацији, раду и поступању са притвореницима у Посебној притворској јединици
04 Закон о организацији и надлежности државних органа за борбу против високотехнолошког

криминала
05 Закон о организацији и надлежности државних органа у поступку за ратне злочине
06 Закон о Безбедносно-информативној агенцији
06-01 Уредба о начину евидентирања, обраде, чувања, коришћења, заштите и достављања другим надлежним државним органима информација и докумената о пословима из надлежности Безбедносно-информативне агенције
07 Закон о Војнобезбедносној и Војнообавештајној агенцији
07-01 Уредба о посебним критеријумима и поступку за пријем у радни однос и престанак радног односа у Војнобезбедносној агенцији и Војнообавештајној агенцији
08 Закон о полицији
08-01 Уредба о специјалној и посебним јединицама полиције
08-02 Правилник о полицијским овлашћењима
08-03 Правилник о начину обављања појединачних полицијских послова
08-04 Правилник о начину и условима примене полицијских овлашћења према малолетним лицима
08-05 Правилник о криминалистичко-форензичкој регистрацији, узимању других узорака и криминалистичко-форензичким вештачењима и анализама
08-06 Правилник о начину спровођења и методологији примене полиграфског испитивања
08-07 Правилник о начину вршења унутрашње контроле
08-08 Правилник о начину спровођења теста интегритета
09 Закон о спречавању прања новца и финансирања тероризма
10 Закон о ограничавању располагања имовином у циљу спречавања тероризма и ширења оружја за масовно уништење
11 Закон о националној бази података за спречавање и борбу против тероризма
12 Закон о спречавању корупције
12-01 Правилник о Регистру јавних функционера и Регистру имовине и прихода јавних функционера
13 Закон о одговорности правних лица за кривична дела
14 Закон о програму заштите учесника у кривичном поступку
14-01 Правилник о начину спровођења Програма заштите учесника у кривичном поступку у заводима за извршење заводских санкција
15 Закон о одузимању имовине проистекле из кривичног дела
16 Закон о информационој безбедности
16-01 Уредба о безбедности и заштити деце при коришћењу информационо-комуникационих технологија
16-02 Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја
16-03 Правилник о подацима које садржи евиденција оператора информационо-комуникационих система од посебног значаја
17 Закон о заштити података о личности

18 Закон о тајности података
19 Закон о међународној правној помоћи у кривичним стварима

Од великог значаја за анализу и имплементацију нормативног оквира су и други прописи, стратегије и други документи којима је циљ оперативно спровођење закона и политика, Током 2021. године, Народна скупштина Републике Србије је усвојила Закон о националној бази података за спречавање и борбу против тероризма који установљава јединствену националну базу података као „платформу која садржи скуп података као део већ ускладиштених података у постојећим базама надлежних органа, и која омогућава приступ тим подацима и контролисану и безбедну размену података“ (Народна скупштина 2021: чл. 2а) о индексираним лицима. Решења садржана у овом закону имају за циљ да на јасан и прецизан начин уреде поступак похрањивања података у базу, њену садржину, приступ подацима, њихово коришћење и заштиту, са посебним нагласком на поштовању међународних стандарда заштите људских права и слобода. Са друге стране, циљ одредаба ово закона је обезбеђивање ефикасне размене података између државних органа надлежних за превенцију и борбу против тероризма и подизање способности система безбедности за благовремен и ефикасн одговор на претњу коју представља тероризам. Закон предвиђа да су предмет индексирања сва физичка и правна лица, као и групе или организације „које су означене и стављене на међународну или националну листу терориста, терористичких организација или финансијера тероризма“ (Народна скупштина 2021: чл. 2, ст. 4). Тако ограничен предмет индексирања, према одредбама Закона, не искључује иностранa лица или организације које су већ регистроване од стране Уједињених нација и/или међународних организација, као ни са „консолидоване листе успостављене на основу закона који уређује међународне мере ограничавања“ (Народна скупштина 2021). Закон предвиђа и коришћене већ постојећих база података других државних органа које укључују лица која су осумњичена, оптужена или осуђена за кривично дело тероризам и са њим повезана кривична дела (2021: чл. 5).

Закон о националној бази података је добро законско решење које има и неколико својих мана. Разлози заштите података и приступа подацима су недвосмислено јасни и Закон предвиђа да „надлежни орган који је проследио упит може од надлежног органа који је индексирао лице (прим. аут. БИА) захтевати достављање проширених података, ако је то неопходно за обављање конкретног посла из његове надлежности“ (2021: чл. 8.). Како акт прецизира органе које имају надлежност делимичног приступа подацима, било би адекватно на овај списак допунити и научноистраживачке институције које у својим акредитованим студијским програмима имају научне области студије безбедности. Тиме би се пружила могућност академској заједници да, у оквирима контролисане употребе појединих сетова података, оствари значајне увиде у обрасце испољавања терористичких активности у земљи и иностранству.

Оно што је добра страна приказаних аката јесте инсистирање на проценама ризика као алату који уједначено приказује хазарде који су улазни параметри за све анализе нарушавања (националне) безбедности. Међутим, ниједан од три приказана документа

не прецизира ниво систематизације ризика као ни методологију за израду процене ризика у креирању стратешких аката и њиховом ажурирању.

Као позитиван пример у правцу уважавања и примене међународно признате методологије у процени ризика требало би истаћи неколико докумената: Национална процена ризика од прања новца и национална процена ризика од финансирања тероризма, Процена ризика од прања новца и финансирања тероризма у сектору дигиталне имовине и Процена ризика од финансирања ширења оружја за масовно уништење (Закључак Владе РС 2021). Поменуте процене ризика резултат су усклађивања стратешко-нормативног оквира Републике Србије са Препорукама Радне група за финансијску акцију (Financial Action Task Force – FATF 2012; 2022). Препоруком бр. 1, под насловом „Процена ризика и примена приступа заснованог на процени ризика“ (risk-based approach), сугерише се државама да идентификују, процене и схвате ризике с којима се суочавају на плану прања новца и финансирања тероризма и да предузму кораке, укључујући и одређивање органа или механизма који ће координисати мере за процену ризика, те да определе ресурсе у циљу делотворног смањења тих ризика. Циљ процене ризика јесте да се дође до закључака о томе који сектори и какво поступање носе потенцијално виши ризик од прања новца и финансирања тероризма, а које нижи, како би држава могла адекватно да одговори на утврђене ризике кроз мере и активности које предузима, као и да у складу са процењеним ризицима донесе адекватне одлуке о расподели ресурса, чиме би се обезбедило да мере за спречавање или ублажавање прања новца и финансирања тероризма буду сразмерне идентификованим ризицима.

Законом о спречавању прања новца и финансирања тероризма, прописује да се „процена ризика од прања новца и финансирања тероризма на националном нивоу израђује у писменој форми и ажурира најмање једном у три године, а сажетак процене ризика ставља се на располагање јавности и не сме садржати поверљиве информације“ (2017, члан 70.), чиме је процена ризика успостављена и као нормативна обавеза.

Поменуте Националне процене ризика, осим што успостављају основу за доношење стратешко-политичких докумената у овој области, представљају и значајно унапређење и посматрано са методолошког аспекта, што смо идентификовали као слабост претходно анализираних стратешких докемената у овом раду. Према наводима у самом тексту Националних процена ризика, као основа, коришћена је методологија Светске банке (National Money Laundering and Terrorist Financing Risk Assessment Toolkit), при чему је она у одређеним областима допуњавана. Развијени су домаћи критеријуми за процену ризичних форми привредних друштава, те допуњени критеријуми за процену ризика који се односе на прекограничне претње.

Користећи поменуту методологију, Национална процена ризика од прања новца заснована је на анализи података о: кривичним делима чијим се извршењем стиче противправна имовинска корист (потенцијална предикатна кривична дела), предикатним кривичним делима поводом којих је покренут поступак и за кривично дело прање новца, учесталости извршења предикатних кривичних дела, висини скривене – одузете - процењене противправне имовинске користи из предикатног кривичног дела и укључености организованих криминалних група у извршењу

кривичних дела. Методологија је укључивала и увид у предмете јавних тужилаштава и судова , те професионално искуство чланова радне групе за израду процене ризика.

Претња од тероризма, темељи се на: информацијама и статистичким подацима прикупљеним од стране јавног тужилаштва, служби безбедности и других надлежних државних органа. Не улазећи дубље у анализу текст поменутих националних процена ризика, можемо констатовати да је методолошки поступак коришћен у њиховој изради, путоказ за будуће стратешко политичке документе у овој области.

Насиље на спортским приредбама, јавним скуповима и другим местима окупљања грађана

Насиље на спортским приредбама поприма озбиљне размере и изазива узнемирење и забринутост јавности. Кривичноправна заштита, која је, у складу са општм правним принципима, ultima ratio, последњих година има израженију улогу, не само због високог степена апстрактне друштвене опасности ове појаве, већ и чињенице да конкретни облици њеног манифестовања постају бројнији, учесталији и све тешње повезани са другим формама криминалног деловања. Степен апстрактне друштвене опасности и чињеница да прописивање и примена санкција других правних грана није у довољној мери утицала на спречавање и сузбијање ове појаве, у потпуности оправдавају кривичноправну реакцију. Потреба подизања нивоа безбедности јавних окупљања, посебно спротских манифестација, због присуства великог броја људи и могућности угрожавања безбедности, као и живота и тела присутних лица, утицала је на законодавца да пропише посебно кривично дело.

Не треба сметнути с ума да је кривичноправна реакција на нереде на спортским приредбама постојала и раније, али у ограниченом обиму – искључиво у односу на службена или одговорна лица која не предузму мере обезбеђења услед чега дође до последице која се огледа у нередима или, у случају тежег облика, наступању тешке телесне повреде лица или оштећивања имовине веће вредности, Реч је о кривичном делу неспречавања нереда на спортској приредби или другом јавном скупу из чл. 230а Кривичног закона Србије, уведеном изменама и допунама из 2002. године (Кривични закон Србије, „Сл. гласник СРС, бр. 26/77, 28/77, 43/77, 20/79, 24/84, 39/86, 51/87, 6/89 и 42/89, „Службеник гласник РС“, бр. 21/90, 16/90, 26/91, 75/91, 9/92, 49/92, 51/92, 23/93, 67/93, 47/94, 17/95, 44/98, 10/02, 11/02, 80/02, 39/03 и 67/03). Дакле, није постојало засебно кривично дело којим би се инкриминисало друштвено опасно понашање самих изгредника на спортској приредби, већ само кривично дело нечињења које се односило на одговорна лица из редова организатора спортске приредбе.

Кривични законик („Сл. гласник РС“, бр. 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19; у даљем тексту: КЗ) прописује кривично дело насилничког понашања на спортској приредби или јавном скупу чланом 344а, у склопу Главе XXXI (кривична дела против јавног реда и мира). (Делић, 2013; Петровић-Мрвић, 2019). Заштитни објекат је јавни ред и мир, а сама инкриминација представља посебан случај дела из члана 344 КЗ (насилничко понашање). Пре увођења кривичног дела из члана 20 ЗНСП и, касније, члана 344а КЗ, насиље на спортским приредбама је санкционисано уколико су њиме остварена обележја одређеног кривичног дела (нпр. тешке телесне повреде, уништења и оштећења туђе ствари, итд.). Ипак, нереди на спортским приредбама и јавним скуповима, њихове последице и интензитет, утицале су на

законодавца да посебно квалификује околност места и времена извршења, креирајући ново кривично дело. Наравно, када се уводи ново кривично дело, комбинацијом елемената постојећих кривичних дела и одређених, нарочитих околности, у пракси се јављају и проблеми приликом правне квалификације.

И поред тога, упоредни трендови и криминалнополитички разлози оправдавају овај законодавни потез, јер вршење насиља на и у току спортске приредбе (као уосталом и јавног скупа) је у квалитативном смислу другачије понашање у односу на насиље на другим јавним местима, и то не само због ризика од тешких последица због броја и просторног распореда окупљених лица, већ и ради потребе да се посебно заштите такве манифестације и пошаљу одговарајуће криминалополитичке поруке. Спортска приредба је место на ком би требало да се промовишу позитивне социјалне вредности и негује дух толеранције, пријатељства и фер плеја.

У том смислу, а знајући да спортске приредбе код нас, у последње време, врло често постају поприште озбиљних физичких сукоба којима се угрожавају остали, мирни учесници (међу њима су и породице, деца, старији суграђани) и оштећује туђа имовина, кривичноправна реакција је постала неопходна, барем када су у питању опаснији видови насилничког понашања (за оне мање интензивне облике насиља је довољна и прекршајноправна реакција).

Специфичне околности које чине елементе бића кривичног дела из члана 344а КЗ и разликују га од кривичног дела насилничког понашања (чл. 344 КЗ) се односе на време и место извршења кривичног дела, као и својство учиниоца. Значење ових појмова утврђујемо на основу одредби ЗНСП.

Место извршења кривичног дела је спортска приредба. Под спортским приредбама ЗНСП подразумева утакмице и манифестације. Судска пракса је појаснила опсег појма утакмице. У образложењу пресуде Апелационог суда у Београду се истиче: „Пријатељска фудбалска утакмица која није била пријављена спортском савезу одређеног ранга, не може се сматрати спортском приредбом, у смислу члана 2. став 1. Закона о спречавању насиља и недоличног понашања на спортским приредбама..... спортски савез није делегирао судије том приликом, нити је на тој утакмици било делегата, помоћних судија, нити се водио записник, па се, у том смислу, наведена утакмица не може сматрати спортском приредбом“. (Пресуда Апелационог суда у Београду, Кж1 221/13, од 5. фебруара 2013. године).

Извршилац кривичног дела је лица које има својство учесника спортске приредбе. Сва лица присутна на спортској приредби (од спортиста, делегата, судија, па до публике, редара, новинара итд) имају својство учесника спортске приредбе. (Пресуда Врховног касационог суда Кзз. 24/12, од 11. априла 2012. године). Тако, суд утврђује да је остварено кривично дело на спортској приредби када је један од играча, незадовољан одлуком, напао судију и нанео му тешку телесну повреду. (Решење Апелационог суда у Београду Кж1 5612/12 од 18. новембра 2013. и пресуда Вишег суда у Београду К 1115/12 од 18. априла 2013. године).

ЗНСП дефинише спортски објекат као „објекат намењен за одржавање спортских приредби, који поред спортског терена има простор за гледалиште и који може имати и пратећи простор (санитарни, гардеробни, спремишни и др.), као и простор на који је

улазак и кретање физичких лица условљено поседовањем улазнице или дозволе коју издаје организатор спортске приредбе“. (ЗНСП, чл. 2 ст. 6). Под спортским тереном законодавац разуме део простора на ком се обавља сама спортска игра односно такмичење, као и преостали простор до гледалишта. (ЗНСП, чл.2 ст. 7).

Место извршења је углавном управо спортски објекат, мада се одређене манфестације, па и утакмице, одржавају на просторима који нису класични спортски објекти већ су прилагођени ради привременог или повременог одржавања спортских приредби. На пример, у једној судској одлуци се утврђује одговорност професионалног кошаркаша за дело из члана 344а ст.1 у стицају са кривичним делом тешке телесне повреде, јер је напао и повредио судију (ударцем главом у јагодичну кост лица) током утакмице која се одвијала на простору испред једног београдског тржног центра, у кошаркашкој дисциплини баскет 3х3, под покровитљством одговарајућег спортског ентитета. (Пресуда Вишег суда у Београду, Спк.бр. 33/18 од 26. 02. 2018. године).

Организатор спортске приредбе је „спортски савез, спортско друштво, спортска организација - клуб, друго правно или физичко лице које се стално или повремено бави организацијом спортских приредби, односно које је преузело организовање одређене спортске приредбе, или вршење одређених послова у организовању спортске приредбе“. (ЗНСП, чл. 2 ст. 2). Појам организатора је значајан и због одговорности за један од облика овог кривичног дела.

Време извршења је такође одређено одредбама ЗНСП. Чл. 2 ст. 3 ЗНСП одређује да је време спортске приредбе: „временски интервал од два часа пре почетка спортске приредбе до два часа након њеног завршетка, односно, кад се одржавају спортске приредбе повећаног ризика, временски интервал од четири часа пре почетка спортске приредбе до четири часа након њеног завршетка“.

Према томе, појмовни оквир на основу ког утврђујемо испуњеност објективних елеемената бића кривичног дела из члана 344а је, у претежном делу, прописан одредбама ЗНСП.

Радња основног облика кривичног дела из члана 344а представља, као што смо већ поменули, посебну врсту насилничког понашања, које је, због квалитативних разлика у односу на „матично“ кривично дело, стипулисано као засебна инкриминација.

Треба, додуше, имати у виду да се ово кривично дело не односи само на спортске приредбе већ и на јавне скупове, па се узимају у обзир и одредбе Закона о јавном окупљању („Сл.гласник РС“, број 6/16). Ипак, предмет нашег истраживања је кривичноправна реакција на насиље на спортским приредбама па ћемо нагласак ставити на овај аспект. У погледу организације обезбеђивања јавног скупа и спортске приредбе, потребно је узети у обзир и одредбе Закона о приватном обезбеђењу („Сл. гласник РС“, бр. 104/13, 42/15, 87/18). Због односа са прекршајном одговорношћу, потребно је сагледати и одредбе Закона о јавном реду и миру („Сл.гласник РС“, бр. 6/16, 24/18). Важан извор међународног права у овој области је Европска конвенције о насиљу и недоличном понашању гледалаца на спортским приредбама, посебно на фудбалским утакмицама, коју је ратификовала још СФРЈ („Сл. лист СФРЈ – Међународни уговори”, бр. 9/90).

Радња кривичног дела је алтернативно одређена. Милошевић (2022: 2019, 220) врши систематичан приказ алтернативних облика радње извршења основног облика на следећи начин:

1. Вршење насиља или оштећивање имовине веће вредности током приредбе или скупа, или приликом одласка или доласка: када учинилац „физички нападне или се физички обрачунава са учесницима спортске приредбе или јавног скупа, врши насиље или оштећује имовину веће вредности приликом одласка или доласка са спортске приредбе или јавног скупа“. Вреди обратити пажњу на чињеницу да се код овог облика радње као кључан елемент истиче време извршења.

2. Уношење и/или коришћење пиротехничких, запаљивих, експлозивних и сличних средстава, када лице „унесе у спортски објекат или баца на спортски терен, међу гледаоце или учеснике јавног скупа предмете, пиротехничка средства или друге експлозивне, запаљиве или шкодљиве супстанце које могу да изазову телесне повреде или угрозе здравље учесника спортске приредбе или јавног скупа“.

3. Неовлашћени улазак у одређени део спортског објекта уз изазивање насиља: када учинилац „неовлашћено уђе на спортски терен или део гледалишта намењен противничким навијачима и изазове насиље“. И овде је нагласак на месту извршења јер се радња врши уласком на тачно одређени, ограничени простор уз изазивање насиља.

4. Умишљајно наношење имовинске штету спортском објекту, које постоји када учинилац „оштећује спортски објекат, његову опрему, уређаје и инсталације“. И овде је битан елемент место извршења.

5. Изазивање националне, расне, верске или друге мржње на јавном скупу или спортској приредби, које проузрокује насиље односно физичке обрачуне, односно ако учинилац „понашањем или паролама на спортској приредби или јавном скупу изазива националну, расну, верску или другу мржњу или нетрпељивост засновану на неком дискриминаторном основу услед чега дође до насиља или физичког обрачуна са учесницима“. (члан 344а став 1).

С обзиром на значај места извршења, али и могућности које дају савремене технологије, занимљиво је подсетити се случајева изазивања нереда „даљински“, коришћењем дронова или сличних средстава извршења. Наравно, и у овом случају су испуњена обележја бића кривичног дела, јер је последица наступила на спортској приредби. Додуше, овде се може сматрати и да је место радње спортска приредба, јер се учинилац, иако није био физички присутан, послужио средством да непосредно изврши радњу.

За основни облик предвиђена је казна затвора од једне до пет година уз новчану казну. Дело се може извршити са умишљајем, директним или евентуалним. (Милошевић, 2022, Чејовић, 2008). Умишљајем учиниоца треба да буду обухваћени сви објективни елементи кривичног дела (радња, последица, време и место извршења).

Први тежи облик, за који је запрећена казна од две до осам година затвора, постоји уколико је дело извршено од стране групе. (Делић, 2021; Милошевић, 2022). Казна од три до дванаест година затвора је запрећена коловођи групе (други тежи облик). Коловођа је лице које руководи групом, припрема и планира њене акције, издаје

наређења и упутства члановима, организационо је структурише итд. (Милошевић, 2022; Стојановић, 2018; Делић, 2021; Чејовић, 2008; Ђорђевић, Коларић, 2020).

Овде вреди поставити питање зашто као најтежи облик није предвиђен случај када дело из ст. 1 изврши организована криминална група. Иако на први поглед изгледа да ово кривично дело није део стандардног „репертоара“ организованог криминала, бројни наводи па и докази о постојању веома озбиљних веза ових група са навијачким организацијама као и коришћењу спортских трибина за вршење других кривичних дела, дају основа да се размишља и у овом правцу.

Трећи квалификовани облик је присутан уколико је приликом извршења основног облика из става 1 „дошло до нереда у коме је неком лицу нанета тешка телесна повреда или је оштећена имовина веће вредности“. (члан 344а став 4). Предвиђена је казна од три до дванаест година затвора. С обзиром на изражавање законодавца, закључујемо да је овде реч о делу квалификованом тежом последицом („дошло до“) , што значи да у односу на нереде у којима су се десиле тешка телесна повреда или велика имовинска штета, учинилац поступа из нехата.

Међутим, овде се оправдано поставља питање да ли се тежа последица дела огледа у изазваном нереду или у проузрокованој тешкој телесној повреди односно знатној имовинској штети. Прво могуће тумачење је да је последица тежег облика конкретна опасност (неред) док је резултат нереда (тешка телесна повреда или имовинска штета) објективни услов инкриминације, који не мора да буде обухваћен кривицом учиниоца (слично као код кривичног дела Угрожавања јавног саобраћаја из члана 289 ст. 1 КЗ, где је последица изазвана опасност по живот и тело учесника у саобраћају или имовину великих размера, док је објективни услов инкриминације лака телесна пореда или имовинска штета изнад 200.000 динара). Овако схваћен смисао инкриминације би се огледао у томе да учинилац строже одговара јер је његова радња проузроковала велику опасност која се огледа у нередима на спортској приредби, уз резултујућу околност која се збила независно од његовог психичког односа (нпр. тешка телесна повреда).

Друго тумачење би било да се и тешка телесна повреда односно знатна имовинска штета имају посматрати као тежа последица, у односу на које мора да буде присутна кривица учиниоца.

Посматрајмо оправданост ових супротстављених тумачења кроз хипотетички пример. Уколико више лица изврши дело из става 1 овог члана, али дође до нереда у којима један од учинилаца умишљајно нанесе тешку телесну повреду оштећеном, поставља се питање правне квалификације. Ако заузмемо став да је тешка телесна повреда елемент бића кривичног дела а не објективни услов инкриминације, учинилац који је нанео тешку телесну повреду би одговарао за лакше кривично дело у односу на остале учиниоце, који нису умишљајно нанели тешку телесну повреду, већ су само изазвали нереде. Наиме, он би одговарао за стицај дела из члана 344а став 1 и чл 121 ст. 1 КЗ, док би они одговарали за дело из члана 344а ст. 4.

Распон казне за стицај дела из чл. 344а ст. 1 и тешке телесне повреде је нижи од распона казне прописаног за тежи облик насилничког понашања на спортској приредби (члан 344а ст. 4 КЗ).

На пример: особа А и три особе: Б, Ц и Г су заједно изазвали нереде својим насилничким понашањем на трибинама, при чему је особа А и умишљајно нанела тешку телесну повреду у односу на коју су Б, Ц и Г поступали из нехата. Кривичноправна „комбинаторика“ запрећених казни, међутим, доводи нас до ситуације у којој закључујемо да је лицу А запрећен нижи распон казне него лицима Б, Ц и Г.

Ипак, овакав резултат би био криминалнополитички неоправдан и у потпуном нескладу са важним кривичноправним начелом правичности и сразмерности.

Ако, пак, прихватимо другачију интерпретацију (да је тешка телесна повреда само објективни услов инкриминације), закључујемо да је лице А учинило дело из члана 344а став 4 у вези ст. 1 КЗ у стицају са тешком телесном повредом. Овде би кривичноправна комбинаторика донела правичнији резултат, јер би лицу А био запрећен значајно строжи распон казне у односу на лица Б, Ц и Г.

Иако делује да овај закључак правнодогматски није лако бранити, треба узети у обзир да два посматрана кривична дела (насилничко понашање на спортској приредби или јавном скупу и тешка телесна повреда) имају различите заштитне објекте (јавни ред и мир наспрам живота и тела). Прихватањем овог тумачења, долазимо до криминалнополитички релативно прихватљивог решења, јер учинилац који је нанео тешку телесну повреда током нереда у чијем је изазивању учествовао, бива строже кривичноправно третиран у односу на учеснике у догађају чији се допринос огледа искључиво у стварању конкретне опасности односно изазивању нереда на спортској приредби, из којих је произашао објективни услов инкриминације. Уосталом, ово решење је применљиво код помињаног кривичног дела угрожавање јавног саобраћаја, односно његовог квалификованог облика - тешког дела против безбедности јавног саобраћаја.

У том духу, ово тумачење се правнодогматски (можда) може бранити аргументом да је реч о стицају две инкриминације које имају различит смисао и циљ, јер једна штити јавни ред и мир и последица јој се огледа у изазваном нереду, док друга санкционише умишљајно нарушавање телесног интегритета пасивног субјекта.

Међутим, и ово решење је само релативно прихватљиво са становишта криминалне политике. Проблем је у запрећеној казни, која је, објективно гледано, веома строга (од три до дванаест година затвора). Питање је да ли је оправдано предвидети овако строг распон казне за кривично дело код ког није нужно утврђивати кривицу учиниоца у односу на насталу тешку телесну повреду или знатну имовинску штету. Другим речима, зар предвиђена казна од три до дванаест година затвора није престрога ако је учиниочев умишљај обухватио само изазивање нереда, док он није имао психички однос (у форми нехата) према конкретној тешкој телсној повреди или знатној имовинској штети? Дакле, оба тумачења су помало криминалнополитички спорна.

Посебан облик кривичног дела из чл. 344а КЗ предвиђен је за службено или одговорно лице које својим пропуштањем доведе до угрожавања живота или тела већег броја људи или имовине веће вредности. Уколико лице одговорно за организацију спортске приредбе или јавног скупа пропусти да спроведе одговарајуће мере обезбеђења како би онемогућило или спречило нереде, запрећена је казна затвора од три месеца до три године кумулативно са новчаном казном.

Примери за непредузимање адекватних мера обезбеђења су бројни. Ту спадају невршење контроле уласка, пропуштање да се физички одвоје навијачи супарничких тимова, пропуштање да се ангажују редари или службеници обезбеђења, невршење или неадекватно вршење процене ризика од насиља, итд. (Стојановић, Перић, 2006: 334).

Веома је интересантно и питање одговорности правног лица – организатора спортске приредбе, за учињена кривична дела на спортској приредби. Одговорност правног лица је уведена Законом о одговорности правних лица за кривична дела („Сл. гласник РС“, број 97/08; у даљем тексту: ЗОПЛКД). (Милошевић, 2012). Одговорност правног лица се заснива на кривици одговорног лица. У складу са чл. 6 ст. 1 и 2 ЗОПЛКД кривично дело правног лица постоји уколико одговорно лице, у склопу својих послова и у намри да оствари корист за правно лице учини кривично дело, али и када је „због непостојања надзора или контроле од стране одговорног лица омогућено извршење кривичног дела у корист правног лица од стране физичког лица које делује под надзором и контролом одговорног лица“. (Кековић, Милошевић, 2011; Милошевић, 2012).

У погледу субјективног елемента, дакле, довољно је да је одговорно лице поступало из нехата услед чега је другом лицу, које је оно иначе дужно да надзире и контролише, омогућено извршење кривичног дела. Ова ситуација није незамислива у вези посебног облика кривичног дела из члана 344а, с тим што би у пракси било тешкоћа приликом доказивања да је правно лице остварило корист од кривичног дела (нпр. желећи да избегну трошкове по клуб, одговорно лице или други запослени који је под његовим надзором, не ангажују редаре и службенике обезбеђења и не организују контролу уласка на спортску пориредбу, услед чега дође до насиља и нереда).

Питање одговорности организатора спортске приредбе се може поставити и када постоји сумња да су нереде подстакла или чак организовала управо одговорна лица из одређеног клуба, савеза или другог спортског правног лица. Иако се и овде јавља проблем доказивања, тешко се може тврдити да оваквих случајева није било. Наравно, ту се не би радило о овом облику кривичног дела.

Ипак, чињеница да за готово 14 година важења овог закона судска пракса готово да не постоји, јер је број осуђујућих кривичних пресуда (али и подигнутих оптужница а чак и поднетих кривичних пријава) против правних лица занемарљиво мали, (Милошевић, Симовић 2018; Бановић, Милошевић, 2014) не даје основа за уверење да ће се тужилаштва и судови у скоријој будућности бавити овим аспектом криминалног феномена насиља на спортским приредбама.

Законодавац у ставу 6 овог члана предвиђа и обавезно изрицање мере безбедности забране присуствовања одређеним спортским приредбама. (Вуковић, 2021; Стојановић, 2018).

Списак прописа и препоручена литература

Закон о јавном окупљању, „Сл.гласник РС“, број 6/16.

Закон о јавном реду и миру, „Сл.гласник РС“, бр. 6/2016, 24/2018.

Закон о спречавању насиља и недоличног понашања на спортским приредбама, „Сл. гласник РС“, бр. 67/03, 101/05,, 90/07, 72/09, 111/09, 104/13, 87/18.

Закона о приватном обезбеђењу („Сл. гласник РС“, бр. 104/13, 42/15, 87/18).

Кривични законик Републике Србије, „Сл. Гласник РС“, бр. . 85/05, 88/05 , 107/05, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19.

Кривични закон Србије, „Сл. гласник СРС, бр. 26/77, 28/77, 43/77, 20/79, 24/84, 39/86, 51/87, 6/89 и 42/89, „Службеник гласник РС“, бр. 21/90, 16/90, 26/91, 75/91, 9/92, 49/92, 51/92, 23/93, 67/93, 47/94, 17/95, 44/98, 10/02, 11/02, 80/02, 39/03 и 67/03

Европска конвенције о насиљу и недоличном понашању гледалаца на спортским приредбама, посебно на фудбалским утакмицама, коју је ратификовала још СФРЈ („Сл. лист СФРЈ – Међународни уговори”, бр. 9/90

Biringer, Betty E., Rudolph V. Matalucci, and Sharon L. O'Connor. 2007. Security Risk Assessment and Management: A professional practice guide for protecting buildings and infrastructures. John Wiley & Sons

Britannica. 2022. Uyghur people, Приступљено 29.9.2022. https://www.britannica.com/topic/Uyghur

Cassese, Antonio. 2006. "The multifaceted criminal notion of terrorism in international law." Journal of International Criminal Justice 4.5 2006: 933-958.

China Law. 2021. Public Security Organ Provisions on Efforts to Counter Organized Crime Приступљено 8.10.2022. https://www.chinalawtranslate.com/en/police-organized-crime-rules

Føllesdal, Andreas, Ramses A. Wessel, and Jan Wouters, eds. 2008. Multilevel regulation and the EU: the interplay between global, European, and national normative processes. BRILL

Greitens, Sheena Chestnut, Myunghee Lee, and Emir Yazici. 2019. "Counterterrorism and preventive repression: China's changing strategy in Xinjiang." International Security 44.3 9-47.

Hart, Stephen D., Christine Michie, and David J. Cooke. 2007. "Precision of actuarial risk assessment instruments: Evaluating the ‘margins of error’of group v. individual predictions of violence." The British Journal of Psychiatry 190.S49 s60-s65.

Monahan, John. 2016. "The individual risk assessment of terrorism: Recent developments." The handbook of the criminology of terrorism 520-534.

OHCHR. 2022. Fight agaiinst Terrorism and Extremism in Xinjiang: Truth and Facts, Приступљено 14.09.2022.: https://www.ohchr.org/sites/default/files/documents/countries/2022-08-31/ANNEX_A.pdf

Seymour, James D., and Michael R. Anderson. 2015. New Ghosts, Old Ghosts: Prisons and Labor Reform Camps in China: Prisons and Labor Reform Camps in China. Routledge

Woo, Gordon.2002. "Quantitative terrorism risk assessment." The Journal of Risk Finance

Влада Србије. 2017. Национална стратегија за спречавање и борбу против тероризма за период 2017–2021. године, „Службени гласник РС“, бр. 94 од 19. октобра 2017, Београд.

Влада Србије. 2020. Стратегија за борбу против прања новца и финансирања тероризма за период 2020–2024. године, „Службени гласник РС“, бр. 14/2020 Београд.

Народна скупштина. 2019. Стратегија националне безбедности Републике Србије, „Службени гласник РС“, бр. 94/2019-13, Београд.

National Money Laundering and Terrorist Financing Risk Assessment Toolkit. World bank. Приступљено 25.10.2022. https://www.worldbank.org/en/topic/financialmarketintegrity/brief/national-money-laundering-and-terrorist-financing-risk-assessment-toolkit-disclaimer-and-terms-of-useБ.Бановић, М. Милошевић, (2014), Повреде људских права од стране корпорација и могућности кривичноправне заштите. Теме, Vol. XXXVIII, no. 3 (јул – септембар 2014), 1251 – 1273

И. Вуковић, (2021), Кривично право – општи део, Београд: Правни факултет Универзитета у Београду.

И. Вуковић (2021а). Прекршајно право, четврто измењено и допуњено издање. Београд: Правни факултет Универзитета у Београду.

Н. Делић, (2013), Нова решења у глави кривичних дела против јавног реда и мира (XXXI). Анали Правног факултета у Београду, 61 (2), стр. 278-294.

Н. Делић, (2021). Кривично право – посебни део. Београд: Правни факултет Универзитета у Београду.

Ђ. Ђорђевић, (2013). Прекршајно право са основама привреднопреступног права. Београд: Криминалистичко-полицијска академија.

Ђ. Ђорђевић, Д. Коларић, (2020). Кривично право – посебни део. Београд: Криминалистичко-полицијски универзитет.

B. M. Zupančič, (2011), Ne bis in idem (zabrana ponovnog suđenja za isto delo): la belle dame sans merci, Crimen: časopis za krivične nauke, 2 (2), pp. 171–178

E. Ivičević-Karas, & D. Kos (2012). Primjena načela ne bis in idem u hrvatskom kaznenom pravu, Hrvatski ljetopis za kazneno pravo i praksu, 19 (2), pp. 555–584. URL: https://hrcak.srce.hr/110872

З. Кековић, М. Милошевић (2011), Криминалитет корпорација – криминолошки и културолошки аспекти, Социолошки преглед, бр. 1/2011, стр. 19-44

М. Милошевић (2012). Одговорност правних лица за кривична дела, докторска дисертација. Правни факултет Универзитета у Београду

М. Милошевић (2022), Кривично право – посебни део: изабране инкриминације за студије наука безбедности, Универзитет у Београду-Факултет безбедности, Београд.

М. Милошевић, И. Симовић (2018). Појам одговорног лица у Закону о одговорности правних лица за кривична дела, стр. 365-382 у: Кривично законодавство и

функционисање правне државе, међународна научно-стручна конференција, Требиње, 20. и 21. 04. 2018. године, Министарство правде Републике Српске, Српско удружење за кривичноправну теорију и праксу, Град Требиње.

Н. Мрвић-Петровић (2014). Коментар новог Закона о прекршајима. Београд: Параграф.

Н. Мрвић-Петровић, (2019). Кривично право – посебни део. Београд: Правни факултет Универзитета Унион и ЈП Службени гласник.

З. Стојановић, (2018). Коментар Кривичног законика. Београд: Службени гласник.

З. Стојановић, О. Перић, (2006). Кривично право – посебни део, 11. издање. Београд: Правни факултет Универзитета у Београду.

Б. Чејовић (2008), Кривично право у судској пракси, III издање, Лион Марк, Крагујевац.

Извештај 2

Предлози за измене и допуне важећих прописа

Прописи у области безбедности информација и сајбер простора. Република Србија је последњих година значајно унапредила национални правни оквир за супротстављање високотехнолошком криминалу и изградњу безбеднијег сајбер простора, али, на основу изнете анализе, закључујемо да исти још увек није на потребном нивоу.

Ово се посебно односи на чињеницу да још увек нису донете посебне стратегије сајбер безбедности и сајбер одбране (иако су надлежни скупштински одбор и владина Канцеларија Савета за националну безбедност указивали на неопходност њеног доношења још од 2013. године), што указује на непостојање системског приступа питању које је од суштинске важности за очување националне безбедности. Новодонети Закон о информационој безбедности није праћен одговарајућом подзаконском регулативом иако су законски рокови за њено доношење истекли. Хармонизација нашег права са одговарајућим међународним стандардима ће остати пуко испуњавање форме уколико се не предузму конкретни потези за усаглашавање друштвене и нормативне стварности, како би потоња постала чврст оквир за одговор на актуелне безбедносне ризике.

Забрињавајуће је и што одредбе закона којима се додељују овлашћења за предузимање специјалних истражних техника, посебних мера и поступака, низ година нису били усклађени са Уставом и међународним уговорима и стандардима заштите неповредивости тајности писма и других средстава комуникације. Иако су, након одговарајућих одлука Уставног суда и каснијих законодавних промена, отклоњене неусаглашености са Уставом, остаје утисак да је ова материја и даље помало конфузна, нејасна и недоречена. Тако, не чини се практичним и функционалним да закони који регулишу рад различитих служби безбедности, те Законик о кривичном поступку, имају прилично различиту и неуједначену терминологију, па се и врсте посебних мера и

поступака разликују (можда не суштински, али и ту остаје простор за недоумице и различита тумачења).

Ово се посебно односи на Закон о БИА и Закон о ВБА и ВОА, који би, с једне стране, свакао требали да се појмовно и материјално ускладе са Закоником о кривичном поступку, али, са друге стране, и да се међусобно поклапају. Можда би боље решење било да Закон о основама уређења служби безбедности на јединствен начин пропише врсте и начин примене посебних мера и поступака служби безбедности, а да предметни закони регулишу само специфичности у начину предузимања мере (посебно у односу на врсту физичких и правних лица према којима се одређују, услед различитог опсега деловања војних служби безбедности). На овај начин би се постигла већа правна сигурност грађана, а обавештајно-безбедносни подсистем сектора националне безбедности би деловао јединственије и хармоничније. Свакако, треба имати у виду да висок степен тајности нужно карактерише рад са обавештајно-безбедносним подацима, услед чега је потребно поштовати и начело ефикасности и економичности рада служби безбедности, које не сме бити нарушено неоправдано рестриктивним приступом законодавца. Очигледно, у овој области је неопходно еквилибрирати између различитих захтева – транспарентности и демократске контроле и заштите безбедности државе, при чему тасови на ваги не смеју отићи исувише на једну или другу страну.

Кривичноправна регулатива превара у сајбер простору омогућава адекватно санкционисање учинилаца и пружа правне квалификације под које се могу подвести бројна друштвено опасна дела изведена коришћењем информационо-комуникационих технологија.

Али, уочен је простор за измене и допуне важећих прописа. У погледу рачунарске преваре, тако, остаје питање да ли је било нужно ограничити законски опис кривичног дела рачунарске преваре на ситуације у којима се као средство извршења и објект радње појављују рачунари и рачунарске мреже, односно процеси електронске обраде и преноса података, или га је требало конструисати тако да се односи на све врсте преварног поступања употребом високих технологија. Уколико се сложимо с ставом да би таква формулација могла да буде сувише уопштена, екстензивна и неодређена, остаје друга могућност – увођење засебног кривичног дела интернет преваре.

Чини нам се ипак, да правно-технички најпогоднije решење може да буде јединствена формулација којом би се објединила рачунарска и интернет превара, и поред потенцијалне ширине и мање одређености таквог законског описа. Наиме, верујемо да би се евентуални приговори могли отклонити стварањем прецизне али и флексибилне формулације која би била сачињена у складу са природом ове врсте инкриминисаног понашања. Мислимо да би биће кривичног дела рачунарске преваре, de lege ferenda, могло да гласи: ко унесе нетачан податак, пропусти да унесе тачан пода- так, на други начин лажно прикаже или прикрије податак или ко- ришћењем интернета или сличних платформи информационо-ко- муникационе технологије, утиче на резултат електронске обраде или преноса података, или доведе или одржава у заблуди друго лице и тиме проузрокује имовинску штету, казниће се...

Наведеном инкриминацијом би се истовремено обухватили случајеви деловања на аутоматску обраду података уношењем или неуношењем података и случајеви

интернет превара чији су објект радње корисници информационо-комуникационих технологија, чиме би се пружила потпунија и адекватнија кривичноправна заштита.

Што се тиче употребе рансомвер малвера, а имајући у виду изнете тешкоће у вези са правном квалификацијом, потребно је размотрити могућност уподобљавања законских решења савременим начинима извршења кривичних дела у сајбер-простору, односно проблем коришћења рансомвер малвера. Важеће кривичноправне норме не пружају адекватну заштиту од злоупотребе рачунарских малвера у форми рансомвер-напада. Постојеће одредбе доводе до озбиљних тешкоћа у тумачењу, односно компликују правну квалификацију дела, а и не обухватају сва друштвено опасна понашања која заслужују кривичноправну реакцију. Изменом постојеће инкриминације из члана 300 КЗ-а или увођењем новог кривичног дела (рачунарска изнуда/принуда) које предлажемо, ове противречности и непотпуности би биле отклоњене, а кривичноправна заштита од савремених начина извршења кривичних дела у сајбер-простору значајно побољшана.

Овде би кривичноправна заштита могла да буде унапређена увођењем допунских облика кривичног дела из члана 300 или новог кривичног дела. Овај нови облик/ дело би постојао ако би учинилац унео рачунарски вирус или други малициозни код у туђ рачунар или рачунарску мрежу и тако стекао контролу над радом рачунара, што би искористио тако што би ставио у изглед оштећеном да ће му коришћење тих програма и података на даље бити онемогућено уколико не поступи по његовим захтевима. Дакле, учинилац „заробљава“ туђ рачунар, односно програме и податке који се налазе на њему и принуђава оштећеног на одређено чињење или нечињење, јер ће у супротном рачунар остати закључан или ће подаци бити злоупотребљени.

Сама законска формулација бића кривичног дела могла би да гласи: ко са наме- ром да принуди другог да нешто учини, не учини или трпи, унесе рачунарски вирус или сличан рачунарски програм или скуп наредби у туђ рачунар или рачунарску мрежу и тиме стекне контролу над радом рачунара или појединих података или програма, казниће се...

Уз то, било би оправдано да се уведе и још тежи облик, који би гласио: уколико је извршењем дела из претходног става учинилац стекао противправну имовинску корист или проузроковао имовинску штету у износу од ..., или су наступиле друге тешке последице, казниће се...Могући најтежи облик би се односио на изазивање опасности по живот или здравље грађана или угрожавање функционисања привреде или критичне инфраструктуре (снабдевање природним енергентима, саобраћај итд.).

Првопоменути облик би инкриминисао само употребу рансомвер-програма у одређеној намери, док би тежи облик прописивао строже казне уколико је дошло до наношења штете, стицања противправне имовинске користи или других тешких последица (нпр. последица по приватни живот, здравље, углед и част или радно ме- сто оштећеног, односно, у случају да је пасивни субјект правно лице – блокаду рада, репутациону штету, одговорност према трећим лицима и сл.).

Запрећена казна би требало да буде адекватна и сразмерна стварној друштвеној опасности. Сматрамо да тренд коришћења ове врсте малвера и потенцијалне кон-

секвенце његове употребе, оправдају увођење новог кривичног дела или стварање допунских облика дела из члана 300.

Такође, овако би се избегле практичне тешкоће приликом примене права, јер би се решиле недоумице око правне квалификације. Ново дело – рачунарска изнуда/ принуда (или, евентуално, нови облици кривичног дела из члана 300), јасно би се разликовало у односу на остала кривична дела и имало би адекватан распон казне, посматрајући из аспекта апстрактне друштвене опасности ових противправних по- нашања. Увођењем квалификованих облика које предлажемо, обухватио би се читав делокруг радњи којима се пасивни субјекти угрожавају помоћу рансомвер-вируса, односно малициозних кодова.

У области казненоправне заштите тајних података, дошли смо до следећих предлога de lege ferenda. У области кривичноправне заштите има више идентификованих проблема које је потребно отклонити законодавном интервенцијом. Проблем односа КЗ и ЗТП Ковачевић и Милошевић третирају на следећи начин: „поставља се питање да ли су у КЗ-у оправдано задржана кривична дела одавање службене тајне (чл. 369) и одавање војне тајне (чл. 415).

Те категорије тајних података укинуте су доношењем ЗТП-а (видети члан 109), али сигурно није извршено (или у јавности није познато) преиспитивање ознака свих докумената и података који су проглашени за војну или службену тајну по прописима који су важили до ступања на снагу ЗТП-а, иако је члан 105 став 2 овог прописа експлицитно одредио да је то потребно учинити у року од две године од ступања закона на снагу. Ипак, члан 105 став 1 ЗТП-а јасно одређује да документи и по- даци означени по одредбама раније важећих прописа задржавају врсту и степен тајности које су имали (члан 105, став 1 ЗТП-а). Интенција законодавца да се преиспитају све раније утврђене ознаке тајности тешко је могла бити спроведена у пракси због претпостављеног обима и бројности означених података и докумената.

Имајући у виду одредбу члана 105 став 1 ЗТП-а, јасно је да одредбе КЗ-а којима се инкриминишу одавање војне и службене тајне морају остати на снази докле год су присутни документи и подаци који су означени као наведене врсте тајних података“ (Ковачевић, Милошевић, 2022: 101, 102).

Чињеница да је од доношења ЗТП протекло 13 година не улива оптимизам у погледу оначног уједначавања законских одредби о санкционисању друштвено опасних радњи против различитих категорија тајних података. У литератури се истичу и други недостаци законског одређења свих наведених кривичних дела. (Милошевић, 2022; Ковачевић, Милошевић, 2022).

У погледу прекршајне одговорности, налазимо следеће. Помало је спорна радња извршења прекршаја из чл. 99 тач. 13 ЗТП, која постоји када лице „тајне податке достави правним и физичким лицима супротно одредби члана 46. овог закона“. Овде се ради о достављању тајних података на основу уговорног односа између органа јавне власти и правног или физичког лица које му пружа одређене услуге. Достављање тајних података у случају постојања оваквог уговорног односа је могуће уз испуњење законских услова (правно или физичко лице испуњава организационе и техничке услове за чување тајних података у складу са овим законом и другим прописима; за

лица која обављају уговорене послове су извршене безбедносне провере и издати сертификати и она писаном изјавом потврде да су упозната са овим законом и другим прописима који уређују чување тајних података и обавезују се да ће са тајним подацима поступати у складу са тим прописима; приступ тајним подацима је неопходно потребан ради реализације послова из уговора – чл. 46 ст. 1 тач. 1 до 4 ЗТП). Међутим, у пракси неће бити једноставно разграничити радњу овог прекршаја од радње нехатног облика кривичног дела (чл. 98 ст. 5 ЗТП), а понекад чак и од умишљајног облика дела. У оба случаја непозвано лице се упознаје са садржином тајног податка од стране овлашћеног лица (дакле, лица ком су тајни подаци поверени). Сматрамо да је биће овог прекршаја требало да буде уже и прецизније дефинисано, посебно знајући огромне разлике у одговорности и запрећеној казни између прекршаја и кривичног дела против тајности података.

Такође, чини нам се да је законодавац начинио пропуст тиме што није донео посебне казнене одредбе којим би ближе регулисао одговорност правног или физичког лица које по основу уговорног односа остварује увид у тајне податке органа јавне власти ради обављања послова предвиђених уговором. Мислимо да је материја довољно важна и осетљива те да заслужује посебне одредбе а не санкционисање кроз квалификовање путем других казнених одредби.

У погледу казненоправне заштите пословне тајне, закључци су следећи. Дефинисана радња извршења прекршаја се у највећој мери поклапа са радњом кривичног дела из чл. 240 ст. 1 КЗ. Штавише, она је шира од радње кривичног дела јер обухвата и акте незаконитог прибављања и коришћења пословне тајне од стране непозваног лица, док се кривично дело односи само на одавање пословне тајне које учини овлашћени држалац пословне тајне. Имајући у виду изузетне разлике у запрећеним казнама (нпр. и казна за нехатни облик дела из чл. 240 је далеко строжа од прописаних казни због привредних преступа и прекршаја), констатујемо да је овде реч о озбиљним системским неусаглашеностима. (Milošević, 2021a: 62, 63). Оправдано се поставља питање да ли је кривичноправна заштита неопходна или је довољно да се држаоцу пословне тајне остави само заштита коју осигуравају друге гране права. Ако кривичноправна заштита јесте потребна, нужне су законске измене у циљу усаглашавања прописа.

Прописи у области управљања ризицима од катастрофа. Потребно је извршити измене подзаконских прописа којима се регулише методологија за процену ризика од катастрофа. Републички штаб за ванредне ситуације треба у што краћем временском року да усвоји Национални план заштите и спасавања. Изменама и допунама прописа треба увести строже санкције за непоштовање прописа у области ванредних ситуација и створити услове за кадровско попуњавање органа односно служби задужених за спровођење инспекцијског надзора.

Прописи у области заштите од појединих форми криминалитета. Уставно уређење и национална безбедност неспорно представљају важан објект кривичноправне заштите. Ипак, специфичности тзв. политичких добара, недовољна одређеност појма јавног или општег добра и сложен и динамичан однос између заштите безбедности заједнице и остваривања основних индивидуалних права и слобода постављају низ

дилема пред субјекте криминалне политике, међу којима је најважније питање граница и легитимитета кривичноправне репресије.

Одређене легислативне промене су заиста потребне, а неке су већ и учињене. Тако, измештањем кривичног дела тероризма из једне у другу главу КЗ-а законодавац је пропустио да засебно предвиди кажњавање припремних радњи за ово кривично дело, тако да су оне практично биле декриминализоване. Додуше, један облик припремања је био инкриминисан кроз члан 393а (терористичко удруживање). Знајући степен друштвене опасности припремања тероризма, овај пропуст се мора сматрати значајним. Срећом, доношењем ЗИД КЗ из 2016. године овај недостатак је отклоњен.

Друго, занимљиво је приметити да је најтежи облик кривичног дела тероризма, из члана 391 став 4 КЗ-а, које постоји уколико је приликом извршења терористичке радње једно или више лица са умишљајем лишено живота, дело са најстрожом запрећеном казном у домаћем законодавству. Ово закључујемо на основу посебног минимума. Иако има још кривичних дела за која је запрећена казна доживотног затвора алтернативно са казном затвора, ово је једино чији посебни минимум износи чак 12 година (код тешког убиства минимум је 10, а код геноцида, злочина против човечности и ратних злочина пет година затвора). Питање је да ли је ово решење оправдано. С друге стране, код најтежег облика тероризма постоји могућност условног отпуста, за разлику од кривичних дела наведених у чл. 46, ст. 5 КЗ-а, што је такође дубиозно.

Инкриминација из члана 391а, која инкриминише јавно изношење или проношење идеја којима се посредно или непосредно позива на вршење дела из члана 391а је оправдано унета у домаће кривично законодавство, и поред недовољне прецизности појединих појмова (нпр. појма идеје). (Бановић 2019: 360–361). Иако је законодавчева интенција усаглашавање са међународноправним актима, судска пракса треба да буде изузетно пажљива приликом примене ове „каучук" норме. Практично, овде се кажњава и „неодређено проношење идеја, које посредно подстичу на извршење таквог акта". (Вуковић 2019: 156). Тек ће правилна примена права показати пуну оправданост уношења овог кривичног дела у домаће законодавство. У досадашњој пракси присутна је само једна правноснажна пресуда за кривично дело из члана 391а, па свакако треба бити опрезан приликом доношења закључака (Бановић 2019: 356).

Учесници пројекта су у свом раду вршили и упоредну анализу нормативно-стратешког оквира за супротстављање ризицима од организованог криминала, тероризма и екстремизма НР Кине и Р. Србије и дошли до следећих запажања. НР Кина представља академски релевантан случај велике силе у међународном систему, чији би пример правног регулисања тероризма, екстремизма и унутрашњих претњи националној безбедности, могао да послужи као релевантан извор за систематичније уређивање правних решења у случају других земаља. У наставку ће бити приказана важни проблеми која су третирани правним актима на стратешком нивоу – супротстављање тероризму и етно-религијском екстремизму, прецизније ситуација у кинеској западној провинцији Синђанг, али и изазови са проблемима унутрашње безбедности који се односе на ситуацију у Хонг Конгу, као и проблеми са оспореном сувереношћу на делу кинеске територије коју званични Пекинг третира делом Кине – Тајваном.

Провинцију Синђанг насељавају претежно Ујгури, туркофона национална мањина, сунитских муслимана којих у Кини има око 10 милиона (Britannica 2022). Међуетничке

тензије које су настајале током претходне три деценије у овој провинцији између Кинеза (Хан) и Ујгура, кулминирале су серијом инцидената током 2009. године у којима је живот изгубило око 200 Хан Кинеза што је условило систематичну борбу централних власти против екстремизма и, како су их тада оцениле, „тероризма у овој области“. Једно од првих нормативних одговора централних власти на изазове у поменутој провинцији био је кинески Закон о супротстављању тероризму из 2015. године. Он третира тероризам као сваки „предлог или радњу која ствара друштвену панику, угрожава јавну безбедност, нарушава личност и имовину или врши принуду над националним властима или међународним организацијама, методама као што су насиље, уништавање, застрашивање, како би постигле њихове политичке, идеолошке или друге циљеве“ (China Counter-terrorism Law 2015: art. 3). Занимљиво је да Закон укључује Кинеску народноослободилачку армију, кинеске народне оружане полицијске снаге и организације народне милиције у спречавање и руковођење терористичким активностима уз ангажовање институција на националном, али и на нивоу провинција, за борбу против тероризма. Посебно поглавље Закона посвећено је анализи безбедносне проблематике и превенције терористичких активности на територији Кине. Закон предвиђа да сви телекомуникациони и интернет оператори морају да, када открију информације које указују на могуће планирање терористичких или екстремистичких аката, одмах обуставе њихов пренос и избришу релевантне информације или затворе релевантне веб странице и укину релевантне услуге, а такве кориснике пријаве надлежним органима (China Counter-terrorism Law 2015: art. 19).

Закон додатно регулише услове под којима се суди за специфична кривична дела тероризма и осталих екстремистичких активности – попут распиривања међуетничке, верске или идеолошке мржње, као и битнија нарушавања јавне безбедности. Међутим, оно што је особеност овог закона, а што је један од коренитих узрока због којих званични Пекинг трпи критике међународне заједнице и оптужбе западних држава предвођених САД, односи се на третирање затвореника након одслужења затворске казне. Према одредбама овог акта, за осуђенике који су одслужили казну затвора пре пуштања на слободу по одслужењу казне, „надлежне инстанце врше процену њихове опасности по друштво на основу природе, околности и штете по друштво њиховог злочина, њиховог понашања током издржавања казне и утицаја њиховог пуштања на слободу на њихову заједницу“ (China Counter-terrorism Law 2015: art. 30). Када процене укажу да осуђеници представљају опасност по друштво, затворски службеници имају задатак да доставе суду препоруку за упућивање у „едукативне кампове“ у месту издржавања казне, а копију писмене препоруке шаљу и тужилаштву за исти степен (2015, art. 30).

Следећа важна одлика овог закона јесте и сарадња између државних институција и органа у пословима супротстављања тероризму и то између министарстава (ориг. „одељења Државног савета“) који у својим портфељима имају различите ресоре. Тако закон предвиђа да министарства НР Кине за спољне послове, јавну безбедност, националну безбедност, развој и реформу, индустрију и информатичко друштво, трговину и туризам, треба да успоставе системе за процену ризика која би повећала степен безбедносне заштите кинеских држављана у земљи и иностранству, и осигурала кинеске компаније, објекте инвестирања или средства са седиштем ван територије копна, ради спречавања и реаговања на терористичке нападе (2015, art. 41). Закон још

регулише питања прикупљања обавештајних података, одговора на кризе, затим врсте и начине истражних поступака, те облике међународне сарадње.

У мају 2021. године Кина је усвојила посебан акт са снагом закона који се односи на улогу јавних органа безбедности у супротстављању организованом криминалу. Закон регулише превенцију и управљање процесом борбе против организованог криминала које имплементирају државни органи Кине, као и верификацију за прикупљање података. Према одредбама акта, органи јавне безбедности дужни су да користе савремену информациону технологију у складу са законом за успостављање механизма за прикупљање, истраживање и процену трагова организованог криминала и руковање њима путем оцењивања и класификације. Органи јавне безбедности благовремено спроводе „статистичке, аналитичке, истраживачке и судске послове о траговима организованог криминала и организују инспекцијски надзор у складу са законом; за питања која не спадају у делокруг органа јавне безбедности, предају се надлежним надлежним органима на решавање у складу са законом“ (China Law 2021).

Паралелно са нормативно-правном регулацијом проблема са којима се суочава Кина у погледу националне безбедности, теку активности званичног Пекина на мултилатералном нивоу које се огледају у активностима испољеним нарочито према међународним организацијама, а доминантно у систему Уједињених нација. Крајем августа 2022. године, Кина је предала извештај под називом "Борба против тероризма и екстремизма у Синђангу: истина и чињенице" канцеларији високог комесара Уједињених нација за људска права (енг. The Office of High Commissioner for Human Rights – OHCHR). У документу на преко 100 страница, Кина настоји да оправда постојање „кампова за едукацију“ као борбу против тероризма и екстремизма која је потребна и оправдана (OHCHR, 2022). Коначно, наводи се да због последица терористичких активности у западној провинцији испаштају бројне етничке групе, и да је борба централних власти против екстремизма у овом делу државе управо подржана од стране свих народа који настањују Кину (2022: 12). Према тврдњама из извештаја, „кампови за едукацију“ су места за дерадикализацију који су успостављени у складу са законом“ (2022: 47).

По закључцима аутора потребно је:

1. Спровести процену ризика по безбедност критичне енергетске инфраструктуре, а нарочито оне која је подложна саботажама и терористичким активностима.

Диверсификација снабдевања енергентима је нарочито постала актуелна током кризе у Украјини, што је додатно учинило сложеним међународнополитички положај у ком се Република Србија тренутно налази. Нова безбедносна архитектура у Европи условила је различите модалитете допремања нафте и гаса који укључују употребу знатно ширег опсега инфраструктурних објеката и инсталација које су подложне намерно изазваним кваровима – саботажама. Због тога је потребно индексирати јавно доступне податке ресорних министарстава и других надлежних органа о критичној (енергетској) инфраструктури и спровести систематичну анализу ризика по њену безбедност и последице које би настале услед кварова.

2. Спровести процену безбедносних ризика и заштиту дипломатских и конзуларних објеката Републике Србије у иностранству од екстремистичких и терористичких активности.

Заштита држављана Републике Србије и њихова ванредна репатријација у случају инцидентних ситуација у иностранству одговара једној од одредби Стратегије националне безбедности из 2019. године. Међутим, Стратегија не препознаје дипломатско-конзуларна представништва као објекте заштите, који нарочито могу бити изложени екстремистичком деловању, нарочито због осетљивих спољнополитичких одлука које званични Београд доноси у погледу тренутних дешавања у међународним односима. Због тога би требало спровести систематичну процену ризика по објекте дипломатског представљања Србије у иностранству уз коришћење бројних варијабли помоћу којих би се идентификовао ниво ризика.

3. Учинити део варијабли Националне базе података за спречавање и борбу против тероризма доступним за академска проучавања.

Национална база је тренутно (2022) у процесу оснивања, пошто је Закон који је предвиђа, усвојен 2021. године. Узимајући у обзир да се индексирање и унос веће количине података може очекивати током ове и наредних година, одређене варијабле могу представљати плодотворну основу за спровођење статистичких и других анализа које ће бити од значаја за даље побољшање општег нивоа безбедности Републике Србије. Могућу препреку таквом напору представља члан 11 Закона који предвиђа да се подаци садржани у Националној бази чувају „у електронској форми и штите у складу са одредбама закона који уређује заштиту тајних података, закона који уређује заштиту података о личности и закона који уређује информациону безбедност“ (Народна скупштина 2021: чл. 11), а приступ подацима осим БИА која администрира базом, имају само надлежни државни органи на основу посебног захтева који мора бити оправдан. Из тог разлога, било би пожељно да се део варијабли попут броја индексираних (потенцијалних) учинилаца кривичних дела у вези с тероризмом, или других статистичких података који би представљали значајан улазни параметар за софтверску симулацију, учини доступним академским институцијама зарад прецизнијег објашњења и предикције трендова у будућности. Такво решење видљиво је и у кинеском закону о учешћу органа јавне безбедности у супротстављању тероризму.

4. Укључивање представника академске заједнице и повећање сарадње ресорних министарстава у погледу креирања нове стратегије за борбу против тероризма.

Слично као и у случају НР Кине, Национална стратегија Србије (која је од 2021. године застарела), предвиђала је структурисана буџетска средства и сарадњу у њеном спровођењу између Министарства правде, Министарства културе и информисања, Министарства трговине, туризма и телекомуникација, МУП-а, Безбедносно-информативне агенције, Министарства спољних послова и Тужилаштва за организовани криминал. Поред јаче међуресорне сарадње, потребно је основати радну групу за израду нове стратегије за период 2023-2027, коју би чинили и представници академске заједнице.

Кривичноправна реакција је крајње средство казнене политике, које се примењује када су репресивне мере предвиђене другим прописима недовољно ефикасне, неприкладне или несразмерне друштвеној опасности датог понашања. Иако су се кривична дела учињена током спортских приредби могла санкционисати на основу постојећих инкриминација, законодавац је исправно одлучио да прописивањем новог кривичног дела изрази и адекватно казни понашања која су квалитативно различита у односу на друге инкриминације управо због околности да су учињена током и на утакмици или манифестацији односно јавном скупу.

Такође, законодавац се руководио и чињеницом да одређена понашања на спортским приредбама нису испуњавала обележја ниједног од постојећих кривичних дела, али су због степена друштвене опасности заслуживала кривичноправну реакцију. Увођењем кривичног дела из члана 344а КЗ, кривичноправна заштита од насилничког понашања на спортској приредби или јавном скупу је добила садашњи изглед.

Инкриминација из члана 344а је релативно обухватна тако да се под њен опсег могу уврстити типичне радње извршења друштвено опасних дела на утакмицама и манифестацијама. Формулације су флексибилне и омогућавају да се, у дозвољеним границама тумачења, под ово кривично дело подведу акти који заслужују кривичноправни третман.

Ипак, формулација има и недостатке, чије превазилажење представља велики и тежак практични изазов. Прво, супротстављена тумачења приликом примене члана 344а постављају озбиљне дилеме. Ако се прихвати да учинилац који умишљајно нанесе тешку телесну повреду пасивном субјекту приликом вршења насилничког понашања на спортској приредби одговара за стицај дела из чл. 344а ст. 1 и чл. 121 ст. 1, долазимо до криминалнополитички непримерене и неприхватљиве ситуације у којој ће њему бити запрећена нижа казна у односу на лица која су учинила дело из чл. 344а ст. 4, односно за која није утврђено да су умишљајно нанела тешку телесну повреду неком. Имајући у виду да кривичноправне норме треба тумачити уско и да аналогија није дозвољена, а да су правнодогматски могућа оба тумачења, сматрамо да би једино законодавна интервенција могла да отклони овај недостатак.

Законодавац би требао јасно да раздвоји ове ситуације, прописивањем засебног става у ком би био прописан најтежи облик кривичног дела из члана 344а, који би гласио: „ако је при извршењу дела из става 1 неком лицу са умишљајем нанета тешка телесна повреда...“. Уз постојање овог става, претходна расправа о тумачењу обележја тежег облика кривичног дела из чл. 344а ст. 4 би изгубила на значају, јер не би долазило до неприхватљивих криминалнополитичких ефеката.

Други недостатак, по нама, је непостојање квалификованог облика који би посебно строго санкционисао злоупотребу спортских приредби за вршење дела организованог криминала. Сумње да се поједине навијачке групе или њихови делови односно појединци годинама користе за обрачуне организованих криминалних група, као и да се насилнички испади на стадионима понекад врше ради остваривања циљева организованог криминала, оправдавају законодаван потез који би уважио криминалну реалност.

Треће, управо због запрећених казни би требало размислити и о увођењу још једног квалификованог облика, који би постојао у случају да је услед нереда дошло до смрти једног или више лица. Таквим обликом би се могао прописати адекватнији распон казне од оног који би се добио у случају одмеравања казне за стицај овог кривичног дела и нехатног лишења живота.

Коначно, веома је важно размотрити питање односа прекршајне и кривичне одговорности код насилничког понашања на спортским приредбама. (Ђорђевић, 2013; Вуковић, 2021а). Слични описи прекршајних дела из ЗНСП и кривичног дела из члана 344а ст. 1 доводе до практичних проблема, попут оног да због једноставности и брзине поступања, полиција по правилу далеко чешће подноси прекршајне него кривичне пријаве, иако су у конкретном случају можда била испуњена и обележја кривичног дела. (Мрвић-Петровић, 2014).

Овде се сусрећемо и са важењем процесног начела не двапут о истом, услед чијег дејства није дозвољено водити кривични поступак након што је прекршајни већ довршен, уколико су у чињенични супстрат пресуде унета обележја казненог догађаја. Овде се јављају бројна спорна питања, о којима је одлучивао и Европски суд за људска права. (Zupančič, 2011; Ivičević-Karas, Kos, 2012). Такође, питање је и да ли је било заиста нужно укључити све алтернативне радње извршења у биће кривичног дела из члана 344а уколико се прекршајна заштита показала довољном У сваком случају, прецизније разграничење између бића кривичног дела и прекршаја је неопходно ради правне сигурности и економичности и ефикасности приликом примене права.

Извештај 3

Смернице и стандарди за оцену квалитета и применљивости правног оквира

Безбедност сајбер простора и информација. У области безбедности сајбер простора и информација још увек нису донете посебне стратегије сајбер безбедности и сајбер одбране (иако су надлежни скупштински одбор и владина Канцеларија Савета за националну безбедност указивали на неопходност њеног доношења још од 2013. године), што указује на непостојање системског приступа питању које је од суштинске важности за очување националне безбедности. Новодонети Закон о информационој безбедности није праћен довољно разгранатом подзаконском регулативом иако су законски рокови за њено доношење истекли. Хармонизација нашег права са одговарајућим међународним стандардима ће остати пуко испуњавање форме уколико се не предузму конкретни потези за усаглашавање друштвене и нормативне стварности, како би потоња постала чврст оквир за одговор на актуелне безбедносне ризике.

Борба против високотехнолошког криминала захтева улагање додатних напора ради унапређења правног оквира, о чему смо писали у оквиру Извештаја 2. Поред тога,

нужно је побољшати услове за имплементацију прописа, првенствено кроз јачање кадровских и логистичких капацитета посебних одељења државних органа задужених за супротстављање и превенцију високотехнолошког криминала.

Иста оцена се може изнети и у погледу прописа којима се регулише обрада и заштита података. Могућности за злоупотребу података су се последњих деценија значајно увећале. Дигитална ера је донела бројне погодности, али и ризике и изазове. Суочавање са новим безбедносним ризицима на плану заштите података захтева изградњу солидног и хармоничног правног оквира, усаглашеног са међународним изворима права, стандардима и добрим праксама.

Казненоправни оквир заштите података у Републици Србији је релативно развијен и обухватан, али не и у потпуности кохеренатан и непротивречан. У извештају су изнете озбиљне критике поводом појединих законских решења, односно међусобне неусаглашености прописа и проблема који настају у практичној примени права, услед судара прекршајних и кривичних (негде и привреднопреступних) норми, нарочито у контексту процесне забране не двапут о истом.

Правни оквир се не може оценити као потпуно адекватан док се законодавном интервенцијом не отклоне примећени недостаци. Посматрајући казненоправне одредбе о тајним подацима, пословној тајни, подацима о личности и професионалној тајни, закључили смо да су потребне измене и допуне закона, првенствено ради међусобне хармонизације. Такође, знајући колико је област заштите података у дигитално доба динамична и развијена, сматрамо да субјекти криминалне политике морају да буду свесни потребе за честим мењањем односно ажурирањем прописа, како би правна реалност „ухватила корак“ са брзо растућим ризицима, првенствено у сајбер простору.

Коначно, правни прописи имају велику улогу на репресивном и превентивном плану. Мислимо да је изградња адекватног правног оквира од суштинског значаја и за јачање безбедносне културе, као и очување основних људских права и заштиту важних и легитимних личних, националних и корпорацијских интереса.

Безбедност у области управљања ризиком од катастрофа. И поред унапређења нормативног оквира и побољшања кадровских и логистичких услова, потребна су додатна побољшања позитивноправних решења и већи степен имплементације прописа. Важно је обезбедити пуно поштовање законских обавеза субјеката у области смањења ризика од катастрофа. Нужно је да се израђују плански документи и процене на локалном, корпоративном и националном нивоу јер број завршених и усвојених докумената ни изблиза није довољан.

Борба против појединих форми криминалитета (организованог криминала, екстремизма и тероризма и других одабраних облика насилничког криминалитета). Кривична дела којима се штите политичка добра у најужем смислу, односно витални елементи система националне безбедности, представљају легитиман и деликатан предмет кривичног права. Кривично право је неопходан инструмент заштите система националне безбедности, иако је кључ у превентивној, а не репресивној компоненти заштите. Премда су законска решења генерално прихватљива, потребан је велики опрез судске праксе приликом тумачења и примене одредби кривичног законодавства због инхерентне опасности од злоупотребе права у политичке сврхе. Намера кривичног

законодавца није да се онемогући опозиционо политичко деловање или изношење супротних политичких гледишта, већ да се забране све противуставне радње којима се покушава довести у питање сувереност државе. Без обзира на различите политичке приступе и мотиве, под делокруг кривичног права морају да дођу сви облици политичког деловања који циљају ка угрожавању уставног уређења и безбедности, што оправдава постојање ових инкриминација, уз одговарајуће тумачење њихових елемената у судској пракси. Уједначавање стратешких докумената, израда нацпоналних процена и евиденционих интерактивних база представљају велики корак напред. Разумевање и усвајање појединих елемената упоредних система је значајно за даље изграђивање и одрживост националног система борбе против најттежих форми криминалитета. Насиље на спортским приредбама је посебно опасно због оправданих сумњи у повезаност изгредника који организовано делују са другим формама криминалног деловања, пре свега организованим криминалом.

Смернице и стандарди: Степен хармонизације са политикама, стратегијама и прописима ЕУ. Потпуна и адекватна подзаконска регулатива у свим посматраним областима. Одговорајуће измене и допуне прописа. Законодавна интервенција ради отклањања судара између одредаба различитих прописа. Развијенија судска пракса, број покренутих и довршених кривичних, прекршајних, привреднопреступних и парничних поступака поводом кршења права у области заштите безбедности информација и заштите сајбер простора. Примена законских механизама којима се уводи одговорност правних лица за кривична дела.

Строжа казнена политика у области смањења ризика од катастрофа. Фреквентније и адекватније спровођење инспекцијског надзора у области процене ризика од катастрофа и планирања заштите и спасавања као и заштите од пожара и заштите од хемијских удеса. Измене прописа којима се уређује методологија процене ризика. Испуњавање законских обавеза државних органа везаних за планирање заштите и спасавања на националном нивоу. Доношење планских докумената на републичком нивоу. Усаглашавање прописа у области одбране, ванредних ситуација, заштите лица, имовине и пословања, противпожарне заштите и заштите критичне инфраструктуре.

Јасније уређење обавеза субјеката корпоративне безбедности уз строжу контролу усаглашености њиховог рада са законским нормама. Нормативно уређење питања од значаја за развој безбедносне културе грађана, посебно у области личне и колективне заштите, првенствено кроз образовне програме. Учинити систем сањења ризика од катастрофа прилагодљивијим и резилијентнијим на националном, корпоративном и локалном плану. Уједначавање садржине процена и планских докумената на локалном и корпоративном нивоу.

Поновно разматрање места и улоге система цивилне заштите, у контексту њеног унапређења, јачања и делимичне професионализације. Поновно разматрање предности и недостатака концепта цивилне одбране и њеног места у систему одбране, као и стандардизовање система управљања континуитетом пословања на различитим нивоима.

Измене и допуне извесних кривичноправних одредби о санкционисању кривичних дела против уставног уређења и безбедности ради њихове међусобне хармонизације. Израда стратешких докумената и њихова пуна оперционализација у области борбе против организованог криминала, тероризма и екстремизма. Разматрање потребе за засебним нормативним уређењем феномена сајбер тероризма. Адекватније нормативно уређење и уједначавање судске праксе у областиборбе против насиља на спортским приредбама.