Сајбер безбедност у Србији: преглед нормативног оквира

Горан Сандић
Марина Радовановић

30. јун 2023.

Сајбер безбедност подразумева низ активности усмерених на заштиту мрежа и информационих система, корисника тих система и других особа на које сајбер претње утичу. Неспорно је да је у протеклом периоду уложен значајан напор у нормирању области сајбер безбедности у Србији. Преглед нормативног оквира показује да усвојене стратегије, закони и подзаконски акти (уредбе, правилници и упутства) обухватају различите димензије сајбер безбедности.

Будући да је скоро цео домаћи законодавни и стратешки оквир у овој области настао након 2009. године, постоји висок ниво хармонизације са Конвенцијом Савета Европе о високотехнолошком криминалу. Но, потребно је да Република Србија чим пре усклади своје прописе са новоратификованим Другим додатним протоколом уз Конвенцију и усвоји неопходне подзаконске акте за његово спровођење.

Теме дигитализације и развоја информационог друштва постале су нарочито заступљене. Међутим, утисак је да не постоји јасан и свеобухватан приступ који би интегрисао дигитализацију и сајбер безбедност и тако предупредио ризике које савремене технологије доносе.

Стога је, у циљу постизања интегрисаног и холистичког приступа сајбер безбедности у Србији, потребна координација између релевантних институција, сектора и стручњака из области дигитализације и сајбер безбедности. То би омогућило да **дигитализација буде безбедна** и да се ризици минимизирају, чиме би се створило повољно окружење за даљи развој информационог друштва и искоришћавање предности које модерне технологије пружају.

Увод

У брзом развоју технологија у 21. веку, сајбер безбедност је постала једна од кључних глобалних брига која превазилази државне границе и утиче на сваки аспект друштва.

Иако не постоји универзално прихваћена дефиниција, уврежено схватање сајбер безбедности подразумева **активности које су неопходне за заштиту мрежа и информационих система, корисника тих система, као и других особа на које сајбер претње утичу**.

Сајбер безбедност обухвата и наше приватне поруке, лозинке, документе на рачунарима, као и онлајн куповину.

Зато је битно да у правним оквирима обезбедимо заштиту свих уређаја и система, без обзира на величину и сложеност.

То значи да су потребни закони и правила која штите како ваш мобилни телефон, тако и системе које користе и државне институције.

Значај правног регулисања сајбер безбедности уочава се и на примеру Србије. Убрзана дигитализација, посебно у домену јавне управе, важан је елемент укупног привредног и друштвеног развоја Србије. Међутим, упоредо са ширењем дигитализације – из године у годину повећава се број инцидената у сајбер простору. Осим тога, прекогранични карактер сајбер криминала отежава спровођење истрага, али и мере превенције.

Тако се сајбер безбедност у Србији тиче информационог друштва, ризика, електронског пословања, мрежа, високотехнолошког криминала, електронске управе, критичне инфраструктуре, електронских комуникација, заштите малолетника и других осетљивих група, вештачке интелигенције, али и саме националне безбедности.

На странама које следе је преглед међународноправног и домаћег правног оквира за сајбер безбедност у Србији.

Међународноправни оквир

Република Србија је потписница неколико међународних уговора у области сајбер безбедности и стратешки је усмерена на праћење развоја одређених међународних стандарда у овој области. Будући да Устав Републике Србије предвиђа да су општеприхваћена правила међународног права и потврђени међународни уговори саставни део правног поретка Републике Србије и да се непосредно примењују, важно је представити којим уговорима је Република Србија обавезана.

- **Конвенција Савета Европе о високотехнолошком криминалу** је најзначајнији уговор у овој области, а Република Србија ју је ратификовала 2009. године.
- **Додатни протокол уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система**.
- **Други додатни протокол уз Конвенцију о високотехнолошком криминалу о појачаној сарадњи и откривању електронских доказа**.

Кривична дела која су одређена конвенцијом су:
- неовлашћени (противправни) приступ;
- неовлашћено (противправно) пресретање;
- ометање тока података;
- ометање рачунарског система;
- злоупотреба уређаја;
- фалсификовање извршено помоћу рачунара;
- превара извршена помоћу рачунара;
- кривична дела дечје порнографије; и
- кривична дела ауторских и сродних права.

Међународни уговор који се посредно односи на сајбер безбедност је и **Опциони протокол о продаји деце, дечјој проституцији и дечјој порнографији** из 2001. године који је Република Србија ратификовала 2002. године, а који у преамбули помиње интернет као начин дистрибуције дечје порнографије.

На нивоу Уједињених нација још увек не постоји међународни уговор у области сајбер безбедности, али је у току рад на његовој изради. Генерална скупштина је **Резолуцијом 75/282 о супротстављању употреби информационо-комуникационих технологија у криминалне сврхе** основала ad hoc међувладин комитет експерата.

Иако представници Републике Србије нису стални чланови комитета (officers), они су учествовали на досадашњим заседањима. Предложена конвенција ће вероватно обухватити неколико тема као што су суштинске одредбе о сајбер криминалу, међународна сарадња, приступ потенцијалним дигиталним доказима органа за спровођење закона, укључујући и прекограничну сарадњу, као и људска права и процедуралне гаранције.

Почев од 2016. године, када је усвојена Директива о безбедности мрежа и информационих система (NIS Directive), државе чланице ЕУ у обавези су да у националним оквирима одреде органе надлежне за послове информационе безбедности и размену информација, те да успоставе центре за превенцију безбедносних ризика у ИКТ системима (CERT). Сарадња држава чланица у сузбијању сајбер криминала заснована је на размени раних упозорења о инцидентима.

Почетком ове године усвојена је тзв. **NIS 2 Директива** по којој одговорност за превенцију, откривање и одговор на инциденте деле и приватне компаније, као и пружаоци дигиталних услуга (онлајн продавница, *cloud* сервиса, претраживача, и др). Кључну улогу у пружању савета државама чланицама у процесу имплементације овог акта има **Агенција ЕУ за сајбер безбедност** (ENISA). Координацију држава чланица помаже и **Европски оквир за стандардизацију сајбер безбедности**, као механизам усмерен на креирање јединственог дигиталног тржишта ИКТ производа, услуга и процеса.

Настојања да се на на нивоу ЕУ на општи и директан начин регулишу питања сајбер безбедности уобличена су почетком 2022. године, када је Европска комисија предложила усвајање **Регулативе** (уредбе) **о сајбер безбедности**. Циљ предложеног акта је успостављање заједничких мера за сајбер безбедност којима би биле обавезане и институције, помоћна тела и агенције ЕУ, као и јачање капацитета ЕУ ЦЕРТ-а.

Усклађивање са правним тековинама ЕУ у домену сајбер безбедности део је приступног процеса Србије, првенствено у смислу преговарачког поглавља 24 (Правда, слобода, безбедност). Осим тога, неупитан је и шири друштвени значај усклађивања са прописима ЕУ, посебно имајући у виду окруженост Србије државама чланицама Уније, те неопходност заједничког одговора на сајбер претње које превазилазе границе националних држава.

Домаћи оквир

Сајбер безбедност у Србији обухвата низ елемената и актера. Најважније области у нормативном оквиру за сајбер безбедност су:

1. **Информациона безбедност**
2. **Високотехнолошки криминал**
3. **Електронска управа**
4. **Дигитална агенда**

Ове опште области у нормативном оквиру пружају основу за *заштиту информационих система, критичне инфраструктуре, података о личности, електронског пословања и заштиту од високотехнолошког криминала*.

У зависности од конкретних потреба и изазова, могуће је доћи и до другачије категоризације или додати додатне области.

Информациона безбедност

Два најважнија закона у овој области су **Закон о информационој безбедности** и **Закон о критичној инфраструктури**.

Закон о информационој безбедности из 2016. године је својеврсни кровни закон у овој области у домаћем правном систему. Законодавац се определио за *информациону безбедност* пре него за сајбер безбедност. Иако су у питању два сродна концепта, информациона безбедност се односи на податке без обзира на њихову форму - електронска форма, папир, разговор, и тако даље.

Као саставни део процеса усклађивања законодавства са NIS 2 Директивом – у априлу ове године формирана је **Радна група за израду Нацрта закона о изменама и допунама Закона о информационој безбедности**. Међу најзаступљенијим темама су: дефинисање приоритетних оператора ИКТ система, укључујући средња и велика предузећа која послују у областима енергетике, саобраћаја, здравства, банкарства, телекомуникационих услуга; усвајање националног плана реаговања на инциденте који значајно угрожавају информациону безбедност, јачање улоге Националног ЦЕРТ-а; и, успостављање агенције за информациону безбедност.

Критична инфраструктура подразумева развој ресурса који су неопходни за несметано функционисање државе и њених грађана – попут физичких објеката, система снабдевања, информационих мрежа и технологија. Закон о критичној инфраструктури из 2018. године први је нормативни акт у потпуности усмерен на регулисање ове сложене области. Овај закон је значајна надградња постојећој нормативној архитектури сајбер безбедности у Републици Србији.

Стратегија за развој информационог друштва и информационе безбедности у Републици Србији (2021-2026) је најважнији документ стратешког карактера који регулише поједина питања сајбер безбедности у Републици Србији. Као кључне димензије у регулисању информационе безбедности наводе се:

- информациона безбедност грађана;
- информациона безбедност привреде: и
- информациона безбедност ИКТ система од посебног значаја.

Стратегија исправно препознаје потребу да се изгради друштвена свест о ризицима које доносе нове технологије, а посебно у смислу високотехнолошког криминала.

Стратегија националне безбедности из 2019. године истиче и ближе одређује изазове, ризике и претње (ИРП) који могу угрозити националну безбедност Републике Србије. Премда је у преамбули наглашен „свеобухватни приступ“ у погледу дефинисања ИРП – претње у сајбер простору се помињу у контексту глобалног стратешког окружења, као део „међународне безбедносне реалности“. Развој и присуство нових технологија нашли су своје место у попису кључних ИРП. Додуше, у самом зачељу ове листе.

Закон о заштити података о личности уређује питање обраде (прикупљања, чувања, коришћења, итд) података о личности. Закон дефинише појам повреде података о личности као повреду безбедности података о личности која доводи до случајног или незаконитог уништења, губитка, измене, неовлашћеног откривања или приступа подацима о личности који су пренесени, похрањени или на други начин обрађивани. Међу основним начелима обраде података о личности, Закон предвиђа начело интегритета и поверљивости података, као и одговорност руковаоца подацима за примену Закона. Такође, Закон прописује поступак у случају повреде података о личности, односно обавезу руковаоца подацима да о повреди података која може да произведе ризик по права и слободе физичких лица, без одлагања обавести Повереника за информације од јавног значаја и заштиту података о личности.

У случају повреде права на заштиту података о личности, могуће је обратити се Поверенику за информације од јавног значаја и заштиту података о личности притужбом или захтевом за остваривање права у вези са обрадом података о личности/захтевом остваривање права поводом извршеног увида.

Подзаконска акта битна за информациону безбедност су:

Уредба о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије; Уредба о безбедности и заштити деце при коришћењу информационо-комуникационих технологија, *Сл. гласник РС* 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* 24/16; Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја *Сл. гласник РС* 94/16; 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* 94/16; Уредба о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја, *Сл. гласник РС* 11/20; Правилник о врсти, форми и начину достављања статистичких података о инцидентима у информационо-комуникационим системима од посебног значаја, *Сл. гласник РС* 76/20; Правилник о садржају, начину уписа и вођења евиденције посебних центара за превенцију безбедносних ризика у информационо-комуникационим системима, *Сл. гласник РС* 37/20; Правилник о подацима које садржи евиденција оператора информационо-комуникационих система од посебног значаја, *Сл. гласник РС* 9/20; Одлука о образовању Тела за координацију послова информационе безбедности, *Сл. гласник РС*, 8/2020-9, 159/2020-33, 30/2021-24, 44/2022-8, 115/2022-42; Уредба о обезбеђивању и заштити информационих система државних органа, *Сл. гласник СРС*, 41/1990-1520; Упутство за израду и усвајање пројеката информационих система органа управе *Сл. гласник СРС*, 49/1989-1731.

Високотехнолошки криминал

Нормативни оквир за високотехнолошки криминал регулише превенцију, откривање, гоњење и сузбијање кривичних дела у вези са информационо-комуникационим технологијама и системима.

Кривични законик препознаје одређена кривична дела против безбедности рачунарских података:

- Оштећење рачунарских података и програма (чл. 298);
- Рачунарска саботажа (чл. 290);
- Прављење и уношење рачунарских вируса (чл. 300);
- Рачунарска превара (чл. 301);
- Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (чл. 302);
- Спречавање и ограничавање приступа јавној рачунарској мрежи (чл. 303);
- Неовлашћено коришћење рачунара или рачунарске мреже (чл. 304, 304а).

Поред ових, Кривични законик наводи и:

- Неовлашћено прикупљање личних података (чл. 146);
- Искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу (договорање састанка са малолетном особом) (чл. 185 б);
- Приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију (укључујући и електронско објављивање и продају) (чл. 185);
- Неовлашћено искоришћавање ауторског дела (нелегално умножавање, објављивање или продаја рачунарских програма или збирка података) (чл. 199).

Законик о кривичном поступку прописује доказне радње које се примењују у случају кривичних поступака против учинилаца дела које гони Посебно јавно тужилаштво за борбу против високотехнолошког криминала.

Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала упућује на дефиниције из Кривичног законика и одређује да ће се *Посебно јавно тужилаштво* бавити гоњењем кривичних дела високотехнолошког криминала. Високотехнолошки криминал представља вршење кривичних дела код којих 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.

Национални програм усвајања правних тековина Европске уније (НПАА) 2022-2025 предвиђа да се до четвртог квартала 2023. године оснаже капацитети Посебног тужилаштва тако што ће се број заменика јавног тужиоца повећати са пет на 10, број тужилачких помоћника повећати са пет на 10, а број административних радника повећати са шест на 20.

Електронска управа

- Закон о електронској управи

- Уредба о ближим условима за успостављање електронске управе: 104/2018-3
- Уредба о безбедности и заштити деце при коришћењу информационо-комуникационих технологија, Сл. гласник РС 13/20;
- Програм развоја електронске управе у Републици Србији за период од 2023. до 2025. године са акционим планом за његово спровођење: 33/2023-127
- Уредба о одржавању и унапређењу Државног центра за управљање и чување података: 18/2022-30
- Уредба о ближим условима за израду и одржавање веб презентације органа: 104/2018-10
- Уредба о начину рада Портала отворених података: 104/2018-9
- Уредба о начину вођења Метарегистра, начину одобравања, суспендовања и укидања приступа сервисној магистрали органа и начину рада на Порталу еУправа: 104/2018-6
- Уредба о организационим и техничким стандардима за одржавање и унапређење Јединствене информационо-комуникационе мреже електронске управе и повезивање органа на ту мрежу: 104/2018-4

Дигитална агенда

Стратегија развоја мрежа нове генерације до 2023. године истиче усклађивање са јединственим дигиталним тржиштем ЕУ као важан сегмент у оквиру ширег економског и друштвеног развоја Р. Србије. Развој брзог и ултрабрзог интернета и интероперабилних апликација, уз њихову доступност свим грађанима, носећи су стуб Дигиталне агенде и јединственог дигиталног тржишта ЕУ.

Стратегија јединственог дигиталног тржишта ЕУ подразумева:

- бољи приступ дигиталним добрима и сервисима за потрошаче и предузећа широм Европе;
- подстицање развоја дигиталних мрежа и сервиса уз стварање окружења једнаких услова;
- искоришћавање пуног потенцијала дигитализације, као покретача развоја.

Унапређење дигиталних знања и вештина свих грађана, укључујући припаднике осетљивих друштвених група, препознато је као основни циљ **Стратегије развоја дигиталних вештина у Републици Србији од 2020. до 2024. године**. Као кључна подручја за постизање овог најопштијег циља издвојени су:

- Унапређивање дигиталних компетенција у образовном систему;
- Унапређење основних и напредних дигиталних вештина за све грађане;
- Развој дигиталних вештина у односу на потребе тржиште рада;
- Целоживотно учење ИКТ стручњака.

Најважнији актери