

Ljuba Slijepčević

Pravosudna akademija

Novi Sad

Zaštita dece pri korišćenju informaciono-komunikacionih tehnologija u domaćem i međunarodnom pravu

Uvod

Informaciona bezbednost se odnosi na bezbednosne rizike povezane sa upotrebom IKT, uključujući bezbednost podataka, uređaja, informacionih sistema, mreža, organizacija i pojedinaca.

Informaciona bezbednost je definisana kao skup mera koje omogućavaju da podaci kojima se rukuje putem kompjuterskih sistema budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti integritet, raspoloživost, autentičnost i neporecivost tih podataka, da bi taj sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica.

ZAKON O INFORMACIONOJ BEZBEDNOSTI¹ članu 1 reguliše predmet uređivanja

„Ovim zakonom se uređuju mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornosti pravnih lica prilikom upravljanja i korišćenja informaciono-komunikacionih sistema i određuju se nadležni organi za sprovođenje mera zaštite, koordinaciju između činilaca zaštite i praćenje pravilne primene propisanih mera zaštite.“

Nesporno je da su internet i digitalna tehnologija postali sastavni deo života ljudi širom sveta, i da pružaju mogućnost za napredovanje i obrazovanje, bržu komunikaciju, odnosno pronalaženje informacija, učenje, istraživanje, ali i za zabavu.

Međutim, nove tehnologije nose sa sobom i rizike, pa je potrebno preduzeti određene mere zaštite radi bolje digitalne bezbednosti. To uključuje bezbednost podataka, uređaja, informacionih sistema, mreža, organizacija, ali i pojedinaca, posebno mlađe populacije kao izuzetno ranjive.

Bezbedno ponašanje prilikom korišćenja novih tehnologija predstavlja jedan od ključnih aspekata digitalne pismenosti koja je neophodna veština za „preživljavanje“ u 21. veku.

Broj dece i mladih koji svakodnevno koriste internet je u stalnom porastu, i u svetu i kod nas. Internet predstavlja necenzurisani izvor informacija koji nije uvek primeren deci. Cljna grupa kojoj posebno treba posvetiti pažnju su deca i mladi.

Zaštita dece na Internetu podrazumeva fizičku, psihičku i moralnu bezbednost maloletnih lica tokom obavljanja svakodnevni aktivnosti na Internetu (surfovanje, četovanje, korišćenje društveno-socijalnih mreža, online igrice). Cilj je zaštititi decu od neprimerenih sadržaja, negativnih efekata korišćenja Interneta i podići nivo svesti i znanja o tome na koji način virtuelna stvarnost utiče na decu i dokle smeju da se upuštaju u digitalni svet, a da to bude bezbedno i bez posledica.

„Najpoznatiji Veb čitači za decu: Buddy Browser, PikLuk, My Kids browser , KidZui, KidRocket, Surf Knight, Zac Broswer.

¹ ZAKON O INFORMACIONOJ BEZBEDNOSTI ("Sl. glasnik RS", br. 6/2016, 94/2017 i 77/2019)

Zaštita dece na internetu je moguća, uz pomoć aplikacija kao što je NetNanny, CyberPatrolParentalControls, SafeEyes, SentryPC, KidsWatch, Time Sheriff, Web Watcher, Time Boss² koja roditeljima omogućava da na kompjuterima blokiraju određene internet sadržaje. Aktivna uloga roditelja je jedna od ključnih aktivnosti, ali ne i dovoljna. Posebnu pažnju treba posvetiti edukaciji dece.

Postoje organizacije, kako u svetu, tako i kod nas koje se bave edukacijom dece i omladine o korišćenju interneta. S druge strane, kao što je rečeno, uloga roditelja je veoma bitna.

Brojni sadržaji na internetu nisu namenjeni deci i često stoji obaveštenje na samim sajtovima o tome, ali to se vrlo lako zaobiđe, a sankcije nema, jer ne postoji mogućnost kontrole, već se ide na poverenje.

Većina dece ima pristup internetu, ali ne zna dovoljno kako da se zaštiti od zloupotrebe na globalnoj mreži. Ovom problemu potrebno je pristupiti globalno.

Pretnje po emocije dece, njihovu svest, pa i fizičko stanje su više izražene nego na pravom igralištu. Internet nosi različite rizike po bezbednost dece. Neki od njih kao što su uznemiravanje, vređanje ili govor mržnje isti su za decu i za odrasle. Postoje, međutim, i rizici pre svega od seksualne zloupotrebe koji posebno ugrožavaju decu, zbog njihove znatiželje i neiskustva na Internetu. Zaštita dece na Internetu podrazumeva fizičku, psihičku i moralnu bezbednost maloletnih lica tokom obavljanja svakodnevnih aktivnosti na Internetu. Cilj je zaštititi decu od neprimerenih sadržaja, negativnih efekata korišćenja Interneta i podići nivo svesti i znanja o tome na koji način virtuelna stvarnost utiče na decu i dokle smeju da se upuštaju u digitalni svet, a da to bude bezbedno i bez posledica.

Iskorišćavanje dece na internetu

Na Internetu postoji nekoliko hiljada organizacija koje se bave nekim od mnogobrojnih načina iskorišćavanja dece. Veliki broj tih organizacija legalno su prijavljena preduzeća, humanitarne ili nevladine organizacije sa pravnim identitetom. Njihovo predstavljanje u javnosti nedvosmisleno upućuje na službe za pružanje raznih vrsta pomoći, počev od humanitarnih materijalnih donacija, preko psihološke pomoći ugroženim grupama -deci razvedenih roditelja, deci sa lošim materijalnim i socijalnim statusom, itd. pa sve do poslovnih ponuda sa dobrim i sigurnim zaradama.

Često se ispod primamljivih mogućnosti za bolji život najčešće kriju ciljevi trafikinga, prostitucije, raznih vrsta krađa i drugih načina iskorišćavanja žrtava. S druge strane, postoje anonimni sajtovi iza kojih stoje kriminalističke grupe koje deluju potpuno ilegalno, dok u treću grupu spadaju pojedinci koji su psihijatrijski slučajevi koji imaju direktan pristup žrtvi u nameri da ostvare svoje ciljeve, od kojih je na prvom mestu seksualno zlostavljanje. Zajednička osobina takvih „lovaca“ jeste njihov neverovatno iskren nastup, pun emocija, razumevanja i saosećanja prema potencijalnoj žrtvi.

Najčešći oblici zloupotrebe dece na internetu:

Trafiking

Krađa

Blud -Seksualna zloupotreba dece na Internetu-pedofilija

² <https://kliknibezbedno.wordpress.com/zloupotrebe-dece-na-internetu/>

Sugestija

Vršnjačko nasilje

Hakerisanje

Trafiking

Ubrzani rast primene informaciono-komunikacione tehnologije doveo je i do pojave sajber kriminala kao novog oblika kriminala koji je vezan za zloupotrebu društvenih mreža. Trgovina ljudima, pa i ljudskim organima menja se u skladu sa najnovijim tehnološkim dostignućima tj. postaje sve više karakteristična i za sajber prostor. Usvajanje odgovarajuće regulative na nacionalnom i međunarodnom planu predstavlja važan korak u rešavanju problema trgovine ljudima i ljudskim organima putem interneta.

Krađa

Krađa- u direktnom ili indirektnom obliku je još jedna u nizu vrsta zloupotrebe maloletnika preko interneta. Na sajtovima se često nudi pomoć tipa savetovališta koje ima za cilj prepoznavanje psihološkog profila maloletnika oko kojeg se naizgled stvara prijateljsko i zaštitničko okruženje. U drugim varijantama u istu svrhu moguće je iskoristiti informacije o brojevima kreditnih kartica kojima maloletnik plaća svoje učešće u nagradnim igrama.

Blud- Seksualna zloupotreba dece-pedofilija

Blud- Seksualna zloupotreba dece-pedofilija na Internetu je jedan od najrasprostranjenijih oblika zloupotrebe dece. Statistički je dokazano da je svaka četvrta devojčica i svaki šesti dečak dožive neki oblik seksualnog zlostavljanja. Opasnost za decu koja provode slobodno vreme na društvenim mrežama, forumima, chat sobama i drugim internet lokacijama na kojima je moguća komunikacija s nepoznatim osobama, vrebaju od strane pedofila. Oni se deci obično lažno predstavljaju uglavnom kao vršnjaci i pokušavaju da s njima ostvare kontakt i odnos poverenja. Potom pokušavaju da na razne načine ucenom, na primer, navedu decu da rade nešto što će zadovoljiti njihove bolesne potrebe. Obično se traži slanje snimaka dece sa seksualnom konotacijom, ili se detetu zakazuje sastanak.

Kako bi smanjio šanse da bude otkriven, zlostavljač po pravilu prikuplja informacije o žrtvinim roditeljima i prijateljima kako bi izabrao što ranjiviju mladu osobu.

Sve aktivnosti koje imaju veze sa ugrožavanjem polne slobode maloletnika i dece zabranjene su Krivičnim zakonikom, a posebna kazna predviđena je u slučajevima kada je krivično delo izvršeno iskorišćavanjem računarske mreže ili komunikacije drugim tehničkim sredstvima.

Sugestija

Sugestija- oblik napada sa ciljem da se žrtva navede na samopovređivanje, svesno ili nesvesno. Ova vrsta napada opasna je naročito stoga što može da rezultuje teškim bolestima, pa čak i smrtnim slučajevima. Lakši vidovi delovanja sugestijom na potencijalnu žrtvu, mogu se naći na sajtovima čiji sadržaji obiluju raznim vrstama dijeta, preparata za brzo mršavljenje, telesnih vežbi i sličnih aktivnosti. Ciljnu grupu ovakvih sajtova čine u najvećoj meri devojčice tinejdžerskog uzrasta.

Vršnjačko nasilje

Vršnjačkim nasiljem putem interneta naziva se podsticanje grupne mržnje, napadi na privatnost, uznemiravanje, praćenje, vređanje, nesavestan pristup štetnim sadržajima i širenje nasilnih i uvredljivih komentara. Ono može uključivati još i slanje okrutnih, zlobnih, nekad i pretećih poruka, kao i kreiranje internet stranica koje sadrže priče, crteže, slike i šale na račun vršnjaka. Takvo nasilje odnosi se i na postavljanje fotografija vršnjaka na galerijama sajtova, uz zahtev posetiocima da ih procenjuju po određenim karakteristikama, odnosno da glasaju za osobu koja je najružnija, najnepopularnija ili najdeblja u školi.

Hakerisanje

Hakerisanje je oblik uznemiravanja mladih na internetu. Hakeri koriste svoje napredno kompjutersko znanje i veštine da bi neovlašćeno ušli u tuđe kompjuterske sisteme i time napravili štetu, ali, ponekad, i dobit za sebe. Jedan od načina odbrane od hakera je da se prave dobre tzv. "jake" šifre, koje se ne mogu lako otkriti. Preporučuje se kombinacija slova i brojeva, upotreba velikih i malih slova. Važno je šifru čuvati samo za sebe i ne deliti je ni sa prijateljima.

Programi za zaštitu dece na Internetu

Najbolja zaštita dece na Internetu jeste da u svakom momentu roditelj zna šta dete radi na Internetu. Postoje softveri koji beleže šta je sve rađeno na računaru, adrese koje su posećivane i sve to snima u određene log fajlove sa tekstom koje je dete kucalo (chat programi, dopisivanje, fejsbuk itd) tako da se može uvek biti u toku šta dete radi.

K9 WEB protection predstavlja program veličine dva do tri MB, kojim na jednostavan način se zabranjuju, prate ili limitiraju određene veb-sajtove, upotrebu chat klijenata i ostalih online alata. Na sajtu pored navedenog postoje još i programi za prečišćavanje sadržaja. Ovi programi su napravljeni tako da prepoznaju sadržaj web stranica koji bi mogao da bude štetan za mlade korisnike. Ti programi omogućavaju odraslima, koji brinu o deci, da spreče dete da posećuje te neprimerene veb-sajtove. Programi za prečišćavanje koriste tri glavna modela: crnu listu, belu listu i neutralnu listu. Crna lista blokira prilaz upisanim sajtovima, dok bela lista omogućava odlazak samo na navedene sajtove, blokirajući sve ostale.

„Postoji mnogo proizvođača softvera koji su napravili specijalizovane web čitače za decu. To nisu samo klasični čitači kao Internet Explorer ili Firefox, već predstavljaju čitav jedan zatvoreni svet koji je napravljen tako da bude siguran za decu, a da im ipak dopusti da donekle pretražuju Internet. Ovakvi programi po pravilu su šareni i imaju mnogo zvučnih efekata tako da privlače pažnju dece, a često su i „nafilovani“ gomilom sadržaja – od pristupa online Flash igrama, preko predefinisanih portala za decu, pa sve do spiska proverenih web stranica sa sadržajima primerenim datom uzrastu.

Najpoznatiji Veb čitači za decu: Buddy Browser, PikLuk, My Kids browser , KidZui, KidRocket, Surf Knight, Zac Browser.“³

Akcija 'Klikni bezbedno', koju sprovodi Ministarstvo za telekomunikacije i informaciono društvo pod nazivom „Razmisli pre nego što postaviš“ organizovala je edukaciju za nastavno osoblje, psihološko-pedagoške službe i savete roditelja najpre u osnovnim školama u Beogradu, a potom i u školama u celoj Srbiji.

³ Web čitači za decu i programi za roditeljsku kontrolu I za decu i za roditelje

<https://www.sk.rs/arhiva/clanak/8041/web-citaci-za-decu-i-programi-za-roditeljsku-kontrolu-i-za-decu-i-za-roditelje>

Praktično je nemoguće trajno eliminisati određeni sadržaj na Internetu, pa pojam zabrane treba uzeti s rezervom. Čak i sadržaju koji se svugde smatra zabranjenim (npr. dečja pornografija) u principu je uz manje ili više truda uvek moguće pristupiti, neretko i direktno s pretraživača.

Postoje, međutim, i zabranjeni sajtovi koje policija ima u svojoj evidenciji. Na njima je onaj ko pretražuje dočekan znakom „Stop“.

Kada je reč o sadržajima koji nisu izričito zabranjeni, ali se smatraju nepoželjnim, kao što su pornografija, uznemirujuće poruke, rasizam ili mržnja, kao i sadržajima koji su neprihvatljivi može da se aktivira mehanizme za zabranu pristupa.

Nacionalni pravni okviri

Strategija razvoja informacionog društva u Republici Srbiji do 2020. Godine⁴ sadrži odredbe o informacionoj bezbednosti, gde su određeni sledeći prioriteti: unapređenje pravnog i institucionalnog okvira za informacionu bezbednost, zaštita kritične infrastrukture, borba protiv visokotehnološkog kriminala, naučno -istraživački i razvojni rad u oblasti informacione bezbednosti.

Strategija ukazuje na to da je, pored povećanja potrebe za veštinama u vezi sa primenom IKT, internet promenio način i dinamiku širenja znanja i informacija u svim oblastima. Neophodno je integrisanje IKT u sve aspekte obrazovnog procesa, sa ciljem efektivnijeg i efikasnijeg obrazovanja.

Prema Strategiji, informaciona bezbednost znači zaštitu sistema, podataka i infrastrukture u cilju očuvanja poverljivosti, integriteta i raspoloživosti informacija.

Odgovarajući stepen informacione bezbednosti u svim oblicima primene IKT jedan je od preduslova stvaranja održivog informacionog društva . Potrebno je doneti propise iz oblasti informacione bezbednosti kojima će se dodatno urediti standardi informacione bezbednosti, područja informacione bezbednosti, kao i nadležnosti i zadaci pojedinih institucija u ovoj oblasti. U ovom dokumentu se ukazuje i na značaj naučno-istraživačkog rada u oblasti informacione bezbednosti bezbednosti.

Vlada Republike Srbije donela je, 30. juna 2016. godine, Uredbu o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija. Uredba o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija objavljena je u „Sl. glasnik RS“, br. 61/2016 ,a primenjivala se od 15. jula 2016. god.

Donošenjem Uredbe počeo sa radom Nacionalni kontakt centar za bezbednost dece na internetu. Građani mogu da prijave zloupotrebu interneta i ugrožavanje bezbednosti dece na internetu na broj telefona 19833, slanjem mejla na adresu bit@mtt.gov.rs ili putem elektronske prijave na portalu www.pametnoibezbedno.gov.rs

Nacionalni kontakt centar za bezbednost dece na internetu počeo je sa radom 27. februara 2017. godine.

⁴ ("Sl. glasnik RS", br. 51/2010)

Potom je doneta nova UREDBA O BEZBEDNOSTI I ZAŠTITI DECE PRI KORIŠĆENJU INFORMACIONO-KOMUNIKACIONIH TEHNOLOGIJA 2020.⁵

Članom 1 ove Uredbe je zaštita dece na internetu definisana kao aktivnost od javnog interesa. Pomenuta aktivnost se sprovodi edukacijom, prvenstveno dece, roditelja, zakonskih zastupnika i nastavnika. Akcentat se stavlja na dobre i loše strane interneta, tj. prednosti i rizike, ali i na postupanje u slučajevima kada je bezbednost dece na internetu ugrožena. Cilj uredbe je jasno definisan u članu 2. Tu se navodi sledeće:

Cilj Uredbe je da se:

- 1) podigne nivo svesti i znanja o prednostima i rizicima korišćenja interneta i načinima bezbednog korišćenja interneta;
- 2) unaprede digitalne kompetencije dece, odnosno učenika, roditelja i drugih zakonskih zastupnika i nastavnika (u daljem tekstu Uredbe: dece, roditelja i nastavnika);
- 3) unapredi međuresorna saradnja u oblasti bezbednosti i zaštite dece na internetu.

Uzimajući u obzir činjenicu da deca veoma rano pristupaju internetu, čak i pre šeste godine, što je utvrđeno istraživanjem UNICEF-a iz 2017. godine deca mnogo više znaju o internetu od svojih roditelja i nastavnika, zbog toga je potrebno da se i oni edukuju i budu upućeni u sve što internet pruža, kako bi deca bila bezbedna na online platformama. Jedan od načina da roditelji podignu nivo bezbednosti dece jesu i programi za filtriranje. Naime, programi za filtriranje obezbeđuju ograničavanje pristupa Internet lokacijama zasnovano na sadržaju. To znači da program sprečava pristup lokacijama koje sadrže materijale definisane kao štetne (pornografija, nasilje itd.).

Već pomenuta Uredba o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija članom 3 navodi preventivne mere za bezbednost i zaštitu dece na internetu:

Ministarstvo nadležno za poslove informacione bezbednosti preduzima preventivne mere za bezbednost i zaštitu dece na internetu, kao aktivnosti od javnog interesa, putem:

- 1) edukacije i informisanja dece, roditelja i nastavnika;
- 2) jedinstvenog mesta za pružanje saveta i prijem prijavi u vezi sa bezbednošću i zaštitom dece na internetu.

Shodno preventivnim merama od strane Ministarstva iz člana 3 Uredbe stvoren je i Nacionalni kontakt centar za bezbednost dece na internetu kome se svaka vrsta nasilja na internetu može prijaviti. Ministarstvo trgovine, turizma i telekomunikacija je osnovalo Nacionalni kontakt centar za bezbednost dece na internetu. Nacionalni kontakt centar je povezan sa policijom, tužilaštvom, domovima zdravlja, kao i centrima za socijalni rad, Ministarstvom prosvete i u zavisnosti od problema, dalje informacije se prosleđuju nadležnim institucijama.

Bitnu ulogu u očuvanju zaštite bezbednosti dece na internetu ima centar za socijalni rad, a član 7 Uredbe o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija opisuje način postupanja u slučajevima kada se prijavi internet nasilje. Ukoliko su bilo koja prava deteta

⁵("Sl. glasnik RS", br. 13/2020)

narušena, pa tako i prava deteta na internetu, Porodični zakon Republike Srbije garantuje mogućnost podnošenja tužbe.

Tužbu za zaštitu prava deteta mogu podneti: dete, roditelji deteta, javni tužilac i organ starateljstva, kako je definisano članom 263 Porodičnog zakona. Pravo i dužnost da obaveste javnog tužioca ili organ starateljstva o razlozima za zaštitu prava deteta imaju sve dečje, zdravstvene i obrazovne ustanove ili ustanove socijalne zaštite, pravosudni i drugi državni organi, udruženja i građani.

Današnja porodica je izložena brojnim teškoćama i problemima koje informatička era „vuče“ za sobom, a problemi se ogledaju, prvenstveno, u zanemarivanju brige o deci. Razmatrajući ove činjenice, postavlja se pitanje da li se poštuje član 6 Porodičnog zakona Republike Srbije koji u stavu 1 kaže: „Svako je dužan da se rukovodi najboljim interesom deteta u svim aktivnostima koje se tiču deteta.“

Saglasno Zakonu o obligacionim odnosima,⁶ član 165, roditelji odgovaraju za štetu koju prouzrokuje njihovo dete drugom licu, do navršene sedme godine, bez obzira na svoju krivicu. Oni se oslobađaju odgovornosti ako postoje razlozi za isključenje odgovornosti prema pravilima o odgovornosti bez obzira na krivicu. Odgovornost roditelja za štetu prouzrokovanu od strane njihovog maloletnog deteta uzrasta do sedam godina je objektivne prirode. To znači da roditelji odgovaraju bez obzira na to da li su krivi. Mogu biti oslobođeni odgovornosti ako postoje razlozi za isključenje objektivne odgovornosti, a to su viša sila, radnja oštećenog i/ili radnja trećeg lica. Takođe, roditelji se oslobađaju odgovornosti i u slučaju ako je drugo lice odgovorno za štetu nastalu dok mu je dete bilo povereno na čuvanje drugoj osobi ili instituciji.

Prava deteta predviđena Konvencijom o pravima deteta, pa i Porodičnim zakonom Republike Srbije moraju da se štite i da se svakom detetu obezbedi nesmetan razvoj, bez izloženosti bilo kojoj vrsti nasilja. Kao što je to predviđeno članom 6, stav 2 i stav 3 Porodičnog zakona, „država ima obavezu da preduzima sve potrebne mere za zaštitu deteta od zanemarivanja, od fizičkog, seksualnog i emocionalnog zlostavljanja te od svake vrste eksploatacije“, kao i da „država ima obavezu da poštuje, štiti i unapređuje prava deteta“.⁷

Također je doneta Uredba o postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja 2020. godine⁸

Ovom uredbom uređuju se preventivne mere za bezbednost i zaštitu dece pri korišćenju informaciono-komunikacionih tehnologija, odnosno na internetu i postupanje u slučaju narušavanja ili ugrožavanja bezbednosti dece na internetu. Republika Srbija je prepoznala potrebu da institucionalno reaguje na znatan porast prijave štetnog i nelegalnog sadržaja na internetu koji ugrožavaju bezbednost dece, i da na taj način spreči da ovaj problem eskalira.

⁶ Zakon o obligacionim odnosima (“Sl. list SFRJ”, br. 29/78, 39/85, 45/89 - odluka USJ i 57/89, “Sl. list SRJ”, br. 31/93, “Sl. list SCG”, br. 1/2003 - Ustavna povelja i “Sl. glasnik RS”, br. 18/2020

⁷ Porodični zakon („Sl. glasnik RS“, br. 18/2005, 72/2011 – dr. zakon i 6/2015), čl. 6, stav 2 i stav 3

⁸ (“Službeni glasnik RS” broj 11/20)

Postupak obaveštavanja prema članu 4 Uredba o postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja.

„Operator IKT sistema od posebnog značaja obaveštenje o incidentu dostavlja ministarstvu nadležnom za informacionu bezbednost (u daljem tekstu: Nadležni organ), Narodnoj banci Srbije odnosno regulatornom telu za elektronske komunikacije pisanim putem bez odlaganja, najkasnije narednog radnog dana od dana saznanja o nastanku incidenta, a operatori IKT sistema za rad sa tajnim podacima postupaju u skladu sa propisima kojima se uređuje oblast zaštite tajnih podataka.

Obaveštenje o incidentu mora da sadrži vrstu i opis incidenta, vreme i trajanje incidenta, posledice koje je incident izazvao, preduzete aktivnosti radi ublažavanja posledica incidenta i, po potrebi, druge relevantne informacije.

U slučaju hitnosti informacija o incidentu se dodatno prijavljuje telefonskim putem, putem elektronske pošte ili na drugi odgovarajući način.

Nadležni organ, Narodna banka Srbije i regulatorno telo za elektronske komunikacije mogu bliže urediti postupak obaveštavanja o incidentima, u skladu sa ovom uredbom.“

Uredba je u skladu sa Zakonom o ratifikaciji Konvencije Ujedinjenih nacija o pravima deteta .

Srbija ove godine dobija novi Zakon o informacionoj bezbednosti i Strategiju razvoja veštačke inteligencije.

Pravni sistem Republike Srbije prema KRIVIČNOM ZAKONIKU ⁹reguliše krivično delo zlostavljanja i iskorišćavanja dece i putem Interneta .Član 185b Krivičnog zakonika- Iskorišćavanje računarske mreže ili kominukacije drugim tehničkim sredstvima za izvršenje krivičnih dela protiv polne slobode prema maloletnom licu navodi da izvršenje krivičnih dela Silovanja (član 178,stav 4,) Obljube nad detetom (član 180,stav 1 I 2), Obljube zloupotrebom službenog položaja (član 181,stav2 I 3), Nedozvoljenim polnim radnjama (član 182,stav 1), Podvođenje ili omogućavanje vršenja polnog odnosa (član 183,stav 2), Posredovanja u vršenju prostiucije (član 184,stav 2), Prikrivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje dece za pornografiju (član 185, stav 2) i Navođenje maloletnog lica na prisustvovanje polnim radnjama (član 185a), koristeći računarsku mrežu ili komunikaciju drugim tehničkim sredstvima dogovori sa mloletnikom sastanak i pojavi se na dogovorenom mestu radi sastanka, kazniće se zatvorom od šest meseci do pet godina i novčanom kaznom. Ako je ovo delo učinjeno prema detetu kazniće se zatvorom od jedne do osam godina.

Najvažnije izmene su da se po prvi put u Krivičnom zakoniku Republike Srbije kao krivično delo smatra posedovanje i pribavljanje fotografija, audio-vizuelnih zapisa ili drugih predmeta pornografske sadržine nastale iskorišćavanjem maloletnog lica.

Motivi za izvršenje ovih krivičnih dela su takođe širokog spektra i predmet su psihološkog profilisanja izvršilaca u zavisnosti od slučaja do slučaja.

⁹ KRIVIČNI ZAKONIK ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019)

Jedan od relevantnih dokumenata za zaštitu dece od nasilja je i Opšti protokol za zaštitu dece od zlostavljanja i zanemarivanja koji je usvojila Vlada RS u august u2005. godine svi oblici nasilja, zlostavljanja, zloupotreba ili zanemarivanja dece, kojima se ugrožavaju ili narušavaju fizički, psihički i moralni integritet ličnosti deteta, predstavljaju povredu jednog od osnovnih prava deteta sadržanih u Konvenciji Ujedinjenih nacija o pravima deteta (u daljem tekstu: Konvencija), a to je pravo na život, opstanak i razvoj.

Opšti protokol se odnosi na svu decu, bez diskriminacije, odnosno bez obzira na porodični status, etničko poreklo i bilo koje druge socijalne ili individualne karakteristike deteta (rasu, boju, pol, jezik, veroispovest, nacionalnost, mentalne, fizičke ili druge specifičnosti deteta i njegove porodice).

Opšti protokol se odnosi na svu dece čija je dobrobit ugrožena, odnosno decu u neposrednoj ili životnoj opasnosti, decu koja su (dokazano ili pod sumnjom) žrtve zlostavljanja i zanemarivanja i decu za koju se smatra da su pod rizikom od zlostavljanja i zanemarivanja.

Opšti protokol se odnosi na decu u svim situacijama:

- u porodici (biološkoj, hraniteljskoj, usvojiteljskoj);
- van porodice, odnosno u ustanovama gde deca borave privremeno ili trajno (škole, predškolske ustanove, letovališta, dnevni boravci, školski internati, domovi za decu, odnosno druge ustanove socijalne zaštite).

Prevažnost najboljeg interesa deteta podrazumeva da najbolji interes deteta ima prednost nad interesom roditelja, odnosno staratelja, ustanove ili zajednice, u situacijama kada se ovi interesi razlikuju od interesa deteta.

Participacija deteta obezbeđuje se tako što deca treba da budu pitana, da dobiju adekvatne informacije i mogućnost da izraze svoje želje, stavove i mišljenje o svim pitanjima koja ih se tiču i u svim fazama procesa zaštite i to na način koji odgovara njihovom uzrastu i razumevanju situacije.

Međunarodni propisi

Prema Konvenciji o kompjuterskom kriminalu iz 2001. godine koju je naša država ratifikovala¹⁰ i primenila u svom Krivičnom zakoniku i konvencijama koje se bave zaštitom prava deteta te Preporuke Rec(2001)16 o zaštiti dece od seksualnog iskorištavanja iz 2007, ovaj problem stavljen je u žižu interesovanja evropske i svetske javnosti, a u pojedinim državama je proglašena prioritetom brojem jedan kada je u pitanju kompjuterski kriminal i organizovani kriminal uopšte. Kod nas se kao izvršiocima ovih krivičnih dela javljaju lica iz svih društvenih struktura, tako da ne postoji profil izvršilaca ovih krivičnih dela u tom smislu.

¹⁰ ZAKON O POTVRĐIVANJU KONVENCIJE UJEDINJENIH NACIJA PROTIV TRANSNACIONALNOG ORGANIZOVANOG KRIMINALA I DOPUNSKIH PROTOKOLA ("Sl. list SRJ - Međunarodni ugovori", br. 6/2001)

Konvencija o visokotehnološkom kriminalu Saveta Evrope čiji je Republika Srbija potpisnik i jedan je od temeljnih pravnih akata u ovoj oblasti.

Neophodnost međunarodnog povezivanja državnih organa je osnovni preduslov suprostavljanja kompjuterskom kriminalu. Republika Srbija je ratifikovala Konvenciju o visokotehnološkom kriminalu Saveta Evrope u martu 2009. godine uz Dodatni protokol koji se bavi inkriminisanjem akata rasističke i ksenofobične prirode putem računara.

Konvencija je doneta 23. novembra 2001. godine u Budimpešti, i pored Srbije ratifikovana je još od 31 države članice Saveta Evrope, a potpisale su je i Kanada, Japan, Južnoafrička Republika i SAD.

Osnovni ciljevi donošenja Konvecije su harmonizacija nacionalnih zakonodavstava u domenu materijalnopravnih odredbi u oblasti visokotehnološkog kriminala, uvođenje odgovarajućih procesnih instrumenata radi boljeg procesuiranja ovih krivičnih dela i uspostavljanje brzih i efikasnih institucija i procedura međunarodne saradnje.

U preambuli same Konvecije naglašena je potreba za procesuiranjem počilaca krivičnih dela visokotehnološkog kriminala, koja imaju međunarodni karakter. Unapređenje saradnje nadležnih nacionalnih organa jedan je od osnovnih prioriteta s ciljem suzbijanja visokotehnološkog kriminala.

Konvencija se sastoji iz preambule, i četiri poglavlja.

Konvencija i precizno reguliše šta se sve smatra pornografskim sadržajem, i definiše kao kao pornografski materijal koji vizuelno prikazuje :

1. maloletnika koji učestvuje u eksplicitno seksualnoj radnji;
2. lice koje izgleda kao maloletnik, koje učestvuje u eksplicitno seksualnoj radnji;
3. realistične slike, koje predstavljaju maloletnika koji učestvuje u eksplicitno seksualnoj radnji.

Konvencija je podigla starosnu granicu po kojoj se decom smatraju sva lica do svoje 18. godine

Članovima 14 Konvecije regulisana su procesna ovlašćenja državnih organa prilikom istraživanja krivičnih dela visokotehnološkog kriminala.

Pored opštih odredbi koje nalažu državama potpisnicama Konvecije, da u svoja nacionalna krivična prava uvedu gore pomenuta krivična dela, velika pažnja usmerena je načinu prikupljanja podataka koji se nalaze u računarima ili prenosnim uređajima, kao i zaštiti osnovnih prava pojedinca garantovanih Evropskom konvencijom o ljudskim pravima iz 1950. godine.

Nadležni i organi, u skladu sa Konvencijom, imaju pravo uvida i zaplene svakog računara ili nosača podataka, ukoliko postoje osnovi sumnje, da se tu mogu nalaziti nedozvoljeni materijali, kao i da od provajdera prikupljaju podatke, koji se odnose pre svega, na upotrebu interneta, telefona i kartica.

Konvencija predviđa i odredbe koje se tiču presretanja podataka, odnosno praćenja elektronske komunikacije, prevashodno one koje se obavlja putem interneta.

Član 15. Zakona o potvrđivanju Konvecije o visokotehnološkom kriminalu¹¹ predviđa pravo na privatnost i pravo na prepisku, a Konvencija ne predviđa odgovarajuća ograničenja da takva prava neće biti zloupotrebljena. Kako se presretanje odnosi samo na teška dela, države imaju punu

¹¹ ("Sl. glasniku RS", br. 19. mart 2009.)-

slobodu da same odrede kada će i u kojim slučajevima ovo pravo koristiti. Konvencija u čl.21.stv.3 određuje da:

“ Svaka Strana ugovornica treba da usvoji zakonodavne i druge mere, neophodne da obavežu davaoca usluga da čuva u tajnosti sprovođenje svakog ovlašćenja predviđenog ovim članom i svaku informaciju u vezi sa tim.“

Kada se imaju u vidu istrage za terorizam i zlostavljanje dece ovakva procedura je opravdana i prihvatljiva, međutim ni ovde nije predviđen mehanizam zaštite građana koji bi se zloupotrebom ovog stava našli na udaru vlasti određene zemlje.

Konvencijom nije predviđena ni obaveza provajdera da skladišti podatke o svojim korisnicima, koji bi možda kasnije bili od koristi nadležnim organima, i to zbog očigledne povrede prava na privatnost korisnika. Kako je Konvencija međunarodni instrument, države imaju mogućnost da prilikom ratifikacije izrade pravne propise koji bi nadomestili ove nedostatke.

Pitanje nadležnosti uređeno je članom 22. Konvencije koji u stavu 1. previđa da države imaju nadležnost za procesuiranje ukoliko je krivično delo izvršeno :

- 1.na njenoj teritoriji ;
- 2.na brodu pod zastavom te strane ugovornice;
- 3.u vazduhoplovu registrovanom u skladu sa zakonima te strane ugovornice;
- 4.od strane njenog državljanina, ako je delo kažnjivo po krivičnom zakonu zemlje gde je izvršeno I li ako je delo izvršeno na mestu izvan nadležnosti bilo koje države.

Po stavu 2. istog člana države imaju mogućnost da ne primenjuju pravila o nadležnosti u određenim slučajevima. Države potpisnice su obavezne da ukoliko ne izvrše ekstradiciju svog državljanina , da mu sude za dela koja su izvršena na teritoriji druge države potpisnice.

Treći deo Konvencije je posvećen međunarodnoj saradnji , gde predviđene odredbe uređuju načine radi prevazilaženja prepreka prilikom sprovođenja nacionalnog zakonodavstva za krivična dela koja po pravilu podrazumevaju učešće nekoliko zemalja, a često i pojedince iz više zemalja.

Većina odredbi Konvencije reguliše saradnju država koja sa se tiče eventualne razmene podataka za izvršena krivična dela, kao i ekstradicije počinilaca. U posebnim slučajevima može biti i uspostavljena i direktna saradnja između pravosudnih organa dve države, kao i Interpola, bez ikakvog posredovanja organa izvršne vlasti. Konvencija je propisala krivična dela usmerena protiv poverljivosti, integriteta i dostupnosti računarskih podataka i sistema, dajući precizne definicije krivičnih dela, koje omogućavaju vođenje krivičnih postupaka i uklanjaju opasnost od duplog gonjenja u više država.

Države potpisnice Konvencije mogu tražiti jedna od druge sprovođenje istražnih radnji u slučaju kada :

- 1.ima osnova da se veruje da su odgovarajući podaci naročito podložni gubitku ili izmeni
- 2.instrumenti, dogovori i zakoni inače nalažu brzu saradnju.

Konvencija služi i kao osnov za ekstradiciju ukoliko države to pitanje nisu regulisale.

Države neće biti obavezne da sprovedu ekstradiciju ukoliko postoji nedostatak dvostruke inkriminacije.

Dodatni uslov da se ekstradicija može izvršiti, je da su krivična zakonima obe strane ugovornice kažnjiva zatvorskom kaznom od najmanje godinu dana ili težom kaznom.

Konvencija predviđa osnivanje dežurne službe koja bi radila danonoćno sedam dana u nedelji (24/7), za čije potrebe države potpisnice moraju da uspostave u svojim policijskim službama jedinicu za saradnju, koja bi pružala trenutnu pomoć istragama ili postupcima u vezi sa krivičnim delima koja se odnose na računarske sisteme i podatke, ili radi prikupljanja dokaza u elektronskom obliku o krivičnom delu.

Takva pomoć treba da obuhvati olakšavanje ili, ukoliko to domaće pravo i praksa dozvoljavaju, neposredno sprovođenje sledećih mera: davanje tehničkih saveta ;zaštitu podataka;prikupljanje dokaza, davanje informacija pravne prirode i lociranje osumnjičenih. Konvencija obavezuje potpisnice na gonjenje počinioca i za ona dela koja nisu predviđena u njihovim zakonodavstvima, kao i zbog suviše širokog tumačenja nedozvoljenog sadržaja.

Dodatni protokol uz Konvenciju o visokotehnološkom kriminalu donet je 28. januara 2003. godine u Savetu Evrope u Strazburu i odnosi se u na inkriminaciju radnji rasističke i ksenofobične prirode učinjenih uz pomoć računara.

DRUGI DODATNI PROTOKOL UZ KONVENCIJU O VISOKOTEHNOLOŠKOM KRIMINALU O POJAČANOJ SARADNJI I OTKRIVANJU ELEKTRONSKIH DOKAZA

Među 34 države koje su do sada potpisale Drugi dodatni protokol, Republika Srbija je prva država koja ga je ratifikovala.

Drugi protokol ima za cilj stvaranje zajedničkih normi, na međunarodnom nivou, za jačanje saradnje u borbi protiv visokotehnološkog kriminala i prikupljanje elektronskih dokaza u vezi sa krivičnim istragama ili postupcima.

Protokol pruža sredstva za poboljšanu saradnju i otkrivanje elektronskih dokaza, koja su predmet sistema ljudskih prava i vladavine prava, uključujući zaštitne mere zaštite podataka.

Drugi dodatni protokol uz Konvenciju o visokotehnološkom kriminalu o pojačanoj saradnji i otkrivanju elektronskih dokaza usvojio je Komitet ministara Saveta Evrope na 1417 bis sastanku zamenika ministara (17. novembar 2021) i otvoren je za potpisivanje u Strazburu 12. maja 2022.

Evropska unija je, povodom dana Sigurnijeg interneta 9.2.2023. , lansirala novu verziju Deklaracije o digitalnim principima prilagođenu deci, zajedno sa online igrom na temu digitalnih principa, kako bi deca i mladi naučili o svojim pravima u digitalnom svetu. End Violence Against Children, ukazuje na to da iako internet donosi veliki broj mogućnosti za decu, on takođe predstavlja nove pretnje za bezbednost i da je seksualno zlostavljanje i zloupotreba dece na internetu (CSEA) je najbrže rastući oblik nasilja nad decom. Ove godine, End Violence daje prioritet stavovima i rešenjima dece – jača njihove pozive na akciju za vladu i tehnološku industriju.

Kancelarija Ujedinjenih nacija za drogu i kriminal (UN Office for Drugs and Crime, UNODC) i ITU su 2013. godine predložili da Program Ujedinjenih nacija za razvoj (United Nations Development Programme, UNDP) postane vodeća agencija za programsku podršku u oblasti sajber bezbednosti, koja se pruža zemljama u razvoju (koje tu pomoć moraju da zatraže od UN). Tako, od 2014. godine, UNDP pruža državama usluge u oblasti sajber bezbednosti u vidu radionica za obuku, procenu i prevazilaženje rizika, izgradnju kapaciteta za odgovore na incidente, otpornost, razvoj i evaluaciju politika i standarda koji se odnose na sajber bezbednost i sertifikaciju po ISO 27001 standardima.

U oblasti informacionih tehnologija, Srbija trenutno koristi resurse UNDPa u okviru

inicijative otvaranja podataka, koju u saradnji sa Svetkom bankom sprovodi Ministarstvo državne uprave i lokalne samouprave.

Donošenjem Zakona o ratifikaciji Konvencije Ujedinjenih nacija o pravima deteta¹² država se obavezala da preduzme mere za sprečavanje i da obezbedi zaštitu deteta od svih oblika nasilja u porodici, institucijama i široj društvenoj sredini.

Odredbe Konvencije odnose se na zaštitu deteta od:

- fizičkog i mentalnog nasilja, zlopotrebe i zanemarivanja ili nemarnog odnosa, maltretiranja ili eksploatacije, uključujući i seksualnu zlopotrebu, (član 19);
- svih oblika seksualnog iskorišćavanja i seksualnog zlostavljanja U tom cilju, države članice posebno preuzimaju sve odgovarajuće nacionalne, bilateralne i multilateralne mere za sprečavanje:
 - (a) navođenja ili prisiljavanja deteta da učestvuje u nezakonitim seksualnim aktivnostima;
 - (b) eksploatatorskog korišćenja dece u prostituciji ili drugim nezakonitim seksualnim radnjama;
 - (c) eksploatatorskog korišćenja dece u pornografskim predstavama i časopisima. (član 34);
- otmice i trgovine decom (član 35);
- svih drugih oblika iskorišćavanja (eksploatacije) štetnih po bilo koji vid detetove dobrobiti (član 36);
- nehumanih i ponižavajućih postupaka i kažnjavanja (član 37).

Takođe, odredbom člana 39. Konvencije određena je obaveza države da obezbedi mere podrške za fizički i psihički oporavak deteta – žrtve nasilja i njegovu socijalnu reintegraciju.

Da bi se prava deteta na zaštitu od zlostavljanja i zanemarivanja ostvarila, neophodno je uspostavljanje sistema koji će delovati preventivno u smislu sprečavanja zlostavljanja i zanemarivanja dece I istovremeno, omogućiti da se u situacijama zlostavljanja i zanemarivanja pokrene brz i koordinisan postupak koji prekida zlostavljanje, štiti dete od daljeg zlostavljanja i zanemarivanja i obezbeđuje odgovarajuću intervenciju za oporavak i dalji bezbedan razvoj deteta.

Svi oblici nasilja, zlostavljanja, zlopotreba i zanemarivanja dece, kojima se ugrožava ili narušava fizički, psihički I moralni integritet ličnosti deteta, predstavljaju povredu jednog od osnovnih prava deteta navedenih u Konvenciji Ujedinjenih nacija o pravima deteta, a to je pravo na život, opstanak i razvoj. Donošenjem Zakona o ratifikaciji Konvencije Ujedinjenih nacija o pravima, država se obavezala da preuzme mere za sprečavanje nasilja u porodici, institucijama i široj društvenoj sredini i da obezbedi zaštitu deteta.

Fakultativni Protokol uz Konvenciju o pravima deteta o prodaji dece, dečijoj prostituciji i pornografiji

U smislu ovog Protokola:

- a) prodaja dece podrazumeva bilo koju radnju ili transakciju kojom bilo koje lice ili grupa lica prebacuje dete nekom drugom licu za novčanu ili bilo koju drugu naknadu;

¹² ("Službeni list SFRJ" – dodatak: Međunarodni ugovori, broj 15/90 i "Službeni list SRJ" –dodatak: Međunarodni ugovori, br. 4/96 i 2/97)

b) dečja prostitucija podrazumeva korišćenje dece u seksualnim aktivnostima za novčanu ili bilo koju drugu naknadu;

c) dečija pornografija podrazumeva bilo kakvo predstavljanje, bilo kojim sredstvom, deteta u stvarnim ili simuliranim eksplicitnim seksualnim aktivnostima ili bilo kakvo predstavljanje seksualnih delova tela (primarnih i seksualnih organa deteta), prvenstveno u seksualne svrhe

Član 12. Fakultativnog protokola nalaže svakoj državi članici da u roku od dve godine po stupanju na snagu ovog Protokola, podnese izveštaj Komitetu za prava deteta obezbeđujući sveobuhvatne informacije o merama koje je preduzela na sprovođenju ovog Protokola. Nakon podnošenja ovog sveobuhvatnog izveštaja, svaka država članica ima obavezu da dostavi i sve dodatne informacije u pogledu sprovođenja ovog Protokola, u skladu sa članom 44. UN Konvencije o pravima deteta. Države članice su obavezne podneti izveštaj svakih pet godina. Pored toga, Komitet za prava deteta može da traži od država članica i dodatne informacije relevantne za sprovođenje ovog Protokola.

Rezolucija u o pravu na privatnost u digitalnom dobu

Generalna skupština Ujedinjenih nacija, koju čine predstavnici sve 193 svetske države, 20. decembra 2013. godine jednoglasno je usvojila Rezoluciju o pravu na privatnost u digitalnom dobu, što je prvi dokument UN koji se bavi zaštitom privatnosti posle 25 godina. Nemačka i Brazil su pokrenuli inicijativu u Ujedinjenim Nacijama da se ova Rezolucija usvoji zbog masovnog nadgledanja koje su vršile vlade širom sveta. Rezolucija je jednoglasno usvojena pred Trećim komitetom Ujedinjenih nacija, da bi potom, opet jednoglasno bila usvojena i u Generalnoj skupštini. U preambuli se ističe velika zabrinutost zbog negativnog uticaja koje prisмотра ili presretanje komunikacije mogu imati na ljudska prava, ističući da ista prava koja ljudi imaju kada su offline moraju biti zaštićena i kada su online, uključujući i pravo privatnosti.

Rezolucijom je ukazano na to da ubrzan napredak tehnološkog razvoja omogućava pojedincima iz celog sveta da koriste nove IKT, ali i da istovremeno povećava mogućnost da države, kompanije i pojedinci vrše nadzor, presretanje i prikupljanje podataka, što može da dovede do kršenja ljudskih prava, posebno prava na privatnost. Rezolucija je takođe potvrdila ljudsko pravo na privatnost, u skladu sa kojim niko ne može biti podvrgnut arbitrarnom i nezakonitom mešanju u njegovu privatnost, porodičan život, dom i prepisku, kao i pravo na pravnu zaštitu u odnosu na takvo mešanje. Takođe je potvrdila da je pravo na privatnost važno za realizaciju slobode izražavanja i mišljenja, bez ikakvog uznemiravanja, ali i jedan od osnova demokratskog društva.

Rezolucijom se još zahteva da Visoki komesar za ljudska prava UN Generalnoj skupštini podnese izveštaj o zaštiti prava na privatnost u kontekstu nacionalnog i ekstrateritorijalnog nadzora i/ili presretanja digitalnih komunikacija i sakupljanja ličnih podataka, uključujući takvo postupanje i na masovnom nivou. U Rezoluciji se takođe navodi da, iako se prikupljanje i obrada podataka može opravdati zaštitom javne bezbednosti, države moraju da osiguraju poštovanje obaveza koje imaju u skladu sa međunarodnim standardima ljudskih prava. Rezolucija pruža mogućnost da se problem zaštite privatnosti dalje razmatra u Ujedinjenim nacijama. Iako nije pravno obavezujuća za države članice UN, značaj ove Rezolucije je nesporan i predstavlja prvi korak ka usvajanju pravno-obavezujuće zaštite privatnosti u digitalnom dobu. Ovo nije prvi put da se jedna rezolucija UN smatra za deo običajnog prava, koje je jedan od glavnih izvora međunarodnog prava, s obzirom da se glasanjem u Generalnoj skupštini najbolje oslikava praksa država, ali i njihov stav o obavezujućoj

prirodi norme koju usvajaju. Imajući ovo u vidu, može se reći da je jednoglasno usvajanje ove Rezolucije dokaz o opštem stavu država članica o neophodnosti zaštite privatnosti u digitalnom dobu.

Ujedinjene nacije je dodeljuju Međunarodnoj telekomunikacionoj uniji (ITU), svojoj agenciji za pitanje informacionih i komunikacionih tehnologija (IKT). ITU je maja 2007. godine predstavila dokument pod nazivom Memorandum o globalnoj sajber bezbednosti (A Global Cybersecurity Agenda – GCA) u kom su navedeni osnovni problem i preporuke za poboljšanje bezbednosti (Newbury, 2017).

Preporuke Rec(2001)16 o zaštiti dece od seksualnog iskorištavanja iz 2007

Preporuka utvrđuje osamnaest principa koji se odnose na: pretragu i zaplenu predmeta, tehnički nadzor, obavezu saradnje istražnih organa, elektronske dokaze, upotrebu enkripcije, istraživanje, dokumentovanje podataka i trening, kao i međunarodnu saradnju. U odnosu na elektronske (digitalne) dokaze Preporuka određuje da prikupljanje, čuvanje i prezentacija ovih dokaza treba da bude učinjena na način na koji se najbolje osigurava njihov integritet i neoboriva autentičnost.

Preporuka Komiteta ministara Saveta Evrope R(91)11

Preporuka Komiteta ministara Saveta Evrope R(91)11 o seksualnom iskorištavanju, pornografiji i prostituciji i trgovini decom i omladinom poziva da se u programe osnovnog i srednjeg obrazovanja uključe informacije o opasnostima od seksualnog iskorištavanja i zlostavljanja, da se u sudskom i administrativnom postupku obezbedi tajnost, odnosno poštovanje prava deteta na privatnost, da se obezbede sankcije protiv svih onih koji su uključeni u proizvodnju i distribuciju pornografskog materijala koji uključuje decu.

Evropska konvencija o zaštiti ljudskih prava i osnovnih sloboda

Evropska konvencija je međunarodni ugovor između država članica Saveta Evrope i temeljni akt na kojem se zasniva zaštita osnovnih ljudskih prava i sloboda. Ova konvencija sadrži niz prava koja su na direktan ili indirektan način štite sledeća prava

: pravo na život (član 2.), zabranu mučenja i podvrgavanja neljudskom ili ponižavajućem postupku (član 3.), zabranu držanja u ropstvu ili primoravanju na obavljanje prinudnog ili obaveznog rada (član 4.), pravo na slobodu i sigurnost ličnosti (član 5.), pravo na poštovanje privatnog i porodičnog života (član 8.), zabranu diskriminacije po bilo kojem osnovu (član 14.), zabranu zloupotrebe prava (član 17.), itd.

Evropska unija je usvojila Strategiju sajber bezbednosti Evropske unije 2013. godine, kao prvi krovni dokument kojim Evropska komisija usvaja sveobuhvatni strateški pristup pitanju sajber bezbednosti u EU.

Literatura :

1. Milan Škulić: Kompjuterski kriminalitet
2. L. Komlen Nikolić :Suzbijanje visokotehnološkog kriminala,; Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd;2010
3. Mirjana Drakulić:Osnovi kompjuerskog prava, Beograd, 1996. godina

4. Slobodan Petrović:Kompjuterski kriminal, Beograd, 2000. godina

5.Ljuba Slijepčević : Zaštita dece pri korišćenju informaciono-komunikacionih tehnologija u domaćem I međunarodnom pravu s osvrtom na Uredbu o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija,„Sl. glasnik RS“, br. 61/2016 koja se primenjuje se od 15. jula 2016. god. Tužilačka reč

6. Darijević V. 2021. Sajber kriminal kao bezbednosni rizik na internetu,Megatrend revija, 2(18): 257-266

7. Perović, M. 2018. Sajber kriminal kao globalna prijetnja u svijetu, Vojno delo 3: 157-164

8.Uredba o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija. „Sl. glasnik RS“, br. 61/2016 primenjuje se od 15. jula 2016. god

9.UREDBA O BEZBEDNOSTI I ZAŠTITI DECE PRI KORIŠĆENJU INFORMACIONO-KOMUNIKACIONIH TEHNOLOGIJA("Sl. glasnik RS", br. 13/2020)

10.Uredba o postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja ("Službeni glasnik RS" broj 11/20)

O objavljeno Ljuba Slijepčević , Pravosudna akademija Novi Sad Zaštita dece pri korišćenju informaciono-komunikacionih tehnologija u domaćem I međunarodnom pravu Radno pravni savetnik br 3/2024 ISSN1451-1231