NARUČITELJ PROJEKTA

Bosna i Hercegovina
Regulatorna agencija za komunikacije
Босна и Херцеговина
Регулаторна агенција за комуникације
Bosnia and Herzegovina
Communications Regulatory Agency

IZVRŠITELJ PROJEKTA

MANIA D.O.O.

MANIA

Analiza stanja ispunjavanja obaveza davatelja pristupa internetu u pogledu zaštite maloljetnika, pregleda međunarodne prakse i preporuke za unapređenje regulatornog okvira u BiH

BANJA LUKA
2022. GODINE

AUTORI STUDIJE:

DR ANĐELA KUPREŠANIN VUKELIĆ,
DOCENTKINJA NA FAKULTETU POLITIČKIH NAUKA UNIVERZITETA U BANJOJ LUCI

DR ZORAN ĐURIĆ,
REDOVNI PROFESOR NA ELEKTROTEHNIČKOM FAKULTETU UNIVERZITETA U BANJOJ LUCI

MILORAD SAVIĆ,
DIPL. ING. INF.

Skraćenice

BiH	Bosna i Hercegovina
FBiH	Federacija Bosne i Hercegovine
RS	Republika Srpska
ISP	engl. Internet Service Provider/Davalac pristupa internetu/pružalac usluga interneta
IKT	Informaciono-komunikacione tehnologije
ITU	engl. International Telecommunication Union/Međunarodna unija za telekomunikacije
EU	Europska unija
RAK	Regulatorna agencija za komunikacije
HTTP	engl. HyperText Transfer Protocol/Protokol za prijenos hipertekstualnih dokumenta
HTTPS	engl. Hypertext Transfer Protocol Secure/Protokol za siguran prijenos hipertekstualnih dokumenata
SMTP	engl. Simple Mail Transfer Protocol/Standradni protokol za slanje e-mail poruka
FTP	engl. File Transfer Protocol/Protokol za prijenos datoteka
OSI referentni model	engl. Open Systems Interconnection Basic Reference Model/Referentni model za otvoreno povezivanje sustava
ADSL	engl. Asymetric Digital Subscriber Line/Asimetrična digitalna pretplatnička linija
IPTV	engl. Internet Protocol Television/Internet protokol televizija
d.o.o.	društvo s ograničenom odgovornošću
UN	Ujedinjene nacije
GDPR	engl. General Data Protection Regulation/Opća uredba o zaštiti podataka
VSP	engl. Video Sharing Platforms/Platforme za dijeljenje videozapisa
NIS direktiva	engl. EU Network and Information Security Directive/Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacionih sustava
OSCE	engl. Organization for Security and Cooperation in Europe/Organizacija za europsku sigurnost i suradnju
CERT	engl. Computer Emergency Response Team/Tim za odgovor na računarsku opasnost
CSIRT	engl. Computer Security Incident Response Team/Tim za odgovor na računarske sigurnosne incidente
MIL/MIP	engl. Media and Information Literacy/Medijska i informaciona pismenost
ENISA	engl. European Union Agency for Cybersecurity/Agencija Europske unije za mrežnu i informacionu sigurnost
UNICEF	engl. United Nations International Children's Emergency Fund, od 1953. United Nations Children's Fund/ Dječiji fond Ujedinjenih nacija
OECD	engl. Organisation for Economic Co-operation and Development/Organizacija za gospodarsku suradnju i razvoj
%	Postotak
tj.	to jeste
i dr.	i drugi
npr.	na primjer

SADRŽAJ

UVOD 7
Predmet analize 14
Metodološki okvir analize 15
Ciljevi analize 15
Društvena i stručna opravdanost analize 16
ANALIZA MJERA ZA ZAŠTITU DJECE KOJE PODUZIMAJU PRUŽATELJI PRISTUPA INTERNETU (ISP) U BIH 17
Analiza rezultata istraživanja na temelju odgovora davatelja pristupa internetu o mjerama za zaštitu djece 18
Da li postoje tehnički uvjeti za filtriranje prometa po različitim protokolima (HTTP, SMTP, ...) na strani ISP-a? 18
Da li postoji filtriranje neželjenog prometa bez znanja krajnjih korisnika (pretplatnika) koje se radi na strani ISP-a? 18
Da li postoji mogućnost kupovine usluge filtriranja prometa na strani ISP-a? 18
Da li se filtriranje prometa primenjuje na sve oblike povezivosti koje ISP nudi (ADSL, kabelska, optička veza, mobilni internet, itd.)? 19
Da li postoje pretplatnici za koje se ne vrši filtriranje prometa na strani ISP-a? 19
Da li postoji mogućnost inspekcije enkriptovanog prometa na strani ISP-a? 19
Da li pretplatnici samostalno mogu da uključuju/isključuju opcije filtriranja prometa na strani ISP-a? 20
Da li postoji mogućnost kreiranja različitih profila za filtriranje prometa i primijeniti ih na različite uređaje u mreži pretplatnika (npr. poseban profil za filtriranje prometa za uređaj koji koristi dijete)? 20
Da li postoje razlike po pitanju filtriranja prometa ako su pretplatnici obrazovne institucije, posebno ako se radi o osnovnim i srednjim školama? 20
Da li ste provodili testiranja ispravnosti primjene pravila za filtriranje prometa? 21
Kada je pristup nekom resursu blokiran, da li se i koje informacije o tome dostavljaju pretplatniku? 21
Da li postoje usluge/paketi koji se odnose na filtriranje prometa, a koji je nepoželjan za djecu? 21
Analiza odgovora Upitnika o temi sigurnost/bezbjednost djece na internetu 22
PREGLED MEĐUNARODNIH PRAVNIH INSTRUMENATA RELEVANTNIH ZA BIH U PODRUČJU ZAŠTITE MALOLJETNIKA NA INTERNETU 39
Referenca međunarodnih dokumenata za zaštitu prava djeteta 39
Konvencija UN-a o pravima djeteta 39
Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda 41
Referenca međunarodnih dokumenata za zaštitu privatnosti na internetu 42
Konvencija o sajber kriminalu 44
Konvencija za zaštitu pojedinaca u vezi sa automatskom obradom osobnih podataka (Konvencija 108)/ Konvencija 108+ (Modernizirana konvencija) 45
General Data Protection Regulation (GDPR) 45
Direktiva o audiovizuelnim medijskim uslugama 46
PREGLED PROPISA – OBVEZA DAVATELJA PRISTUPA INTERNETU (ISP) U POGLEDU ZAŠTITE DJECE NA INTERNETU (EU I REGIJA) 48
Regulativa u EU 48
Zakon o digitalnim uslugama 48
Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava (NIS direktiva - EU Network and Information Security Directive) 49
CSIRTs Network (engl. Computer Security Incident Response Team / Tim za odgovor na računalne sigurnosne incidente) 50
Agencija Evropske unije za sajber sigurnost/European Union Agency for Cybersecurity (ENISA) 51
UREDBA (EU) 2021/1232 EUROPSKOG PARLAMENTA I VIJEĆA od 14. SRPNJA 2021. o privremenom odstupanju od određenih odredaba Direktive 2002/58/EZ u pogledu tehnologija koje pružatelji brojevno neovisnih interpersonalnih

komunikacijskih usluga upotrebljavaju za obradu osobnih i drugih podataka u svrhu borbe protiv seksualnog zlostavljanja djece na internetu....52
Konvencija Vijeća/Savjeta Europe o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja....54
Praktičan vodič za tvrtke koji im pomaže da razumiju i poboljšaju svoj utjecaj na dečija prava....55
Primjeri zemalja Evropske unije....55
Upute Međunarodne unije za telekomunikacije (ITU)....58
Upute za IKT tvrtke u vezi sa sigurnošću djece na internetu....58
Upute za kreatore politika o zaštiti djece na internetu....59
Transnacionalni modeli za zaštitu djece na internetu....59
Globalni savez *WePROTECT,* Globalni strateški odgovor na seksualno iskorištavanje i zlostavljanje djece na internetu....61
Preporuka OECD-a (Organisation for Economic Co-operation and Development/Organizacija za gospodarsku suradnju i razvoj) u pogledu bezbjednosti djece na internetu....61
Projekat *deSHAME - Facebook* i Evropska unija....62
Ministarski dobrovoljni principi pet država za borbu protiv seksualnog iskorištavanja i zlostavljanja djece....63
Globalno partnerstvo i fond za zaustavljanje nasilja nad djecom, Sigurno za učenje: Poziv na akciju....63
Dječje dostojanstvo u digitalnom svijetu, Savez za dostojanstvo djeteta: Izvješće radne skupine za tehnologiju....63
Opća uredba Europske komisije o zaštiti osobnih podataka....64
Izvještaji o indeksu digitalne učtivosti (Microsoft)....65
Multimedijalni program FACES (NHK Japan i javni servisi - prihvatili Facebook, UNESCO, Vijeće Europe)....65
Dokument o pravima djeteta i igranje na internetu: Mogućnosti i izazovi za djecu i IKT industriju (UNICEF)....65
Nacionalni modeli za zaštitu djece na internetu....66
Kodeks dizajna prilagođen dobi/ Introduction to the Age appropriate design code - Velika Britanija....66
Bijela knjiga *'Online Harms'* /Bijela knjiga o štetnim onlajn sadržajima....**67**
Uloga javnih servisa u zaštiti djece na internetu....67
Zakon o štetnim digitalnim komunikacijama (Novi Zeland)....68
Povjerenik eSafety (Australija)....68
Propisi u regiji....69
Srbija....69
Crna Gora....71
Hrvatska....72
PREGLED REGULATIVE I MEHANIZAMA USMJERENIH NA ZAŠTITU DJECE NA INTERNETU U BIH....76
Normativni okvir BiH relevantan za zaštitu djece na internetu....76
Regulatorna agencija za komunikacije BiH (RAK)....79
Aktivnosti, upute i strategije RAK- a usmjerene na zaštitu djece u medijskom/digitalnom okruženju....79
Aktivnosti i programi usmjereni na podizanje nivoa sigurnosti djece na internetu u BiH....83
PREPORUKE....85
KORIŠTENI IZVORI....88
PRIVITKE....94

Definicije kategoričnih pojmova

Dijete - Svaka osoba mlađa od osamnaest godina života. (*UN Konvencija o pravima djeteta*, 1989)

Adolescenti - Osobe starosti od 10 do 19 godina. Adolescenti nisu obavezujući pojam prema međunarodnom pravu, a oni mlađi od 18 godina smatraju se djecom, dok se 19-godišnjaci smatraju odraslima, osim ako punoljetstvo nije ranije dostignuto prema nacionalnom zakonu. (UNICEF i ITU, *Smjernice za industriju o zaštiti djece na internetu*, 2015, prema *Smjernice za kreatore politika o zaštiti djece na internetu*, 2020)

Digitalni domoroci - Ljudi koji su odrasli s digitalnom tehnologijom, u digitalnom svijetu i kojima digitalni mediji predstavljaju prirodni okoliš. Digitalni domoroci navikli su na brzo primanje informacija. Oni su višenamjenski i skloniji slučajnom pristupu (kao u hipertekstu). Najbolje funkcioniraju u internetskom okruženju. (*Prensky*, 2005)

IKT - Informacijske i komunikacijske tehnologije opisuju sve informacijske tehnologije koje naglašavaju spektar komunikacije. Ovdje uključujemo sve usluge i uređaje koji se mogu povezati s internetom, kao što su računala, prijenosna računala, tableti, pametni telefoni, igraće konzole, televizori i satovi. (UNICEF i ITU, Upute *za industriju o zaštiti djece na internetu*, 2015.). Usluge kao što su radio, kao i širokopojasni internet, mrežni hardwer i satelitski sustavi, dodatno su uključene. (*Upute za kreatore politika o zaštiti djece na internetu*, 2020.)

IKT industrija - Konvergencija telekomunikacijske industrije sa računalnom i radiodifuzijskom industrijom. IKT industrija uključuje svu opremu i usluge vezane uz emitiranjem, preradom i telekomunikacijama. Sve ove usluge i oprema prihvaćaju i prikazuju informacije u elektroničkom obliku. (*IGI Global*, 2018, prema Puharić, 2019)

Internet Service Provider (ISP) - Davatelj usluga pristupa internetu je tvrtka koja korisnicima pruža pristup internetu i usluge na internetu. Pristup se može omogućiti upotrebom različitih tehnologija povezivosti: takozvane "tehnologije povezivosti". Dial-up, kabelska tehnologija, DSL itd. Uobičajeno je da ISP-ovi korisnicima omogućuju komunikaciju vlastitom uslugom e-pošte, a u novije vrijeme telefonijom, televizijom itd., ovisno o pojedinačnom ISP-u. (Tehnopedia, 2018. , prema Puhariću, 2019.)

Informacijska sigurnost – Zaštita informacija i informacijskih sustava od neovlaštenog pristupa, korištenja, otkrivanja, prekida, izmjene ili uništenja kako bi se osigurala povjerljivost, cjelovitost i dostupnost. (NIST 800-37, prema Milanović i Radovanović, 2020.)
Informacijska sigurnost ogleda se u: sigurnoj primjeni računala i nterneta, sigurnom elektroničkim poslovanju, zaštićenoj komunikaciji, jamstvu privatnosti itd., a manifestira se kao sigurnost računala od kvara, virusa i prisluškivanja, sigurne i nenadzirane komunikacije na internetu, sigurne korporativne mreže, neprekidne kupnje, plaćanje ili prodaja preko računala, uživanje u vlastitoj privatnosti i zaštiti osobnih podataka itd. (Marković 2009, prema Milanović i Radovanović, 2020)

Cyber - odnosi se na ljude, stvari, politike, koncepte i ideje povezane s računalnim uređajima i računalnim mrežama, a posebno Internetom i informacijskim tehnologijama. (*Upute za strateški okvir cyber sigurnosti u Bosni I Hrcegovini*, 2019)

Cyber kriminal - kriminalne aktivnosti u kojima su informacijski I komunikacijski sustavi podložni, sredstvima, meti ili mjesto kaznenog djela. (*Upute za strateški okvir kibernetičke sigurnosti u Bosni i Hrcegovini*, 2019)

Cyberbullying/uznemiravanje putem interneta - u svrhu izrade skupa pravila za kreatore politike zaštite djece na internetu, *cyberbullying* se opisuje kao namjerni agresivni čin koji više puta provodi grupa ili pojedinac pomoću digitalne tehnologije i usmjeren je na žrtvu koja se ne može lako braniti. Obično uključuje "korištenje digitalne tehnologije i Interneta za objavljivanje štetnih informacija o nekome, namjerno dijeljenje privatnih podataka, fotografija ili videozapisa na štetan način, slanje prijetećih ili uvredljivih poruka (putem e-pošte, izravnih poruka, chatova, tekstualnih poruka), širenje glasina i lažnih informacija o žrtvi ili namjerno isključivanje iz mrežnih komunikacija." Može uključivati izravne (kao što su chatovi ili tekstualneporuke), polujavne (poput objavljivanja uznemirujuće poruke na popisu e-pošte) ili javne komunikacije (poput stvaranja web stranice posvećene ismijavanju žrtve). (*Upute za kreatore politika o zaštiti djece na internetu*, 2020.)

Iskorištavanje djece na internetu - Iskorištavanje djece na internetu, odnosno, putem IKT-a, podrazumijeva nasilje, iskorištavnje i zlostavljanje djece od strane njihovih vršnjaka ili odraslih. Iskorištavanje uključuje prikazivanje neprikladnog sadržaja djeci, vrbovanje djece za nezakonite aktivnosti, vrbovanje (*grooming*), slanje eksplicitnih poruka (*sexting*), virtualno zlostavljanje (*cyber-bulling*) i druge vrste nasilničkog ponašanja koje ugrožavaju prava djeteta. (Regionalno izvješće *Iskorištavnje djece na internetu*, 2013)

Alati za roditeljski nadzor - program koji korisnicima, obično roditelju, omogućuje kontrolu nekih ili svih značajki računala ili drugog uređaja koji se mogu povezati s Internetom. Takvi programi obično mogu ograničiti pristup određenim vrstama ili klasama web stranica ili internetskih usluga. Neki pružaju i mogućnosti upravljanja vremenom, odnosno uređaj se može postaviti tako da ima pristup internetu samo između određenih sati. Naprednije verzije mogu snimiti sve tekstualne poruke poslane ili primljene s uređaja. Programi će obično biti zaštićeni lozinkom. (*Upute za kreatore politika o zaštiti djece na internetu*, 2020.)

Digitalni jaz - Pojam koji opisuje neravnomjernu raspodjelu IKT-a u društvu. Digitalni jaz obuhvaća razlike u pristupu (digitalni jaz razine 1) i upotrebi (digitalni jaz razine 2) računala i interneta između (1) industrijaliziranih zemalja i zemalja u razvoju (globalni jaz), (2) različitih socioekonomskih skupina unutar jedne nacionalne države (socijalna podjela) i (3) različitih vrsta korisnika s obzirom na njihov politički angažman na internetu (Demokratske podjele). Digitalni jaz može se odrediti različitim čimbenicima (životna dob, spol, etnička pripadnost, dohodak, zanimanje, mjesto stanovanja itd.). Digitalnom jazu ili digitalnoj nejednakosti posebno pridonose razlike u razini znanja i vještina potrebnih za upotrebu IKT-a i Interneta. (https://www.britannica.com/topic/digital-divide)

Osobni podaci – "Svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi ("ispitanik"); pojedinac čiji se identitet može utvrditi je osoba koja se može identificirati izravno ili neizravno, posebno uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili s jednim ili više čimbenika karakterističnih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili društveni identitet te osobe." (GDPR) Pojam opisuje podatke o pojedincima koji se mogu pojedinačno identificirati i prikupiti na mreži. To uključuje puno ime i prezime, podatke za kontakt kao što su kućna adresa i adresa e-pošte, telefonski brojevi, materijali poput otisaka prstiju ili prepoznavanja lica, brojeve osiguranja ili bilo koji drugi čimbenik koji omogućuje fizički ili internetski kontakt ili lokalizaciju osobe. U tom se kontekstu nadalje odnose na sve informacije o djetetu i njegovoj okolini koje pružatelji usluga prikupljaju na internetu, uključujući igračke povezane s internetom i internet stvari te bilo koju drugu tehnologiju povezanu s internetom. (*Upute za kreatore politika o zaštiti djece na internetu*, 2020.)

Seksualno eksplicitni materijal (SEM) - je bilo koji materijal koji prikazuje seksualno eksplicitne organe, usmjerene na seksualno uzbuđenje ili poticanje mašte s prikazima jasno eksplicitnih seksualnih činova. Učestalost korištenja različitih vrsta SEM-a povezana je s različitim seksualnim ponašanjima i stavovima. (Buovac i Vidaković, 2019.)

UVOD

Studija pod nazivom „Analiza stanja zaštite djece od strane davatelja pristupa internetu, međunarodna praksa i preporuke za unaprjeđenje regulatornog okvira u Bosni i Hercegovini" izrađena je u sklopu projekta „Zaštita djece na Internetu u licencnim sustavima Regulatorne agencije za komunikacije", koji je pokrenula Regulatorna agencija za komunikacije (RAK) u Bosni i Hercegovini (BiH). Projekt se provodi u sklopu strateškog cilja 5.8. iz Plana razvoja RAK-a za razdoblje 2017-2021. godinu, i predviđa provođenje niza aktivnosti kojima se nastoji poboljšati razina zaštite djece na internetu, u skladu sa najboljom praksom i regulatornim okvirom koji je na snazi u zemljama Europske unije (EU). Izrada ove studije obuhvaća prvu fazu projekta, koja uključuje analizu postojećih mjera koje primjenjuju pružatelji usluga pristupa internetu (ISP) u pogledu zaštite djece, sačinjavanje pregleda međunarodne prakse i izradu preporuka za poboljšanje regulatornog okvira u BiH.

U suvremenom informacijskom društvu, a u odnosu na intenzitet korištenja informacijskih i komunikacijskih tehnologija (IKT) i njihovo uključivanje u svakodnevni život, u svim domenama (zabava, komunikacija, obrazovanje, informiranje itd.), djecu označavamo kao digitalne domoroce (Prensky, 2005). Pod ovom sintagmom podrazumijevamo ljude koji su odrasli s digitalnom tehnologijom, u digitalnom svijetu. Intenzivnom prodoru digitalnih medija, koji predstavljaju prirodno okruženje digitalnih domorodaca, uglavnom se pristupalo iz perspektive prednosti koje moderni ICT donosi sa sobom. Međutim, u 21. stoljeću znanstvena i stručna javnost sve je više usredotočena na negativne tendencije tehnološkog razvoja, apostrofirajući pitanja sigurnosti, zlouporabe, narušavanja privatnosti, izloženosti neprimjerenom sadržaju itd. U odnosu na digitalne pridošlice (Prensky, 2005), koji su odrasli prije digitalnog doba i u njega ulaze s posebnim oprezom, digitalni domoroci nisu u stanju uočiti, komparativnom analizom, ne samo prednosti, već i opasnosti koje sa sobom donosi informacijska revolucija.

Vidljiva je tendencija povećanja broja korisnika interneta i stope penetracije, kako na globalnoj razini tako i na razini BiH.

Tablica 1.1. Broj korisnika interneta u BiH (2011-2020)[1]

Godina	Broj korisnika interneta
2011.	2.113.100
2012.	2.174.250
2013.	2.188.429
2014.	2.648.176
2015.	2.782.107
2016.	2.909.236
2017.	3.064.072
2018.	3.195.294
2019.	3.330.502
2020.	3.336.591

[1]Podaci predstavljeni u tabeli preuzeti su iz Godišnjeg izvješća Regulatorne agencije za komunikacije za 2020. godinu.

U sljedećoj su tablici prikazani podaci o broju ISP-ova i broju pretplatnika na fiksni i mobilni internet u BiH za 2020. godinu.

Tablica 1.2. Broj ISP-ova i korisnika fiksnog i mobilnog interneta u BiH za 2020. godinu[2]

III FIKSNI INTERNET	31.12.2020.
Broj ISP-ova	60
Ukupan broj pretplatnika fiksnog Interneta	770.775
Broj dial up pretplatnika	351
Ukupan broj broadband pretplatnika	770.424
Broj pretplatnika putem xDSL priključka	411.850
Broj pretplatnika putem kabelskog modema	258.020
Broj pretplatnika putem FWA (fiksni bežični pristup) priključka	53.567
Broj pretplatnika putem iznajmljenih linija	1.689
Broj pretplatnika putem FTTH priključka	45.046
Broj pretplatnika putem ostalih tehnologija	252
IV MOBILNI INTERNET	**31.12.2020.**
Broj pretplatnika mobilnog Interneta putem standardnog mobilnog širokopojasnog (broadband) pristupa.	1.608.820
Broj pretplatnika mobilnog Interneta putem namjenskih širokopojasnih (broadband) pristupa.	14.903

Svakodnevno umrežavanje i besplatan pristup internetu, uz brojne prednosti u smislu brzine informiranja i komunikacije, dostupnosti brojnih i raznolikih sadržaja, rezultirali su brojnim izazovima u smislu zaštite djece, a u kontekstu njihove privatnosti, integriteta, tj. njihovog odrastanja koje bi osim virtuelnog, kao nezaobilaznog segmenta u njihovom životu, trebalo podrazumijevati i stvarni fizički svijet. „Od pitanja privatnosti, nasilja vršnjaka i nasilnog i/ili neprikladnog sadržaja za određenu dob, do prevaranata na internetu i kaznenih djela nad djecom kao što su vrbovanje, seksualno zlostavljanje i iskorištavanje na internetu, današnja djeca suočavaju se sa mnogim rizicima. Prijetnje se umnožavaju, a počinitelji sve više istovremeno djeluju preko granica, što otežava njihovo praćenje, a još teže ih procesuira“ (Bogdan-Martin, 2020: v).

Rizici s kojima se djeca, kao primatelji, sudionici ili dionici u sajber prostoru suočavaju, mogu se razvrstati u četiri područja:

- *Neprikladan sadržaj* - Djeca i mladi mogu naići na neprikladan i nezakonit sadržaj dok traže nešto drugo klikom na moguće bezopasnu vezu u trenutnoj poruci, blogu ili dijeljenjem datoteka. Također, mogu tražiti i dijeliti neprikladan materijal ili materijal koji nije primjeen dobi. Ono što se smatra štetnim sadržajem razlikuje se od zemlje do zemlje; primjeri uključuju sadržaj koji promiče zlouporabu opojnih droga, rasnu mržnju, rizično ponašanje, samoubojstvo, anoreksiju ili nasilje.
- *Neprimjereno ponašanje* - Djeca i odrasli mogu koristiti internet za uznemiravanje ili čak iskorištavanje drugih ljudi. Djeca mogu ponekad emitirati uvrjedljive komentare ili neugodne slike ili mogu ukrasti sadržaj ili ozlijediti autorska prava.
- *Neprimjeren kontakt* - I odrasli i mladi mogu putem interneta tražiti djecu ili druge mlade ljude koji su ranjivi. Često im je cilj uvjeriti metu da su razvili smislen odnos, ali osnovna svrha je manipulativna. Oni mogu pokušati uvjeriti dijete da izvrši seksualna ili druge izopačene radnje na internetu, koristeći veb kameru ili drugi uređaj za snimanje, ili će pokušati dogovoriti osobni sastanak i fizički kontakt. Taj proces se često naziva „vrbovanje“.

[2]Podaci predstavljeni u tabeli preuzeti su iz dokumenta RAK-a Telekomunikacijski indikatori/pokazatelji BiH u 2020. godini.

- *Komercijalni rizici* - Ova kategorija odnosi se na rizike kršenja privatnosti podataka povezanih s prikupljanjem i korištenjem podataka o djeci, kao i digitalnim marketingom. Internetska sigurnost izazov je zajednice i prilika za IKT tvrtke, vlade i civilno društvo da surađuju na uspostavi sigurnosnih načela i praksi. IKT tvrtke mogu ponuditi čitav niz tehničkih pristupa, alata i usluga za roditelje, djecu i mlade, a prije svega treba napraviti proizvode koji su jednostavni za upotrebu, sigurni po dizajnu i primjereni dobi za njihov širok raspon korisnika. Dodatni pristupi uključuju ponudu alata za razvoj odgovarajućih susatava za provjeru dobi koji poštuju prava na privatnost djece i pristup ili ograničavaju pristup djeci i mladima sadržaju koji je neprikladan njihovim godinama ili ograničavaju ljude sa kojima djeca mogu imati kontakt ili vrijeme u kojem mogu koristiti internet. Ono što je najvažnije, okviri „sigurnost dizajna", uključujući i privatnost, moraju biti uključeni u procese razvijanja inovacija i dizajna proizvoda. Sigurnost djece i odgovorno korištenje tehnologije moraju se pažljivo razmotriti i o njima se ne smije misliti naknadno.[3]

Zaštita interesa djeteta jedna je od društvenih impercija, koja se odnosi na višedesetljetnu normaciju zaštite prava i sloboda djece, kako na međunarodnoj tako i na nacionalnoj razini. Pravovremeno i sustavno djelovanje društva usmjereno u tom smjeru podrazumijeva uključivanje svih relevantnih društvenih subjekata, institucija i pojedinaca, što može značajno doprinijeti zaštiti djece na internetu i suzbijanju negativnih tendencija koje mogu uvelike ugroziti njihovu sigurnost, prava i interese. U tom smislu, oni su također vrlo važni pružatelji pristupa internetu (ISP), koji, osim pružanja ove vrste usluge, moraju preuzeti dio odgovornosti za uspostavljanje i ugradnju mehanizama koji će omogućiti sigurnije korištenje internetskih usluga od strane svojih korisnika, posebno djece. "Tamo gdje domaći zakoni još nisu sustigli međunarodno pravo, svaka tvrtka ima priliku - i odgovornost - uskladiti svoje operativne okvire s najvišim standardima i najboljom praksom" (Bogdan-Martin, 2020.: vi).

O zastupljenosti globalne tendencije ekspanzivnog rasta broja djece kao korisnika interneta u BiH i njihovom sve većem sudjelovanju u internetskoj sferi, što istovremeno podrazumijeva njihovu veću izloženost različitim vrstama rizika, prikazani su podaci izneseni u završnom izvješću "Medijske navike djece i stavovi roditelja" (2020.) Studija pruža opsežno izvješće o korištenju medija djece i adolescenata, kao i o stavovima roditelja u BiH, kao rezultat angažmana RAK-a i njegove suradnje s UNICEF-om. Ovo istraživanje obuhvaća različite aspekte koji su prvenstveno relevantni za postizanje potpunog uvida u intenzitet i način na koji djeca u BiH koriste medije i IKT. U nastavku će biti predstavljeni neki rezultati ovog istraživanja važni u kontekstu identificiranja intenziteta i načina korištenja interneta:

- *Pristup internetu* - djeca u dobi od 7-18 godina za pristup internetu koriste različite uređaje. Većina njih, uz ostale uređaje, u tu svrhu koristi smartphone/mobilne telefone. U dobi 7-10 godina devet od deset (87%) djece koristi ih da bi bilo online, što čine i skoro sva djeca starijeg uzrasta (95% djece uzrasta 11-14 i 97% uzrasta 15-18). Znatno manje djece ističe da za pristup internetu koristi prijenosna računala i stolna raćunala. Njihova uporaba povećava se sa dobi djeteta (prijenosno računualo: 19% dobi 7-10, 31% dobi 11-14 i 40% dobi 15-18; stolno računalo: 18% dobi 7-10, 26% dobi 11-14 i 29% dobi 15-18). Slijedi tablet, koji se češće koristi za pristup internetu djece u dobi od 7-10 nego starija djeca (22% dobi 7-10, 16% dobi 11-14 i 14% dobi 15-18), pa Smart TV i, nešto rjeđe, igraće konzola, gdje nema dobnih razlika u korištenju u te svrhe (16% i 8%).
- *Sadržaji koje djeca gledaju/prate/stvaraju na internetu* – podaci dobiveni anketom o djeci pokazuju da, nakon što navrše 11 godina gotovo svi koriste *YouTube web* stranicu ili aplikaciju (97% dobi 11-14 i 99% dobi 15-18), a ona se široko koristi kod mlađe djece - u dobi 7-10 godina prati je devet od desetoro djece (90%). U kontekstu najpraćenijeg sadržaja, podaci ukszuju na to da djeca njačešće prate *YouTubere* (šest od deset djece, tj. 60%). Igrice su najčešći omiljeni sadržaj djeci u dobi 11-14 godina. Na računalu, tabletu ili mobilnom telefonu/smartphonu djeca dobi 7-18 godina stvaraju određeni sadržaj. Obično mijenjaju ili uređuju fotografije (61%) i snimaju video zapise (53%). Devet od deset (85%) djece udobi od 7-18 godina koristi barem jednu društvenu mrežu i/ili stranicu i/ili aplikaciju za razmjenu poruka. Njihova se uporaba povećava sa godinama, pa ih koristi šest od desetoro djece dobi 7-10 godina (64%), devet od deset djece dobi 11-14 godina (91%) i svi adolescenti (99%). Izneseni podaci pakazuju da

[3] Sonia Livingstone i dr. , "EU Kids Online: Završni izvještaj", Londonska škola ekonomije, 2009. U: Upute za IKT kompanije u pogledu sigurnosti djece na internetu, 2020, str. 15-16.

korištenje interneta od strane djece ne podrazumijeva uvažavanje preporuke da „se korištenje društvenih mreža ne savjetuje prije navršenih 13 godina" (Čengić, Dokić Mrša, Kafedžić i dr, 2021: 15).

- *Vrijeme provedeno na internetu* - djeca dobi 11-14 godina i adolescenti koji svakodnevno koriste mobilni telefon/smartphone svakodnevno su na internetu, što nije slučaj sa dijelom mlađe djece (7-10) (svakodnevno online: 61% dobi 7-10, 80% dobi 11-14 i 93% adolescenata). Podaci od djece pokazuju da, tijekom uobičajenog radnog dana (kada su prva smjena u školi i kada nije online nastava), djeca u prosjeku uz mobilni telefon/smartphone provedu dva i po sata i da shodno tome u prosjeku dva i po sata budu online. Roditelji u usporedbi s djecom procjenjuju da ona, u prosjeku, više vremena provode koristeći mobilni telefon/smartphone i budu na internetu. Što su stariji, to duže vremena provode uz informacijsko-komunikacijske tehnologije, jer se korištenja mobitela/smartphona i vrijeme provedeno na mreži povećava sa godinama.

- *Pravila od strane roditelja u vezi sa korištenjem interneta* – podaci pokazuju da su najčešće pravila uspostavili roditelji djece dobi 7-14 godina (90% roditelja djece dobi 7-10 i 82% roditelja djece dobi 11-14). To je nešto rjeđa praksa kod roditelja djece dobi 4-6 godina (72%), a polovica je prisutna kod roditelja adolescenata (56%). S obzirom na učestalost pristupa internetu i mogućnosti korištenja, najmanji dio roditelja djece u dobi 0-3 godine smatra da postoji potreba, te postavlja pravila o njegovoj uporabi (41%). Roditelji uglavnom postavljaju tri vrste pravila o korištenju interneta: ona koja se odnose na vrste web stranica ili aplikacija koje djeca mogu koristiti, pravila o tome s kim djeca kontaktiraju putem interneta i pravila o tome koliko vremena provode na internetu. S porastom dobi djece raste postotak roditelja koji ne prate dijete dok je na internetu. Tako da skoro da nema roditelja koji ne nadziru boravak na internetu svoje djece dobi 0-10 godina (4%), jedan od deset roditelja to ne čini u dobi od 11-14 godina (11%), što se povećava na četiri od deset roditelja adolescenata (37%). Najčešći načini praćenja ovise od dobi djeteta. Tako da boravak u blizini i redovita provjera šta dijete radi predstavlja jedan od dva najraspostranjenija načina za djecu u dobi 0-14 godina, ali je rijetko prisutan kao oblik kontrole adolescenata. Uz njega mlađu djecu (0-6 godina) roditelji najčešće prate sjedeći pored i gledanjem ili pomaganjem dok je dijete na internetu, dok je kod starije (7-18 godina) najčešće pitaju o tome šta rade na internetu. Kod dobi 7-10 godina svaki treći roditelj koristi i provjeru povijesti internetskog preglednika/uređaja nakon uporabe. Dok instalitrane *softwere,* te ostale vrste nadzora roditelji vrlo rijetko koriste, bez obzira na dob svoje djece. S porastom dobi djece raste postotak roditelja koji ne prate dijete dok je na internetu. Gotovo svi roditelji (90%) ističu da su nekada razgovarali sa svojom djecom o tome kako biti siguran na internetu. Naime, devet od deset roditelja djece dobi 7-18 godina navode da su nekad razgovarali s svojim djetetom o potencijalnim opasnostima poput neprilagođenog sadržaja na web stranicama, otkrivanje/davanje osobnih podataka na internetu, kontakta s ljudima koje ne poznaju, itd.

- *Stavovi roditelja prema korištenju interneta* - podaci pokazuju da je zabrinutost roditelja osrednja u vezi sa potencijalno štetnim aspektima aktivnosti njihovog djeteta na internetu (prosječna ocjena zabrinutosti - na ljestvici od 1 do 5, na kojoj 1 znači „uopće me ne brine", a pet „iznimno mnogo me brine"). Ocjena zabrinutosti roditelja je od 2,78 za sadržaj na web stranicama ili u aplikacijama koje dijete prati do 3,11 za gledanje sadržaja koji djecu potiču na samoozljeđivanje. Također, roditelji nisu sigurni da li, kada je riječ o njihovom djetetu, prednosti interneta nadmašuju rizike.

- *Samopercepcija roditelja o njihovoj sposobnosti da obezbijede sigurno korištenje medija od strane njihovog djeteta/djece* - većina roditelja djece uzrasta 0-14 godina smatra da ima dovoljno znanja da donese odluke o korištenju medija od strane njihovog djeteta/djece. Jedino roditelji djece najstarijeg uzrasta (15-18 godina) imaju više sumnji, te tek u polovini slučajeva procjenjuju da su znaju dovoljno da bi donijeli pravilne odluke (84% uzrasta 0-3, 83% uzrasta 4-6, 78% uzrasta 7-10, 77% uzrasta 11-14, 55% uzrasta 15-18). Oko polovine roditelja uzrasta 0-14 godina procjenjuje da su upoznati sa regulativom, odnosno pravilima za pružanje medijskih sadržaja. Opet su roditelji koji imaju djecu najstarijeg uzrasta (15-18 godina) ti koji češće od ostalih smatraju da im znanje ni po ovom pitanju nije dovoljno (47% roditelja djece uzrasta 0-3, 48% uzrasta 4-6, 54% uzrasta 7-10, 47% uzrasta 11-14, 58% uzrasta 15-18). Mali dio roditelja nekada je prijavio neprimjeren sadržaj, tim češće što imaju djecu mlađeg uzrasta (21% uzrasta 0-3, 17% uzrasta 4-6, 13% uzrasta 7-10, 13% uzrasta 11-14, 8% uzrasta 15-18). Najčešće su se obratili direktno društvenoj mreži na kojoj je bio prisutan neprimjeren sadržaj (18% uzrasta 0-3, 13% uzrasta 4-6,

9% uzrasta 7-10, 9% uzrasta 11-14, 5% uzrasta 15-18). Obraćanje Regulatornoj agenciji za komunikacije vrlo je rijetko (1%-2%).

- *Samopercepcija djece o njihovom znanju o medijima* - svojim znanjem o medijima zadovoljnija su starija djeca (11-14 godina) i adolescenti. Većina njih, osam od deset (81% dobi 11-14 i 84% adolescenata) u odnosu na šest od deset (59%) djece dobi 7-10 godina misle da o medijima znaju dovoljno. Djeca najčešće smatraju da bi o medijima trebali učiti od roditelja (58%) i prosvjetnih radnika (54%). S tim da djeca dobi 7-14 godina češće nego adolescenti misle da bi to trebali biti roditelji (67% dobi 7-10, 60% dobi 11-14 i 46% adolescenata), dok kod nastavnika nema dobnih razlika (51% dobi 7-10, 54% dobi 11-14 i 57% adolescenata). Adolescenti češće od mlađih uzrasta žele da se o medijima uči na *web* stranicama (8% dobi 7-10, 17% dobi 11-14 i 29% adolescenata). I za televiziju/radio i za ostale članove porodice svih dobnih skupina jednako je zastupljeno mišljenje da bi trebali biti izvor tih informacija.

- *Izvori iz kojih se roditelji informiraju o sigurnom korištenju medija* - informacije i savjete o tome kako pomoći svom djetetu da bude sigurno prilikom korištenja medija roditelji djece svih dobi, trećina njih (tri od deset), su najčešće tražili/dobili od članova porodice ili prijatelja (33%). Petina njih (dva od deset) konsultovali su *web* stranice ili aplikacije s informacijama o tome kako ostati siguran na internetu (20%), a tek nešto manje (16%) je ove informacije našlo na TV-u, radiju, u novinama ili časopisima, te, ukoliko dijete ide u školu, u školi djeteta (14%). S dobi djeteta raste broj roditelja kojima djeca (kojim žele pomoći) predstavljaju izvor ovih informacija, tako da u dobi od 11-18 godina oko trećine roditelja razgovara sa djecom ne bi li uvidjelo na koji način da osigura njihovu sigurnost prilikom korištenja medija. Škola je izvor od kojeg bi najveći dio, polovica roditelja (48%), željela dobiti ove informacije. Slijede izvori koji se već često koriste: porodica i prijatelji (koje „bira" trećina roditelja – 32%), te *web* stranice ili aplikacije i TV, radio i časopise (koje bi za izvore željela po četvrtina roditelja – po 27%). Sljedeća skupina ukjljučuje državne institucije (22% ili dva od deset roditelja), proizvođači ili trgovci koji prodaju uređaj i internet provajderi (po 20%). S dobi djece raste i broj roditelja koji bi od njih željeli dobiti informacije o tome kako im pomoći da budu sigurni pri korištenju medija – od 15% roditelja djece dobi 0-3 godine do 28% roditelja adolescenata.

- *Sigurno korištenje interneta* – sedam od deset djece nekada je čulo informacije o tome kako sigurno koristiti internet. Tako je ove informacije nekada dobilo 57% djece dobi 7-10 godina, 70% dobi 11-14 godina, te 78% adolescenata. Roditelji su najčešći izvor informacija o sigurnom korištenju interneta i to tim značajniji što su djeca mlađa (90% djece dobi 7-10, 80% dobi 11-14, te 60% adolescenata). Slijede prosvjetni radnici i to značajno češće profesori nego učitelji i nastavnici. Za djecu dobi 7-14 godina treći izvor po zastupljenosti su drugi članovi porodice, dok su za adolescente to *web* stranice. Što su djeca starija to češće ove informacije dobijaju i od prijatelja (16% djece dobi 7-10, 20% dobi 11-14, 25% adolescenata), s televizijskih/radijskih programa (7% djece dobi 7-10, 14% dobi 11-14, 19% adolescenata) i na predavanjima koja policija održava u školi (2% djece dobi 7-10, 7% dobi 11-14, 9% adolescenata) (Hasanagić, Papović i Kovačević, 2020).

Iz prethodno predstavljenih rezultata u pogledu izvora od kojih djeca u BiH najčešće dobijaju informacije o tome kako sigurno koristiti internet, a koji su pokazali da su to u najvećem postotku odrasli (roditelji, prosvjetni radnici, drugi članovi porodice), proizilazi značaj njihovih navika kao korisnika interneta i kompetencija u smislu njegovog sigurnijeg korištenja, a koje se neminovno odražavaju i na način korištenja interneta od strane djece. U ovom kontekstu su veoma vrijedni rezultati istraživanja objavljeni u obliku finalnog izvješća pod nazivom „Medijske navike odraslih u BiH" (2021). Ova Studija je izrađena uz podršku Vijeća Evrope i projekta Medijska i informacijska pismenost: za ljudska prava i demokratiju, u okviru Akcijskog plana za BiH 2018-2021. Naime, istraživanje o medijskim navikama i stavovima odraslih u Bosni i Hercegovini (BiH) provedeno je na incijativu Savjeta Evrope i Regulatorne agencije za komunikacije kako bi se stekao detaljan uvid u medijske navike i stavove odraslih, kao osnova za razvoj inicijativa medijskog opismenjavanja i razvoj regulatornog okvira. Istraživanje, kako navode autori Studije, pruža detaljan uvid u to kako se odrasle osobe u BiH nose sa trenutno složenim i brzo mijenjajućim medijskim ekosustavom (Hasanagić, Papović I Lević, 2021). U narednom dijelu sažeto će biti predstavljeni rezultati kojima su obuhvaćene isključivo njihove navike prilikom korištenja interneta prema predmetu ove analize:

- *Pristup internetu* - devet od deset stanovnika BiH koriste internet (87%). Oni ubjedljivo najčešće, uz ostale uređaje, internetu pristupaju preko *Smartphone-a* (93%). Slijedi računalo (43%), te pametni televizor (29%), a desetina (10%) u ove svrhe koristi i tablet. Pristup sa drugih uređaja prilično je rijedak. Rezultati, također, pokazuju da spol,

dob, obrazovna razina, radni status i mjesto stanovanja značajno utječu na pristup internetu u BiH.

- *Vrijeme provedeno onlajn* - dvije petine odraslih korisnika interneta u BiH (39%) u tipičnoj sedmici (i radnim danima i vikendom) na njemu provode do sat i pol dnevno. Ostali provedu više, s tim što se sa povećanjem vremena koje se provodi na internetu smanjuje postotak stanovnika koji toliko sati tjedno provode online. Analiza prema prosječnim vrijednostima pokazuje da stanovnici BiH koji koriste internet na njemu u prosjeku provedu 19 sati tjedno tj. 2 sata i 43 minute dnevno. Mladi ispitanici na internetu provode duplo više vremena od starih (28 naprema 15 sati tjedno), tako da učenici na internetu provode 31 sat tjedno, studenti 27 sati, a penzioneri 10 sati tjedno. Na interentu duže borave i više obrazovani u odnosu na niže obrazovane stanovnike, kao i stanovnici grada u odnosu na osobe koje žive na selu.

- *Digitalin jaz* - podaci istraživanja pokazuju da nijednu digitalnu uslugu i internet ne koristi 11% stanovnika BiH. Dakle, svaki deveti stanovnik BiH je u takozvanom digitalnom jazu. Korištenje/nekorištenje internetskih/digitalnih usluga znatno ovisi od dobi, radnog statusa, obrazovanja i, u znatno manjoj mjeri, mjesta stanovanja osoba. Naime, među mladima nema onih koji su u digitalnom jazu (0%), dok ih je među starijima 46% (sa vrlo blagim porastom od 45. godine, pa značajnim rastom od 55. godine, te uznemirujućim skokom od 65. godine starosti).

- *Korištenje interneta* - upućivanje glasovnih ili video poziva pomoću *VoIP* usluge i gledanje kratkih video isječaka najčešće su aktivnosti koje su stanovnici BiH koji koriste internet nekad obavljali online (61% i 57%). Slijedi slanje ili primanje e-mailova, što je nekada učinilo više od polovice stanovnika koji koriste internet (53%). U pogledu korištenja aplikacija za razmjenu poruka/poziva, podaci pokazuju da devet od deset (88%) stanovnika BiH koristi barem jednu aplikaciju za razmjenu poruka/poziva. Ubjedljivo najčešće se upotrebljava Viber, kojeg koristi 81% stanovnika BiH. Slijedi *Facebook Messenger* (52%). Zatim *WhatsApp* (30%), pa *Instagram DM/Threads* (14%). Ostale aplikacije se jako rijetko upotrebljavaju. Osam od deset (78%) stanovnika BiH koristi barem jednu društvenu mrežu. Najčešća društvena mreža je *Facebook*, na kojoj aktivan profil imaju skoro tri četvtine (73%) stanovnika. Znatno rjeđe se koriste *Instagram* (39%) i *YouTube* (38%). Sve ostale društvene mreže koristi manje od 10% stanovnika. Kada je riječ o preovlađujućem načinu upotrebe društvenih web stranica ili aplikacija, podaci pokazuju da stanovnici BiH najčešće (28%) „samo" čitaju sadržaje na društvenim mrežama, a rijetko poduzimaju neku aktivnost („lajkuju" ili objavljuju nešto). Manje od petine stanovnika (19%) povremeno kreira/objavljuje sadržaj, a u još manjem procentu (16%) dijeli/komentira sadržaj.

- *Načini za provjeru činjenica/informacija dostupnih na internetu* – više od polovice stanovnika BiH koji koriste internet (56%) ne provodi nikakve provjere činjenica/informacija objavljenih na internetu. Ostali koriste jedan od sedam načina za njihovu provjeru. Najčešće uspoređuju prisustvo i sadržaj pojedinih informacija na više različitih *web* stranica (22%). Postotak zastupljenost stanovnika koji onlajn sadržaje procjenjuju na temelju vjerodostojnosti adrese *web* stranice (16%) i profesionalnog izgleda stranice (15%), provjeravanjem redovitosti ažuriranja stranice (10%) i kredibiliteta informacija provjerom autora i linka za originalnu publikaciju (9%) je manja. Način provjere koji podrazumijeva utvrđivanje istinitosti činjenica/informacija dostupnih na internetu raspitivanjem da li (i) ljudi kojima vjeruju koriste te stranice, primjenjuje 13% korisnika interenta.

- *Stav prema slobodi govora na društvenim mrežama/online platformama* – trećina stanovnika BiH (33%) podržava ograničenja u slučajevima nezakonitog ili štetnog sadržaja, četvrtina (23%) smatra da je potrebno imati ograničenja, jer naše mišljenje može utjecati na druge, dok petina (19%) smatra da određene stavove i mišljenja ne treba uopće iznostiti na društvenim mrežama/onlajn platformama. Moderaciju tj. brisanje neprimjerenih komentara korisnika portala/platformi za dijeljenje video zapisa/društvenih mreža podržava sedam od deset stanovnika (71%).

- *Znanje i učenje o medijima i IK uslugama* – polovica stanovnika BiH (50%) smatra da imaju dovoljno znanja o tome kako da od negativnog uticaja medija i IK tehnologija zaštiti i sebe i mlađe ili ranjivije članove obitelji, tj. one koji trebaju potporu, pouku i nadzor pri korištenju medija i IK tehnologija. Istovremeno, samo trećina (32%) zna kako da prijave sadržaj koji smatraju neprimjerenim na različitim medijima i IK uslugama, pri čemu je posjedovanje ove kompetencije izraženije kada su u pitanju onlajn mediji (39%) u odnosu na tradicionalne medije

(28%). Znatan postotak stanovnika (35%) bio je izložen nekom od potencijalno štetnih sadržaja u medijskom i IK okruženju - govoru mržnje (48%), uvredljivom jeziku i psovkama (45%), nasilnim sadržajima (33%) i sadržajima koji su diskriminatorni (32%). Neprimjeren sadržaj prijavila je samo petina stanovnika (19%). Unatoč svemu navedenom, gotovo dvije petine stanovnika BiH (38%) ističu da nemaju potrebu za učenjem o medijima i IK tehnologijama. Naime, da im je ovo učenje nepotrebno, smatra skoro polovina (49%) stanovnika koja ne zna kako od negativnog uticaja medija i IK usluga zaštiti ni sebe, a ni mlađe i ranjive članove obitelji, 58% stanovnika koji navode da nisu kvalificirani za prepoznavanje dezinformacija i 53% onih koji ne provode nikakva sredstva provjere činjenica/informacija objavljenih na interentu. Prostali stanovnici, najčešće za učenje o medijima i IK tehnologijama koriste *web* stranice (28%), TV (26%), potom društvene mreže (21%) i platforme za dijeljenje videa (18%). Rjeđe koriste informacije dobijene od prijatelja i/ili poznanika (16%) i posredstvom onlajn portala (14%). Ostali izvori informacija značajni u ovom kontekstu još su rjeđe zastupljeni i koristi ih manje od desetine stanovnika BiH - knjige/udžbenici (9%), organizirane edukacije (7%), djeca i njihovi prijatelji (6%), radio (5%) i tisak (4%) (Hasanagić, Papović i Lević, 2021).

Predmet analize

Sve je više analiza, preporuka i strategija koje ukazuju na važnost tehnološke industrije u smislu zaštite djece na internetu, što je sasvim opravdan pristup, jer mnoge tvrtke u ovoj industriji imaju najveću kapitalnu vrijednost na svjetskom tržištu, a da uglavnom ne podrazumijevaju poštivanje određenih obveza koje pripadaju području društvene odgovornosti. Naročito, kada je riječ o jednom od globalnih interesa, a to je zaštita interesa djeteta, svaka društveno odgovorna tvrtka u privatnom ili javnom sektoru, a čije usluge koriste djeca, trebala bi jasno definirati i revnosno koristiti sve dostupne mehanizme zaštite te populacije. Napori da se osigura zaštita djece u digitalnom okruženju "neće donijeti značajan rezultat bez aktivnog uključivanja predstavnika IKT industrije, prvenstveno pružatelja internetskih usluga (ISP)... Tehnološka industrija ima ključnu ulogu u postavljanju temelja za sigurno korištenje usluga koje pruža digitalno okruženje" (Puharić, 2019.: 9).

Predmet ovog istraživanja je upravo ispitivanje stanja zaštite djece od strane pružatelja usluga pristupa internetu (ISP) na razini BiH. Određivanjem postojećeg stanja, odnosno na koje pružatelji internetskih usluga primjenjuju mehanizme važne u kontekstu zaštite djece i koriste li dostupne tehničke resurse u tom pogledu, omogućit će se potpuniji uvid u vrstu i razinu angažmana predstavnika IKT industrije u području zaštite djece od različitih rizika u sve izazovnijem digitalnom okruženju. Analiza obuhvaća i druge aspekte značajne u tom kontekstu.

Kvalitativnom analizom međunarodnih pravnih instrumenata relevantnih za BiH u području zaštite djece na internetu, obuhvaćeni su međunarodni dokumenti za zaštitu prava djeteta i za zaštitu privatnosti na internetu, na čiju ugroženost ukazuju brojna znavstvena i stručno releventna istraživanja. Posebna pozornost posvećena je revidiranoj Direktivi o audiovizuelnim medijskim uslugama (2018), kao obavezujućem dokumentu za BiH, u smislu usklađivanja njezina normativnog okvira sa odredbama sadržanim u novoj Direktivi. Unaprjeđenje i modernizacija regulatornog okvira BiH usmjereni na podizanje nivoa zaštite djece, proizilaze iz obaveze zemlje prema Sporazumu o stabilizaciji i pridruživanju da svoje zakonodavstvo uskladi s pravnom stečevinom EU. Osim međunarodnih pravnih instrumenta, kvalitativnom analizom obuhvaćene su i preporuke i strategije usmjerene na zaštitu djece u digitalnom okruženju.

Posebno značajan segment predmeta analize jeste pregled propisa u Europskoj uniji (EU) i u regiji, kojom se normira obveze ISP-ova u pogledu zaštite djece na internetu. U tom smislu posebno je kvalitativno analizirana regulativa u EU i smjernice donesene na razini Međunarodne telekomunikacijske unije (ITU) usmjerene na osiguranje i podizanje razine sigurnosti i zaštite djece na internetu. Potom su izdvojeni i analizirani pojedini transnacionalni i nacionalni modeli za zaštitu djece na internetu (programi, preporuke, projekti i sl).

Zbog uspješne komparativne analize stanja u BiH u pogledu normativne i institucionalne zaštite djece na internetu u odnosu na stanje u EU i zemljama u regiji, kvalitativnom analizom su obuhvaćeni i aktuelni propisi u BiH, koji se svojim sadržajem odnose i na zaštitu djece na internetu. Komparativna analiza, s jedne strane omogućuje identifikaciju razine usklađenosti propisa u BiH sa europskom regulativom, a, s druge strane, predstavlja osnov za izradu preporuka koje značajno mogu doprinijeti podizanju razine zaštite djece na internetu u BiH.

Metodološki okvir analize

Metodologija analize osmišljena je na temelju jasno definiranih ciljeva, što će biti razjašnjeno u nastavku. U svrhu postizanja definiranih ciljeva kao tehnike za prikupljanje emiprijskih podataka korišteno je sljedeće: ispitivanje i analiza dokumenata.

U segmentu istraživanja koji podrazumijeva ispitivanje, prikupljajnje podataka provedeno je na sustavnom, tj. reperezenatativnom i pogodnom uzorku, te na neslučajnom odabiru ispitanika. S druge strane, primijenjena je kvalitativna (nefrekvencijska) tehnika prikupljanja podataka analizom dokumenta. Ovisno o razini na kojoj su dokumenti doneseni, odnosno od toga da li se sadržaj dokumenta u potpunosti odnosi na područje zaštite djece na internetu ili samo jednim dijelom, utvrđene su i perfektuirane jedinice analize (dokument u cjelini, pasus, stavak itd.).

U pogledu prvog segmenta istraživanja, a u svrhu uvida u raspoložive mehanizme zaštite djece na internetu ISP-ovima na prostoru BiH je 7. ožujka 2022. godine upućen na popunjavanje upitnik „Zaštita djece na Internetu u sustavima korisnika dozvola Regulatorne agencije za komunikacije - Pitanja za ISP". Rok za dostavljnje ispunjenog upitnika utvrđen je 15. ožujak 2022. godine. Upitnikom su obuhvaćna pitanja koja se odnose isključivo na raspoložive tehničke alate, a struktura i sadržaj upitnika o mjerama koje ISP-ovi na prostoru BiH poduzimaju u cilju zaštite djece na internetu detaljno su pojašnjeni u drugom poglavlju (Analiza mjera za zaštitu djece koje poduzimaju pružatelji pristupa internetu (ISP) u BiH). Ovim poglavljem obuhvaćena je i deskripcija uzorka istraživanja, kao i analiza rezultata istraživanja na temelju odgovora ISP-ova o mjerama zaštite djece.

Ciljevi analize

Ciljevi analize sukladni su sa ciljevima projekta „Zaštita djece na Internetu u sustavima korisnika dozvola Regulatorne agencije za komunikacije". Rukovodeći se navedenim općim ciljevima realizacije projekta, izdvojeno je nekoliko pojedinačnih ciljeva analize, koji su sukladni sa predmetom, metodološkim okvirom i sa različitim dijelovima istraživanja. U tom smislu kao primarni izdvojeni su sljedeći ciljevi:

- Određivanje razine korištenja tehničkih resursa, tj. raspoloživih mehanizama za zaštitu djece na internetu od strane ISP-ova;
- Identifikacija razine usklađenosti načina funkcioniranja i djelovanja ISP-ova u praksi sa relevantnim dokumentima;
- Kreiranje polazne osnove za unaprjeđenje djelovanja relevantnih institucija u domenu zaštite djece na internetu;
- Kreiranje preporuka za unaprjeđenje zaštite djece na internetu, kojima će biti obuhvaćeni različiti aspekti – normativni okvir, tehnički aspekt, edukativni programi, modeli sustavnog djelovanja na nacionalnoj i transnacionalnoj razini i sl;
- Utvrđivanje potencijala postojećih mehanizama u pogledu zaštite djece na internetu, u smislu njihove učinkovitosti i djelotvornosti;
- Decidno formuliranje prijedloga koji će doprinijeti kvalitativnoj i kvantitativnoj nadogradnji postojećih mehanizama u pogledu zaštite djece na internetu po ugledu na europsku praksu i na napredne sustave njihove zaštite, prilagođavajući ih društvenom kontekstu BiH;
- Apostrofiranje važnosti adekvatne zaštite djece na internetu kroz analizu i eksplikaciju izazova i opasnosti sa kojima se ova populacija svakodnevno suočava.

Društvena i stručna opravdanost analize

Posljednih godina u fokusu znanstvenih i stručne javnosti, međunarodnih i nacionalnih politika, su izazovi sa kojima se svakodnevno suočavaju dominantni korsnici interneta, djeca i mladi. Neadekvatno korištenje suvremenih IKT-a, koje je najvećim dijelom determinirano neposjedovanjem odgovarajućih kompetencija njihovih korisnika, koje se stječu informacijskim, medijskim, informatičkim, digitalnim opismenjavanjem, i izostankom pravovremenog uvođenja mjera zaštite korisnika IKT-a i njihovog normiranja na nacionalnoj i međunarodnoj razini, ugrozilo je značajne aspekte života građana u suvremenom digitalnom okruženju. U tom smislu najosjetljiva populacija su svakako djeca, koja odrastaju uz digitalne tehnologije i aktivno ih koriste, bez prethodnog educiranja o njihovim potencijalima, koji osim niza mogućnosti i prednosti, sa sobom nose brojne opasnosti. U tom smislu bilo koji oblik znavstveno i stručno utemeljenog angažmana usmjerenog ka unapređenju zaštite djece na internetu, podrazumijeva znavstvenu, stručnu i društvenu opravdanost.

Predmetna anliza jeste rezultat aktivnog sudjelovanja predstavnika akademske zajednice, relevantnih za različite aspekte (socijalni, normativni, tehnički, psihološki) koji su neizostavni u proaktivnom djelovanju usmjerenom ka unaprjeđenju zaštite djece na internetu, predstavnika instutucije relevantne za regulaciju komunikacija na području BiH (RAK) i tvrtke koja je relevantna kao tehnička podrška u kontekstu realizacije i promocije brojnih aktivnosti usmjerenih na zaštitu djece na internetu. Naime, ovaj projekat, čiji je jedan dio izrađena analiza, primjer je zajedničkog i koordniranog odgovora nekoliko dionika okupljenih radi postizanja zajedničkog i društveno važnog cilja, a to je unaprjeđenje zaštite djece na internetu na području BiH.

ANALIZA MJERA ZA ZAŠTITU DJECE KOJE PODUZIMAJU PRUŽATELJI PRISTUPA INTERNETU (ISP) U BIH

U svrhu analize mjera za zaštitu djece koje poduzimaju ISP-ovi u BiH kreiran je upitnik, koji je 7. ožujka 2022. godine uspješno dostavljen putem elektronske pošte na adrese 60 ISP-ova u BiH. Upitnik se sastoji od 12 osnovnih pitanja koja se prvenstveno odnose na tehničke aspekte filtriranja internetskog prometa. Osim osnovnih pitanja, upitnik sadrži i 25 dodatnih pitanja koja služe za pojašnjenje primijenjenih tehničkih mjera.

Od ukupnog broja upućenih upitnika, odgovore su dostavila 44 ISP-a, odnosno 73%.

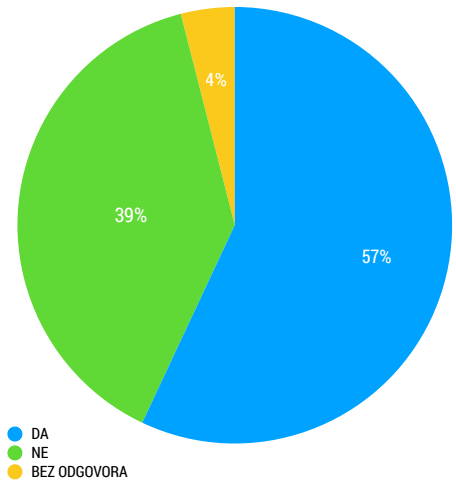
Tablica 2.1. Lista ISP-ova koji su dostavili popunjen uptnik

1. K-NET DOO TELEKOMUNIKACIJE ELEKTRON GROUP DOO DERVENTA	16. BH Telecom Sarajevo	30. Terc Trade Company doo, Prnjavor
2. TRION TEL D.O.O BANJA LUKA	17. Blic Net	31. Net Flet d.o.o
3. Formea d.o.o.	18. Media Sky doo Živinice	32. Team Consulting d.o.o. Sarajevo
4. Telrad net doo Bijeljina	19. MISS.NET d.o.o. Bihać	33. EUROPRONET BOSNIA D.O.O. SARAJEVO
5. TXTV doo Tuzla	20. Mtel a.d. Banja Luka	34. STOKIĆ doo
6. ELIT M d.o.o Bijeljina	21. TELEKLIK d.o.o.	35. TELINEA d.o.o. Bihać
7. „HKB net“ d.o.o. Sarajevo	22. Univerzitetski tele-informatički centar	36. AMB-NET d.o.o
8. ITS doo	23. ZIPZAP DOO ZENICA	37. Integra Inženjering d.o.o.
9. KATV „HS“ d.o.o. Sarajevo	24. Katarina d.o.o. Mostar	38. Neon Solucije doo Kalesija
10. „M&H“ Company d.o.o. Sarajevo	25. Logosoft d.o.o. Sarajevo	39. TEAM:MEDIA doo
11. Gigaherc doo	26. Ortak doo	40. TELEKLIK d.o.o.
12. Telemach BH d.o.o. Sarajevo	27. Akt Online	41. Elta-Kabel doo
13. KTV E-G-E d.o.o.	28. Eronet	42. WIRAC.NET d.o.o.
14. Dasto Semtel d.o.o.	29. DINNET D.O.O. GRAČANICA	43. XENTO D.O.O.
15. SoftNET d.o.o. Sarajevo	44. DSL-Elektronika doo, Modriča.	

Analiza rezultata istraživanja na temelju odgovora davatelja pristupa internetu o mjerama za zaštitu djece

Da li postoje tehnički uvjeti za filtriranje prometa po različitim protokolima (HTTP, SMTP, ...) na strani ISP-a?

Od 44 ISP-a, na ovo pitanje potvrdno je odgovorilo njih 25 (57%), negativno je odgovorilo 17 (39%), dok 2 ISP-a (4%) nisu odgovorila na pitanje (Slika 1). Najveći broj ISP-ova kod kojih postoje tehnički uslovi za filtriranje prometa može da filtrira: HTTP(S) promet (68% - 17 od 25), SMTP promet (60% - 15 od 25) i FTP spromet (24% - 6 od 25). Osim toga, većina ovih ISP-eva za potrebe filtriranja prometa koristi opremu kompanije Cisco (40% - 10 od 25), Mikrotik uređaje (24% - 6 od 25), te PowerDNS (16% - 4 od 25). Na temelju analize odgovora na ovo pitanje može se zaključiti da bi većina ISP-ova kod kojih postoje tehnički uslovi za filtriranje prometa mogla filtrirati i promet po drugim protokolima aplikativnog sloja OSI referentnog modela.

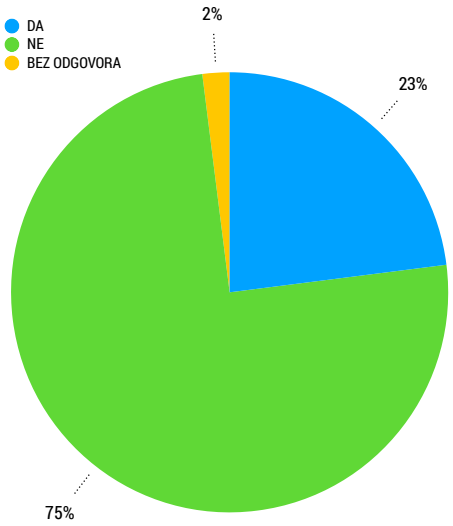


Slika 1. Postojanje tehničkih uvjeta za filtriranje saobraćaja po različitim protokolima (HTTP, SMTP, ...) na strani ISP-a.

Da li postoji filtriranje neželjenog prometa bez znanja krajnjih korisnika (pretplatnika) koje se radi na strani ISP-a?

Filtriranje neželjenog prometa bez znanja krajnjih korisnika (pretplatnika) radi se kod 23% ISP-ova (10 od 44), dok 75% ISP-ova (33 od 44) to ne radi (Slika 2). Jedan ISP nije dostavio ovaj podatak.

Ovdje je bitno istaći da ISP-ovi bez znanja krajnjih korisnika (pretplatnika) uglavnom filtriraju SMTP promet (60%, 6 od 10). U 20% slučajeva ISP-ovi bez znanja krajnjih korisnika (pretplatnika) filtriraju potencijalno maliciozni HTTP(S) promet. I za ovu namjenu se uglavnom koriste Cisco i Mikrotik



Slika 2. Filtriranje neželjenog saobraćaja bez znanja krajnjih korisnika na strani ISP-a.

uređaji, uz dodatak u vidu odgovarajućeg antivirusnog softvera.

Da li postoji mogućnost kupovine usluge filtriranja prometa na strani ISP-a?

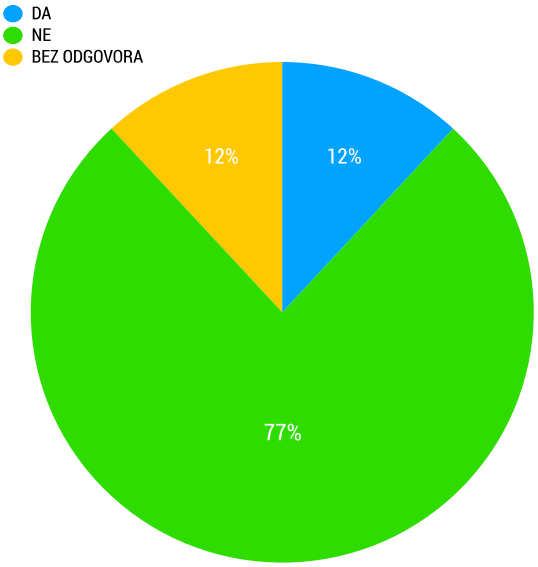
Kao što se može vidjeti na slici 3, ogromna većina ISP-ova ne nudi mogućnost kupovine usluge filtriranja prometa na strani ISP-a (86% - 37 od 44). Jedan ISP nije dostavio ovaj podatak.

Slika 3. Mogućnost kupovine usluge filtriranja prometa na strani ISP-a.

Samo 5 ISP-ova navelo je da postoji mogućnost kupovine usluge filtriranja prometa na strani ISP-a (12% - 5 od 44).

Da li se filtriranje prometa primjenjuje na sve oblike povezivosti koje ISP nudi (ADSL, kabelska, optička veza, mobilni internet, itd.)?

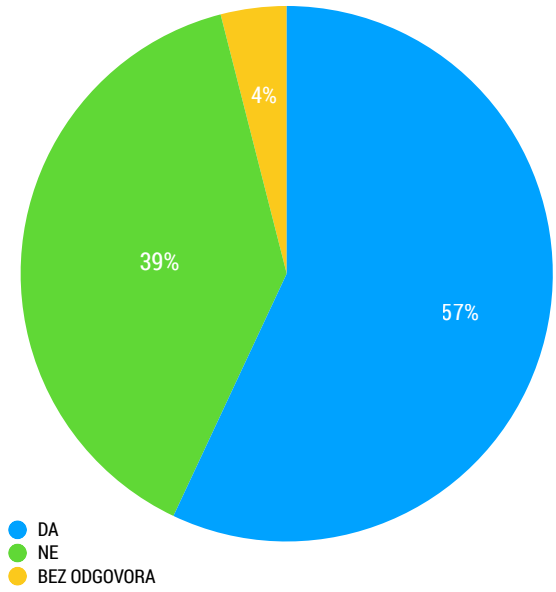
Samo 5 od 44 ISP-ova (12%) navelo je da se filtriranje prometa primjenjuje na sve oblike povezivosti koje ISP nudi (slika 4). Pet ISP-ova nije dostavilo ovaj podatak (12%). Od preostalih ISP-ova (77%, 33 od 44) kod kojih se filtriranje prometa ne primjenjuje na sve oblike povezivosti koje ISP nudi, 21% (7 od 33) primjenjuje filtriranje prometa na neke oblike povezivosti koje ISP nudi.



Slika 4. Primjena filtriranja prometa na sve oblike povezivanja koje ISP nudi.

Da li postoje pretplatnici za koje se ne vrši filtriranje prometa na strani ISP-a?

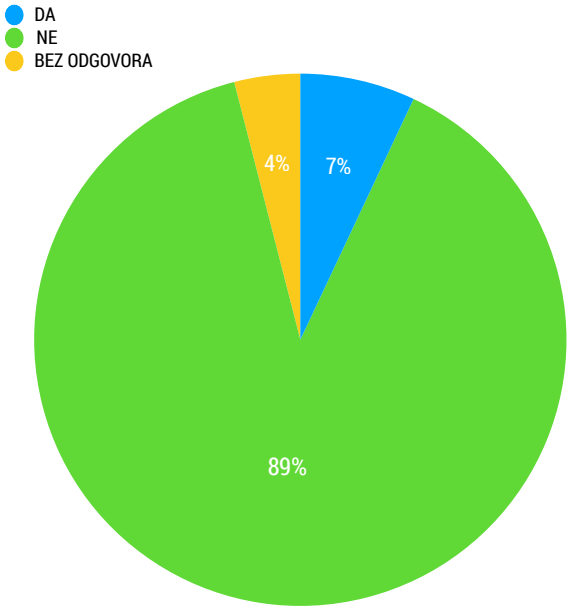
U slučaju 39% ISP-ova (17 od 44) postoje pretplatnici za koje se ne vrši filtriranje prometa na strani ISP-a (slika 5). Dva ISP-a nisu odgovorila na ovo pitanje, a u slučaju 57% ISP-ova (25 od 44) ne postoje pretplatnici za koje se ne vrši filtriranje prometa (slika 5).



Slika 5. Postojanje pretplatnika za koje se ne vrši filtriranje saobraćaja na strani ISP-a.

Da li postoji mogućnost inspekcije enkriptovanog prometa na strani ISP-a?

Kao što se može uočiti na slici 6, kod ogromne većine ISP-ova ne postoji mogućnost inspekcije enkriptovanog prometa na strani ISP-a (89%, tj. 39 od 44). Dva ISP-a nisu dostavila ovaj podatak.

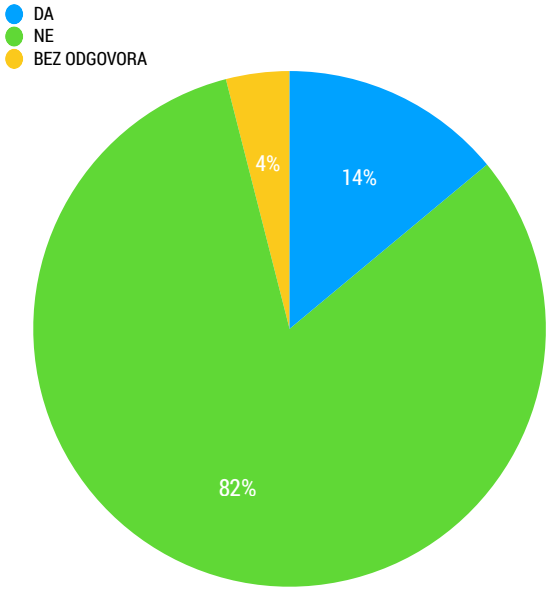


Slika 6. Inspekcija enkriptovanog prometa na strani ISP-a.

Samo tri ISP-a (7% - 3 od 44) imaju tehničke mogućnosti za inspekciju enkriptovanog prometa na strani ISP-a.

Da li pretplatnici samostalno mogu da uključuju/ isključuju opcije filtriranja prometa na strani ISP-a?

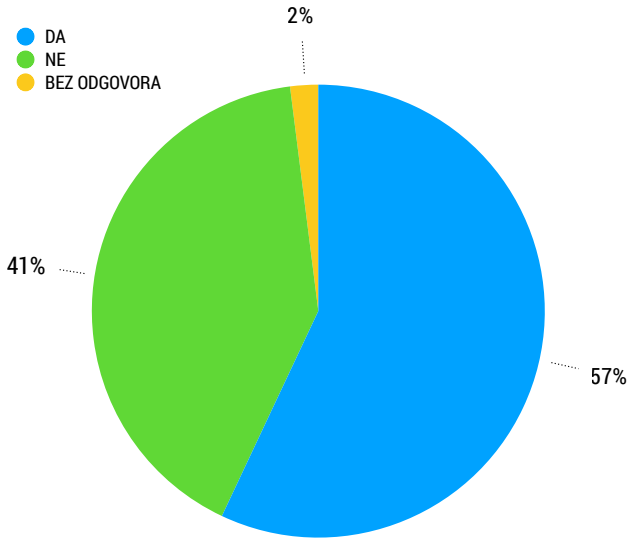
U 14% slučajeva (6 od 44) pretplatnici mogu samostalno da uključuju/isključuju opcije filtriranja prometa na strani ISP-a (slika 7). Kod četiri od ovih šest ISP-ova (67%, 4 od 6) pretplatnici za potrebe samostalnog uključivanja/ isključivanja opcije filtriranja prometa na strani ISP-a koriste *EON Connect* aplikaciju, dok kod dva od ovih šest ISP-ova (33%, 2 od 6) pretplatnici za potrebe samostalnog uključivanja/ isključivanja opcije filtriranja prometa na strani ISP-a koriste odgovarajuću *web* aplikaciju (slika 7). U 82% slučajeva (36 od 44) pretplatnici ne mogu samostalno da uključuju/isključuju opcije filtriranja prometa na strani ISP-a (slika 7). Dva ISP-a (4%, 2 od 44) nisu dostavila odgovor na ovo pitanje.



Slika 7. Mogućnost pretplatnika da samostalno uključuju/isključuju opcije filtriranja prometa na strani ISP-a.

Da li postoji mogućnost kreiranja različitih profila za filtriranje prometa i primijeniti ih na različite uređaje u mreži pretplatnika (npr. poseban profil za filtriranje prometa za uređaj koji koristi dijete)?

Na ovo pitanje potvrdno je odgovorilo 25 od 44 ISP-a (57%), negativno je odgovorilo 18 (41%), dok 1 ISP (2%) nije odgovorio na pitanje (slika 8).

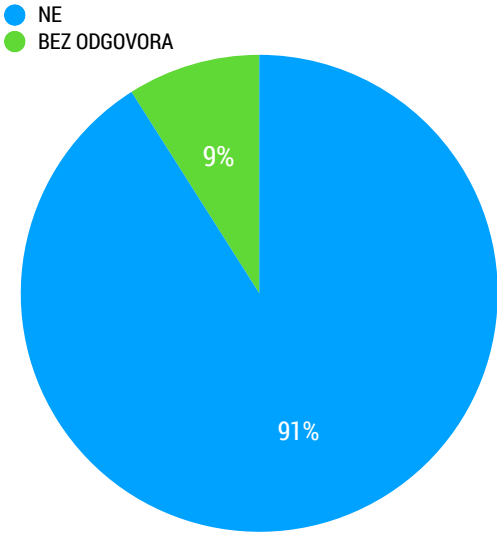


Slika 8. Mogućnost filtriranja prometa na strani pretplatnika.

Najveći broj ISP-ova kod kojih postoji mogućnost kreiranja različitih profila za filtriranje prometa i njihove primjene na različite uređaje u mreži pretplatnika ovo radi isključivo na zahtjev (28% - 7 od 25). Ostali ISP-ovi ovu mogućnost ne primjenjuju.

Da li postoje razlike po pitanju filtriranja prometa ako su pretplatnici obrazovne institucije, posebno ako se radi o osnovnim i srednjim školama?

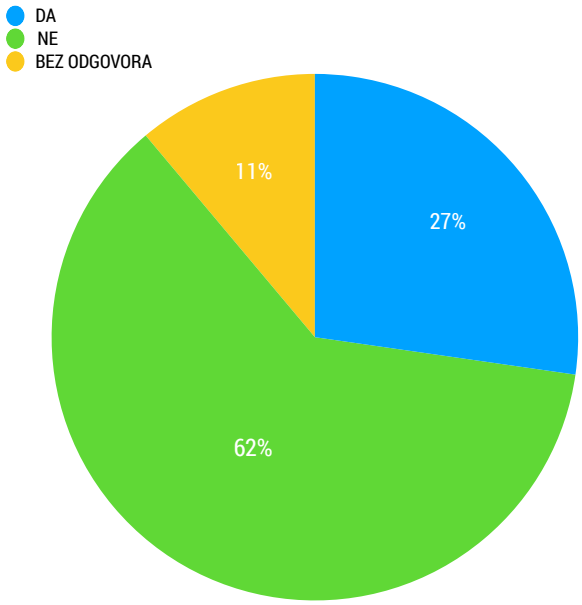
Kao što se može uočiti na slici 9, osim kod 9% (4 od 44) ISP-ova koji nisu odgovorili na ovo pitanje, kod svih ostalih (91% - 40 od 44) ne postoje razlike po pitanju filtriranja prometa ako su pretplatnici obrazovne institucije (posebno ako se radi o osnovnim i srednjim školama).



Slika 9. Postojanje razlike po pitanju filtriranja prometa ako su pretplatnici obrazovne institucije.

Da li ste provodili testiranja ispravnosti primjene pravila za filtriranje prometa?

Od ukupno 44 ISP-a, na ovo pitanje potvrdno je odgovorilo njih 12 (27%), negativno je odgovorilo 27 (62%), dok 5 ISP-ova (11%) nisu odgovorila na pitanje (slika 10). Testiranja ispravnosti primjene pravila za filtriranje se uglavnom ne provodi periodično, već samo prilikom instalacije ili nadogradnje sustava.

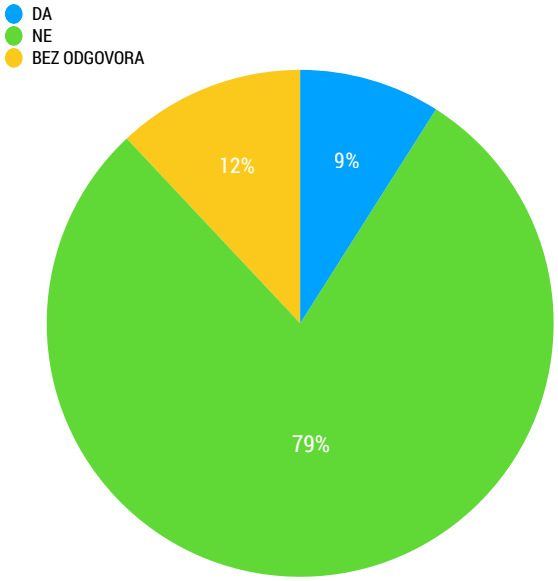


Slika 10. Provođenje testiranja ispravnosti primjene pravila za filtriranje prometa.

Kada je pristup nekom resursu blokiran, da li se i koje informacije o tome dostavljaju pretplatniku?

Ogromna većina ISP-ova ne dostavlja pretplatnicima informacije o tome da je pristup nekom resursu blokiran (79% - 34 od 44). Pet ISP-ova (12%, 5 od 44) nije dostavilo ove podatke (slika 11). Od četiri ISP-a (9%, 4 od 44) koji pretplatniku dostavljaju informacije o tome da je pristup nekom resursu blokiran, dva (50% - 2 od 4) ISP-a ove informacije čuvaju 30, odnosno 365 dana.

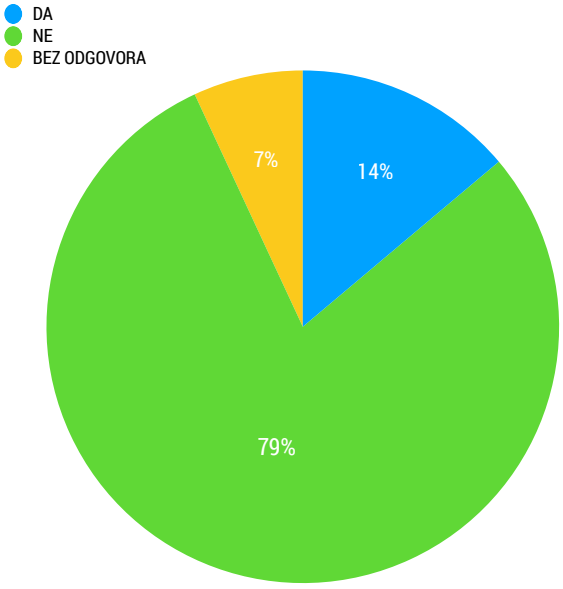
Korisnici imaju mogućnost prijave nepravilno blokiranog prometa na različite načine: putem mobilne aplikacije, web interfejsa i sl.



Slika 11. Dostavljanje informacije o blokiranju pristupa resursima.

Da li postoje usluge/paketi koji se odnose na filtriranje prometa, a koji je nepoželjan za djecu?

Na ovo pitanje potvrdno je odgovorilo 6 od 44 ISP-a (14%), negativno je odgovorilo 35 (79% - 35 od 44), dok 3 ISP-a (7% - 3 od 44) nisu odgovorila na pitanje (slika 12).



Slika 12. Postojanje usluge/paketi koji se odnose na filtriranje prometa koji je nepoželjan za djecu.

Četiri od šest ISP-ova (67%, 4 od 6) kod kojih postoje usluge/paketi koji se odnose na filtriranje prometa, a koji je nepoželjan za djecu, koristi *EON Connect* aplikaciju, uz dodatak odgovarajućeg antivirusnog softvera.

Na temelju rezultata istraživanja u pogledu mjera za zaštitu djece (tehnički aspekt) koje poduzimaju ISP-ovi u BiH može se zaključiti da:

1. 57% (25 od 44) ISP-ova ima tehničke mogućnosti za filtriranje prometa po različitim protokolima aplikacijskog sloja OSI referentnog modela, te da se za ove potrebe uglavnom koriste
2. 23% (10 od 44) ISP-ova filtrira neželjeni promet bez znanja krajnjih korisnika (pretplatnika), te da je to uglavnom SMTP promet (60%, tj. 6 od 10),
3. mogućnost kupovine usluge filtriranja prometa na strani ISP-a postoji kod svega 12% (5 od 44) ISP-ova,
4. se kod samo 12% (5 od 44) ISP-ova filtriranje prometa primjenjuje na sve oblike povezivosti koje ISP nudi,
5. da postoje pretplatnici za koje se ne vrši filtriranje prometa na strani ISP-a kod 39% (17 od 44) ISP-ova,
6. kod 89% (39 od 44) ISP-ova ne postoji mogućnost inspekcije enkriptovanog prometa na strani ISP-a, tj. da samo 7% (3 od 44) ISP-eva ima opremu koja omogućava inspekciju enkriptovanog prometa na strani ISP-a,
7. kod 14% (6 od 44) ISP-ova pretplatnici mogu samostalno da uključuju/isključuju opcije filtriranja prometa na strani ISP-a,
8. 57% (25 od 44) ISP-ova ima tehničke mogućnosti za izradu različitih profila za filtriranje prometa i njihovu primjenu na različite uređaje u mreži pretplatnika,
9. kod ISP-ova ne postoje razlike po pitanju filtriranja prometa ako su pretplatnici obrazovne institucije (posebno ako se radi o osnovnim i srednjim školama),
10. 27% (12 od 44) ISP-ova provodi testiranja ispravnosti primjene pravila za filtriranje prometa, ali ne povremeno, već samo pri instaliranju ili nadogradnji sustava,
11. samo 9% (4 od 44) ISP-ova pretplatniku dostavljaju informacije o tome da je pristup nekom resursu blokiran i
12. samo 14% (6 od 44) ISP-ova posjeduje usluge/paketi koji se odnose na filtriranje prometa, a koji je nepoželjan za djecu.

Analiza odgovora Upitnika o temi sigurnost/ bezbjednost djece na internetu

Predstavljenom istraživanju, koje je provedeno tijekom ožujka 2022. godine i koje je prvenstveno bilo usmjereno na tehničke aspekte filtriranja internetskog prometa, prethodilo je istraživanje Područja za telekomunikacije RAK-a. Zbog potpunijeg uvida u aktivnosti i mjere koje ISP-ovi u BiH poduzimaju u smislu zaštite djece, u ovom dijelu bit će predstavljeni rezultati prethodnog istraživanja.

U sklopu aktivnosti sigurnost/bezbjednost djece na Internetu Područje za telekomunikacije RAK-a kreiralo je Upitnik o temi sigurnost/ bezbjednost djece na Internetu, koji je naslovljen na sve davatelje pristupa Internetu. Svrha Upitnika je sagledati trenutnu situaciju u pogledu aktivnosti, poduzetim koracima, mogućim mjerama i procedurama koje pružatelji pristupa internetu imaju implementirane o temi sigurnost/bezbjednost djece na internetu.

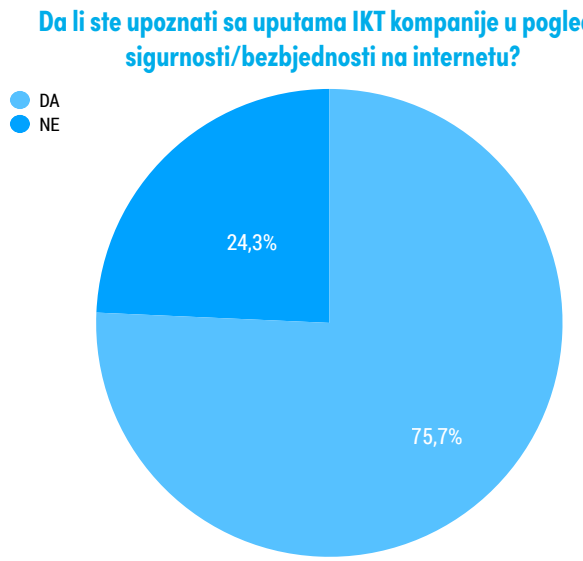
S tim u vezi Odjel za telekomunikacije poslao je putem pošte dopis na 61 kontakt adresu davatelja pristupa internetu i *mail* sa elektronskom verzijom Upitnika, na kontakt *mail* adrese davatelja pristupa Internetu. Od ukupnog broja upućenih dopisa sa Upitnicima pružateljima pristupa internetu, RAK-u je dostavljeno ukupno 37 popunjenih Upitnika, odnosno 62,3%. Gledano sa aspekta udjela operatera u ukupnom broju korisnika pristupa internetu, ispunjene Upitnike dostavilo je oko 95 % davatelja pristupa Internetu.

Tablica 2.3.1. Lista ISP-ova koji su dostavili ispunjen upitnik

1. BH Telecom d.d.	14. Team Consulting d.o.o.	27. Teleklik d.o.o.
2. Mtel a.d. Banja Luka	15. Gigaherc d.o.o.	28. Dinnet d.o.o.
3. JP HT d.d. Mostar	16. Katarina d.o.o.	29. Triontel d.o.o.
4. Telemach BH d.o.o.	17. Neon solucije d.o.o.	30. Formea d.o.o.
5. M&H Company d.o.o.	18. UTIC	31. Terc Trade Company d.o.o.
6. KTV HS d.o.o..	19. Elektron Group d.o.o.	32. Teledigital d.d.
7. HKB net d.o.o.	20. Media Sky d.o.o.	33. KTV EGE d.o.o.
8. Elta Kabel d.o.o.	21. ELIT M d.o.o.	34. K-Net d.o.o.
9. BlicNet d.o.o.	22. Alfanet d.o.o.	35. Wirac Net d.o.o.
10. Logosoft d.o.o.	23. Elta MT d.o.o.	36. AMB NET d.o.o.
11. Dasto Semtel d.o.o.	24. Telesky d.o.o.	37. ITS d.o.o.
12. TX TV d.o.o.	25. ZipZap d.o.o.	38. Integra inženjering d.o.o.
13. Akt.online d.o.o.	26. SoftNet d.o.o.	

U sljedećem dijelu Analize prikazani su rezultati ovog istraživanja. Rezultati istraživanja predstavljaju značajne pokazatelje razine zastupljenosti različitih vrsta aktivnosti i mehanizama važnih u kontekstu podizanja razine sigurnosti/bezbjednosti djece na internetu od strane ISP-ova. Njihov značaj ogleda se i u tome što predstavljaju vrijedan resurs u stvaranju, razvoju i provedbi budućih strategija i politika usmjerenih na unaprjeđenje zaštite djece u digitalnom okruženju.

Grafikon 2.3.1. Postotna zastupljenost ISP-ova koji su/nisu upoznati sa uputama za IKT tvrtke u pogledu sigirnosti/bezbjednosti djece na internetu



Uvid u grafikon ukazuje na to da je zastupljenost ISP-ova koji su upoznati sa uputama za IKT tvrtke u pogledu sigurnosti/bezbjednosti djece na internetu (28 ispitanika, tj. 75,7%) znatno veća u odnosu na ISP-ove koji nisu upoznati sa ovom vrstom uputa (9 ispitanika, tj. 24,3%).

Na temelju odgovora na pitanje otvornog tipa koje je podrazumijevalo navođenje konkretnih aktivnosti koji su ISP-ovi poduzeli u pogledu sigurnosti/bezbjednosti djece na internetu, uočene su različite vrste angažmana ISP-ova. U nastavku će biti izdvojne neke od aktivnosti poduzete od strane davatelja pristupa internetu.

Tablica 2.3.2. Prikaz aktivnosti usmjerenih na podizanje razine sigurnosti/bezbjednosti djece na internetu od strane pojedinih ISP-ova

ISP	Aktivnosti
Alfanet d.o.o.	Dostavljanje materijala o *online* sigurnosti djece putem korisničkog *maila*
AMB NET d.o.o.	U promotivnim letcima svoje firme smo uvrstili klauzulu koja se odnosi na to da roditelji trebaju maksimalno voditi računa koje stranice posjećuju njihova djeca,kome daju svoje brojeve telefona, po potrebi da nas kontaktiraju kako bih smo im dali konkretnije savjete. Uključili smo *connection tracking* kako bismo mogli po potrebi imati kompletan historijat sadržaja kojeg je korisnik pretraživao
BH Telecom	Partnerstvo sa organizacijama koje promoviraju sigurnost djece na Internetu, kampanje na ovu temu, ponuda proizvoda koji nude ove funkcionalnosti.
Blicnet d.o.o.	Posebna sekcija za roditelje o načinima zaštite djece od neprimjerenih sadržaja na televiziji https://www.blic.net/latn/?page=161. Posebna sekcija za roditelje o načinima zaštite djece od neprimjerenih sadržaja na Internetu https://www.blic.net/latn/?page=162 kao i obavještavanje roditelja o važnim sadržajima na stranici www.sigurnodijete.ba. Posebna sekcija On line sigurnost djece - ITU – gdje su predstavljeni edukativni materijalai o *online* sigurnosti djece Međunarodne telekomunikacijske unije ITU – slikovnice, radne knjige, upute za edukatore i roditelje, itd. https://www.blic.net/latn/?page=181. Obilježavanje Dana sigurnosti na Internetu, obavještavanje roditelja putem *web* stranice i profila na društvenim mrežama. Uvođenje usluge Siguran Internet. Praćenje aktivnosti ITU i RAK-a na temu online sigurnosti djece (radionice, prezentacije, i sl.), te objavljivanje edukativnih materijala na društvenim mrežama i web stranici. Uvođenje usluge Siguran internet.
Elektron Group d.o.o.	Edukacija roditelja i ugradnja naprednih rutera.
ELIT M d.o.o.	Preko *web* stranice promoviramo sigurnost djece na internetu.
Elta Kabel d.o.o	Na našoj *WEB* stranici kreirali smo posebnu sekciju pod nazivom Bezbjednost djece na Internetu https://www.elta-kabel.com/bezbjednost-djece-na-internetu/, u okviru koje smo učinili dostupnim tematske materijale Regulatorne agencije za komunikacije, a također objavljujemo tematske vijesti i istraživana iz ove oblasti.
Formea d.o.o.	Usmeno informiranje roditelja o mogućoj zlouporabi.
HKB net d.o.o., KATV HS d.o.o., M&H Company d.o.o., Telemach BH d.o.o.	Razvili smo EON Connect aplikaciju koja postaje saveznik djeci, ali i roditeljima, u bezbjednom korištenju Interneta.

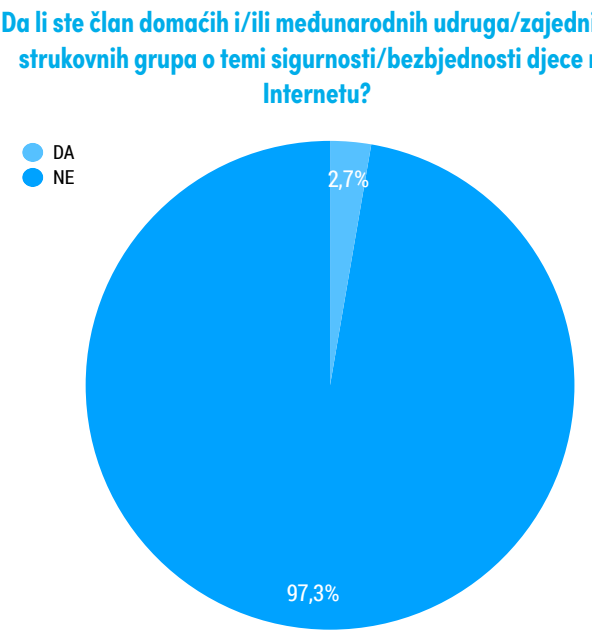
HKB net d.o.o., KATV HS d.o.o., M&H Company d.o.o., Telemach BH d.o.o.	Uvjetima poslovanja smo propisali da ćemo, na osnovu posebnih propisa ili odluke nadležne institucije u Bosni i Hercegovini kojom se određeni sadržaji oglašavanu nezakonitim, primjenom odgovarajućih tehničkih mjera onemogućeni pristup internet adresama za koje je takvim posebnim propisima ili odlukama nadležnih institucija u Bosni i Hercegovini utvrđeno da su štetni ili nezakoniti, a posebno ukoliko se tim sadržajima širi dječja pornografija i slični štetni sadržaji, omogućava nezakonito online kockanje, šire računalni virusi ili opasni programi, nezakonito pribavljaju lični podaci, ugrožava opća sigurnost, javni red i mir, omogućava protivpravna uporaba računalnih programa i aplikacija, kao i druge opasnosti po sigurno korištenje Interneta.
Integra inženjering d.o.o.	Obzirom da Uslugu pristupa Internetu dajemo isključivo pravnim subjektima kao DPI, nismo u mogućosti/potrebi za filtriranjem prometa koji ide ka krajnjim korisnicima. Mjere koje primjenjujemo interno je savjetovanje zaposlenih sukladno Općim uputama za IKT kompanije. Postavljanje jasno istaknut tok linka ka dokumentu "Smjernice za IKT kompanije u pogledu bezbjednosti djece na Internetu 2020. Na ISP *web* sajtu.
K-NET d.o.o.	Samo po zahtjevu roditelja zabranjujemo određeni sadržaj.
KTV EGE d.o.o.	Često obavještavanje putem *web* stranice, *Facebook*, Viber.
Logosoft d.o.o.	Podržavamo event Dan sigurnijeg Interneta u organizaciji EMMAUS (MFS-EMMAUS)/Centra za sigurni Internet BiH i Komiteta za obilježavanje Dana sigurnijeg Interneta u Bosni i Hercegovini. Osim toga, barem jednom godišnje održavamo besplatne radionice za roditelje i škole, odnosno sve zainteresirane, o temi Kako zaštiti djecu na Internetu. Implementirani su tehnički zahtjevi za zakonito presretanje telekomunikacija. Na našoj web-stranici smo objavili upute za korisnike Kako se zaštiti na Internetu. Certificirali smo naše usluge sa ISO/IEC 27001 te ISO/IEC 27701 normama.
Media Sky d.o.o.	U nekoliko navrata smo informirali naše korisnike putem promotivnih letaka na našem naplatnom mjestu te na mjestu gdje korisnici prijavljuju kvarova. Postavili smo sadržaj informativnog karaktera koji se tiče zaštite djece na Internetu, na našoj službenoj web stranici.
Neon solucije d.o.o.	Printanje, podjela letaka, emitovanje spota.
Team Consulting d.o.o.	Objavili smo preuzete brošure sa vašeg sajta, *online* sigurnost djece-ITU, na našem sajtu.
Teledigital d.o.o.	Edukacija djelatnika Teledigital d.d. i pripreme za *online* komunikaciju i objave prema krajnjim korisnicima Interneta.

Mtel a.d. Banja Luka	M:tel je na svojim internet stranicama mtel.ba i blog.mtel.ba istaknuo aplikacije koje nude funkcionalnost za zaštitu djece od neprimjerenih sadržaja. Tu se ističu: Dječja TV – aplikacija u okviru IPTV platforme koja omogućuje uređivanje TV sadržaja tako da budu primjereni samo za djecu. Funkcionalnost SiguranNET koja svim korisnicima mobilne mreže omogućava bezbjednije korištenje Interneta blokiranjem zlonamjerne stranice. iKids satovi: U ponudi m:tel-a se nalaze i specijalizirani iKids satovi koji omogućavaju roditeljima da lakše ostvare vezu sa svojom djecom ili prime SOS poruke. U sklopu incijative za bezbjedno korištenje interneta m:tel je podržao i projekat https://djecanainternetu.com/ koji nudi edukativne sadržaje kako sigurno koristiti internet. Primjeri: http://blog.mtel.ba/mtel-podrzava-bezbjedno-koriscenje-interneta-za-djecu-i-omladinu/ http://blog.mtel.ba/ikids-watch-i-kombinujs-junior-za-bezbrizne-roditelje-i-sigurnu-djecu/ http://blog.mtel.ba/kako-da-aktivirate-uslugu-siguran-net/
Telesky d.o.o.	Upozorili roditelje.
Triontel d.o.o.	Objava na *web* stranici – dan sigurnosti djece na Internetu.

Osim tebelarno prikazanih aktivnosti koje su navedeni ISP-ovi realizirali s ciljem podizanja razine sigurnosti/bezbjednosti djece na internetu i ostali ISP-ovi obuhvaćeni ispitivanjem naveli su neki vid angažmana značajan u ovom kontekstu.

Počevši od činjenice da je angažman koji podrazumijeva članstvo ISP-ova u nekom od domaćih i/ili međunarodnih udruga/zajednica/strukovnih grupa o temi sigurnosti/bezbjednosti djece na internetu, značajan u kontekstu sinhroniziranog djelovanja i postizanja značajnijih rezultata u kontekstu zaštite djece na internetu, ISP-ovima je postavljeno i pitanje usmjereno na utvrđivanje razine ove vrste njihovog angažmana.

Grafikon 2.3.2. Postotna zastupljenost ISP-ova koji su/nisu članovi u nekom od domaćih i/ili međunarodnih udruga/zajednica/strukovnih grupa o temi sigurnosti/bezbjednosti djece na internetu

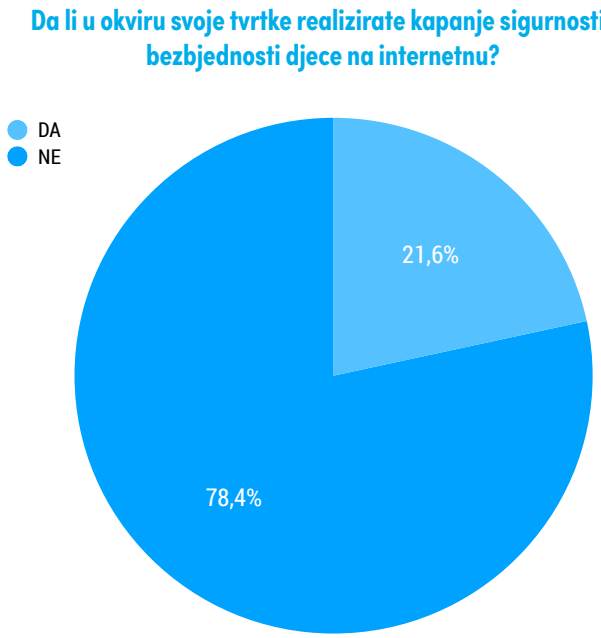


Uvid u grafikon ukazuje na to da je postotna/brojčana zastupljenost ISP-ova koji nisu član neke domaće i/ili međunarodne udruge/zajednice/strukovne grupe o temi sigurnosti/bezbjednosti djece na internetu (97,3%, tj. 36 ispitanika) značajno veća u odnosu na ISP-ove koji su u ovom smislu aktivni (2,7%, tj. 1 ispitanik).

BH Telecom je jedini davatelj pristupa internetu koji je član neke udruge o temi sigurnost/bezbjednost djece na internetu i to kroz članstvo u međunarodnim organizacijama u okviru kojih postoje različite grupe koje uključuju i teme sigurnosti na Internetu.

Jedan od značajnih oblika angažmana u kontekstu zaštite djece na internetu jeste svakako realiziranje kampanja usmjerenih na podizanje svijesti o značaju njihove zaštite i o mehanizmima koji uvelike mogu doprinijeti podizanju razine njihove bezbjednosti u digitalnom okruženju. U tu svrhu, ISP-ovima je postavljeno pitanje o tome da li u okviru svoje tvrtke realiziraju kampanje sigurnosti/bezbjednosti djece na internetu.

Grafikon 2.3.3. Postotna zastupljenost ISP-ova koji (ne)realizuju kampanje sigurnosti/bezbjednosti djece na internetu



Podaci prikazani na grafikonu pokazuju da su ISP-ovi koji realiziraju kampanje sigurnosti/bezbjednosti djece na internetu (21,6%, tj. 8 ispitanika) postotno/brojčano značajno manje zastupljeni u odnosu na ISP-ove koji ovu vrstu kampanja ne provode (78,4%, tj. 29 ispitanik). U ovom kontekstu važan je i podatak da kampanje sigurnosti/bezbejdnosti djece na internetu uglavnom organiziraju ISP-ovi sa velikim brojem korisnika.

ISP-ovima koji su u tom smislu angažirani, ponuđena je mogućnost da navedu konkretne aktivnosti usmjerene na kampanje sigurnosti/bezbjednosti djece na internetu.

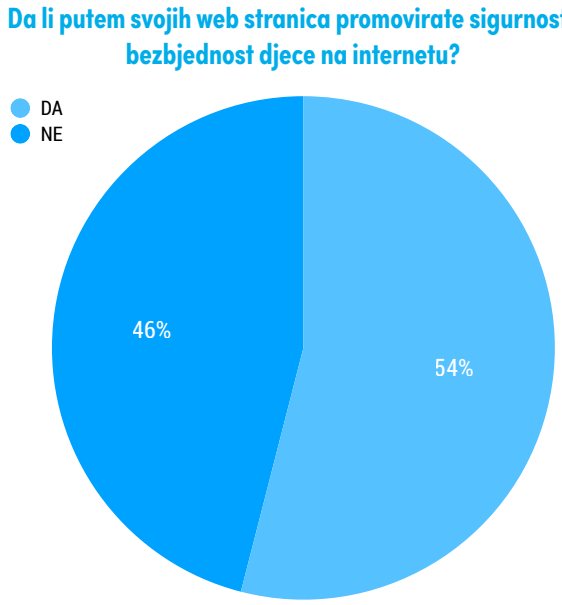
Tablica 2.3.3. Prikaz aktivnosti usmjerenih na kampanje sigurnosti/bezbjednosti djece na internetu od strane pojedinih ISP-ova

ISP	Kampanje sigurnosti/bezbjednosti djece na internetu
BH Telecom d.d.	Obilježavanja dana sigurnosti djece na Internetu. https://www.bhtelecom.ba/drustvena-odgovornost/2020/02/dan-sigurnijeg-interneta/ https://www.bhtelecom.ba/drustvena-odgovornost/2019/12/dr-rajovic-skole-i-roditelji-moraju-djecu-nauciti-da-funkcionalno-razmisljaju/ Oglašavanje kampanja putem društvenih mreža BH Telecoma.
Mtel a.d. Banja Luka	Podrška sigurnom korištenju Interneta za djecu, npr.: http://blog.mtel.ba/mtel-podrzava-bezbjedno-koriscenje-interneta-za-djecu-i-omladinu/
JP HT Mostar	Uvedena je roditeljska zaštita kao opcija na adsl-u kojima roditelji mogu provjeriti i zaštititi dijete od neželjenih sadržaja.
Elta Kabel d.o.o.	U okviru usluge koju nudimo korisnicima, aplikacije *Kaspersky Safe Kids*, proveli smo nekoliko kampanja na društvenim mrežama u proteklom razdoblju, a koje se izravno tiču sigurnosti djece na Internetu. Također, povremeno objavljujemo tekstove na sajtu i društvenim mrežama Elta-Kabela u odjeljku Blog o temi sigurnijeg surfanja Internetom, a koje uključuju i preporuke za antivirusne programe i slično. Linkovi: https://www.instagram.com/p/CB2umnGK4CL/ https://www.facebook.com/eltakabel/photos/3238692659525038 https://www.elta-kabel.com/bezbjednost-djece-na-internetu/14801/bezbjednost-djece-na-internetu/ https://www.elta-kabel.com/blog/11509/zajedno-za-bolji-internet/

Blicnet d.o.o.	Tvrtka u svom portfoliju usluga nudi uslugu Siguran Internet, osim toga imamo stalnu kampanju zaštite djece u TK uslugama, a onda posebno zaštite na Internetu, sa konkretnim uputama.
Logosoft d.o.o.	Podržavamo *event* Dan Sigurnijeg Interneta u organizaciji EMMAUS (MFS-EMMAUS)/Centra za Sigurni Internet BiH i Komiteta za obilježavanje Dana Sigurnijeg Interneta u Bosni i Hercegovini. Osim toga, minimalno jednom godišnje održavamo besplatne radionice za roditelje i škole o temi Kako zaštiti djecu na Internetu. Svi eventi su javno podržani putem naše *web* stranice i društvenih mreža, a za besplatne radionice objavljujemo na portalu www.klix.ba i javne pozive za sudjelovanje našoj besplatnoj radionici.
Formea d.o.o.	Usmeno informisanje, letci, plakati.
AMB NET d.o.o.	Pazite kome dajete svoj broj telefona, pazite kakve slike objavljujte na društvenim mrežama, pazite s kim se dopisujete, ne prihvaćajte ljude za prijatelje koje ne poznajete.

Zbog važnosti kontinuirane promocije sigurnosti/bezbjednosti djece na internetu shodno navikama djece i njihovom kontinuiranom korištenju interneta, ISP-ovima je postavljeno pitanje u vezi sa ovom vrstom angažmana.

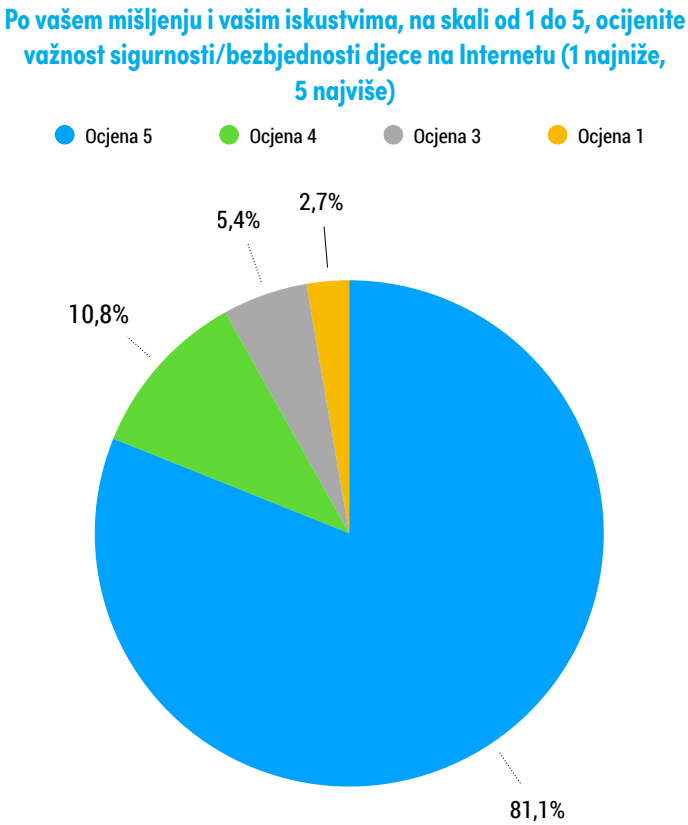
Grafikon 2.3.4. Postotna zastupljenost ISP-ova koji na svojim web stranicama promoviraju/ne promoviraju sigurnost/bezbjednost djece na internetu



U uvidu u grafikon nvedeno je da je postotak/brojčana zastupljenost ISP-ova koji na svojim *web* stranicama promoviraju sigurnost/bezbjednost djece na internetu (54%, tj. 20 ispitanika) veća u odnosu na ISP-ove koji na svojim web stranicama ne promoviraju sigurnost/bezbjednost djece na internetu.

Ispitanicima je ponuđeno da iz svoje perspektive, a na osnovu svog iskustva procijene važnost sigurnosti/bezbjednosti djece na internetu, ocjenama u rasponu od 1 (najniže) do 5 (najviše).

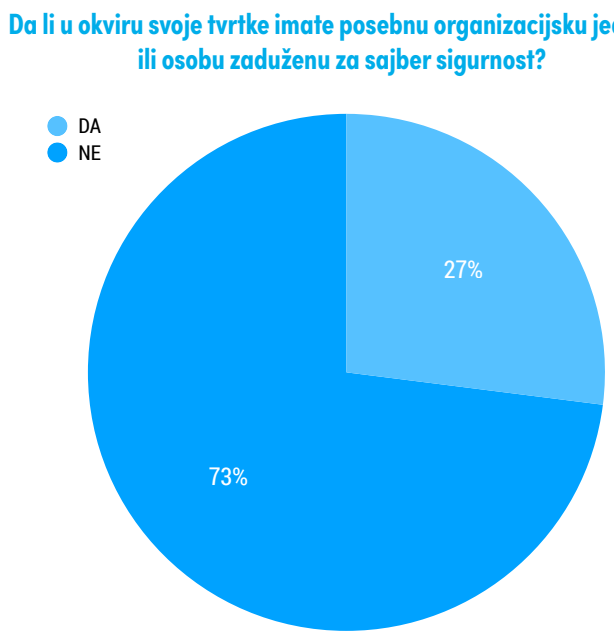
Grafikon 2.3.5. Postotna zastupljenost ISP-ova u smislu procjene važnosti sigurnosti/bezbjednosti djece na internetu



Podaci na grafikonu pokazuju da ispitanici u najvećem broju pitanje sigurnosti/bezbjednosti djece na internetu smatraju veoma važnim, jer je 30 ispitanika (81,1%) ocijenilo važnost sigurnosti/bezbjednosti djece na internetu ocjenom 5. U znatno nižem postotku zastupljeni su ispitanici koji su ovaj aspekt ocijenili manje značajnim. Ocjenu 1 dao je samo jedan ispitanik (2,7%), ocjenom dva nijedan ispitanik, dok su ocjenom 3 samo dva ispitanika (5,4%) ocijenila važnost sigurnosti/bezbjednosti djece na internetu. Nešto izraženija zastuljenost je onih ispitanika koji su ovaj aspekt procijenili dodjeljući ocjenu 4 (10,8%, tj. četiri ispitanika).

U cilju procijene potencijala kojim ISP-ovi raspolažu u kontekstu sigurnijeg korištenja interneta, ISP-ovima je postavljeno pitanje o tome da li njihova tvrtka ima posebnu organizacijsku jedinicu ili osobu koja se isključivo bavi kibernetičkom sigurnošću.

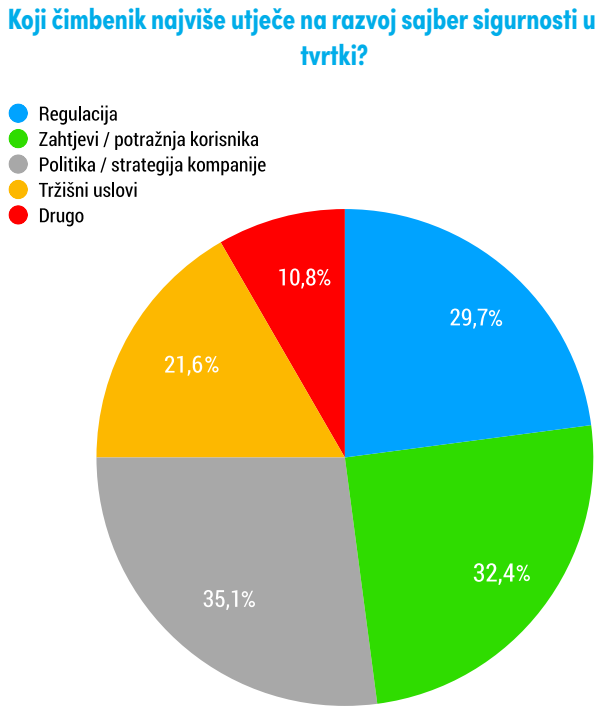
Grafikon 2.3.6. Postotna zastupljenost ISP-ova koji imaju/nemaju posebnu organizacijsku jedinicu/osobu zaduženu za sajber sigurnost



U uvidu u grafikon uočljivo je da je postotna zastupljenost ISP-ova koji nemaju posebnu organizacijsku jedinicu ili osobu koja je isključivo zadužena za sajber sigurnost (73%, tj. 27 ispitanika) značajno veća u odnosu na ISP-ove koji raspolažu ovim organizacijskim kapacitetima ili ljudskim resursima (27%, tj. 10 ispitanika).

S obzirom na složenost procesa pružanja sigurnijeg korištenja interneta, tj. na čimbenike koji ovaj koncept na različite načine određuju, ispitanici su upitani o čimbenicima koji unutar njihove tvrtke prvenstveno utječu na razvoj sajber sigurnosti.

Grafikon 2.3.7. Postotna zastupljenost ISP-ova u odnosu na čimbenike koji u njihovoj tvrtki najviše utječu na razvoj sajber sigurnosti

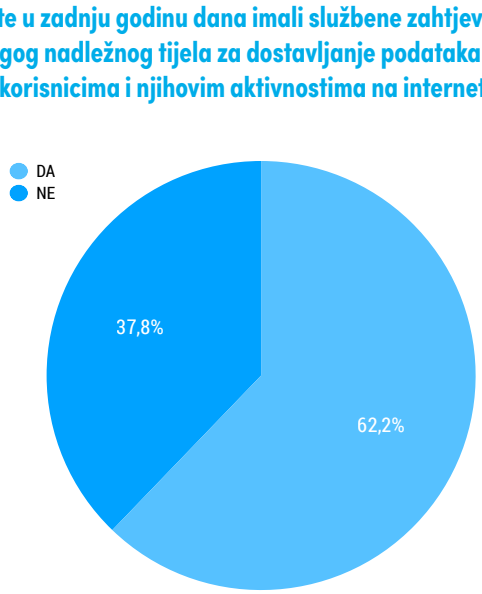


Rezultati prikazani na grafikonu pokazuju da je razvoj sajber sigurnosti u najvećem postotku određen unutarnjim čimbenikom, tj. politikom/strategijom tvrtke (35,1%, tj. 13 ispitanika), a potom zahtjevima/potražnjom korisnika (32,4%, tj. 12 ispitanika). U nešto manjem postotku ispitanici su utvrdili regulaciju (29,7%, tj. 11 ispitanika) i tržišne uvjete (21,6%, tj. 8 ispitanika), kao vanjske čimbenike koji prvenstveno određuju razvoj sajber sigurnosti u njihovoj tvrtki. U značajno manjem postotku zastupljeni su ispitanici koji neke druge čimbenike smatraju važnim u ovom kontekstu (10,8%, tj. 4 ispitanika).

Pružatelji pristupa Internetu su se odlučili za ponuđene odgovore, ali i za više ponuđenih odgovora uz određena objašnjenja.[5]

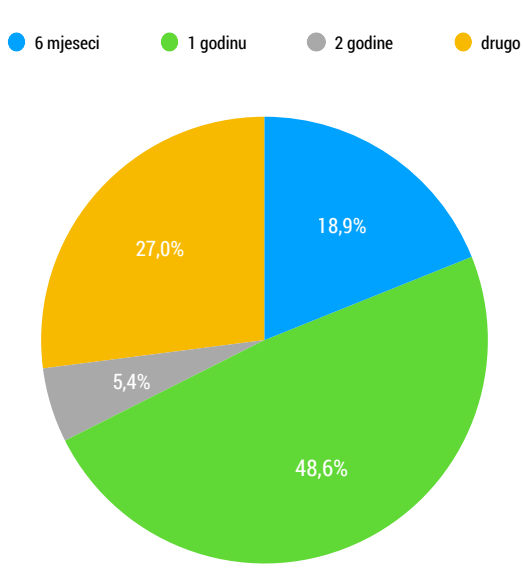
[5]BH Telecom u okviru svoje politike/strategije promovira stalni razvoj i u ovoj oblasti, prateći zahtjeve korisnika, ali i regulatorne i zakonske obveze. (BH Telecom)
Strategija tvrtke ide u tom smjeru, ali su nam bitni i zahtjevi korisnika, uz poštivanje regulatornih mjera. (Triontel d.o.o.)
Pored gore navedenih opcija, postoji još i moralni faktor koji utječe na nas da na najviši način dajemo podršku i zaštitu sigurnosti djeci a i odraslih na Internetu. (AMB NET d.o.o.)

Grafikon 2.3.8. Postotna zastupljenost ISP-ova u odnosu na službene zahtjeve policije ili drugog nadležnog tijela za dostavljanje podatka o svojim korisnicima i njihovim aktivnostima na Internetu u zadnju godinu dana



Rezultati prikazani na grafikonu pokazuju da su ISP-ovi u značajno većem postotku bili suočeni sa obvezom da dostave podatke o svojim korisnicima i njihovim aktivnostima na internetu na temelju službenog zahtjeva policije ili drugog nadležnog tijela (62,2%, tj. 23 ispitanika). Ovu vrstu službenih zahtjeva nije imalo 14 ispitanika, tj. 37,8% od ukupnog uzorka.

Grafikon 2.3.9. Postotna zastupljenost ISP-ova u odnosu na razdoblje pohrane podataka (logova) svojih korisnika

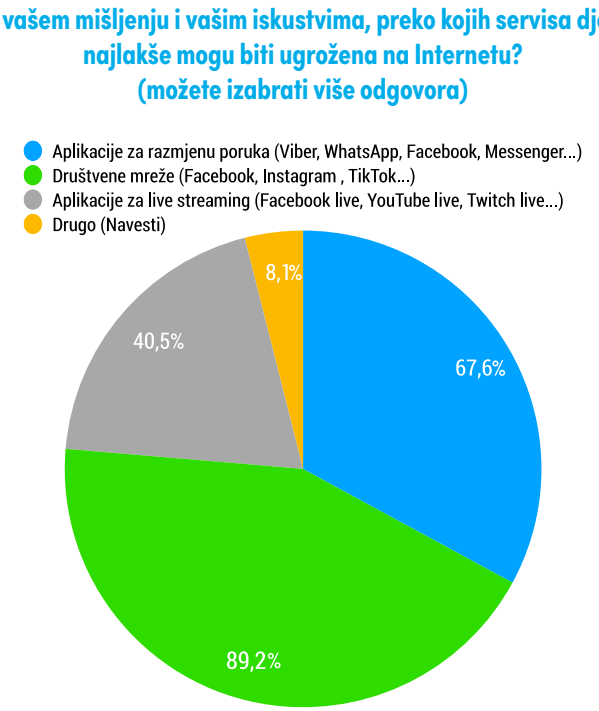


Uvid u grafikon pokazuje da ISP-ovi u najvećem postotku godinu dana pohranjuju podatke (logove) svojih korisnika (48,6%, tj. 18 ispitanika), dok ih dvije godine pohranjuju samo dva ispitanika, tj. 5,4% od ukupnog uzorka. Pola godine, tj. šest mjeseci podatke (logove) svojih korisnika čuva sedam ISP-ova (18,9%). U pogledu opcije Drugo uočljiva je značajna postotna/brojčana zastupljenost ispitanika (27%, tj. 10 ispitanika), a ISP-ovi koji su izabrali ovu opciju kroz svoje odgovore konkretizirali su svoj pristup u kontekstu razdoblja čuvanja podataka (logova) svojih korisnika.

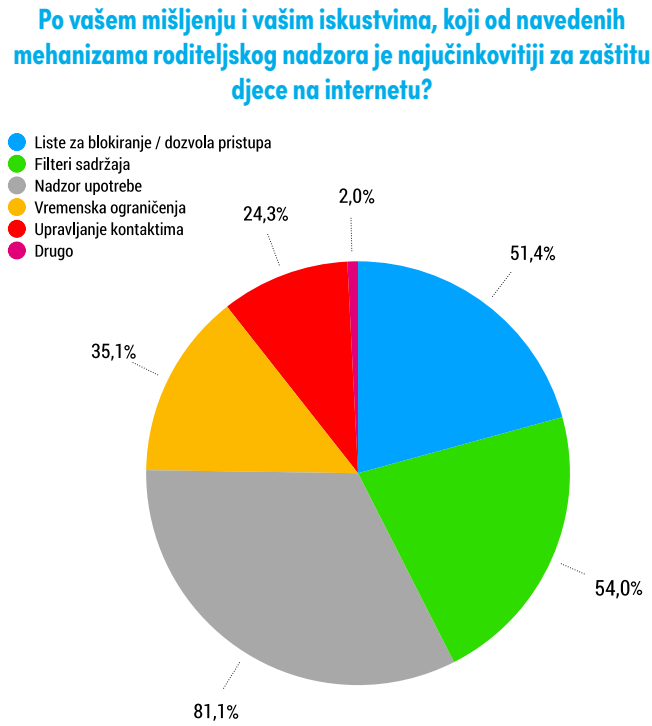
Zbog zastupljenosti različitih servisa na internetu i njihove dostupnosti korisnicima usluge pristupa internetu, ispitanicima je ponuđeno pitanje koje podrazumijeva samopercepciju ispitanika na osnovu njihovog iskustva o uslugama posredstvom kojih su djeca u najvećoj mjeri ugrožena na internetu. Ispitanicima je ostavljena mogućnost odabira više ponuđenih odgovora, kao i da u tom smislu navedu uskugu koja nije obuhvaćena pitanjem.

[6] Zavisi od sistema, čuvanje log-ova se usklađuje sa zakonskim, regulatornim i ugovornim obavezama. (BH Telecom)
U skladu sa uslovima koje zahtjeva zakonito presretanje telekomunikacija. (Logosoft d.o.o.)
13 godina (Dasto Semtel d.o.o.)
Nemamo niti jednog korisnika koji koristi NAT usluge na našoj opremi niti pružamo servis preko DHCP protoka te iz tog razloga ne pravimo logove. Svi naši korisnici su sa statičkim IP adresama. (AKT Online d.o.o.)
5 godina. (Neon Solucije d.o.o.)
30 dana. (ZipZap d.o.o.)
Više od 5 godina (određene logove imamo od 2011. godine). (Teledigital d.o.o.)
Ne čuvamo, ne pratimo sadržaja korištenja naših pretplatnika. (Wiracnet d.o.o.)
Trenutno čuvamo logove zadnje 3 godine, jer smo nedavno imali zahtjev od više MUP-ova iz cijele države oko pronalaska osobe koja je vršila krivična djela prevare na Internetu, te je ista uspješno otkrivena uz našu pomoć. (AMB NET d.o.o.)

Grafikon 2.3.10. Postotna zastupljenost ISP-ova u odnosu na njihovu samopercepciju o uslugama putem kojih djeca najlakše mogu biti ugrožena na internetu



Grafikon 2.3.11. Postotna zastupljenost ISP-ova u odnosu na njihovu samopercepciju o najučinkovitijim mehanizmima roditeljskog nadzora za zaštitu djece na internetu



Uvid u grafikon prikazuje da je postotna/brojčana zastupljenost ispitanika koji društvene mreže prepoznaju kao platforme na kojima su djeca najugroženija najveća (89,2%, tj. 33 ispitanika), a potom su najzastupljeniji ISP-ovi koji su aplikacije za razmjenu poruka u ovom kontekstu percipirali kao potencijalno najproblematičnije (67,6%, tj. 25 ispitanika). Aplikacije za *live streaming* 15 ispitanika (40,5%) percipiralo je kao servis na kojem djeca najlakše mogu biti ugrožena na internetu, dok su tri ispitanika (8,1%) izabrala opciju Drugo.

Pružatelji usluge pristupa internetu izabrali su ponuđene odgovore uz pojedine komentre.[7]

Zbog važnosti roditeljskog nadzora u pogledu zaštite djece na internetu, ispitanicima je postavljeno pitanje u vezi sa mehanizmima roditeljskog nadzora, koji su prema njihovom mišljenju najučinkovitiji za zaštitu djece na internetu. Ispitanicima je ponuđena mogućnost odabira više odgovora i omogućeno im je navođenje nekog drugog mehanizma, koji nije uključen u pitanje.

Podaci prikazani na grafikonu ukazuju na to da je iz perspektive ispitanika najefikasniji mehanizam roditeljskog nadzora za zaštitu djece na internetu prvenstveno nadzor upotrebe interneta (81,1%, tj. 30 ispitanika). Zatim su kao najučinkovitije mehanizme identifikovali upotrebu filtera sadržaja (54%, tj. 20 ispitanika) i liste za blokiranje/dozvola pristupa određenim sadržajima (51,4%, tj. 19 ispitanika). Vremenska ograničenja, kao mehanizam roditeljskog nadzora u kontekstu njegove učinkovitosti za zaštitu djece na internetu, izabralo je 13 ispitanika (35,1%), dok je upravljanje kontaktima, kao jedan od najučinkovitijih mehanizama roditeljskog nadzora, percipiralo devet ispitanika (24,3%). Samo dva ispitanika (5,4%) su se oprodijelila za opciju koja podrazumijeva upotrebu drugih mehanizama u odnosu na ponuđene.

Osim odabira ISP-ova u odnosu na ponuđene mehanizme roditeljskog nadzora za zaštitu djece na internetu, pojedini ispitanici dostavili su i dodatne komentare.[8]

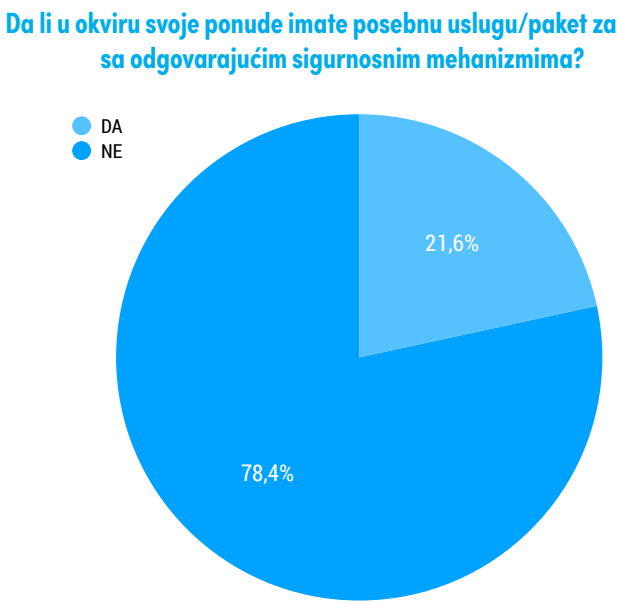
---

[7]Zavisno od uzrasta djece i sadržaja koji se gleda na svakom od kanala može biti dostupan sadržaj koji nije primjeren uzrastu djece. (BH TELECOM)
Putem bilo kojeg pretraživača može se pristupiti neprikladnom sadržaju. (Team Consulting d.o.o.)
Različiti uzrasti djece mogu biti ugroženi na različitim online platformama. Sve platforme predstavljaju potencijalnu opasnost za svako dijete, ali njegova ugroženost ovisi direktno o korisničkim navikama, odnosno činjenici da li koristi ili ne koristi pojedinu aplikaciju/društvene mreže i sl. Kada su u pitanju djeca, mišljenja smo da se svaki Internet servis mora posmatrati kao potencijalna prijetnja. (Logosoft d.o.o.)

[8]Na našim radionicama koje smo organizovali o ovoj temi predstavljali smo besplatna sveobuhvatna rješenja koja obuhvataju: kreiranje korisničkog računa za dijete i označavanje adekvatnog uzrasta djeteta prilikom kreiranja korisničkog računa. Dijete se logira na radne stanice, laptope, mobitele, tablete, game konzole koristeći svoj dječji account.

Počevši od važnosti raspolaganja odgovarajućim sigurnosnim mehanizmima u kontekstu pružanja više razine zaštite djece na internetu, ISP-ovima je postavljeno pitanje u vezi sa tim da li u svojoj ponudi imaju posebne usluge/pakete namijenjene djeci, a koji uključuju odgovarajuće sigurnosne mehanizme.

Grafikon 2.3.12. Postotna zastupljenost ISP-ova koji posjeduju/ne posjeduju posebnu uslugu/paket za djecu sa odgovarajućim sigurnosnim mehanizmima



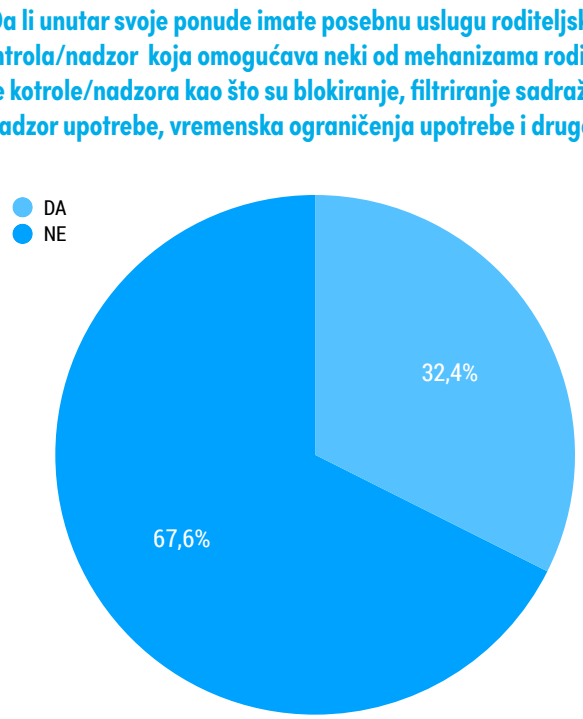
Podaci prikazani na grafikonu pokazuju da posebnu uslugu/paket za djecu sa odgovarajućom sigurnosnim mehanizmima znatno veći postotak ISP-ova ne posjeduje (78,4%, tj. 19 ispitanika) u odnosu na one ISP-ove koji raspolažu ovim mehanizmima (21,6%, tj. 8 ispitanika). Posebnu uslugu/paket za djecu sa odgovarajućim sigurnosnim mehanizmima u okviru svoje ponude imaju pružatelji usluge pristupa internetu sa velikim brojem korisnika usluge pristupa internetu (gledano sa aspekta udjela operatora u ukupnom broju korisnika pristupa Internetu). S obzirom na to da su ispitanici koji su potvrdno odgovorili na postavljeno pitanje, tj. koji imaju poseban paket/uslugu za djecu sa odgovarajućim sigurnosnim mehanizmima, u okviru upitnika upućeni na navođenje naziva i linka ove vrste usluge, određeni ISP-ovi su to dostavili.[9]

Na navedene platforme se instalira aplikacija (dostupne su kao potpuno besplatne) putem koje roditelji pomoću svog accounta mogu apsolutno nadzirati sve ono što dijete radi, uključujući, ali ne ograničavajući se na: dužinu upotrebe uređaja, razdvajanje sati korištenja uređaja za školske aktivnosti i slobodne aktivnosti, mogućnost instalacije aplikacija, vremenske dužine upotrebe aplikacija, mogućnost pretraživanja, automatska blokada pretraživanja pojedinih kategorija itd. Primjeri takvih aplikacija su *Family Link* te *Microsoft Family Safety*. Smatramo da se zaštita djeteta može postići samo sveobuhvatnim mehanizmima roditeljske kontrole. Dodatno, vrlo bitan mehanizam za zaštitu djece jeste psihička potpora i edukacija djece o potencijalnim problemima i opasnostima s kojima mogu da se susretnu prilikom upotrebe Interneta. (Logosoft d.o.o.)
Briga o djeci, redovno kontrolisanje telefona, tableta laptopa itd. te paralelno korištenje profila sa djecom na društvenim mrežama. (AMB NET d.o.o.)

[9] Usluga *Kaspersky Safekids* Antivirus, Link:
https://mojwebshop.bhtelecom.ba/INTERSHOP/web/BOS/BHTelecomWebShop-BHTelecom-Site/bs_BA/-/BAM/ViewProduct-Start?SKU=350591 (BH Telecom)
U M:tel IPTV ponudi se nalazi aplikacija Dječija TV u okviru koje se nalaze kanali i videoteke posebno izdvojeni za dječiji uzrast. U okviru aplikacije Dječija TV postavljen je sigurnosni mehanizam u vidu roditeljske kontrole kojom se može uticati na dužinu trajanja gledanja sadržaja i starosnu granicu sadržaja koji se gleda. (Mtel a.d. Banja Luka)
Internet zaštita. Sami postavite granice korištenja online sadržaja i razinu zaštite kućanstva i privatnosti, Link:
https://www.hteronet.ba/privatni-korisnici/internet-zastita-pg186 (JP HT Mostar)
Upravljaj kućnim Internetom Eon Connect, Link:
https://telemach.ba/aplikacije/eon-connect/ (HKB net d.o.o., KATV HS d.o.o., M&H Company d.o.o., Telemach BH d.o.o.)

Zbog potpunijeg uvida u određene usluge roditeljske kontrole/nadzora koje omugućavaju neki od mehanizama roditeljske kontrole/nadzora kao što su blokiranje, filtriranje sadržaja, nadzor upotrebe, vremenska ograničenja upotrebe i drugo, ISP-ovima je postavljeno pitanje da li nude uslugu koja podrazumijeva neki od navedenih mehanizama roditeljske kontrole/nadzora.

Grafikon 2.3.13. Postotna zastupljenost ISP-ova koji unutar svoje ponude imaju/nemaju posebnu uslugu roditeljska kontrola/nadzor koja omogućava neki od mehanizama roditeljskog nadzora (popis za blokiranje, filtriranje sadržaja, nadzor upotrebe, vremenska ograničenja upotrebe i dr)

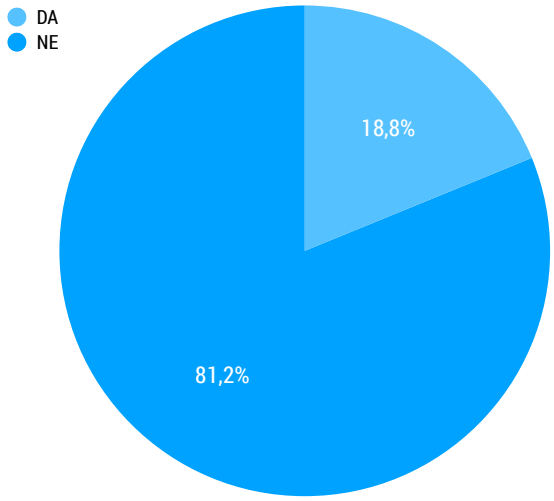


Uvidom u grafikon primjetno je da je postotna zastupljenost ISP-ova koji unutar svoje ponude ne posjeduju posebnu uslugu roditeljska kontrola/nadzor koja omogućava neki od mehanizama roditeljske kontrole/nadzora (popis za blokiranje, filtriranje sadržaja, nadzor upotrebe, vremenska ograničenja upotrebe i dr) veća (67,6%, tj. 25 ispitanika) u odnosu na ISP-ove koji raspolažu ovom vrstom posebne usluge (32,4%, tj. 12 ispitanika). Potvrdan odgovor na ovo pitanje podrazumijevao je dostavljanje konkretnih vrsta usluga kojima ISP-ovi raspolažu.[10]

[10] Usluga *Kaspersky Safe kids* Antivirus osigurava sigurnije korištenje Internet usluga korisnicima, kao i njihovoj djeci. Usluga omogućava zaštitu djece prilikom korištenja Interneta kroz funkcionalnosti kao što su Parental Control i Safe Kids.Link:https://mojwebshop.bhtelecom.ba/INTERSHOP/web/BOS/BHTelecomWebShop-BHTelecom-Site/bs_BA/-/BAM/ViewProduct-Start?SKU=350591 (BH Telecom)
U okviru M:tel IPTV ponude se putem mehanizma roditeljske kontrole može upravljati kategorijama sadržaja koji se gledaju na način da se sadržaj filtrira na osnovu: kategorije sadržaja, starosne granice sadržaja, kao i vremenskog ograničenja gledanja sadržaja. (Mtel a.d. Banja Luka)
U okviru usluga mobilne mreže implementirana je i usluga Siguran net koja omogućava korisnicima mobilnog Interneta u mreži M:tel-a zaštitu, analizu, detekciju i DNS filtriranje Internet prometa u realnom vremenu. Usluga između ostalog omogućava sprovođenje odgovarajućih bezbjednosnih politika korištenjem i do 70 različitih kategorija sadržaja (baza podataka zlonamjernih sajtova). (Mtel a.d. Banja Luka)
Također u fazi su razmatranja različita softverska rješenja trećih strana koja bi omogućila navedene funkcionalnosti. (Telekom Srpske)
Internet zaštita. Sami postavite granice korištenja online sadržaja i razinu zaštite kućanstva i privatnosti, Link:
https://www.hteronet.ba/privatni-korisnici/internet-zastita-pg186 (JP HT Mostar)
Postoji li mogućnost zabrane nekih sadržaja?
https://www.hteronet.ba/korisnicka-podrska/postoji-li-mogucnost-zabrane-nekih-sadrzaja-c123 (JP HT Mostar)
Upravljaj kućnim Internetom Eon Connect, Link:
https://telemach.ba/aplikacije/eon-connect/ (HKB net d.o.o., KATV HS d.o.o., M&H Company d.o.o., Telemach BH d.o.o.)
Kaspersky Safe Kids. (Elta Kabel d.o.o.)
Siguran Internet, Link:
https://www.blic.net/latn/?page=168 (Blicnet d.o.o.)
Ugradnja naprednih modela rutera (Elektron Group d.o.o.)
Samo na zahtjev roditelja blokiranje određenog prometa (K Net d.o.o.)
Imamo lokalni mehanizam u sklopu našeg autorizacijskog software koji korisnicima mreže daje mogućnost kontrole na određenim uređajima (međutim to nikoga ne zanima nažalost) naziv software je com, a link je lokalnog karaktera. (AMB NET d.o.o.)

Grafikon 2.3.14. Postotna zastupljenost ISP-ova koji razvijaju mehanizme kao što su softver za roditeljsku kontrolu/nadzor i drugi alati koji omogućavaju roditeljima da upravljaju pristupom internetu

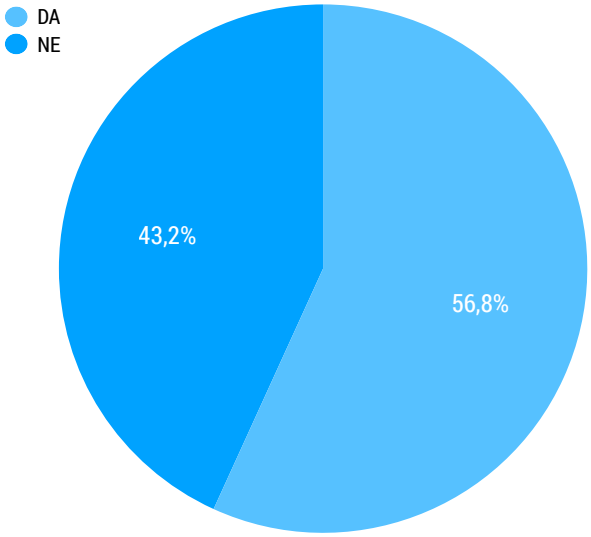
Da li u okviru svoje tvrtke razvijate mehanizme kao što su softver za roditeljsku kontrolu/nadzor i drugi alati koji omogućavaju roditeljima da upravljaju pristupom Interneta djeci?



Podaci prikazani na grafikonu pokazuju da ISP-ovi u znatno većem postotku ne razvijaju mehanizme kao što su softver za roditeljsku kontrolu/nadzor i drugi alati koji omogućavaju roditeljima da upravljaju pristupom internetu (81,1%, tj. 30 ispitanika). Samo sedam ISP-ova, tj. 18,9% od ukupnog uzorka razvija ovu vrstu mehanizama.

Grafikon 2.3.15. Postotna zastupljenost ISP-ova koji posjeduju rutere koji omogućavaju funkciju roditeljske kontole/nadzora na svim uređajima koji su povezani sa njim

Da li u okviru svoje ponude imate rutere koji omogućavaju funkciju roditeljske kontrole/nadzora na svim uređajima koji su povezani sa njim?

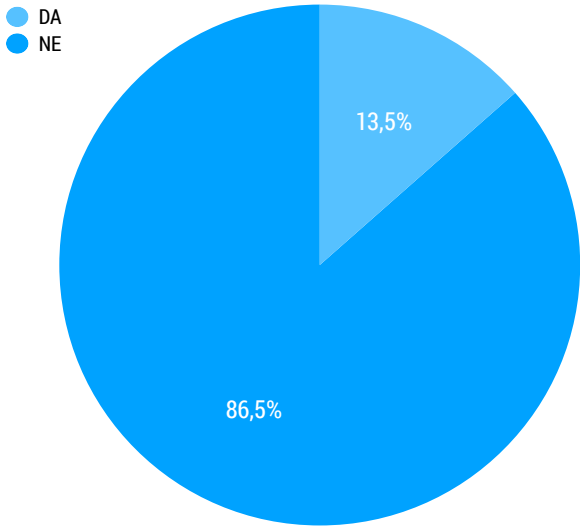


Uvid u grafikon pokazuje je da je procentualna zastupljenost ISP-ova koji posjeduju rutere koji omogućavaju funkciju roditeljske kontrole/nadzora na svim uređajima koji su povezani sa njim veća (56,8%, tj. 21 ispitanik) u odnosu na ISP-ove koji ovu vrstu rutera ne posjeduju (43,2%, 16 ispitanika). Također, u odnosu na prethodno pitanje koje se odnosi na razvijanje softvera za roditeljsku kontrolu/nadzor primjetno je da ove tvrtke u znatno većem postotku raspolažu ruterima koji omogućavaju funkciju roditeljske kontrole/nadzora.

Osim upita o posjedovanju konkretnih mehanizama roditeljskog nadzora, ISP-ovima je postavljeno i pitanje o zahtjevima određenih institucija i organizacija (npr. škole, fakulteti, bolnice i sl.), kao njihovih korisnika, koji u svojim prostorijama daju mogućnost otvorenog pristupa internetu preko Wi-Fi mreže, za blokiranje nekih stranica na internetu za koje se zna da im je sadržaj neprikladan za široku publiku.

Grafikon 2.3.16. Postotna zastupljenost ISP-ova od kojih su određene ustanove/organizacije zbog otvorenog pristupa internetu zahtijevale blokiranje stranica na internetu čiji je sadržaj neprikladan za široku publiku

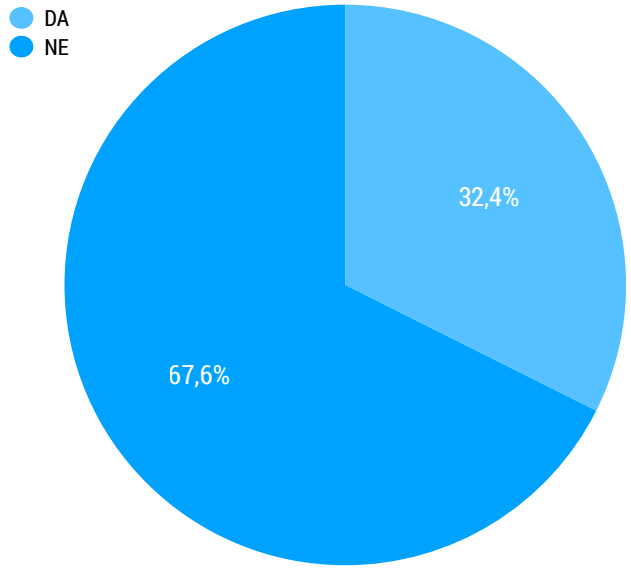
Da li ste imali zahtjeve ustanova i organizacija koji su vaši korisnici (npr. škole, fakulteti, bolnice i sl.), a koji u svojim prostorijama daju mogućnost otvorenog pristupa internetu preko Wi-Fi mreže, za blokiranje nekih stranica na Internetu za koje se zna da im je sadržaj neprikladan za široku publiku?



Podaci izneseni na grafikonu pokazuju da ISP-ovi obuhvaćeni istraživanjem u najvećem postotku nisu imali zahtjeve od određenih ustanova/organizacija za blokiranje nekih stranica na internetu (86,5%, tj. 32 ispitanika), dok je ova vrsta zahtjeva usmerena prema pet ISP-ova, tj. 13,5% od ukupnog uzorka.

Počevši od važnosti promotivnih aktivnosti u kontekstu zaštite djece na internetu, ISP-ovima je postavljno pitanje u vezi sa tim da li promoviraju alate i aplikacije roditeljske kontrole/ nadzora djece na internetu koje su razvile tvrtke zaštitu i sigurnost na internetu.

Grafikon 2.3.17. Postotna zastupljenost ISP-ova koji promoviraju/ne promoviraju alate i aplikacije roditeljske kontrole/nadzora djece na internetu razvijene od strane tvrtki koje se bave zaštitom i sigurnošću na internetu

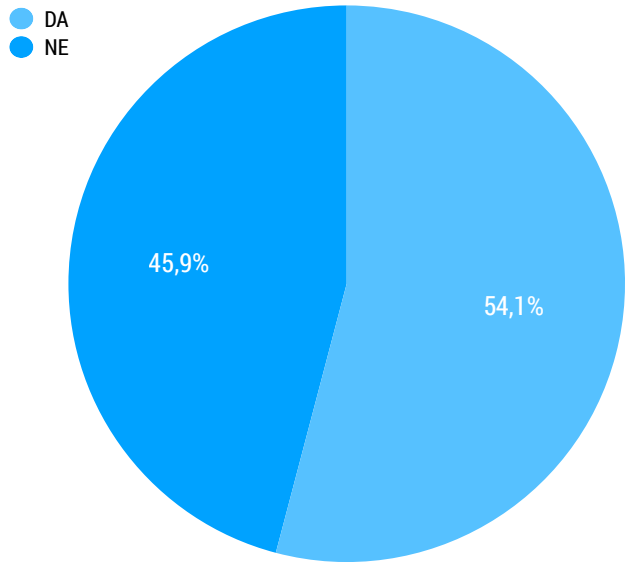


Uvid u grafikon pokazuje da je postotna zastupljenost ISP-ova koji ne promoviraju alate i aplikacije roditeljske kontrole/ nadzora djece na internetu razvijene od strane tvrtki koje se bave zaštitom i sigurnošću na internetu znatno veća (67,6%, tj. 25 ispitanika) u odnosu na ISP-ove koji su u ovom smislu aktivni (32,4%, tj. 12 ispitanika). Upitnikom je predviđeno da ispitanici koji su potvrdno odgovorili na ovo pitanje, navedu konkretne alate i aplikacije roditeljske kontrole/nadzora djece na internetu koje promoviraju.[11]

[11] Alati i aplikacije roditeljske kontrole/nadzora djece na Internetu, razvijene od strane tvrtki koje se bave zaštitom i sigurnošću na Internetu, koje promoviraju pružatelji usluge pristupa Internetu su sljedeće:
Kaspersky i *Zemana* paketi *online* zaštita za sigurnije korištenje Internet usluga svima, posebno djeci. (BH Telecom)
Siguran NET, Link:
https://mtel.ba/n677/Korisnicka-zona/Pomoc/Mobilna/Siguran-Net (Mtel a.d. Banja Luka)
Upravljaj kućnim Internetom Eon Connect, Link:
https://telemach.ba/aplikacije/eon-connect/ (HKB net d.o.o., KATV HS d.o.o., M&H Company d.o.o., Telemach BH d.o.o.)
Kaspersky Safe Kids. (Elta Kabel d.o.o.)
Google Family, Link:
https://families.google.com/familylink/ (Logosoft d.o.o.)
Microsoft Family Safety, Link:
https://account.microsoft.com/family/about (Logosoft d.o.o.)
Kaspersky servisi, Link:
https://zona.ba/kaspersky-servisi (Dasto Semtel d.o.o.)
Qustodio.com, Netnnani.com, Norton.com (Elektron Group d.o.o.)
Centar za sigurni Internet, Link:
www.sigurnodijete.ba
www.sigurnodijete.ba/helpline (Media Sky d.o.o.)
Dani sigurnog djeteta, Link:
www.dansigurnijeginterneta.org (Media Sky d.o.o.)
Mobicip, Link:
www.mobicip.com

Grafikon 2.3.18. Postotna zastupljenost ISP-ova u odnosu na njihovu percepciju o važnosti svih mehanizama i aktivnosti koje doprinose boljoj zaštiti djece na internetu, a u pogledu njihovog uspješnijeg poslovanja

Po vašem mišljenju i vašim iskustvima, da li kampanja sigurnosti/ bezbjednosti djece na Internetu realizirana u okviru vaše tvrtke, kroz razvijanje sopstvenih mehanizama roditeljske kontrole/ nadzora, promoviranje već postojećih aplikacija i alata za zaštitu djece na Internetu, objavljivanja edukativnih sadržaja o zaštiti djece na Internetu i dr., u javnosti stvara pozitivnu sliku vaše tvrtke te na taj način privlači pažnju potencijalnih korisnika vaših usluga?

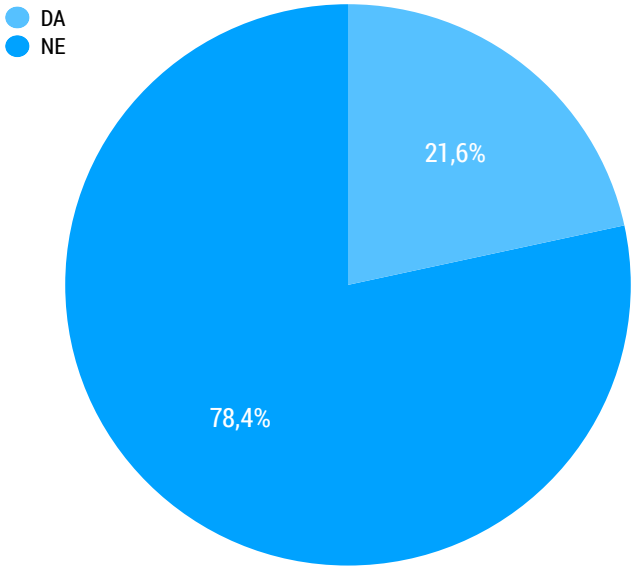


Predstavljeni rezultati pokazuju da je postotna zastupljenost ISP-ova koji navedene aktivnosti i mehanizme usmjerene na podizanje razine zaštite djece na internetu smatraju važnim u kontekstu stvaranja pozitivne slike njihove tvrtke u javnosti i u privlačenju pozornosti potencijalnih korisnika njihovih usluga veća (54,1%, tj. 20 ispitanika) u odnosu na ISP-ove koji ovu vrstu angažmana nisu prepoznali kao značajnu za uspjeh u njihovom poslovanju (45,9%, tj. 17 ispitanika).

Ispitanicima je, također, ponuđena mogućnost da na temelju svog iskustva iznesu stav u pogledu postojanja ili nepostojanja potrebe za dopunom/izmjenom regulative s ciljem efikasnijeg djelovanja u pogledu sigurnosti/bezbjednosti djece na internetu i da u tom kontekstu iznesu konkretne ideje/ prijedloge.

Grafikon 2.3.19. Postotna zastupljenost ISP-ova koji imaju/nemaju ideje/ prijedloge za dopunu/izmjenu propisa u cilju učinkovitijeg djelovanja o temi sigurnost/bezbjednost djece na internetu

Da li imate ideje/prijedloge za dopunu/izmjenu propisa, a u cilju učinkovitijeg djelovanja o temi sigurnost/bezbjednost djece na Internetu?



Uvid u grafikon pokazuje da je značajno veća postotna zastupljenost ISP-ova koji ne uočavaju potrebu za dopunom/izmjenom postojećih propisa, te da u tom smislu nemaju ideje/ prijedloge usmjerene na učinkovitije djelovanje u pogledu sigurmosti/bezbjednosti djece na internetu (78,4%, tj. 29 ispitanika). Samo osam ispitanika, tj. 21,6% od ukupnog uzorka odgovorilo je potvrdno na ovo pitanje, što je podrazumijevalo i da navedu konkretne ideje/prijedloge.[12]

[12] Ideje/prijedloge za dopunu/izmjenu propisa, a u cilju učinkovitijeg djelovanja sigurnost/bezbjednost djece na Internetu, a koje su dali pružatelji usluge pristupa Internetu su sljedeći:
Nije dovoljno zalaganje ISP, potrebna je bolja edukacija korisnika odnosno roditelja od strane šire društvene zajednice, obrazovnog sistema itd. (Blicnet d.o.o.)
Formirati stalni tim pri državnim organima. (TxTv d.o.o.)
Uvrstiti u osnovnoj školi u nastavni plan i program redovno edukaciju o sigurnosti djece na Internetu (opširnije). (Media Sky d.o.o.)
Državni organi za zaštitu svih građana pa i djece. (Elta MT d.o.o.)
Uvođenje informativnih časova u osnovnim školama. (Formea d.o.o.)
Trenutno stanje na terenu je jako komplikovano zbog tehnološke nepismenosti roditelja, zbog toga dosta ovih softverskih rješenja i mehanizama nema neku praktičnu vrijednost na terenu, jer isti ne znaju upravljati tim aplikacijama (ovaj odgovor dajem za područje na kojem mi djelujemo i radimo te je ovaj zaključak izvučen kako iz ličnog iskustva sa terena tako i iz analitike prijavljenih intervencija gdje je 65% intervencija na terenu tipa npr.: isključen Wi-Fi na telefonu itd. te zbog toga korisnici zovu da nemaju usluge, iz toga možemo zaključiti da jedina konkretna zaštita za djecu može biti paralelna kontrola te lična briga roditelja o svojoj djeci i ponašanju svoje djece na Internetu). (AMB NET d.o.o.)
Edukacija roditelja. (Integra Inženjering d.o.o.)

Ispitanicima je ostavljena mogućnost da navedu nešto što nije obuhvaćeno postavljenim pitanjima, a što smatraju važnim u kontekstu sigurnosti/bezbjednosti na internetu. Odgovore su dostavila četiri ISP-a, koji su predstavljeni u sljedećoj tablici.

Tablica 2.3.4. Prikaz prijedloga pojedinih ISP-ova u pogledu unaprjeđenja sigurnosti/bezbjednosti djece na internetu

ISP	Prijedlozi
AMB NET d.o.o.	Povećati osobnu brigu o djeci, raditi lično sa djecom te povećati realan socijalni život djece, a maksimalno smanjiti prisutnost djece na društvenim mrežama, prvenstveno zbog zdravlja djeteta (probleme sa vidom).
K Net d.o.o.	Sve je do roditelja.
Teledigital d.o.o.	Veća promocija od strane RAK-a i nalog ISP operatorima da aktivno sudjeluju u kampanjama.
Wirac net d.o.o.	Sigurnost djece na Internetu je prvenstveno uvjetovana roditeljskim nadzorom pa tek onda aplikacijama. Broj I. u borbi za sigumost djece na Internetu je u edukaciji samih roditelja. Internet ne možemo zabraniti djeci, ali ga možemo kontrolirati. Mi kao operater u svojoj ponudi nudimo savjete roditeljima prilikom spajanja novog korisnika. Na samom modemu je moguće postaviti podešavanja koja će ograničiti pristup određenim web stranicama. Naravno, sve uz pristanak i odobrenje korisnika. Roditelji obično nisu svjesni svega što se može desiti i smatramo da je edukacija ključna u borbi za sigurnost djece na Internetu.

U skladu sa ukupnim brojem dostavljenih Upitnika i postotkom udjela operatora u ukupnom broju korisnika pristupa internetu, odziv davatelja pristupa internetu je zadovoljavajući. Također, odgovori na pitanja iz Upitnika su dobar pokazatelj trenutne situacije u pogledu aktivnosti, poduzetih koraka, mogućih mjera i procedura koje pružatelji pristupa internetu imaju provedene o temi sigurnost/bezbjednost djece na Internetu.

Na temelju rezultata istraživanja sigurnosti/bezbjednosti djece na internetu iz perspektive aktivnosti koje u ovom kontekstu poduzimaju ISP-ovi u BiH može se zaključiti sljedeće:

1. ISP-ovi su u znatno većem postotku upoznati sa uputama za IKT kompanije u pogledu sigurnosti/bezbjednosti djece na internetu (28 ispitanika, tj. 75,7%).
2. Pojedini ISP-ovi su poduzeli niz aktivnosti o temi sigurnost/bezbjednost djece na internetu koje se ogledaju kroz: realizacija kampanje sigurnosti/bezbjednosti djece na Internetu, promicanje sigurnosti/bezbjednosti djece na internetu putem vlastitih *web* stranica, promicaje alata i aplikacija roditeljske kontrole/nadzora djece na internetu koje su razvile tvrtke koje se bave zaštitom i sigurnošću na internetu, te razna tehnička rješenja kao mehanizam zaštite djece na internetu.
3. ISP-ovi nisu aktivni u pogledu angažmana koji podrazumijeva njihovo članstvo u nekom domaćem i/ili međunarodnom udruzi/zajednici/stukovnoj grupi čije su aktivnosti usmjerene na sigurnost/bezbjednost djece na internetu (97,3%, tj. 36 ispitanika). U ovom smislu je aktivan samo jedan ISP (2,7%), što predstavlja značajanu prepeku u kontekstu sinkroniziranog djelovanja i postizanja značajnijih rezultata u pogledu zaštite djece na internetu.
4. Iako su pojedini ISP-ovi poduzeli niz aktivnosti usmjerenih na realizaciju kampanje sigurnosti/bezbjednosti djece na internetu, primjetno je da je njihova brojčana i postotna zastupljenost znatno manja (21,6%, tj. 8 ispitanika) u odnosu na ISP-ove koji ovu vrstu kampanja ne provode (78,4%, tj. 29 ispitanik). U ovom kontekstu je važan i podatak da kampanje sigurnosti/bezbjednosti djece na internetu uglavnom organiziraju ISP-ovi sa velikim brojem korisnika. S druge strane, više od plovine ISP-ova na svojim *web* stranicama promoviraju sigurnost/bezbjednost djece na internetu (54%, tj. 20 ispitanika). Međutim, preostali broj, tj. nešto manje od polovice ispitanika, što nije zanemarljivo,

na svojim *web* stranicama ne promoviraju sigurnost/bezbjednost djece na internetu.

5. Posebno se ističu tehnička rješenja koje su proveli ISP-ovi čiji je udio u ukupnom broju korisnika pristupa internetu preko 95%, bilo da se radi o posebnim paketima za djecu sa odgovarajućim sigurnosnim mehanizmima ili mehanizmima roditeljske kontrole/nadzora kao što su popisi za blokiranje, filtriranje sadržaja, nadzor upotrebe, vremenska ograničenja upotrebe i dr. Pojedini ISP-ovi razvili su softvere i alate koji omogućuju roditeljsku kontrolu/nadzor, odnosno koji omogućuju roditeljima upravljanje pristupom Interneta djeci. Kao jedno od tehničkih rješenja roditeljske kontrole/nadzora pristupa internetu, ISP-ovi realizirali su kroz rutere/modeme koje imaju u svojoj ponudi, a koji omogućuju funkciju roditeljske kontrole/nadzora. To u praksi znači da pravilnom konfiguracijom postavki na ruteru roditelji mogu filtrirati sadržaj, postavljati liste za blokiranje/dozvolu pristupa, nadzirati upotrebu, vremenski ograničiti pristup Internetu i dr., na svim uređajima koji su povezani sa ruterom.

6. Iako su pitanje zaštite djece na internetu u najvećem broju procijenili kao veoma značajno, ISP-ovi uglavnom nemaju posebnu organizacijsku jedinicu ili osobu koja je isključivo zadužena za sajber sigurnost (73%, tj. 27 ispitanika). Dok je broj ISP-ova koji raspolažu ovim organizacionim kapacitetima ili ljudskim resursima značajno manji (27%, tj. 10 ispitanika).

7. Iz perspektive ISP-ova razvoj sajber sigurnosti uvelike je određen unutarnjim čimbenikom, tj. politikom/strategijom tvrtke (35,1%, tj. 13 ispitanika), a potom zahtjevima/potražnjom korisnika (32,4%, tj. 12 ispitanika). U nešto manjem, ali i dalje znatnom postotku, ispitanici su identifkovali regulaciju (29,7%, tj. 11 ispitanika) i tržišne uvjete (21,6%, tj. 8 ispitanika), kao vanjske čimbenike koji prvenstveno određuju razvoj sajber sigurnosti u njihovoj tvrtki.

8. Ispitanici su apostrofirali to da je za svaki od mehanizama zaštite djece na internetu potreban puni angažman roditelja. Kao najučinkovitiji mehanizam roditeljske kontrole za zaštitu djece na internetu ISP-ovi vide mehanizam nadzora uporabe (81,1 %). Kao usluge preko kojih djeca najlakše mogu biti ugrožena na internetu ISP-ovi vide društvene mreže (*Facebook, Instagram, TikTok*...) (89,2%). Mehanizam roditeljskog nadzora za zaštitu djece na internetu u ovom slučaju je nadzor uporabe, što također zahtjeva puni angažman roditelja.

Da bi roditelji mogli u punom kapacitetu koristiti mehanizme tehničkih rješenja za zaštitu djece na Internetu koje su proveli pružatelji pristupa internetu, potrebna je određena razina digitalne pismenosti roditelja. Roditelji prije svega trebaju da znaju za tehničke mogućnosti mehanizama zaštite djece na internetu, da bi na osnovu toga mogli od davatelja pristupa Internetu zatražiti neki od mehanizama zaštite djece na internetu koje pružatelj usluge pristupa Internetu ima u svojoj ponudi.

Navedeno se može postići medijskim kampanjama koje se odnose na podizanje svijesti kod roditelja za sigurnost/bezbjednost djece na internetu, edukacijom djece i roditelja o temi sigurnost/bezbjednost djece na internetu i većom promocijom provedenih tehničkih rješenja mehanizama zaštite djece na internetu od strane pojedinih davatelja- pristupa Internetu.

PREGLED MEĐUNARODNIH PRAVNIH INSTRUMENATA RELEVANTNIH ZA BIH U PODRUČJU ZAŠTITE MALOLJETNIKA NA INTERNETU

Izražena i veoma dinamična penetracija interneta i novih medija, hiperprodukcija sadržaja diseminovanih posredstvom interent platformi, značajno je utjecala na intenzivniju potrebu širenja tradicionalne regulacije u području medija, komunikacija i informacija, u smislu njene nadogradnje i modernizacije. Angažman usmjeren u ovom pravcu naročito je uočljiv na međunarodnoj razini, koji i predstavlja početni okvir za promjene na razinama pojedinačnih država. Naime, polazeći od toga da su međunarodni instrumenti pravno obavezujući, odgovorne nacionalne politike podrazumijevaju angažman usmjeren na prilagodbu nacionalne regulative standardima sadržanim u dokumentima međunarodnog pravnog sustava.

Počevši od važnosti međunarodnog pravnog okvira, tj. dokumenata koji ga čine, u ovom poglavlju predstavit će sažetak međunarodnih pravnih instrumenta relevantnih za BiH u području zaštite djece na internetu. Ovdje će biti elaborirani neki od najvažnijih dokumenta čiji je cilj zaštita djece, njihovih temeljnih prava i sloboda, u novom digitalnom okruženju, tj. pravno obavezujući međunarodni instrumenti koji su jednim dijelom ili u cjelosti u izravnoj korelaciji sa predmetom ove analize, tj. sa zaštitom djece na internetu.

Referenca međunarodnih dokumenata za zaštitu prava djeteta

Zaštita prava djeteta predstavlja mnogo širu kategoriju u odnosu na njegovu zaštitu u onlajn sferi. S druge strane, za tumačenje zaštite prava, sloboda i interesa djeteta u digitalnom svijetu, koji je duboko inkorporian u njegov stvarni život, potrebno je poći od sveobuhvatnih standarda za zaštitu prava djece, bez diskriminacije. Paralelno postojanje stvarnog i virtuelnog okruženja djeteta, podrazumijeva koegzistenciju normativa i koregulaciju mehanizama, koji će oba svijeta učiniti bezbjednijim i pogodnijim za ostvarivanje i zaštitu njegovih prava, umanjujući mogućnosti za zlouporabu, diskriminaciju, narušavanje privatnosti, koji ugrožavaju društvenu, moralnu i duhovnu dobrobit svakog djeteta. U ovom kontekstu kao međunarodno relevantni dokumenti neizbježni su Konvencija UN-a o pravima djeteta i Europska konvencija za zaštitu ljudskih prava i osnovnih sloboda.

Konvencija UN-a o pravima djeteta

Konvencija UN-a o pravima djeteta jedan je od referentnih dokumenata u međunarodnom pravnom sustavu koji izričito normira zaštitu prava djeteta. Važnost Konvencije proizilazi i iz činjenice da je ovaj dokument prvi pravno obavezujući međunarodni instrument i da sadrži sveobuhvatne standarde za zaštitu prava djece i da se primjenjuje na svu djecu, bez diskriminacije. „Konvencija naglašava činjenicu da su djeca (definirana Konvencijom kao svi mlađi od 18 godina) ranjiva skupina u društvu, kojoj je potrebna posebna skrb i zaštita, te stoga obavezuje sve strane da osiguraju zaštitu i skrb o djeci koja je potrebna za njihovu dobrobit, kroz odgovarajuće zakonodavne i administrativne mjere."

Konvencija kao sveobuhvatan insturment različitih prava, između ostalog, regulira i sferu masovnih medija, kao platformu pogodnu za slobodu izražavanja, prava na informacije, za promoviranje interesa djeteta posredstvom kvalitativno vrijednih sadržaja koji doprinose njihovom razvoju i sl, pri čemu se naglašava potreba za zaštitom djece od materijala koji mogu ugroziti njihovu dobrobit. U kontekstu predmetne analize i u segmentu koji se odnosi na zaštitu privatnosti djece općenito, pa tako i na internetu, kao jednog od najvećih izazova digitalnog doba, a to su narušavanje privatnosti i zlouporaba osobnih podataka, značajan je članak 16 (prvi i drugi stavak) Konvencije, a koji glasi:

„Nijedno dijete ne smije biti izloženo proizvoljnom ili nezakonitom uplitanju u njegovu privatnost, obitelj, dom ili prepisku, niti nezakonitim napadima na njegovu čast i ugled." Također, važan je i drugi stavavak ovog članka, u kojem se navodi da dijete ima pravo na pravnu zaštitu od takvog uplitanja, što je vrlo važno i u kontekstu narušavanja njegove privatnosti na internetu.

Na važnost medija i njihovog podticanja u plasiranju vrijednih sadržaja koji doprinose razvoju djeteta, ukazuje članak 17 . Ovaj

članak "prepoznaje važnu funkciju medija u širenju informacija koje pozitivno utječu na djecu i jamči im pristup informacijama i materijalima od različitih nacionalnih i međunarodnih izvora, posebno onih usmjerenih na promociju njihove društvene, duhovne i moralne dobrobiti i fizičkog i mentalnog zdravlja". Odredbe članka 17 su značajne i u kontekstu zaštite djece na internetu, obzirom na izraženu tendenciju prenošenja tradicionalnih medijskih formata u moderne onlajn formate i podatke koji ukazuju na to da se mladi, pored drugih aktivnosti, uglavnom informiraju posredstvom internetskih medija. U ovom smislu je važna i odredba članka 17 koja ukazuje na nužnost podticanja razvoja i primjene odgovarajućih uputa za zaštitu djece od obavijesti i materijala koji štete njegovom razvoju.

Naime, djeca su potencijalno štetnim sadržajima u najvećoj mjeri izložena posredstvom interneta, tj. raznih aplikacija, društvenih mreža, sajtova, medija, kao njihovi dominantni korisnici. Stoga je nephodno uspostaviti mehanizme koji će s jedne strane suzbiti zlouporabu njihovih osobnih podataka i njihovu izloženost nasilnom i štetnom sadržaju, a da pritom, s druge strane, ne bude ugroženo njihovo pravo na slobodu izražavanja, sudjelovanja i informiranja, koji pripadaju kategoriji ljudskih prava i osnovnih sloboda.

Počevši od važnosti digitalnog okruženja za djecu na 86. sastanku Komiteta za prava djeteta usvojen je Opći komentar br. 25 (2021) o pravima djeteta u vezi sa digitalnim okruženjem. Komentar br. 25 pojašnjava važnost digitalnog okruženja u kontekstu ostvarivanja i zaštite dječijih građanskih prava i sloboda, uključujući pravo na privatnost, nediskriminaciju, zaštitu, obrazovanje, igru i dr. Također, potvrđuje odgovornost države kao primarnog nositelja dužnosti u osiguravanju poštovanja odredbi UN-ove Konvencije o pravima djeteta, uključujući postupak povremenog izvješća Komiteta o tome kako su obveze ispunjene. Države su dužne osigurati da svi subjekti čije aktivnosti utječu na djecu iz njihove nadležnosti ispunjavaju svoje odgovornosti u vezi s dječjim pravima. Kao opće mjere primjene Država ugovornica navedene su sljedeće:

- zakonodavstvo;
- sveobuhvatna politika i strategija;
- koordinacija;
- raspodjela resursa;
- prikupljanje podatka, njihovo redovito ažuriranje i kontinuirana istraživanja;
- neovisni nadzor;
- informiranje, podizanje svijesti i osposobljavanje;
- suradnja sa civilnim društvom i dr.

U odjeljku koji obuhvaća građanska prava i slobode, a time i pristup informacijama, navedeno je da bi države ugovornice trebale poticati pružatelje digitalnih usluga koje djeca koriste za primjenu sažetog i razumljivog označavanja sadržaja, npr. o primjerenosti za određenoj dobi ili vjerodostojnosti sadržaja, te da potiču obezbjeđivanje dostupnih uputa, obuka, obrazovnih materijala i mehanizama izvješća, za djecu, roditelje i njegovatelje, odgajatelje i relevantne stručne skupine. Također, Općim komentarom br. 25 se nalaže da države ugovornice trebaju osigurati da se pružatelji digitalnih usluga pridržavaju referncinih uputa, standarda i kodeksa i provode zakonita, potrebna i proporcionalna pravila moderiranju sadržaja. Naglašava se da kontrole sadržaja, sustavi za filtriranje i druge tehnologije orijentirane na sigurnost ne bi trebalo da se koriste za ograničavanje pristupa djece informacijama u digitalnom okruženju, već da ih treba koristiti isključivo za sprječavanje priliva materijala štetnog za djecu. Moderiranje sadržaja i kontrole sadržaja treba da budu uravnoteženi sa pravom na zaštitu od kršenja drugih prava djece, posebno njihovih prava na slobodu izražavanja i privatnost.

Ovim dokumentom se također potvrđuje važnost međunarodne i regionalne suradnje sukladno prirodi digitalnog okruženja u cilju obezbjeđenja da sve zainteresirane strane, uključujući države, poduzeća i druge dionike, učinkovito poštuju, štite i ispunjavaju prava djeteta u odnosu na digitalno okruženje. Navedeno je i da je od ključne važnosti da države ugovornice surađuju bilateralno i multilateralno sa nacionalnim i međunarodnim nevladinim organizacijama, agencijama Ujedinjenih nacija, poduzećima i organizacijama specijaliziranim za zaštitu djece i ljudska prava u vezi sa digitalnim okruženjem. Ističe se i važnost proširenja ovog dokumenta u smislu da države ugovornice treba osigurati da se ovaj opći komentar što je više moguće

širi, što uključuje i upotrebu digitalnih tehnologija, do svih referncnih zainteresiranih strana, posebno parlamenata i državnih tijela, uključujući one odgovorne za međusektorsku i sektorsku digitalnu transformaciju, kao i do pripadnika pravosuđa, poslovnih poduzeća, medija, civilnog društva i šire javnosti, prosvjetnih radnika i djece, i da bude dostupan u više formata i na više jezika, uključujući i verzije prilagođene dobi.

Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda

Nakon usvajanja i stupanja na snagu Univerzalne deklaracije o ljudskim pravima uslijedilo je donošenje Europske konvencije za zaštitu ljudskih prava i osnovnih sloboda na razini Vijeća Europe 1953. godine. U kontekstu predmeta analize, značaj ovog dokumenta ogleda se u ćinjenici da ova Konvencija pravo na slobodu izražavanja normira kao pravo koje nije apsolutno, jer njegovo ostvarivanje podrazumijeva i određene dužnosti i odgovornosti. Ovakav pristup nije u suprotnosti sa osnovim demokratskim načelima, već naprotiv onemogućava zlouporabu prava na slobodu izražavanja. U tom smislu primaran je članak 10 Konvencije. Prvi stavak ovog članka pokazuje da „svako ima pravo na slobodu izražavanja. Ovo pravo uključuje slobodu mišljenja i slobodu primanja i prenošenja informacija i ideja, bez uplitanja javnih ovlasti i bez obzira na granice. Ovaj članak ne sprječava države da traže radne dozvole od radio, televizijskih i filmskih kompanija". Istovremeno u drugom stavku članka 10 Konvencije je jasno navedeno da ostvarivanje ovih sloboda uključuje i obveze i odgovornosti i u tom smislu mogu podlijegati formalnostima, uvjetima, ograničenjima ili sankcijama predviđenim zakonom. Formulacija drugog stavka može se tumačiti na način da sloboda izražavanja nije apsolutno pravo u slučajevima ili situacijima u kojima ostvarivanje ovog prava podrazumijeva ugrožavanje nekih viših interesa.

Gledano iz perspektive predmentne analize, tj. zaštite djece na internetu, a u odnosu na sadržaj navedenog članka, može se zaključiti da internet ne bi trebalo posmatrati kao platformu na kojoj je sloboda izražavanja neograničena, pa čak i u situacijima u kojima se narušava integritet djeteta, njegova sigurnost, privatnost i sl, jer je interes djeteta daleko važniji od interesa pojedinaca, tj. ostvarivanja njihovog prava na slobodu izražavanja koje pritom ima dalekosežne i negativne učinke na razvoj djeteta.

Kao i brojnim drugim međunarodnim instrumentima i ovom Konvencijom normirano je pravo na privatnost (članak 8 – Pravo na poštovanje privatnog i obiteljskog života). Ova odredba je, također, važna za zaštitu prava djece, naročito u kontekstu interneta, kao sfere u kojoj je narušavanje privatnosti jedan od najizraženijih i najproblematičnijih izazova. U prvom stavku ovog članka je navedeno da svako ima pravo na poštovanje svog privatnog života, doma i prepiske, dok drugi stavak podrazumijeva zaštitne mjere, tj. miješanje javnih vlasti u ostvarivanje ovog prava „ako je takvo miješanje predviđeno zakonom i ako je to neophodna mjera u demokratskom društvu u interesu nacionalne sigurnosti, javne sigurnosti, ekonomske dobrobiti zemlje, sprječavanja nereda ili sprječavanja zločina, zaštite zdravlja i morala ili zaštite prava i sloboda drugih".

Referenca međunarodnih dokumenata za zaštitu privatnosti na internetu

Sve ono što određuje identitet, kako odraslih, tako i djece (izgled, interesi, prijatelji, način na koji se provodi slobodno vrijeme) često se dijeli putem interneta.[13] Internet bilježi te informacije, aplikacije i uređaji koji se upotrebljavaju automatski prikupljaju podatke o njihovim korisnicima, tako da znaju koji uređaj koriste, gdje se nalaze, šta gledaju i traže, tj. koja su njihova interesovanja[14]. Kako tehnologija postaje sofisticiranija, umrežena i komercijalno održiva, privatnost na internetu sve je više ugrožena novim oblicima prikupljanja podataka, čemu su posebno izloženi djeca i mladi. U suvremenom digitalnom okruženju, sve aktivnosti na internetu bilježe se i pretvaraju u podatke koji se mogu snimati, pratiti, spajati, analizirati, unovčiti, a trajni su, pretraživi i, praktički, neizbrisivi[15].

Osnova različitih oblika zlouporabe interneta jeste kršenje prava na privatnost, a pravo na privatnost, bilo da se radi o onlajn ili oflajn sferi, jedno je od osnovnih ljudskih prava. Prema Helen Nissenbaum, privatnost nije pravo na tajnost i kontrolu, već pravo na pravilan protok osobnih podataka. Autorka privatnost tumači kao kontekstualni integritet[16], što podrazumijeva da pojedinac, ovisno od situacije i konetksta, ima mogućnost osobno procijeniti što i sa kim podijeliti u digitalnoj sferi. Ovakav pristup određenju pojma privatnosti podrazumijeva da svaka osoba „ima pravo da zna kako i u koje svrhe se koriste njeni podaci, ko ih čuva i koliko dugo, ko sve njima raspolaže, kao i da može zatražiti brisanje osobnih podatka ili korekciju netočnih podataka"[17].

Na složenost koncepta privatnosti ukazuje određenje ovog pojma u pravnoj teoriji, prema kojem privatnost osobe obuhvaća intimnu sferu, privatnu sferu i privatno-javnu sferu.[18] Određenje druge sfere ukazuje na prožimanje pojma privatnosti i ličnih podataka, ali istovremeno i na to da ih nije moguće pojednostavljeno izjednačiti, jer „nije svako uživanje, odnosno povreda prava na privatnost u direktnoj vezi sa zaštitom osobnih podataka, kao što ni zaštita osobnih podataka ne povlači uvijek pitanje prava na privatnost kao ljudskog prava"[19]. Podaci iz ove sfere ne mogu se dijeliti sa trećim stranama bez posebnog odobrenja onoga o čijoj se privatnosti radi. Ovo su podaci koji se svrstavaju u zasebnu kategoriju i nazivaju se osobnim podacima. Upravo je ova sfera privatnosti u fokusu istraživanja u ovom radu, tj. privatna sfera kojom su obuhvaćeni osobni podaci. U odnosu na klasifikaciju privatnosti osobe na prostornu, informacijsku i komunikacijsku privatnost, a u kontekstu zaštite privatnosti na internetu, posebno su važne informacijska i komunikacijska privatnost.[20] Komunikacijska privatnost shodno promjenama same prirode komunikacije, koja je u značajnoj mjeri tehnološki posredovana i određena, prerasta u "e-privatnost"[21]. Pojavom novih rizika u kontekstu prava na poštovanje privatnog života, a kao odgovor na potrebu za posebnim propisima koji reguliraju prikupljanje i korištenje osobnih podataka u informacijskom društvu, u pravne susatve pojedinih država uvedeni su novi koncepti privatnosti pod nazivom „informacijska privatnost" i „pravo na informacijsko samoodređenje"[22].

---

[13] Ovaj dio analize u kojem se pojašnjava značaj zaštite privatnosti na internetu uopće, podrazumijevajući i zaštitu privatnosti djece na internetu, u cjelosti je preuzet je iz rada pod nazivom "Privacy On The Internet Concerning Generation Z In Bosnia And Herzegovina" autorki prof. dr Dragane Trninić i doc. dr Anđele Kuprešanin Vukelić, koji je objavljen u naučnom časopisu „Media Literacy and Academic Research", 2021, str. 180-184.

[14] STOILOVA, M., LIVINGSTONE, S., NANDAGIRI, R.: Children's data and privacy online: Growing up in a digital age. Research findings. London: London School of Economics and Political Science, 2019. [online].

[15] STOILOVA, M., LIVINGSTONE, S., NANDAGIRI, R.: Ibid. p. 4.

[16] NISSENBAUM, H.: Privacy as contextual integrity. In *Washington Law Review*, 2004, Vol. 79, No. 1, p. 120. [online]. [2021-02-15]. Available at: https://core.ac.uk/download/pdf/267979739.pdf.

[17] KUZMANOVIĆ, D.: Zaštita ličnih podataka i privatnosti na internetu. [online]. [2021-02-13]. Available at: https://digitalni-vodic.ucpd.rs/zastita-licnih-podataka-i-privatnosti-na-internetu/#t3_subheading-2.

[18] BOBAN, M.: Pravo na privatnost i pravo na pristup informacijama u suvremenom informacionom društvu. In Zbornik radova Pravnog fakulteta u Splitu, 2012, Vol. 49, No. 3, p.584. [online]. [2021-01-14]. Available at: https://hrcak.srce.hr/86834.

[19] MURTEZIĆ, A. O.: Konvencija 108: aktuelni značaj i primjena. In MRVIĆ PETROVIĆ, N. (ed.): Strani pravni život. Beograd: Institut za uporedno pravo, 2020, 99-110. [online]. [2021-01-29]. Available at: https://www.stranipravnizivot.rs/index.php/SPZ/issue/view/44.

[20] BOBAN, M.: Ibid. p. 585-586.

[21] E-privatnost „predstavlja koncept zaštite podataka vezan uz komunikaciju putem elektroničkih mreža u bilo kojem obliku", BOBAN, M.: Ibid., p. 587.

[22] *Priručnik o evropskom zakonodavstvu o zaštiti podataka. Izdanje iz 2018.* [online]. [2021-01-04]. Available at: https://fra.europa.eu/hr/publication/2020/prirucnik-o-europskom-zakonodavstvu-o-zastiti-podataka-izdanje-iz-2018.

Internetska sigurnost znatno je određena razinom zaštite osobnih podataka.[23] „Naime, postojeće tehnologije omogućile su da se vrlo jednostavno i gotovo besplatno prikupljaju osobni podaci i nadziru online aktivnosti korisnika, što je plodno tlo za njihovu zlouporabu"[24]. Zaštita osobnih podataka sa širnjem i popularizacijom društvenih mreža i različitih aplikacija na internetu dobija nove dimenzije. "Na društvenim mrežama i ostalim internetskim stranicama prikupljaju se i pohranjuju velike količine osobnih podataka, bilo da su te informacije objavljene s namjerom dijeljenja ili su ih izradile same web-lokacije društvenih medija"[25]. Visoka razina prodora društvenih medija, kontinuirano usavršavanje internetskih aplikacija koje ne zahtijevaju veliku uključenost njihovih korisnika, lakši pristup posredstvom različitih uređaja, pruženje brojnih mogućnosti u kontekstu zadovoljavanja različitih potreba, značajno su doprinijeli isticanju pohrane, dijeljenja, zaštite i zlouporabe osobnih podataka u digitalnom formatu. U ovom smislu naročito su značajni podaci koje korisnici interneta ostavljaju u vidu *digitalnog otiska* i *digitalne tetovaže*, a koji doprinose stvaranju *digitalnog identiteta*.

"Digitalni identitet čine „digitalni otisci", tragovi koje za sobom ostavlja korisnik interneta, bilo svjesno ili nesvjesno, aktivno ili pasivno, dok pretražuje, šalje poruke, a najviše korištenjem društvenih mreža i putem povezanih uređaja."[26] Upotrebom sintagme digitalna tetovaža pojedini autori nastoje ukazati na trajnost podataka koje korisnici interneta ostavljaju prilikom njegove uporabe, tj. na njihovu postojanost u digitalnom svijetu.[27] U kontekstu kreiranja digitalnog identiteta, kao i oblikovanja digitalne tetoveže, značajna je podjela digitalnih otisaka na aktivne i pasivne. Kategorija aktivinih digitalnih otisaka pripadaju aktivnosti na internetu usmjerene prema izradi informacija o sebi, dijeljenje osobnih podataka, otvaranje profila na društvenim mrežama, postavljanje komentara na blogovima i društvenim mrežama, dok pasivne otiske korisnici interneta ostavljaju najčešće nenamjerno, poput nesvjesnog ostavljanja IP adrese prilikom pristupa nekoj *web* stranici.[28] Naime, korisnici interneta osim aktivnog participiranja u digitalnoj sferi, koje gotovo nužno podrazumijeva pohranu nekog podatka o njemu, i djelovanjem koje se ne smatra aktivnim učestvovanjem u nekoj korisničkoj radnji na interentu, značajno doprinose nadopunjavanju njihovog digitalnog identiteta.[29]

S obzirom na potencijal interneta u kontekstu pohrane, korištenja i zlouporabe osobnih podataka, kojih njegovi korisnici često nisu svjesni, vrlo je važno korištenje mehanizama i postavki koje doprinose zaštiti osobnih podataka i privatnosti na internetu. Pojedini mehanizmi i postavke privatnosti također predstavlju resurse koji su stavljeni na raspolaganje korisnicima interneta. Neke od aktivnosti čija realizacija svakom korisniku interenta može omogućiti veću razinu sigurnosti i zaštite njegove privatnosti su: odjava sa svih naloga prije pregladanja sadržaja na internetu, instaliranje antivirusnih programa na uređajima za pristup internetu, korištenje programa za skrivanje IP adrese, isključivanje lokacije na mobilnom uređaju, izbjegavanje unošenja os-

---

[23] Pod ličnim podacima podrazumijevaju se podaci ili informacije koje se odnose na ličnost i na osnovu kojih se može utvrditi identitet ličnosti. U ovom smislu razlikuju se identifikacioni podaci i posebni podaci. U identifikacione podatke spadaju: ime i prezime, adresa stanovanja, datum rođenja i jedinstveni matični broj. Kategoriji posebnih podatka pripadaju podaci o: rasnom porijeklu, državljanstvu, nacionalnom ili etničkom porijeklu, političkom mišljenju ili stranačkoj pripadnosti, članstvu u sindikatima, religijskom, filozofskom ili drugom uvjerenju, zdravstvenom stanju, genetskom kodu, seksualnom životu; krivičnim presudama; biometrijskim podacima (npr. otisci prstiju). Agencija za zaštitu ličnih podataka u Bosni i Hercegovini. [online]. [2021-01-18]. Available at: http://azlp.ba/FAQ/Default.aspx?id=281&langTag=bs-BA&template_id=149&pageIndex=1

[24] BRAUTOVIĆ, M.: Zaštita privatnosti kod hrvatskih onlajn medija. In *MediAnali: međunarodni znanstveni časopis za pitanja medija, novinarstva, masovnog komuniciranja i odnosa s javnostima*, 2007, Vol. 1, No. 1, p. 28. [online]. [2021-02-01]. Available at: https://hrcak.srce.hr/41342.

[25] MCPEAK, A.: The facebook digital footprint: Paving fair and consistent pathways to Civil discovery of social media data. In *48 Wake Forest L. Rev. 887*, 2013, Vol. 48, p. 103. [online]. [2021-02-10]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2246990##.

[26] *Medijska i informacijska pismenost; Radni listići za aktivnosti u učionici za nastavnike*. [online]. [2021-01-11]. Available at:https://www.medijskapismenost.hr/wp-content/uploads/2020/12/clemi-materijali.pdf.

[27] Distinkciju između digitalnog otiska i digitalne tetovaže Araoz pojašnjava izdvajajući njihove karakteristike. Kao neke od ključnih obilježja za digitalne otiske autor navodi da su privremeni, pasivno stvoreni, reaktivni, te da mogu biti nenamjerni i nekontrolisani. Za digitalne tetovaže Araoz ističe da su trajne, aktivno stvorene, proaktivne i da se mogu kontrolisati. ARAOZ, L.: Your Online Presence is a digital Tatoo, Not a Footprint. The golden age of education: Highly effective tools and strategies for educators. [online]. [2021-02-03]. Available at: https://thegoldenageofeducation.com/2016/03/12/your-online-behavior-is-a-digital-tattoo-not-a-footprint/.

[28] SETYOWATI, L.: Digital life, digital tattoo and the filter bubble: raising the awareness and the cautions on online activities through information literacy education. In: MURSYID, M. (ed.): *International Conference on Science Mapping and the Development of Science*.Republik Indonesia:Library and Information Management Graduate School, Gadjah Mada University, 137-142. [online]. [Date of access, 2021-02-7]. Available at: https://scholar.google.co.id/citations?user=T1LkTxIAAAAJ&hl=en.

[29] See: BUCHI, M., LUTZ, C. MICHELI, M. *Life Online: The Digital Footprint Gap*. Position Paper for the Partnership for Progress on the Digital Divide 2017 International Conference, 24–26 May 2017, San Diego, California, USA, p. 2. [online]. [2021-01-22]. Available at:https://www.researchgate.net/publication/319943869_Life_Online_The_Digital_Footprint_Gap.

obnih podataka kada god je to moguće, provjera postavki prilikom preuzimanja aplikacija, preuzimanje datoteka isključivo iz pouzdanih izvora i dr.[30]

Međutim, osim korištenja mehanizama zaštite privatnosti koji su dostupni korisnicima interneta, potrebno je ozbiljno angažovanje davatelja pristupa interentu kako bi se zaštitila privatnosti svih korisnika, a posebno djece kao najosjetljive populacije. Prema Uputama za IKT tvrtke u pogledu sigurnosti djece na internetu (2020) IKT tvrtke bi trebale posvetiti posebnu pozornost djeci i mladima kao ranjivoj grupi u pogledu zaštite njihovih podataka i osiguravnja slobode izražavanja. U tom smislu kao referncne navedene su dvije Rezuolucije: Rezolucija Generalne skupštine Ujedinjenih nacija 68/167 o pravu na privatnost u digitalno doba, koja potvrđuje pravo na privatnost i slobodu izražavanja bez izlaganja nezakonitom uplitanju i Rezolucija 32/13 Vijeća UN-a za ljudska prava o promociji, zaštiti i uživanju ljudskih prava na internetu, koja prepoznaje globalnu i otvorenu prirodu interneta kao pokretačke snage u ubrzavanju napretka prema razvoju i potvrđuje da ista prava koja ljudi imaju izvan interneta također moraju biti zaštićena na internetu. Upute, također sugeriraju da "u državama u kojima nedostaje odgovarajući pravni okvir za zaštitu prava djece i mladih na privatnost i slobodu izražavanja, IKT tvrtke bi trebalo da prate pojačanu dubinsku analizu kako bi osigurale da su politike i prakse sukladne međunarodnom pravu. (...) IKT tvrtke imaju veću odgovornost za poštovanje prava djece i mladih, čak i tamo gdje domaći zakoni još nisu sustigli međunarodne standarde".[31]

Konvencija o sajber kriminalu

Konvencija o sajber kriminalu još je jedan od rezultata angažmana Vijeća Europe usmjerenog na zaštitu korisnika interneta, uključujući i djecu. Konvencija „uspostavlja zajednički pristup inkriminaciji kaznenih djela povezanih sa računalnim sustavima i ima za cilj da kaznene istrage u vezi s takvim kaznanim djelima budu učinkovitije. Prema ovoj konvenciji, svako ponašanje koje se odnosi na dječiju pornografiju mora se odrediti kao kazneno djelo".[32]

Osim kategorizacije dječije pornografije kao kaznenog djela, Konvencijom su kao kaznena djela utvrđena i sljedeća: neovlašteni pristup, nezakonito presretanje, ometanje podataka, ometanje rada sustava, zlouporaba uređaja, računalno krivotvorenje, računalna prijevara i djela u vezi kršenja autorskih i srodnih prava. Prvih pet pripada kategoriji *Kaznena djela protiv tajnosti, cjelovitosti i dostupnosti računalnih podataka i sustava*, računalno krivotvorenje i računalna prijevara pripadaju kategoriji *Računalna kaznena djela*, istoimenoj kategoriji pripadaju djela u vezi kršenja autorskih i srodnih prava, dok djela koja se odnose na dječju pornografiju pripadaju kategoriji *Djela u vezi sa sadržajem*.

Prema članku 9 Konvencije izraz „dječja pornografija" obuhvata pornografski materijal koji vizuelno prikazuje:

1. maloljetnika koji sudjeluje u seksualno eksplicitnom ponašanju;
2. osobu koja izgleda kao maloljetnik koji sudjeluje u seksualno eksplicitnom ponašanju;
3. stvarne slike koje prikazuju maloljetnika koji sudjeluje u seksualno eksplicitnom ponašanju.

Ovim člankom se, također, obavezuje svaka strana da će usvojiti zakonske i druge mjere potrebne kako bi se u njenom domaćem pravu kazneno sankcionirao namjerni čin bespravne:

4. proizvodnje dječje pornografije u svrhu njene distribucije putem računalnog sustava;
5. nuđenja ili stavljanja na raspolaganje dječje pornografije putem računalnog sustava;
6. distribucije ili prijenosa dječje pornografije putem računalnog sustava;
7. pribavljanja za sebe ili drugog dječje pornografije putem računalnog sustava;
8. posjedovanja dječje pornografije u računalnom sustavu ili na mediju za pohranu računalnih podataka.

---

[30] STOILOVA, M., LIVINGSTONE, S., NANDAGIRI, R.: My data and privacy online: A toolkit for young people. [online].
[31] Smjernice za IKT kompanije u pogledu bezbjednosti djece na internetu, 2020, str. 16
[32] Regionalna publikacija "Regulatorne agencije za medije i zaštita maloljetnih osoba", 2019, str. 8.

Konvencija o računalnom kriminalu normira i obvezu davatečka usluga da u suradnji sa ovlaštenim nadležnim organima, a u okviru postojećih tehničkih mogućnosti, prikupi ili snimi tražene podatke i da surađuje i pomaže nadležnim tijelima da prikupe i snime podatke o prometu u stvarnom vremenu, u vezi s određenim komunikacijama na svojoj teritoriji prenesenim pomoću računalnog sustava (članak 20 – Prikuplajnje podataka o prometu u stvarnom vremenu).

Kako bi se na odgovarajući način odgovorilo na suvremene izazove u sferi računalnog kriminala Vijeće Europe je pristupilo izradi i usvajanju Drugog dodatnog protokola Konvencije o kibernetičkom kriminalu. Usvajanje ovog Protokola je usmjereno na suzbijanje zlouporabe računalnih tehnologija, unaprjeđenje učinkovitosti rada pravosudnih tijela u pogledu kaznenih djela iz ove oblasti, kao i njihove međunarodne suradnje, i na postizanje uspješnije prekogranične suradnje između policije i ISP-ova po pitanju borbe protiv *cyber* kriminala, uključujući i zlostavljanje djece na internetu. Prepoznajući značaj ovog dokumenta Ministarstvo sigurnosti BiH je pokrenulo proces potpisivanja Drugog dodatnog protokola od strane BiH.

Konvencija za zaštitu pojedinaca u vezi sa automatskom obradom osobnih podataka (Konvencija 108)/ Konvencija 108+ (Modernizirana konvencija)

Zaštita privatnosti i osobnih podataka normirana je međunarodnim pravnim propisima, kao i propisima donesenim na razini država. Bosna i Hercegovina sukladno njenom uređenju normativno je uokvirena pozitivnim pravnim propisima na nacionalno-državnoj, entiteskoj i internacionalnoj razini, kroz norme međunarodnog prava koje su i formalno sastavni dio nacionalnog pravnog susatava. Normiranje prava na zaštitu privatnosti i osobnih podataka u Bosni i Hercegovini potrebno je analizirati sveobuhvatno, tj. analizom ustava i zakona donesenih na nacionalnoj razini i entitetskim razinama, kao i međunarodnih propisa koje je Bosna i Hercegovina, kao članica Vijeća Europe, ratificirala, a kojima je regulirana ova prva.

Kao jedno od temeljnih ljudskih prava, pravo na privatnost zaštićeno je prvenstveno međunarodnim aktima, *Općom deklaracijom o ljudskim pravima* i *Europskom konvencijom za zaštitu ljudskih prava i osnovnih sloboda*. Prvi obavezujući akt, donesen na međunarodnoj razini, koji je važan u kontekstu zaštite osobnih podatka je *Konvencija za zaštitu pojedinaca u vezi sa automatskom obradom ličnih podataka* (*Konvencija 108*). Konvencija je jedinstvena u odnosu na druge međunarodne dokumente, jer je specijalizirana i isključivo se odnosi na zaštitu podataka, po svom članstvu potencijalno je globalna i predviđa izvršni mehanizam. Konvencija 108 je izmijenjena, dopunjena i modernizirana usvajanjem Protokola o izmjenama i dopunama Konvencije (ETC 223) 2018. godine. Konsolidirani tekst Konvencije koji uključuje ovaj protokol naziva se *Konvencija 108+* ili Modernizirana konvencija. Iako se osnovna načela na kojima se temelji Konvencija nisu značajno promijenili, dokument je značajno revidiran u konetsktu konkretizacije općih odredbi i prilagođavanja novim društvenim okolnostima važnim za zaštitu osobnih podataka. Bosna i Hercegovina potpisala je Konvenciju 108+ u srpnju 2020. godine.

General Data Protection Regulation (GDPR)

Osim Konvencije 108+, u kontekstu zaštite osobnih podataka značajan je dokument pod nazivom General Data Protection Regulation (GDPR) koji je Europski parlament usvojio 2016. godine, a primjenjuje se od 25. lipnja 2018. godine. Stupanjem na snagu nove uredbe stavljena je van snage Direktiva 95/46/EC. Usvajanjem i primjenom GDPR osnažena su prava nositelja podataka, kao i obaveze onih koji obrađuju osobne podatke. Osnažuju se nadzorna ovlaštenja i mogućnosti u kontekstu izricanja kazni od strane relevantnih tijela za zaštitu osobnih podataka. GDPR ne odnosi se izravno na BiH jer nije članica EU. Međutim, Sporazumom o stabilizaciji i pridruživanju BiH je preuzela obvezu usklađivanja domaćeg zakonodavstva sa pravnom stečevinom

---

[33] "Niko se ne smije izložiti proizvoljnom miješanju u privatni život, porodicu, stan ili prepisku, niti napadati na čast i ugled. Svako ima pravo na zaštitu zakona protiv ovog miješanja ili napada". Član 12. Univerzalna deklaracija o ljudskim pravima. Generalna skupština UN, 1948/1971.

[34] „Svako ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske. (...)".Član 8. Konvencija za zaštitu ljudskih prava i osnovnih sloboda. Vijeće Evrope, 1953.

[35] Konvencija 108 je donesena na nivou Vijeća Evrope 28.01.1981. godine. Ovaj datum proglašen je Međunarodnim danom zaštite podatka o ličnosti, što istovremeno upućuje na značaj ovog dokumenta.

[36] MURTEZIĆ, A. O.: Konvencija 108: aktuelni značaj i primjena. U: MRVIĆ PETROVIĆ, N. (ed.): Strani pravni život. Beograd: Institut za uporedno pravo, 2020, p. 99-110. [online].

[37] Direktiva je bila ograničena i predstavljala je minimum pravnih standarda koje su članice Europske unije trebale unijeti u svoje nacionalne zakone o zaštiti podataka, pa je svaka članica izrađivala vlastite zakone. Nova Uredba riješila je ovaj problem. Kao Uredba, direktno nameće jedinstveni režim zakona sigurnosti podataka za sve članice EU. Agencija za zaštitu ličnih podataka u Bosni i Hercegovini. [online]

EU tako da se određene obveze normirane Uredbom odnose i na usklađivanje Zakona o zaštiti osobnih podataka BiH sa novim zakonodavstvom EU o zaštiti osobnih podataka.[38]

Osim ratificiranih međunarodnih akata, pravo na privatnost u BiH zaštićeno je i odredbama Ustava na nacionalnoj i na entiteskim razinama nivoima.[39] U kontekstu zaštite ličnih podataka i pravnih propisa donesenih na nacionalnoj razini za BiH je najznačajnije upravo donošenje Zakona o zaštiti osobnih podataka 2006. godine.[40] Donošenjem ovog zakona osnovana je i Agencija za zaštitu osobnih podataka u Bosni i Hercegovini. Kazneni zakoni doneseni na razini entiteta i na nacionalnoj razini, također, normiraju kaznena djela protiv privatnog života.[41] Kao kazneno djelo propisano je i neovlašteno korištenje osobnih podataka.

Iako je potreba za detaljnijim i sveobuhvatnijim regulacijom zaštite privatnosti i osobnih podataka sve izraženija, posebice u kontekstu njihove zaštite u internetskoj sferi, na razini BiH nisu doneseni pravni propisi koji izričito normiraju zaštitu prava na privatnost i osobnih podataka na internetu.

Direktiva o audiovizuelnim medijskim uslugama

Jedan od međunarodnih instrumenata važnih u kontekstu zaštite maloljetnika jeste revidirana Direktiva o audiovizuelnim medijskim uslugama, čija važnost proizilazi i iz obveze BiH prema Sporazumu o stabilizaciji i pridruživanju da svoj regulatorni okvir i zakonodastvo uskladi s pravnom tečevinom EU i da ga modernizira sukladno sa aktuelnim trendovima na suvremenom medijskom tržištu. Direktivom (EU) 2018/1808 Europskog parlamenta i Vijeća od 14. studeni 2018. godine o izmjeni Direktive 2010/13/EU pojačana je zaštita djece od štetnog onlajn sadržaja na svim platformama. U tom smislu važne su dvije izmjene odredbi koje se odnose na zaštitu djece:

- usklađivanje standarda zaštite linearnih i nelinearnih audiovizuelnih medijskih usluga (Član 6a) i
- proširenje obaveze zaštite maloljetnika na platformama za dijeljenje videozapisa[42] (Član 28.b).[43]

Osim normiranja zaštitnih mjera za djece koje su obavezne za pružatelja audiovizuelnih medijskih usluga i platformi za dijeljenje video sadržaja, a koje su uglavnom usmjerene na korištenje sustava za opisivanje potencijalno štetnih sadržaja, sustava praćenja dobi/roditeljskog nadzora, programa za ograničavanje pristupa djeci rasporedom prikazivanja, na korištenje tehničkih mehanizama koji ograničavaju pristup djeci potencijalno štetnim sadržajima i sl, revidirana Direktiva naglašava ulogu i važnost regulatornih tijela u kontekstu uspostave zaštitnih mjera.

Revidirana Direktiva o audiovizuelnim medijskim uslugama regulatorima izričito postavlja zadatak da procijene štetu prilikom odlučivanja o odgovarajućim razinama zaštitnih mjera koje će primijeniti i pružatelji audiovizuelnih medijskih usluga i

---

[38] http://azlp.ba/GDPR_Menu/Sta_je_GDPR/default.aspx?id=2373&langTag=bsBA&template_id=149&pageIndex=1

[39] „Pravo na privatni i porodični život, dom i prepisku". Članak II, stavak 3f. Ustav Bosne i Hercegovine „Službeni glasnik BiH" br. 25/2009 – Amandman I. Ustav Federacije Bosne i Hercegovine propisuje uživanje prava na privatnost. Članak 2. Stavak 1g „Službene novine BiH" br.1/94. „Ljudsko dostojanstvo, tjelesni i duhovni integritet, čovjekova privatnost, osobni i obiteljski život su nepovredivi". Članak 13. Ustav Republike Srpske „Службени гласник Републике Српске" бр. 21/92.

[40] Zakon o zaštiti osobnih podataka „Sl. glasnik BiH", br. 49/2006, 76/2011, 89/2011.

[41] Kazneni zakon Bosne i Hercegovine „Sl. glasnik BiH", br. 3/2003; Kazneni zakon Federacije Bosne i Hercrgovine „Sl. novine FBiH", br. 36/2003; Kazneni zakon Republike Srpske, „Sl.glasnik RS", br. 49/2003.

[42] Neke od najpopularnijih platformi za dijeljenje videozapisa jesu *TikTok, YouTube, Stardeos, Vimeo* i dr. Međutim, pored brojnih prednosti poput jednostavnog korištenja ovih platformi, izražene interaktivnosti, multimedijalnosti, njihovo korištenje podrazumijeva i izloženost određenim rizicima, naročito kada su u pitanju djeca i mladi. "Naime, na *TikToku* su dostupni različiti izazovi, pokatkad izuzetnog spornog sadržaja, što treba imati na umu u kontekstu brige o online sigurnosti djece i adolescenata. Usljed slabe zaštite, djeca na ovoj aplikaciji lako mogu postati meta odraslih pojedinaca ili žrtva vršnjačkog nasilja." (https://medijskapismenost.ba/tiktok-drustvena-mreza-u-usponu/). Na osnovu promjena koje su uvrštene u odredbe koje se odnose na zaštitu djece, čime je Direktiva u nadležnost nezavisnih evropskih regulatora uvrstila i usluge platformi za razmjenu videozapisa, u smislu poduzimanja mjera kako programi, videosadržaji koje su generirali korisnici i audiovizuelne komercijalne komunikacije ne bi naškodili fizičkom, psihičkom ili moralnom razvoju djeteta niti podstakli širu javnost na nasilje, govor mržnje ili terorizam, omogućena je regulacija *YouTube*-a. „Budući da *YouTube*, poput drugih vodećih platformi kao što su *Google, Apple, Facebook i Twitter* ima svoje evropsko sjedište u Irskoj, regulacija YouTubea u skladu sa odredbama Direktive, u nadležnosti je irskog nacionalnog regulatornog tijela. Pored toga, Direktiva je platformama za dijeljenje videozapisa nametnula i niz obaveza u pogledu promocije medijske pismenosti krajnjih korisnika usluga." (https://medijskapismenost.ba/youtube-najveci-svjetski-medij-masovne-komunikacije/)

[43] Jean-François Furnémont (Wagner-Hatfield), Pregled odredbi Kodeksa o audiovizuelnim uslugama u vezi s zaštitom maloljetnika, 2020.

[44] Prema: Jean-François Furnémont (Wagner-Hatfield), Pregled odredbi Kodeksa o audiovizuelnim uslugama u vezi s zaštitom maloljetnika, 2020.

ISP-ovi te da primjenjuju proporcionalan pristup temeljen na takvoj procjeni. Nadalje, regulatori će morati procijeniti prikladnost mjera koje poduzimaju IPS-ovi. Na temelju toga bit će potrebno više nego ikad prije da regulatori shavte kako štetni sadržaj utječe na djecu i što zapravo čini štetni sadržaj kako bi mogli poduzeti proporcionalnu regulatornu mjeru.[45]

Sukladno odredbama sadržanim u revidiranoj Direktivi koje se primarno odnose na davatelje audiovizuelnih medijskih usluga i platformi za dijeljenje video sadržaja, a koje su znatno usmjerene na osiguravanje bolje zaštite djece od štetnih onlajn sadržaja, kao imperativ u budućim aktivnostima nacionalnih i medijskih politika postavlja se uvođenje odgovarajućih regulatornih i samoregulatornih mehanizama prilagođenih onlajn okruženju. Iako pojava interneta počiva na konceptu slobode (govora, pristupa informacijama, iznošenja mišljenja i sl), mnogobrojni i veoma štetni vidovi njegove zlouporabe zahtijevaju iskorak iz regulacije tradicionalnog medijskog okruženja u cilju maksimalnog iskorištavanja pozitivnih potencijala interneta i istovremenog suzbijanja negativnih tendencija koje na različite načine ugrožavaju sigurnost njegovih korisnika. U tom smislu, pored angažmana međunarodnih organizacija, nacionalnih regulatornih tijela i drugih relevantnih javnih i nevladnih organizacija, nužan je angažman davatelja pristupa internetu, koji bi podrazumijevao podizanje razine sigurnosti njihovih korisnika, naročito djece.

[45]Jean-François Furnémont (Wagner-Hatfield), Pregled odredbi Kodeksa o audiovizuelnim uslugama u vezi s zaštitom maloljetnika, 2020.

PREGLED PROPISA – OBVEZA DAVATELJA PRISTUPA INTERNETU (ISP) U POGLEDU ZAŠTITE DJECE NA INTERNETU (EU I REGIJA)

Počevši od ranije elaboriranih izazova sa kojima se suočavaju korisnici interneta i dokumenata prvenstveno usmjerenih na reguliranje ove sfere, a u svrhu njihove zaštite, naročito djece, kao društveno, znanstveno i strukovno relevantno, postavlja se pitanje obveza davatelja pristupa internetu, u kontekstu zaštite djece, kao dominantnih korisnika njihovih usluga. U tom smislu, osim korištenja određenih mehanizama i tehničkih alata koji su na raspolaganju korisnicima interneta, neohodan je ozbiljan angažman davatelja pristupa interentu, koji bi trebalo da bude usmjeren na uključivanje i unaprjeđenje mehanizama zaštite, naročito najosjetljivije populacije, na koju ugrožavanje bilo koje sfere (privatnost, bezbjednost, izlaganje neprimjerenim sadržajima i sl), može imati i ostaviti dalekosežne posljedice. Naime, sadržaj Uputa za IKT kompanije u pogledu sigurnosti djece na intrnetu u cjelosti ukazuje na pruzimanje veće odgovornosti ovih tvrtki u pogledu poštovanja prava djece i mladih i usklađivanja njihovog načina funkcioniranja sa međunarodnim standardima.

Regulativa u EU

S ciljem podizanja društveno odgovornog poslovanja, stavljanja sigurnosti djeteta na internetu kao prioriteta u okviru regulatornih i samoregulatornih mehanizama i njihovog usklađivanja sa međunarodnim standardima koji podrazumijevaju zaštitu interesa djeteta, u ovom poglavlju bit će razrađeni određeni dokumenti, koji značajnim dijelom normiraju pitanja sigurnosti, zaštite i sprječavanja različite zlouporabe na internetu, na razini EU. Sukladno ranije definiranim ciljevima predmetne analize, na osnovu rezultata analize u ovom dijelu, bit će omogućen komparativni pristup regulativi BiH u odnosu na regulativu u EU, a potom u odnosu na regulativu u regiji, što će dati značajan doprinos u revidiranju normativnog okvira BiH i njegovom uslađivanju sa europskim dokumetima i odredbama koje značajno doprinose zaštiti djece na internetu.

Zakon o digitalnim uslugama

"Ako stvarni svijet ne može biti savršen, ne može ni internet. To, međutim, ne znači da ne bismo trebali pokušavati učiniti internet sigurnijim, boljim mjestom, kojim se poštuje sloboda govora i ohrabruju europske kompanije. To je cilj DSA" (predstavnica grupe Renew Europe, evroparlamentarka Dita Charanzova).[46] Rukovodeći se sličnim principima Europski parlament je sa 530 glasova za, 78 protiv i 80 uzdržanih usvojio Zakon o digitalnim uslugama (DSA), koji donosi mjere za suzbijanje nezakonitih proizvoda, usluga i sadržaja na internetu i jasno definira postupke za njihovo uklanjanje. Prema riječima Christel Schaldemose „zakon o digitalnim uslugama sada bi mogao postati novi zlatni standard za digitalnu regulaciju, ne samo u Europi već i širom svijeta".

Zakon podrazumijeva značajno povećanje razine društveno odgovornog poslovanje, jer će se tehnološke tvrtke smatrati mnogo odgovornijima za sadržaj na svojim platformama, također, morat će uspostaviti mehanizme za označenje, te da provode mjere za uklanjanje nezakonitih sadržaja, poput govora mržnje i dr. U ovom smislu internetske platforme postupat će bez nepotrebnog odgađanja nakon primanja prijave, uzimajući u obzir vrstu nezakonitog sadržaja koji se prijavljuje i hitnost poduzimanja radnji. Prema ovom zakonu platforme će morati dijeliti podatke s nevladinim organizacijama i akademskim istraživačima.

Internetske platforme morat će biti transparentnije u pogledu korištenja algoritama koji preporučuju sljedeći videozapis, proizvod za kupovinu ili vijest na vrhu feedova društvenih mreža. Sustavi preporuka temeljeni na algoritmima su kritikovani, jer s vremenom korisniku prikazuju sve ekstremniji ili polarizirajući sadržaj. Usvajanjem zakona prihvaćeno je više opcija za oglašavanje bez praćenja i zabranu korištenja podataka maloljetnika za ciljane oglase, kao i zabranu korištenja tamnih obrazaca kojima se utječe na ponašanje korisnika. Osim toga, korisnicima digitalnih usluga i organizacijama koje ih zastupaju bit će omogućeno traženje naknade za sve štete nastale zbog toga što platforme nisu poštovale svoje obveze.

---

[46] Iva Badnjak, „U Europskom paralamentu usvojen Zakon o digitalnim uslugama-zlatni standard za digitalnu regulaciju".

Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava (NIS direktiva - EU Network and Information Security Directive)

Kao članica međunarodnih organizacija BiH se obvezala poštovati načela i standarde koji proizlaze iz članstva u ovim organizacijama, kao što su UN-a ili OSCE-a. Jedna od ovih obveza BiH jeste „implementacija OSCE-ovih Mjera izgradnje povjerenja za smanjenje rizika od konflikta, koji proizlazi iz korištenja informacijskih i komunikacijskih tehnologija, koje je usvojilo Stalno vijeće OSCE-a, kako bi se osigurao otvoren, interoperativan, siguran i pouzdan internet u državama članicama OSCE-a, te smanjili rizici od pogrešne percepcije i mogućeg izbijanja političke i vojne tenzije ili sukoba".[47] Priključenje EU kroz pristupne pregovore do punopravnog članstva jeste strateški cilj BiH, a jedan od preduslova koji je neophodno ispuniti u ovom procesu jeste osiguranje adekvatnog nivoa *cyber* sigurnosti. U ovom smislu je važna Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća o mjerama za visoki zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije, poznatija kao NIS direktiva, koja svojim sadržajem, između ostalog, nalaže da svaka država članica donosi svoju strategiju za sigurnost informaciono-komunikacijskih sustava.

U Izvješću Europske komisije o napretku BiH za 2016. godinu navedeno je da: „Bosna i Hercegovina nema sveobuhvatni strateški pristup za rješavanje pitanja prijetnji u oblasti *cyber* kriminala i *cyber* sigurnosti." U Izvješću je potvrđena potreba za jačanjem reagiranja na prijetnje u oblasti *cyber* sigurnosti, postojećih kapaciteta za borbu protiv *cyber* kriminala, kao i kapaciteta timova za prevenciju i zaštitu od *cyber* incidenata i prijetnji sigurnosti javnih informacijskih sustava (CERT/ CSIRT).

Direktivom 2016/1148 Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava utvrđuju se mjere s ciljem postizanja visoke zajedničke razine sigurnosti mrežnih i informacijskih sustava unutar Europske Unije kako bi se poboljšalo funkcioniranje unutarnjeg tržišta. Ovom direktivom:

- utvrđuje se obveza za sve države članice da donesu nacionalnu strategiju za sigurnost mrežnih i informacijskih sustava,
- osniva se skupina za suradnju u svrhu podsticanja i olakšavanja strateške suradnje i razmjene informacija među država članicama i razvijanja uzajamnog povjerenja,
- stvara se mreža timova za odgovor na računalne sigurnosne incidente („mreža CSIRT-ova") kako bi se doprinijelo razvoju povjerenja među državama članicama i promoviranju brze i učinkovite operativne suradnje,
- utvrđuju se zahtjevi za sigurnost i obavještavanje za operatere ključnih usluga i za davatelje digitalnih usluga,
- utvrđuju se obveze za države članice da imenuju nacionalna nadležna tijela, jedinstvene kontaktne točke i CSIRT-ove čiji su zadaci vezani za sigurnost mrežnih i informacijskih sustava.

Ovom direktivom definira se da države članice osiguravaju da pružatelji digitalnih usluga poduzimaju odgovarajuće tehničke i organizacijske mjere za upravljanje rizicima kojima su izloženi mrežni i informacijski sustavi kojima se u EU služe u okviru pružanja usluga internet pristupa, internet pretrage i usluga računarstva u oblaku. Uzimajući u obzir najnovija postignuća tim se mjerama osigurava razina sigurnosti mrežnih i informacijskih sustava primjerenih riziku kojem su izloženi te uz vođenje računa o sljedećim elementima:

- sigurnost sustava i objekata,
- rješavanju incidenata,
- upravljanju kontinuitetom poslovanja,
- praćenju, reviziji i testiranju i
- usklađenosti s međunarodnim standardima.

Države članice osiguravaju da pružatelji digitalnih usluga poduzimaju mjere za sprječavanje i minimiziranje učinka incidenata

---

[47] „Smjernice za strateški okvir cyber sigurnosti u Bosni I Hercegovini", 2019. OSCE.

koji utječu na sigurnost njihovih mrežnih i informacijskih sustava na internet pristup, internet pretrage i usluge računalstva u oblaku, a koje se pružaju u EU, s ciljem osiguravanja kontinuiteta tih usluga. Države članice osiguravaju da pružatelji digitalnih usluga bez nepotrebnog odgađanja obavijeste nadležno tijelo ili CSIRT o svakom incidentu koji znatano utječe na pružanje neke od pomenutih usluga koju oni nude unutar EU.

Na temelju znatnog napretka koji je unutar Europskog foruma država članica postignut u poticanju rasprava i razmjeni dobrih političkih praksi, uključujući razvoj načela za europsku suradnju za sajber krize, prema Direktivi 2016/1148, trebalo bi osnovati skupinu za suradnju sastavljenu od predstavnika država članica, Komisije i Agencije Europske unije za mrežnu i informacijsku sigurnost („ENISA") kako bi se poduprla i poboljšala strateška suradnja među državama članicama u pogledu sigurnosti mrežnih i informacijskih sustava. Kako bi ta skupina bila učinkovita i uključiva, potrebno je da sve države članice raspolažu minimalnim sposobnostima i strategijom za osiguravanje visoke razine sigurnosti mrežnih i informacijskih sustava na svom državnom području. Osim toga, zahtjevi za sigurnost i obavještavanje trebali bi se primjenjivati na operatere ključnih usluga i na davatelje digitalnih usluga kako bi se promicala kultura upravljanja rizicima i osiguralo prijavljivanje najtežih incidenata.

Sveučilišta i istraživački centri treba da imaju odlučujuću ulogu u poticanju istraživanja, razvoja i inovacija u područjima sigurnosti mrežnih i informacijskih sustava. Važno je napomenuti i to da se Direktivom ne sprječava operatere ključnih usluga i davaoce digitalnih usluga da primjenjuju i strože mjere od onih koje su propisane Direktivom.

Direktivom se predviđa postojanje čvorišta za razmjenu internetskog prometa (IXP). IXP služi za međusobno povezivanje mreža, ali ne omogućuje pristup mreži i ne djeluje kao davatelj prijenosa, a ni kao nositelj prijenosa. Također, IXP ne pruža ni druge usluge koje nisu vezane za međusobno povezivanje, iako to operatera IXP-a ne sprječava da pruža i nepovezane usluge. IXP služi međusobnom povezivanju mreža koje su tehnički i organizaciono odvojene. Pojam „autonomni sustav" upotrebljava se za opisivanje mreže koja je tehnički neovisna.

Sukladno ovoj direktivi, države članice EU trebale bi osigurati da njihovi CSIRT-ovi (CERT-ovi), dobro funkcioniraju i da poštuju ključne zahtjeve kako bi se zajamčile učinkovite i usklađene sposobnosti za rješavanje incidenata i rizika, te kako bi se osigurala učinkovita suradnja na razini EU. Kako bi sve vrste operatera ključnih usluga i davatelja digitalnih usluga imale koristi od takvih sposobnosti i suradnje, države članice trebale bi osigurati da imenovani CSIRT-ovi pokrivaju sve njih. S obzirom na važnost međunarodne suradnje za sajber sigurnost CSIRT-ovi bi trebali moći, uz mrežu CSIRT-ova uspostavljenu ovom Direktivom, sudjelovati i u međunarodnim mrežama suradnje.

U ovoj direktivi navodi se i da je operatere ključnih usluga i davatelje digitalnih usluga potrebno poticati da slijede vlastite neformalne mehanizme suradnje s ciljem osiguravanja sigurnosti mrežnih i informacijskih sustava. Isto tako, operateri ključnih usluga i pružatelji digitalnih usluga uveliko snose odgovornost za osiguravanje sigurnosti mrežnih i informacijskih sustava.

Pružatelji digitalnih usluga trebali bi osigurati razinu sigurnosti sukladnu sa stepenom rizika kojima je izložena sigurnost usluga koje pružaju, s obzirom na važnost njihovih usluga za rad drugih poduzeća unutar EU. U praksi je razina rizika za operatere ključnih usluga, veća nego za davatelje digitalnih usluga. Stoga bi sigurnosni zahtjevi za davatelje digitalnih usluga trebali biti blaži. Pružatelji digitalnih usluga trebali bi i dalje imati slobodu preduzimanja mjera koje smatraju primjerenima za upravljanje rizicima kojima je izložena sigurnost njihovih mrežnih i informacijskih sustava. Zbog prekogranične prirode davatelja digitalnih usluga na njih bi se trebao primjenjivati usklađeniji pristup na razini EU. Također, kako bi se izbjeglo prekomjerno financijsko i administrativno opterećenje za operatere ključnih usluga i davatelje digitalnih usluga, zahtjevi bi trebali biti srazmjerni riziku kojem je izložen dotični mrežni ili informacijski sustav.

CSIRTs Network (engl. Computer Security Incident Response Team / Tim za odgovor na računalne sigurnosne incidente)

CSIRT je kratica koju je prihvatila stručna javnost i prepoznata kao utvrđeni naziv za tim koji se bavi informacijskom sigurnosti. CSIRT prikuplja i dijeli informacije o rizicima sigurnosti u informaciono-komunikacijskim (IKT) sustavima, kao i događajima koji ugrožavaju sigurnost IKT sustava i u vezi sa tim informira, upozorava i savjetuje osobe koje upravljaju IKT sustavima na određenom području, kao i njenu javnost.

S ciljem doprinosa razvoju povjerenja među državama članicama EU, te promoviranju brze i učinkovite operativne suradnje, Direktivom 2016/1148 osnovana je mreža nacionalnih CSIRT-ova. Mreža CSIRT-ova sastoji se od predstavnika CSIRT-ova iz država članica EU i iz CERT-EU-a.

Zadaci mreže CSIRT-ova su:

- razmjena informacija o uslugama CSIRT-ova te njihovim aktivnostima i mogućnostima suradnju,
- na zahtjev predstavnika CSIRT-a iz države članice na koju bi incident mogao utjecati, razmjenjivanje informacija koje nisu komercijalno osjetljive prirode, a odnose se na taj incident i s njime povezane rizike, te rasprava o tim informacijama. CSIRT svake države članice može odbiti davanje doprinosa takvoj raspravi ako postoji rizik da se u pitanje dovede istraga o incidentu,
- razmjena i stavljanje na raspolaganje na dragovoljnoj osnovi informacija o pojedinačnim incidentima koje nisu povjerljive,
- na zahtjev predstavnika CSIRT-a države članice, razmatranje, a ako je to moguće, i određivanje koordiniranog odgovora na incident koji je utvrđen u području za koje je nadležna ista ta država članica,
- potpora državama članicama u rješavanju prekograničnih incidenata na bazi dragovoljne uzajamne pomoći,
- rasprava o daljnjim oblicima operativne suradnje, te njihovo istraživanje i utvrđivanje, među ostalim u odnosu na:
  - kategorije rizika i incidenata,
  - rana upozorenja,
  - uzajamnu pomoć,
  - načela i načine koordinacije, kada države članice odgovaraju na prekogranične rizike i incidente
- obavještavanje grupe za suradnju o svojim aktivnostima i daljnjim oblicima operativne suradnje,
- rasprava o poukama stečenima u vježbama koje se odnose na sigurnost mrežnih i informacijskih sustava, među ostalim i onima koje organizira ENISA,
- na zahtjev pojedinačnog CSIRT-a, rasprava o sposobnostima i pripravnosti tog CSIRT-a,
- izdavanje uputa radi olakšavanja konvergencije operativnih praksi s ciljem primjene odredaba ovoga članka u pogledu operativne suradnje,

Mreža CSIRT-ova priprema izvještaje o procjeni stečenog iskustva u pogledu operativne saradnje, u vremenskim intervalima od 1,5 godinu. Ti izvještaji se dostavljaju i grupi za saradnju.

Agencija Evropske unije za sajber sigurnost/European Union Agency for Cybersecurity (ENISA)

ENISA je osnovana Uredbom broj 460/2004 EU, od 10.03.2004. godine. ENISA je agencija EU za mrežnu i informacijsku sigurnost koja obavlja dodijeljene zadatke, te time doprinosi visokoj razini mrežne i informacijske sigurnosti u EU, podiže svijest o mrežnoj i informacijskoj sigurnosti, te razvija i potiče kulturu mrežne i informacijske sigurnosti u društvu u korist građana, potrošača, poduzeća i organizacija javnog sektora u EU i na taj način doprinosi uspostavljanju i pravilnom funkcioniranju unutarnjeg tržišta.

Postojanjem ENISA-e ne dovodi se u pitanje nadležnost država članica u pogledu mrežne i informacijske sigurnosti.

ENISA pomaže institucijama, tijelima, uredima i agencijama EU u razvoju politika u vezi s mrežnom i informacijskom sigurnošću. Osim toga, ENISA pomaže institucijama, tijelima, uredima i agencijama EU i državama članicama u provedbi politika potrebnih za ispunjavanje pravnih i regulatornih zahtjeva u vezi s mrežnom i informacijskom sigurnošću sukladno postojećim i budućim pravnim aktima EU, te na taj način doprinosi pravilnom funkcioniranju unutarnjeg tržišta. Također, ENISA pomaže EU i državama članicama u poboljšanju i jačanju njihovih sposobnosti i spremnosti za sprječavanje i otkrivanje problema i nezgoda u vezi s mrežnom i informacijskom sigurnošću, te u pripremi odgovora na njih.

UREDBA (EU) 2021/1232 EUROPSKOG PARLAMENTA I VIJEĆA od 14. SRPNJA 2021. o privremenom odstupanju od određenih odredaba Direktive 2002/58/EZ u pogledu tehnologija koje pružatelji brojevno neovisnih interpersonalnih komunikacijskih usluga upotrebljavaju za obradu osobnih i drugih podataka u svrhu borbe protiv seksualnog zlostavljanja djece na internetu

Ovom Uredbom se utvrđuju privremena i strogo ograničena pravila kojima se odstupa od određenih obveza utvrđenih u Direktivi 2002/58/EZ, s jedinim ciljem da se pružateljima određenih neovisnih interpersonalnih komunikacijskih usluga omogući da, ne dovodeći u pitanje Uredbu (EU) 2016/679, upotrebljavaju posebne tehnologije za obradu osobnih i drugih podataka u mjeri u kojoj je to prijeko potrebno za otkrivanje seksualnog zlostavljanja djece na internetu u okviru svojih usluga i njegovo prijavljivanje, te uklanjanje internetskog materijala koji sadržava seksualno zlostavljanje djece sa svojih usluga.

Članak 5. stavak 1. i članak 6. stavak 1. Direktive 2002/58/EZ ne primjenjuju se na povjerljivost komunikacija koje uključuju obradu, od strane davatelja usluga, osobnih i drugih podataka u vezi s pružanjem brojno neovisnih interpersonalnih komunikacijskih usluga, pod odgovarajućim uslovima, kao što su da je obrada neophodna za upotrebu posebne tehnologije s jedinom svrhom otkrivanja i uklanjanja internetskog materijala koji sadržava seksualno zlostavljanje djece, te njegova prijavljivanja tijelima za izvršavanje zakonodavstva i organizacijama koje djeluju u javnom interesu protiv seksualnog zlostavljanja djece, i otkrivanja mamljenja djece, te njegova prijavljivanje tijelima za izvršavanje zakonodavstva i organizacijama koje djeluju u javnom interesu protiv seksualnog zlostavljanja djece.

Pružatelji usluga treba da:

- utvrde interne postupke za sprječavanje zlouporabe osobnih i drugih podataka, neovlaštenog pristupa ličnim i drugim podacima, te neovlaštenih prijenosa osobnih i drugih podataka,
- osiguraju ljudski nadzor i, ako je potrebno, ljudsku intervenciju prilikom obrade osobnih i drugih podataka upotrebom tehnologija obuhvaćenih ovom Uredbom,
- osiguraju da se materijal koji nije prethodno identifikovan kao internetski materijal koji sadržava seksualno zlostavljanje ili mamljenje djece ne prijavljuje tijelima za izvršavanje zakonodavstva ili organizacijama koje djeluju u javnom interesu protiv seksualnog zlostavljanja djece bez prethodne ljudske potvrde,
- uspostave odgovarajuće postupke i mehanizme pravne zaštite kako bi osigurali da im korisnici mogu u razumnom roku podnijeti pritužbe u kojima iznose svoja stajališta,
- informiraju korisnike na jasan, uočljiv i razumljiv način o tome da su se sukladno s ovom Uredbom pozvali na odstupanje od članka 5. stavak 1. i članka 6. stavak 1. Direktive 2002/58/EZ u pogledu povjerljivosti komunikacija korisnika s tačno određenom svrhom, o logici na kojoj se baziraju mjere koje su poduzeli u okviru odstupanja i utjecaju na povjerljivost komunikacija korisnika, uključujući mogućnost da se osobni podaci dijele s tijelima za izvršavanje zakonodavstva i organizacijama koje djeluju u javnom interesu protiv seksualnog zlostavljanja djece,
- informiraju korisnike o sljedećem ako je njihov sadržaj uklonjen ili je njihov račun blokiran ili je usluga koja im se nudi obustavljena:

- oblicima traženja pravne zaštite od davatelja,
- mogućnosti podnošenja pritužbe nadzornom tijelu i
- pravu na pravni lijek.

- objavljuju, te nadležnom nadzornom tijelu i Komisiji do 31. siječnja svake godine, podnose izvješća o obradi osobnih podataka u okviru ove Uredbe, uključujući informacije o:
  - vrsti i količini obrađenih podataka;
  - specifičnom razlogu za obradu osobnih podataka na bazi Uredbe (EU) 2016/679;
  - razlogu za prenose osobnih podataka izvan EU na temelju poglavlja V. Uredbe (EU) 2016/679, kada je to primjenjivo;
  - broju identifikovanih slučajeva seksualnog zlostavljanja djece na internetu, uz razlikovanje između internetskog materijala koji sadržava seksualno zlostavljanje djece i mamljenje djece;
  - broju slučajeva u kojima je korisnik podnio pritužbu pomoću internog mehanizma pravne zaštite ili je podnio pritužbu pravosudnom tijelu te ishodu takvih pritužaba,
  - broju i omjeru grešaka (lažno pozitivni rezultati) raznih tehnologija koje su upotrebljene,
  - mjerama primijenjenim za ograničavanje stope grešaka i postignutoj stopi grešaka,
  - politici zadržavanja i primijenjenim zaštitnim mjerama za zaštitu podataka na temelju Uredbe (EU) 2016/679,
  - nazivima organizacija koje djeluju u javnom interesu protiv seksualnog zlostavljanja djece na internetu, a kojima su podaci podijeljeni na bazi ove Uredbe.

Sukladno Uredbi pružatelji usluga Komisiji dostavljaju i redovito ažuriraju popis imena organizacija koje djeluju u javnom interesu protiv seksualnog zlostavljanja djece kojima prijavljuju seksualno zlostavljanje djece na internetu sukladno s Uredbom.

Određeni pružatelji usluga određenih brojno neovisnih interpersonalnih komunikacijskih usluga, kao što su usluge elektronske pošte i slanja poruka na internetu, i prije usvajanja ove uredbe, na dobrovoljnoj osnovi, upotrebljavaju posebne tehnologije radi otkrivanja seksualnog zlostavljanja djece na internetu u okviru svojih usluga i njegova prijavljivanja tijelima nadležnima za provedbu zakonodavstva i organizacijama koje djeluju u javnom interesu protiv seksualnog zlostavljanja djece. Pružatelji usluga to čine skeniranjem sadržaja, kao što su fotografije i tekst, te analizom historijskih podataka korisnika. Tehnologija koja se koristi za te aktivnosti mogla bi biti tehnologija hash-iranja („hashing") za fotografije i videozapise, te uporaba klasificiranih algoritama strojnog učenja i umjetne inteligencije za analizu teksta i podataka o prometu. Upotrebom ovakvih tehnologija, internetski materijal koji sadržava seksualno zlostavljanje djece prijavljuje se kada se vrati pozitivan rezultat, tj. podudaranje koje proizlazi iz usporedbe fotografije ili videozapisa s jedinstvenim digitalnim otiskom (koji se ne može izmijeniti bez otkrivanja date izmjene) iz baze podataka koju vodi organizacija koja djeluje u javnom interesu protiv seksualnog zlostavljanja djece koja sadržava provjereni internetski materijal koji sadrži seksualno zlostavljanje djece. Ti se pružatelji usluga obraćaju nacionalnim dežurnim telefonskim linijama za prijavu internetskog materijala koji sadrži seksualno zlostavljanje djece te organizacijama, smještenima kako u EU, tako i u trećim zemljama, čiji je cilj identificirti djecu, smanjiti seksualno iskorištavanje i seksualno zlostavljanje djece, te spriječiti viktimizaciju djece.

Tehnologije koje se upotrebljavaju za potrebe ove Uredbe trebale bi narušavati privatnost u najmanjoj mogućoj mjeri sukladno najsavremenijim postignućima u industriji. Te se tehnologije ne bi trebale upotrebljavati za sustavno filtriranje i skeniranje teksta u komunikacijama, osim ako se to radi isključivo radi otkrivanja obrazaca koji ukazuju na moguće konkretne razloge zbog kojih se sumnja na seksualno zlostavljanje djece na internetu te one ne bi trebale omogućavati donošenje zaključka o sadržaju komunikacija. U slučaju tehnologije koja se upotrebljava za otkrivanje mamljenja djece, takvi konkretni razlozi za sumnju trebali bi se temeljiti na objektivno utvrđenim čimbenicima rizika kao što su razlika u dobi i vjerovatno sudjelovanje djeteta u skeniranoj komunikaciji.

Konvencija Vijeća/Savjeta Europe o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja

Vijeće/Savjet Europe je regionalna međunarodna organizacija osnovana 5. svibnja 1949. godine s namjerom ostvarivanja većeg jedinstva među članicama kako bi se očuvali i promovirali ideali i načela koji su njihova zajednička baština i potaknuo njihov gospodarski i društveni napredak. Vijeće Europe je forum europskih država za međusobno savjetovanje i koordinaciju aktivnosti, posebno na području razvoja demokratije i zaštite prava čovjeka, posebno prava manjina, jednakosti i socijalne pravde, slobode medija, obrazovanja za demokratske promjene, zaštite kulturne baštine i razvoja europskog identiteta, jačanja lokalne i regionalne uprave i samouprave, potpore zemljama u tranziciji srednje i istočne Europe. Vijeće Europe prihvatilo je brojne međunarodne ugovore, među kojima je najznačajnija Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda, na temelju koje djeluje Europski sud za ljudska prava.

Vijeće/Savjet Evrope je 25.10.2007. godine usvojilo Konvenciju o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja. Ciljevi ove Konvencije su:

- sprječavanje i suzbijanje seksualnog iskorištavanja i seksualnog zlostavljanja djece,
- zaštita prava djece žrtava seksualnog iskorištavanja i seksualnog zlostavljanja,
- promoviranje nacionalne i međunarodne saradnje u suzbijanju seksualnog iskorištavanja i seksualnog zlostavljanja djece.

Ova konvencija od država članica traži sljedeće:

1. Mjere prevencije
   - pažljivo ocjenjivati, zaposliti i obučiti osobe koje rade u kontaktu s djecom,
   - osigurati da djeca postanu svjesna rizika seksualnog iskorištavanja i seksualnog zlostavljanja te načina na koji se mogu zaštititi,
   - osigurati redovito nadzirane mjere intervencije za počinitelje i potencijalne počinitelje, usmjerene na sprječavanje seksualnih delikata nad djecom.
2. Mjere zaštite
   - uspostaviti programe za potporu žrtvama i njihovim obiteljima. Uspostaviti terapijsku pomoć i hitnu psihološku skrb,
   - poticati na prijavljivanje sumnji na seksualno iskorištavanje ili seksualno zlostavljanje,
   - uspostaviti telefonske i internetske linije za pomoć i pružanje savjeta.
3. Mjere kaznenog zakonodavstva
   - osigurati da određene vrste ponašanja budu zakonom propisane kao kaznena djela, kao što je sudjelovanje u seksualne aktivnosti s djetetom mlađim od zakonske dobi za takve aktivnosti,
   - kriminalizirati ponašanje koje koristi nove tehnologije, a posebno internet, za seksualno nasilje nad djecom, kao npr. vrbovanje djece u seksualne svrhe,
   - uspostaviti zajedničke jasne kriterijume za osiguranje uspostave djelotvornog, odgovarajućeg i odvraćajućeg kaznenog sustava,
   - prikupljati i pohranjivati podatke o osuđivanim počiniteljima seksualnih delikata nad djecom.
4. Istražni i sudski postupci naklonjeni djeci
   - osigurati dobru zaštitu djece tokom sudskih postupaka kako se doživljena trauma ne bi povećala,

- zaštititi privatnost, identitet i ugled djece žrtava,
- uspostaviti mjere prilagođene potrebama djece žrtava, poštujući prava djece i njihovih obitelji,
- ograničiti broj intervjua s djecom žrtvama, osigurati da se oni odvijaju u okruženju koje umiruje te uz prisutnost stručnjaka koji su prošli odgovarajuću obuku.

5. Nadzor

- uspostaviti poseban nadzorni mehanizam kako bi se osigurala provedba Konvencije. To će osigurati poštovanje Konvencije od strane država te garantirati njenu dugoročnu primjenu.

Praktičan vodič za tvrtke koji im pomaže da razumiju i poboljšaju svoj utjecaj na dečija prava

UNICEF je 2013. godine objavio specijalizirani vodič za tvrtke „Djeca su svima važna", koji treba da pomogne tvrtkama da bolje razumiju i poboljšaju svoj utjecaj na djecu i mlade. Ukoliko tvrtka obezbjeđuje internet usluge, mobilne telefone, odnosno računalne i video igrice, onda uvođenje mjera za zaštitu djece treba da bude standardna praksa pri razvoju novih tehnologija. To obuhvata sljedeće:

- Tehnologiju koja filtrira i procjenjuje sadržaj
- Sustavi procjene za identifikaciju sadržaja koji deca smiju da pregledaju, kao što su Asocijacija za ocenjivanje internet sadržaja (ICRA), međunarodna neprofitna organizacija, ili Odbor za ocenjivanje zabavnog softvera (ESRB), poslovna organizacija koja ocenjuje sadržaj video i računalnih igrica.
- Kontroliranje pristupa veb-sajtovima kroz mogućnost registrovanja za korištenje stranica ukoliko je dostignuta minimalna dob (najčešće 13 godina) i provjeru da li je krajnji korisnik odgovarajuće dobi i da li može da donosi odgovarajuće odluke. Neke dječje web stranice imaju pravila o privatnosti i zahtijevaju dopuštenje roditelja za otkrivanje osobnih podataka i roditeljski „veto" na interakciju sa web stranicom. Ostala potencijalna rješenja uključuju zahtjev da internet provajderi bilježe i provjeravaju podatke o korisnicima kako bi bili sigurni da data imena nisu lažna, zahtjev da internet provajderi vode evidenciju o informacijama koje su prošle kroz njihove servere tijekom dogovorenog minimalnog vremenskog razdoblja i zahtjev da internet provajderi odbiju skupine koje izričito navedu da se u sadržaju njihovih web stranica mogu pronaći i slike zlostavljanja dece.
- Mehanizme izvješćivanja, što podrazumijeva i stranice na veb-sajtovima za sigurnost djece gdje korisnici mogu odmah prijaviti odgovarajući problem.
- Suradnju sa policijskim vlastima u cilju otkrivanja i prijave kaznenih djela počinjenih na Internetu, kao što su priprema djeteta za susret u stvarnom svijetu ili uznemiravanje.
- Uklanjanje i blokiranje nelegalnog sadržaja.
- Zapošljavanje osoblja koji su stručni za zaštitu djece od strane internet provajdera i drugih provajdera informacijskih i komunikacijskih tehnologija.
- Blokiranje plaćanja (slika zlostavljanja djece) kreditnim karticama ili putem nekih drugih platnih sustava.

Primjeri zemalja Evropske unije

Finska

Finska je krajem 2020. godine donijela nacionalni akcijski plan za prevenciju nasilja nad djecom (eng. *Non-Violent Childhoods : Action Plan for the Prevention of Violence against Children 2020–2025*). Cilj ovog akcijskog plana je spriječiti nasilje nad djecom do 17 godina u različitim sredinama. Akcijski plan se bavi pravima djeteta, uključivanjem, čimbenicima koji štite od nasilja, kao i čimbenicima rizika i njihovim posljedicama. Akcijski plan sastoji se od četrnaest poglavlja koja se bave prevencijom

emocionalnog i fizičkog nasilja, kao i seksualnog nasilja iz tri različite perspektive: prevencije, minimiziranja štetnog utjecaja i liječenja, sa glavnim fokusom na prevenciju. Plan nastoji da uzme u obzir pitanja koja se odnose na djecu u posebno ranjivim situacijama u pogledu nasilja, kao i neka trenutačna specifična pitanja. U planu je naglašen značaj multidisciplinarne suradnje. Upravljačka skupina koju imenuje Finski institut za zdravlje i dobrobit (eng. *Finnish Institute for Health and Welfare*) odgovorna je za praćenje i usmjeravanje ciljeva i djelovanja.

Jedno od važnih poglavlja ovog akcijskog plana je poglavlje 11 koje se odnosi na nasilje u digitalnim medijima (eng. *Sexual harassment, grooming and sexual violence in digital media).* Između ostalog, ovdje se ističe važnost ažuriranja zakonske regulative usljed kontinuiranog i brzog tehnološkog razvoja i stalne promjene digitalnih medija. Iz istog razloga policijski i drugi službenici koji djeluju preventivno, ali i istražuju nasilje protiv djece u digitalnim medijima treba da imaju adekvatnu obuku. Sredstva policije, tužilaštva i sudova koji rade na ovakvim slučajevima treba povećati, a sve u najboljem interesu djece. U ovom akcijskom planu ističe se i značaj povećanja svijesti djece i mladih o rizicima povezanim za digitalne medije. Iz tog razloga potrebno je unaprijediti odgovarajuće vještine djece i mladih kroz nastavu i namjenske obuke. Bitno je i da roditelji budu informirani o ovim rizicima. Vještine profesionalaca koji rade sa djecom i mladima treba jačati kroz kontinuirano usavršavanje. Kako se digitalne tehnologije ubrzano razvijaju daje se i značaj informacijama koje su zasnovane na kontinuiranom istraživanju u ovoj oblasti. Akcije navedene u ovom poglavlju su sljedeće:

6. Osposobljavanje o seksualnom uznemiravanju, iskorištavanju i nasilju nad djecom u digitalnim medijima mora biti obezbijeđeno osobama koje rade sa djecom i mladima,
7. Sva djeca i mladi treba da imaju obuku o rizicima vezanim za digitalne medije,
8. Djeca i mladi treba da imaju informacije i uputstva o tome gdje i kako da dobiju pomoć, kao i gdje da prijave seksualno uznemiravanje i nasilje, uključujući i nasilje u digitalnim medijima,
9. Jasna pravila suradnje između odgovarajućih institucija i organizacija za uklanjanje sadržaja koji sadrži prikaze seksualnog nasilja nad djecom treba uspostaviti,
10. Vlasti i svi odgovorni imaju dovoljno informacija i resursa za rješavanje kaznenih djela nasilja nad djecom u digitalnom okruženju.

Za realiziranje ovih akcija odgovorna su odgovarajuća ministarstva zdravlja, socijalne zaštite, obrazovanja, unutarnjih poslova, organizacije koje rade sa djecom, kao i telekomunikacijski operateri.

Njemačka

Zakon o izmjenama i dopunama Zakona o zaštiti mladih (eng. *Second Act amending the German Youth Protection Act*), koji je u Nemačkoj stupio na snagu 1.5.2021. godine, po prvi put pravno definira sudjelovanje djece i mladih u izradi zakona o zaštiti mladih. Njihovo sudjelovanje u kreiranju ovakvih dokumenata je logično, jer su djeca i mladi često među prvima koji usvajaju nove digitalne aplikacije, uređaje i usluge, te mogu biti izloženi različitim rizicima i opasnostima:

- prilikom onlajn komunikacije,
- prilikom kupovine putem interneta,
- onlajn klađenju,
- izlaganju osobnih podataka trećim licima, bez prethodno date saglasnosti,
- štetnom djelovanju reklama i sl.

Ovi, ali i drugi rizici su adresirani ovim zakonom. Zakon obvezuje vlasnike onlajn platformi da poduzmu odgovarajuće mjere opreza za suprotstavljanje takvim rizicima. Ove mjere uključuju, ali se ne ograničavaju na: predstavljanje uvjeta korištenja

određene platforme na djeci razumljiv način, obvezu da su podrazumijevane postavke platforme takve da obezbjeđuju zaštitu djece (npr. da korisnički profil ne može biti indeksiran od strane servisa za pretragu sadržaja), mogućnost nadzora i kontrole pristupa od roditelja (npr. roditeljima mogu biti date mogućnosti ograničavanja pristupa određenim resursima, postavljanja vremenskih ograničenja i sl.), te lako pronalaženje informacija, savjeta i mehanizama za prijavu i pomoć, a koji su obezbjeđeni neovisno od vlasnika onlajn platformi.

Francuska

Zakon br. 2022-300 za jačanje roditeljskog nadzora nad modelima pristupa internetu usvojen je 2.3.2022. godine, nakon ubrzanog zakonodavnog procesa u francuskoj Narodnoj skupštini i Senatu. Ovaj zakon osmišljen je s ciljem da pojača roditeljsku kontrolu nad pristupom djece internetu (fra. *LOI n° 2022-300 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à internet*).

Ovaj zakon se prvenstveno odnosi na proizvođače uređaja koji djeci omogućuju pristup onlajn uslugama i sadržaju, a koji mogu da naškode njihovom fizičkom, mentalnom ili moralnom razvoju (npr. računala, pametni telefoni, tableti, pametni televizori). Zakon, koji se odnosi samo na uređaje koji se prodaju sa operativnim sustavom, zahtijeva od proizvođača takvih uređaja da osiguraju unaprijed instaliran sustav roditeljskog nadzora koji roditelji ili skrbnici mogu da aktiviraju nakon prve upotrebe. Instalacija, upotreba i (gde je to primjenljivo) deinstalacija sustava moraju biti obezbjeđeni krajnjim korisnicima bez dodatnih troškova.

Osim ovih uvjeta, ovaj zakon izričito zabranjuje korištenje osobnih podataka djece koje prikuplja ili generiše sustava roditeljskog nadzora u komercijalne svrhe, kao što su direktni marketing, profiliranje ili ciljano bihejvioralno oglašavanje. Ova zabrana treba da ostati na snazi i nakon što dijete postane punoljetno.

Iako su proizvođači uređaja u srdištu pozornosti ovog zakona, određene obveze se odnose i na druge dionike (npr. dobavljače operativnih sustava, uvoznike, distributere i prodavce rabljenih uređaja). Ovo uključuje obvezu certificiranja (ili provjere postojeće potvrde) da uređaji uključuju sustav roditeljskog nadzora prije nego što postanu dostupni na tržištu.

Zakon precizira i to da će francuska vlada, nakon konzultacija sa francuskim državnim i nadzornim tijelom (CNIL), izdati uredbu kojom će se razjasniti kako će se određeni aspekti zakona provoditi u praksi. Ovom uredbom treba posebno precizirati:

- minimalne funkcionalnosti i tehničke karakteristike sustava roditeljskog nadzora,
- sredstva koja je primijenio proizvođač da bi se olakšala uporaba ovog sustava,
- uvjete pod kojima nadležno tijelo može ograničiti ili zabraniti stavljanje na tržište bilo kojeg uređaja koji predstavlja rizik ili posjeduje neusaglašenost, kao i uslove pod kojima nadležno tijelo može opozvati ili povući takav uređaj s tržišta,
- kako proizvođači mogu da pomognu u podizanju svijesti o rizicima povezanim sa upotrebom onlajn usluga od strane djece, ranom izloženošću djece ekranima i načinima za sprječavanje ovih rizika.

Ovaj zakon je dio širih napora Francuske da bolje zaštiti djecu od neprikladnih sadržaja na internetu.

Upute Međunarodne unije za telekomunikacije (ITU)

Međunarodna telekomunikacijska unija (eng. *International Telecommunication Union - ITU*) je međunarodna organizacija, tj. specijalizirana agencija Ujedinjenih naroda odgovorna za pitanja informacijske i komunikacijske tehnologije. Izvorno je osnovana kao Međunarodna telegrafska unija 17.svibnja 1865. godine te je taj datum i zvanično datum osnivanja ove organizacije. U njeno članstvo uključeno je 193 države sa oko 700 sektora i asocijacija država članica. Bosna i Hercegovina je članica ove unije od 20.listopad 1992. godine.

Upute za IKT tvrtke u vezi sa sigurnošću djece na internetu

Ove Upute su 2020. godine razvile Međunarodna unija za telekomunikacije (ITU) i radna skupina autora koji su dali doprinos, a dolaze iz vodećih institucija aktivnih u sektoru informacijskih i komunikacijskih tehnologija.

Opće upute za IKT kompanije:

- Razmatranja o integraciji prava djeteta u sve odgovarajuće korporativne politike i procese upravljanja
- Razvoj standarda IKT tvrtki za zaštitu djece na internetu
- Razvoj standardnih postupaka za postupanje s materijalima seksualnog zlostavljanja djece
- Stvaranje bezbjednijeg okruženja na internetu prilagođenog dobi
- Edukacija djece, roditelja i odgojitelja o sigurnosti djece i njihovoj odgovornom korištenju IK tehnologija
- Korištenje tehnološkog napretka za zaštitu i obrazovanje djece
- Promoviranje digitalne tehnologije kao načina za povećanje građanskog angažmana
- Ulaganje u digitalno istraživanje

Odgovorne tvrtke poduzimaju niz koraka kako bi spriječile da se njihove mreže i usluge koriste za širenje materijala seksualnog zlostavljanja djece. To uključuje uvođenje jezika u uvjete i odredbe ili kodekse ponašanja koji izričito zabranjuju takav sadržaj ili ponašanje; razvijanje snažnih postupaka informiranja i uklanjanja; te rad i potpora nacionalnim linijama za potporu.

Osim toga, neke tvrtke primjenjuju tehničke mjere kako bi spriječile zlouporabu svojih usluga ili mreža za dijeljenje poznatog materijala seksualnog zlostavljanja djece. Na primjer, neki pružatelji internet usluga blokiraju pristup internet adresama za koje je odgovarajuće tijelo potvrdilo da sadrže materijal seksualnog zlostavljanja djece ako je internet stranica hostirana u zemlji u kojoj nisu uspostavljeni procesi kako bi se osiguralo da će se on brzo ukloniti. Drugi koriste tehnologije heširanja za automatsko otkrivanje i uklanjanje slika seksualnog zlostavljanja djece koje su već poznate policiji ili linijama za potporu. Članovi IKT industrije trebali bi preispitati i uključiti sve relevantne službe u svoje operacije kako bi se spriječilo širenje seksualnog zlostavljanja djece.

Dobra praksa je uporaba umjetne inteligencije u identificiranju materijala koji se odnosi na seksualno zlostavljanje djece.

Microsoft u borbi protiv iskorištavanja djece koristi *PhotoDNA*, *Google API* za sigurnost sadržaja. *Facebook* je također razvio tehnologije za otkrivanje sadržaja seksualnog zlostavljanja djece. Poznate kao PDQ i TMK + PDQF, ove tehnologije su dio skupa alata koje *Facebook* koristi za otkrivanje štetnog sadržaja.

Ove tehnologije stvaraju učinkovit način pohrane datoteka u obliku digitalnih otisaka (heševa) koji mogu utvrditi da li su dvije datoteke iste ili slične, čak i bez izvorne slike ili video zapisa. PDQ i TMK + PDQF su izrađeni za rad u okruženjima koja rade sa velikim brojem slika, podržavajući haširanje video-frejmova i slika u stvarnom vremenu.

Upute za kreatore politika o zaštiti djece na internetu

Ove Upute iz 2020. godine uzimaju u obzir relevantna istraživanja, postojeće modele i materijale i daju jasne preporuke za razvitak nacionalne strategije zaštite djece na internetu:

- Zaštita djece na internetu i uvid u nedavna istraživanja, uključujući aspekte novih tehnologija, ključnih prijetnji i šteta za djecu
- Kako se pripremiti za nacionalnu strategiju zaštite djece na internetu, uključujući referncne interesne strane, postojeće primjere reagovanja na prijetnje i štete na internetu i koristi postojanja nacionalne strategije.
- Preporuke za okvire i provedbu.
- Nacionalni kontrolni popisi za razvitak nacionalne strategije zaštite djece na internetu.
- Korisne referencne materijale.

Razvitak nacionalne strategije zaštite djece na internetu trebao bi:

- zasnivati se na temelju cijele vizije koja uključuje vladu, industriju i društvo;
- biti rezultat sveobuhvatnog razumijevanja i analize cijelokupnog digitalnog okruženja, a ipak prilagođen okolnostima i prioritetima zemlje;
- poštovati i biti usaklađen sa suštinskim pravima djece utvrđenim UN Konvencijom o pravima djeteta i drugim ključnim međunarodnim konvencijama i zakonima;
- poštovati i biti dosljedan postojećim, sličnim i srodnim domaćim zakonima i strategijama koje su na snazi, kao što su zakoni o zlostavljanju djece ili strategije sigurnosti djece;
- poštovati dječja građanska prava i slobode, koje ne bi trebalo žrtvovati radi zaštite;
- biti razvijen uz aktivno sudjelovanje svih relevantnih interesnih strana, uključujući djecu, rješavajući njihove potrebe i odgovornosti i zadovoljavajući potrebe manjinskih i marginaliziranih skupina;
- biti dizajniran sukladno širim vladinim planovima za gospodarsko i socijalno blagostanje i da maksimalizira doprinos IKT održivom razvoju i socijalnoj inkluziji;
- koristiti najprikladnije dostupne instrumente politike za ostvarenje svog cilja, uzimajući u obzir specifične okolnosti zemlje;
- biti postavljen na najviši nivo vlasti, koja će biti odgovorna za dodjeljivanje relevantnih uloga i odgovornosti i raspodjelu dostatnih ljudskih i financijskih resursa;
- pomoći u izgradnji digitalnog okruženja u koje djeca, roditelji / staratelji i interesne strane mogu imati povjerenje;
- usmjeriti napore interesnih strana na pružanje mogućnosti i obrazovanje djece o digitalnoj pismenosti kako bi se zaštitili na internetu.

Transnacionalni modeli za zaštitu djece na internetu

Prema globalnom karakteru interneta, globalnom protoku i globalnoj razmjeni informacija, koji su istovremeno rezultirali i brojinim izazovima i problemima sa kojima se korisnici interneta svakodnevno susreću, na međunardnoj razini kreirani su različiti modeli osiguranja zaštite djece u stvarnom, fizičkom i virtuelnom svijetu. U srži ovih modela su različite strategije koje ukazuju na nužnost uspostave sigurnijeg digitalnog okruženja za djecu, koje se neizbježno odražava i na njihov fizički, tj. stvarni

svijet, nužnost uspostave višestrukog pristupa na nacionalnim razinama uz poštivanje međunarodnih standarda u području zaštite djece na internetu, zatim nužnost kontinuiranog revidiranja nacionalnih regulatornih okvira i politika sukladno dinamici tehnoloških inovacija i istovremenog podizanja razine korporativne društvene odgovornosti.

Ranije razrađene upute koje je kreirala Međunarodna unija za telekomunikacije (ITU) u suradnji sa radnom skupinom autora iz vodećih institucija aktivnih u sektoru informacijskih i komunikacijskih tehnologija (IKT), kao i o pitanjima dječje zaštite (na internetu) i za ovo područje relevantnim organizacijama, nude niz korisnih pristupa i modela aplikacija koji značajno mogu doprinijeti unaprjeđenju zaštite djece na internetu na nacionalnoj i internacionalnoj razini.

Svrha ovih uputa je ponuditi kreatorima politika u državama članicama ITU-a jednostavan i fleksibilan okvir za razumijevanje i postupanje prema njihovoj zakonskoj obvezi da osiguraju zaštitu djece u stvarnom, fizičkom i virtualnom svijetu. Upute to čine bavljenjem sa nekoliko važnih pitanja za kreatore politika:

1. Što je zaštita djece na internetu?
2. Zašto se ja kao kreator politika moram brinuti o zaštiti djece na internetu?
3. Koji je pravni, društveno-politički i razvojni kontekst moje zemlje?
4. Kako kreatori politika trebaju početi razmatrati i oblikovati učinkovitu i održivu politiku zaštite djece na internetu u svojoj zemlji?

Upute se oslanjaju na postojeće modele, okvire i resurse kako bi pružile kontekst i uvid u dobru praksu iz cijelog svijeta.

Jedna od ključnih interesnih strana koji je obuhvaćen ovim uputama je industrija, jer ona posjeduje tehnološko znanje koje kreatori politika trebaju za rješavanje i razumijevanje problema kako bi razvili odgovarajući pravni okvir.

Važno je potaknuti industriju da u svoje poslovanje ugradi sigurnosni pristup već u samom dizajnu pri razvoju nove tehnologije. Jasno je kako bi tvrtke koje razvijaju ili pružaju nove tehnološke proizvode i usluge trebale pomoći svojim korisnicima da shvate kako oni rade i kako ih sigurno i na odgovarajući način koristiti. Osim toga, industrija ima veliku odgovornost da pomogne u promoviranju svijesti o internetu i sigurnosti, posebno djeci i njihovim roditeljima ili skrbnicima, ali i široj zajednici. Uključujući se na ovaj način, interesne strane u industriji saznat će više o brigama ostalih interesnih strana, te rizicima i štetama kojima su krajnji korisnici izloženi. S tim znanjem, industrija može unaprijediti postojeće proizvode i usluge i prepoznati opasnosti tijekom razvoja. Ova dostignuća, također, mogu predstavljati nove rizike za djecu. U nekim zemljama internetom se upravlja u okviru samoregulacije ili koregulacije. Međutim, neke zemlje razmatraju ili su provele zakonske i regulatorne okvire, uključujući obveze za tvrtke da otkriju, blokiraju i / ili uklone štetne sadržaje za djecu s platformi ili usluga, kao i da pruže jasne putove prijavljivanja i pristup tehničkoj i drugoj potpori.

U ovim Uputama se navodi da pružatelji usluga mogu otkriti, blokirati i prijaviti nezakonit sadržaj u svojoj mreži i pružiti odgovarajuće alate, usluge i konfiguracije koje roditelji mogu koristiti u odabiru načina upravljanja pristupom internetu njihove djece. Važno je da pružatelji usluga podjednako osiguraju poštovanje građanskih sloboda i privatnosti.

Preporuke za provedbu, specifične za industriju, definiraju da nacionalni i međunarodni predstavnici industrije trebaju raditi na podizanju svijesti o problemima dječje sigurnosti na internetu i pomoći svim odraslim osobama odgovornim za dobrobit djeteta - uključujući roditelje i skrbnike, škole, organizacije koje pružaju usluge mladima i zajednice - da razviju znanje i vještine koje su im potrebne da čuvaju djecu sigurnom. Industrija bi trebala usvojiti pristup sigurnosti prilikom samog dizajna svojih proizvoda, usluga i platformi, prepoznajući sigurnost kao glavni cilj. Industrija treba pružiti odgovarajuće alate prilagođene obiteljima kako bi svojim korisnicima pomogli da bolje upravljaju zaštitom svojih obitelji na internetu. Osim toga, industrija treba osigurati odgovarajuće mehanizme za svoje korisnike u svrhu prijavljivanja problema i nedoumica. Korisnici bi trebali očekivati pravodobne odgovore na upite koji sadrže informacije o poduzetim radnjama i, ako je primjenjivo, instrukcije gdje korisnici mogu dobiti daljnju potporu. Također, industrija treba promovirati proaktivno prijavljivanje zlostavljanja djece kako bi se otkrila i riješila bilo koja vrsta zlostavljanja (klasificiranog kao kriminalna aktivnost) djece. Ova praksa je pokazala da je, ako sve interesne strane doprinesu otkrivanju, blokiranju i prijavljivanju, moguće razmišljati o tome da postoji sigurniji internet za sve, uključujući i djecu.. Industrija treba razmotriti mogućnost upotrebe svih relevantnih alata u cilju sprječavanja iskorištavanja svojih platformi, poput IWF usluga.

Globalni savez *WePROTECT*, Globalni strateški odgovor na seksualno iskorištavanje i zlostavljanje djece na internetu

Strategija *WePROTECT* Globalnog saveza podržava zemlje da razviju koordinirane odgovore više dionika za borbu protiv seksualnog iskorištavanja djece na internetu, vođene svojim Modelima nacionalnog odgovora (MNR). Model nacionalnog odgovora Globalnog saveza *WePROTECT* djeluje kao nacrt za nacionalnu akciju. Pruža okvir za zemlje na koji bi se trebale osloniti da se pozabave seksualnim iskorištavanjem djece na internetu (OCSE).

Model je namijenjen da pomogne zemlji da:

- procijeni trenutačni odgovor na seksualno iskorištavanje djece na internetu i utvrdi nedostatke:
- da prioritet nacionalnim naporima pri popunjavanju praznina;
- poboljša međunarodno razumijevanje i suradnju

Model ne nastoji propisati aktivnosti ili postavliti jedinstveni pristup. Njegova svrha je opisati vještine potrebne za učinkovitu zaštitu djece i podržati zemlje da razviju ili poboljšaju svoje postojeće sposobnosti. Također, navodi niz mogućnosti koje će, ako postoje i budu učinkovite, ubrzati i poboljšati ishode. Model nacionalnog odgovora uključuje dvadeset i jednu sposobnost, podijeljenu u šest odjela: politika i upravljanje, kazneno pravosuđe, žrtve, društvo, industrija i mediji i komunikacije. Globalni savez *WePROTECT* vjeruje da će djelovanje u svih šest područja pružiti potpun nacionalni odgovor na ovaj zločin.

Globalni strateški odgovor (GSR) *WePROTECT* Globalnog saveza koordinirani je pristup borbi protiv seksualnog iskorištavanja djece na internetu koji uključuje veći globalni uvid, međunarodno usklađivanje nacionalnih pristupa i globalna rješenja koja nadilaze nacionalni odgovor. Globalni strateški odgovor je u osnovi propratni dio Modela nacionalnog odgovora (MNR); dok je Model nacionalnog odgovora usmjeren na sposobnosti potrebne za rješavanje seksualnog iskorištavanja djece na internetu na nacionalnoj razini, globalni strateški odgovor je usmjeren na prioritetna područja za međunarodnu suradnju i izgradnju kapaciteta.

Globalni strateški odgovor uključuje šest tematskih područja, sa povezanim potrebnim mogućnostima i očekivanim ishodima za svako područje, kao i partnere koji bi trebali raditi zajedno preko granice kako bi ih postigli. Ovim strateškim odgovorom predviđeno je šest sljedećih područja:

- politika i zakonodavstvo;
- kazneno pravosuđe;
- utjecaj na žrtve i usluge;
- tehnologija;
- društvo;
- istraživanje i uvid.

Preporuka OECD-a (Organisation for Economic Co-operation and Development/Organizacija za gospodarsku suradnju i razvoj) u pogledu bezbjednosti djece na internetu

Preporuka OECD-a u pogledu bezbjednosti djece na internetu (eng. *Recommendation of the Council on Children in the Digital Environment*) je usvojena 16.02.2012. godine, a ažurirana je 16.05.2021. godine. Prilikom ažuriranja usvojen je i dokument Upute OECD-a za pružatelje digitalnih usluga (eng. OECD *guidelines for digital service providers*).

Dok su pružatelji digitalnih usluga pozvani da poštuju Upute u cjelini, posebne mjere koje pojedinačni pružatelji digitalnih usluga poduzimaju mogu značajno varirati, uzimajući u obzir čimbenike kao što su nacionalni pravni i regulatorni okvir u kojem djeluju, kao i razlike u njihovim ulogama i profilima rizika koji su povezani sa uslugama i proizvodima koje pružaju, pri čemu

mjere koje poduzimaju treba da budu njima primjerene.

Pri razvoju i i pružanju usluga koje su namijenjene djeci ili gdje je razumno predvidljivo da će im djeca pristupati ili ih koristiti, pružatelji digitalnih usluga treba da poduzmu odgovarajuće mjere opreza:

- obratiti pozornost osiguravanja sigurnog i korisnog digitalnog okruženja za djecu kroz dizajn, razvoj, primjenu i rad takvih proizvoda i usluga, uključujući primjenu "safety-by-design" pristupa;
- redovito poduzimati potrebne korake kako bi se djeci onemogućio pristup uslugama i sadržajima koji ne bi trebalo da im budu dostupni, a koji bi mogli biti štetni po njihovo zdravlje i dobrobit ili koji krše bilo koje od njihovih prava,
- redoviti revidirati i ažurirati procedure kako bi se u obzir uzele promjene u tehnologiji, promjene u uporabi, i posljedične promjene u rizicima za djecu,
- kada zakoni ili politike zahtjevaju da postoje ograničenja na temelju dobi kako bi se onemogućila djeca mlađa od određene dobi za pristup usluzi, postaviti odgovarajuća ograničenja koja su proporcionalna riziku i koja poštuju privatnost.

U pružanju informacija djeci i njihovim roditeljima ili skrbnicima, a u vezi sa uslugama za djecu, ili tamo gde je razumno predvidljivo da će im djeca pristupati ili ih koristiti, pružatelji digitalnih usluga trebaju obezbjediti informacije koje su sažete, razumljive, lako dostupne i formulirane jasnim, jednostavnim jezikom koji odgovara dobi djece. Ovo uključuje, ali nije ograničeno na, informacije o postavkama privatnosti, pohrani podataka, uvjetima korištenja usluge, politikama i standardima.

Ako pruža digitalne usluge koje su namijenjene djeci, ili gde je to razumno predvidljiva da će im djeca pristupiti ili ih koristiti, i koji prikupljaju, obrađuju, dijele i koriste osobne podatke, pružatelji digitalnih usluga treba da:

- djeci i njihovim roditeljima i skrbnicima, pruže informacije o tome kako se to njihovi osobni podaci prikupljaju, pohranjuju, stavljaju na raspolaganje ili na drugi način koriste, a na jeziku koji je sažet, razumljiv, jasan i primjeren dobi,
- ograničiti prikupljanje osobnih podataka i njihovu kasniju upotrebu ili otkrivanje trećim osobama, a u najboljem interesu djeteta,
- ne koriste podatke o djeci na bilo koji način koji za djecu može biti štetan,
- ako za to ne postoji valjan razlog i ako postoje odgovarajuće mjere zaštitite djece od štetnih utjecaja, ne smije se dozvoliti profiliranje dece ili automatizirano odlučivanje, uključujući i platforme za e-učenje.

Pružatelji digitalnih usluga treba da uspostave politike i procedure za promoviranje najboljih interesa djece koja pristupaju njihovim uslugama i koriste njihove proizvode. Pružatelji digitalnih usluga bi trebalo da budu u stanju da demonstriraju usklađenost sa svim domaćim politikama, propisima ili zakonima koji su na snazi, a koji se odonse na zaštitu prava djece u digitalnom okruženju.

Projekat *deSHAME - Facebook* i Evropska unija

Facebook je, u nastojanju da suzbije seksualno uznemiravanje na digitalnim platformama, zajedno sa Europskom unijom, sufinancirala projekat *deSHAME*. Cilj ovog projekta je povećati prijavljivanje seksualnog uznemiravanja putem interneta među maloljetnicima i poboljšati višesektorsku suradnju u prevenciji i reagiranju na ovakvo ponašanje. Kako je jedan od glavnih ciljeva *deSHAME* projekta pozicanje korisnika da prijavljuju sadržaje koji su uznemiravajućeg karaktera ili su neprimjereni, *Facebook*-ovi standardi zajednice također su relevantni kao upute o tome šta je dopušteno. *Facebook je* stvorio niz sigurnosnih mehanizama, poput mehanizma "Poznajete li ovu osobu?", *inbox*-a koji prikuplja nove poruke od ljudi koje korisnik ne poznaje, te *popup* prozora koji se pojavljuje na obavijestima u slučaju kada je maloljetnika kontaktirala odrasla osoba koju on ili ona ne poznaje.

Ministarski dobrovoljni principi pet država za borbu protiv seksualnog iskorištavanja i zlostavljanja djece

Ministarski savez od pet država čine Australija, Kanada, Novi Zeland, Velika Britanija i Sjedinjene Američke Države.

Njihov cilj je prevencija seksualnog iskorištavanja i zlostavljanja djece. U tu svrhu, pet vlada, nakon savjetovanja sa vodećom skupinom predstavnika industrije, razvilo je ovaj skup dobrovoljnih načela.

Dobrovoljna načela uspostavljena 2020. godine su:

- Spriječiti uporabu materijala o seksualnom zlostavljanju djece i poduzeti odgovarajuće mjere.
- Identifikacija i borba protiv oglašavanja, regrutacije djeteta radi seksualnog iskorištavanja ili zlostavljanja.
- Borba protiv korištenja usluga livestreaminga za svrhu seksualnog iskorištavanja i zlostavljanja djece,
- Spriječavanje da se rezultati pretraživanja materijala seksualnog iskorištavanja i zlostavljanja djece pronađu i spriječavanje automatskih prijedloga za takve aktivnosti i materijal.
- Pojačane mjere sigurnosti s ciljem zaštite djece, posebno od vršnjaka ili odraslih koji žele da se upuste u štetne seksualne aktivnosti s djecom
- Provjera materijala koji možda nije nezakonit na prvi pogled, ali uz odgovarajući kontekst i potvrdu može biti povezan sa seksualnom eksploatacijom djece i zlostavljanjem.
- Zauzimanje globalnog pristupa u borbi protiv seksualnog iskorištavanja i zlostavljanja djece na internetu uzimajući u obzir razvoj prijetnji kao dio svojih procesa dizajna i razvoja.

Globalno partnerstvo i fond za zaustavljanje nasilja nad djecom, Sigurno za učenje: Poziv na akciju

Globalno partnerstvo i fond za zaustavljanje nasilja nad djecom pokrenuo je glavni tajnik Ujedinjenih naroda 2016. godine sa jednim ciljem: kataliziranje i podupiranje mjera za ustavljanje svih oblika nasilja nad djecom do 2030. godine, kroz jedinstvenu suradnju preko 400 partnera iz svih sektora. Fokus rada je na spašavanju i pružanju potpore žrtvama, tehnološkim rješenjima za otkrivanje i sprječavanje prekršaja, potpora tijelima za provedbu zakona, zakonodavnim i političkim reformama, i generiranju podataka i dokaza o razmjerama i prirodi seksualnog iskorištavanja i zlostavljanja djece na internetu, kao i razumijevanju dječjih perspektiva.

Dječje dostojanstvo u digitalnom svijetu, Savez za dostojanstvo djeteta: Izvješće radne skupine za tehnologiju

U ovom dokumentu iz 2018. godine predstavljene su glavne prepreke optimalnom globalnom odgovoru na onlajn materijal o seksualnom zlostavljanju djece u sljedeća tri područja: provedba zakona, industrija i vlada. Utvrđene barijere su detaljno opisane u izvješću, i date su konkretne preporuke za svaki sektor. Date su i preporuke za zajedničko djelovanje.

Između ostalog, u ovom istraživanju utvrđena je potreba za većom standardizacijom procesa, praksi i politika, kao i potreba za većom suradnjom, koordinacijom i interoperabilnošću zainteresovanih strana.

Osnovane su četiri skupine inicijativa, i to: vladine inicijative, inicijative za provedbu zakona, industrijske inicijative i zajedničke inicijative.

Velike tehnološke tvrtke kao što su *Facebook, Twitter, Google, Snap, Microsoft* i druge bi trebalo da nastave podupirati napore tijela za provedbu zakona, državne entitete i neprofitne organizacije za prijavu incidenata, te da omoguće dijeljenje podataka odgovarajućem formatu i obliku, poput *hash* podataka.

Industrija mora da radi kolektivno na razvoju odgovarajućih tehničkih alata kao što su AI klasifikatori i algoritmi heširanja, a u cilju otkrivanja neželjenog sadržaja.

Industrija treba da surađuje i razmjenjuje operativne podatke i obavještajne podatke o onima koji zloupotrebljavaju svoje mreže za deljenje i distribuciju neželjenog materijala o djeci. Ovdje prvenstveno velike tvrtke koje imaju odgovarajuće podatke treba da iste podijele sa manjim tvrtkama koje takve podatke nemaju.

Tvrtke koje upravljaju značajnim dijelom internet infrastrukture, uključujući ICANN i registre domena, moraju poduzeti potrebne korake za poboljšanje procesa verifikacije identiteta korisnika, naročito pri registriranju novog domena ili u procesu obnove istog.

Industrija treba spriječiti iskorištavanje servisa od predatora, a u cilju zlostavljanja djece na internetu. Ovdje je bitno da vlasnici interaktivnih platformi i servisa prikupljaju detaljnije i tačnije informacije o svojim korisnicima. Ovo će omogućiti proaktivno djelovanje, tj. identifikaciju potencijalnih predatora i ranjivih korisnika, osobito djece.

Opća uredba Europske komisije o zaštiti osobnih podataka

Općom uredbom Europske komisije o zaštiti osobnih podataka, iz 2018. godine, propisuju se pravila zaštite fizičkih osoba tijekom obrade osobnih podataka i pravila u vezi sa slobodnim kretanjem osobnih podataka. Ovom uredbom se štite osnovna prava i slobode fizičkih osoba, a posebice njihovo pravo na zaštitu osobnih podataka. Slobodno kretanje podataka unutar EU se ne smije ograničavati ili zabranjivati iz razloga koji se odnose na zaštitu fizičkih osoba prilikom obrade osobnih podataka.

Ova uredba se primjenjuje na obradu osobnih podataka koja se u cijelosti ili djelomično obavlja automatski i na neautomatiziranu obradu osobnih podataka koji čine dio sustava pohranjivanja ili su namijenjeni da budu dio sustava pohranjivanja.

Ova uredba se ne primjenjuje na obradu osobnih podataka:

- u okviru djelatnosti koja nije obuhvaćena područjem primjene prava EU,
- koju obavlja fizička osoba prilikom isključivo osobne ili kućne aktivnosti,
- koju provode nadležna tijela u svrhu sprječavanja, istrage, otkrivanja ili gonjenja kaznenih djela ili izvršenja kaznenih sankcija, uključujući i zaštitu od prijetnji za javnu sigurnost i njihovo sprječavanje.

Osobni podaci moraju da budu:

- obrađeni zakonito, pošteno i transparentno u odnosu na osobu na koju se podaci odnose („zakonitost, pravednost i transparentnost“),
- prikupljeni u određene, izričite i zakonite svrhe i ne smiju dalje da se obrađuju na način koji nije sukladan s tim svrhama („ograničavanje svrhe“),
- primjereni, relevantni i ograničeni na ono što je neophodno u svrhe u koje se obrađuju („korištenje najmanje moguće količine podataka“),
- točni i prema potrebi ažurirani; potrebno je poduzeti sve prihvatljive mjere kako bi se obezbijedilo da osobni podaci koji nisu tačni, imajući u vidu svrhe u koje se obrađuju, budu bez odlaganja obrisani ili ispravljeni („točnost“),
- pohranjeni u obliku koji omogućuje identifikaciju osoba na koje se podaci odnose i to ne dulje nego što je potrebno u svrhe u koje se podaci obrađuju; osobni podaci mogu da se pohranjuju u dužem periodu ako će se obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, s tim da moraju da se poduzmu odgovarajuće tehničke i organizacijske mjere propisane ovom uredbom radi zaštite prava i sloboda osoba na koja se podaci odnose („ograničenje čuvanja“),
- obrađeni na način kojim se obezbjeđuje odgovarajuća sigurnost osobnih podataka, uključujući i zaštitu od neovlašćene ili nezakonite obrade i od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera („integritet i povjerljivost“).

Uredba propisuje i pravila zakonitosti obrade, uvjete za pristanak za obradu ospbnih podataka, te uvjete koji se primjenjuju na pristanak djeteta u vezi sa uslugama informacijskog društva i dr.

Obrada podataka djeteta je zakonita ako dijete ima najmanje 16 godina. Ako je dijete mlađe od 16 godina, takva obrada je zakonita samo ako i u mjeri u kojoj je pristanak dao ili odobrio skrbnik djeteta. Države članice mogu u ove svrhe zakonom da predvide nižu dobnu granicu, pod uvjetom da takva niža dobna granica nije niža od 13 godina. Kontrolor podataka mora učiniti sve što je u njegovoj moći da u takvim slučajevima provjeri da li je pristanak dao ili odobrio skrbnik djeteta, uzimajući u obzir dostupnu tehnologiju.

Osobi na koju se podaci odnose moraju se dostaviti sve potrebne informacije i sva neophodna saopćenja u vezi sa obradom u sažetom, transparentnom, razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika, što se posebno odnosi na sve informacije koje su izričito namijenjene djetetu. Informacije se pružaju u pisanom obliku ili na druge načine, uključujući i elektronički obrazac kada je to primjereno.

Izvještaji o indeksu digitalne učtivosti (*Microsoft*)

U kontekstu internetskog ili sajber maltretiranja, *Microsoft* je proveo istraživanje digitalne sigurnosti i sajber maltretiranja. Djeca od 8 do 17 godina 2012. godine anketirana su u 25 zemalja, o negativnom ponašanju na internetu. Rezultati su pokazali da je u prosjeku 54% sudionika navelo da se brinu da će biti maltretirani na internetu, 37% je izjavilo da su doživjeli sajber maltretiranje, a 24% je otkrilo da su nekoga maltretirali. Isto istraživanje je pokazalo da je manje od 30% roditelja razgovaralo sa djecom o nasilju na internetu. Od 2016. *Microsoft* provodi redovito istraživanje rizika na internetu dajući godišnja izvješća o indeksu digitalne učtivosti. Izvješća su dostupni za brojne zemlje Sjeverne i Južne Amerike, Azije i Europe.

Multimedijalni program FACES (NHK Japan i javni servisi - prihvatili Facebook, UNESCO, Vijeće Europe)

FACES je multimedijalni program koji je stvorio NHK Japan i konzorcijum različitih javnih servisa sa pričama o žrtvama nasilja na internetu i izvan njega, širom svijeta. Serija se sastoji od portreta adolescenata u kojima protagonisti pred kamerama objašnjavaju kako su reagirali na napade putem interneta. Seriju, koja je također nastala i u formi dvominutnih video isječaka, prihvatili su *Facebook,* UNESCO, i Vijeće Europe, i dostupna je na mnogim jezicima.

Dokument o pravima djeteta i igranje na internetu: Mogućnosti i izazovi za djecu i IKT industriju (UNICEF)

U 2019. godini, UNICEF je objavio dokument o pravima djeteta i igranje na internetu: Mogućnosti i izazovi za djecu i IKT industriju, a kako bi se odgovorilo mogućnostima i izazovima za djecu u jednoj od najbrže rastućih industrija zabave. Ovaj rad istražuje sljedeće teme:

- pravo djece na igru i slobodu izražavanja (vrijeme igranja i zdravstveni ishodi),
- nediskriminacija, sudjelovanje i zaštita od zlostavljanja (socijalna interakcija i uključenost, toksična okruženja, dob i provjera, zaštita od vrbovanja i seksualnog zlostavljanja),
- pravo na privatnost i slobodu od ekonomskog iskorištavanja (poslovni modeli za pristup podacima, besplatne igre i monetizacija, nedostatak transparentnosti u komercijalnom sadržaju).

Nacionalni modeli za zaštitu djece na internetu

Kodeks dizajna prilagođen dobi/ Introduction to the Age appropriate design code - Velika Britanija

Početkom 2019. godine Ured zaklade za informiranje objavio je prijedloge za svoj Kodeks za dizajniranje prilagođeno dobi radi unaprjeđenja zaštite dječijih podataka. Ovim Kodeksom se, kako je navedeno, ne nastoje djeca zaštiti od digitalnog svijeta, već da se zaštite u njemu. Predloženi Kodeks temelji se na najboljem interesu za djecu, kako je utvrđeno u Konvenciji o pravima djeteta UN-a, i u njemu je iznijeto nekoliko očekivanja od IKT tvrtki. Kodeks se sastoji od sljedećih petnaest standarda:

- Najbolji interesi djeteta - primarni čimbenik u dizajniranju i razvijanju internetskih usluga kojima će dijete vjerovatno pristupiti.
- Procjena utjecaja na zaštitu podataka - poduzimanje DPIA (Data Protection Impact Assessments) kako bi se procijenili i otklonili rizici po prava i slobode djece koji su sposobni da pristupe usluzi, a koji proizlaze iz obrade podataka. Uvažavanje različitih uzrasta, kapaciteta i razvojnih potreba i osiguravanje uspostavljanja DPIA sukladno s ovim kodeksom.
- Primjena prema dobi– primjena pristupa koji podrazumijeva prepoznavanje starosne dobi korisnika i omogućavanje efektivne primjene standarda ovog kodeksa za djecu kao korisnike ili primjena standarda ovog kodeksa za sve korisnike.
- Transparentnost - informacije o privatnosti, kao i drugi uvjeti, politike i standardi moraju biti sažeti, istaknuti i navedeni jezikom koji je prilagođen djeci u smislu njihove razumljivosti.
- Štetna uporaba podataka, tj. korištenje osobnih podatka djece na načine koji ugrožavaju njihovu dobrobit ili koji su u suprotnosti s kodeksima prakse u industriji, drugim regulatornim odredbama ili savjetima vlade.
- Pravila i standardi zajednice - pridržavanje objavljenih uvjeta, politike i standarda zajednice (uključujući, ali ne ograničavajući se na politiku privatnosti, dobna ograničenja, pravila ponašanja i politike sadržaja).
- Unaprijed postavljene postavke - postavke moraju biti označene kao "visoka privatnost" (osim ako postoji uvjerljiv razlog za drugu zadanu postavku, uzimajući u obzir najbolji interes djeteta).
- Minimiziranje podataka - prikupljanje i zadržavanje samo minimalne količine osobnih podataka potrebnih za pružanje usluge, u čemu je dijete aktivno i svjesno uključeno. Pružanje izbora djeci koje elemente žele aktivirati.
- Razmjena podataka - neotkrivanje podataka o djeci, osim opravdanog razloga i u tom slučaju uvažavajući najbolji interes djeteta.
- Geolokacija - isključiti opcije geolokacije prema zadanim postavkama. Omogućiti djeci očigledan znak kada je praćenje lokacije aktivno. Opcije koje čine lokaciju djeteta vidljivom drugima moraju se prema zadanim postavkama vratiti na 'isključeno' na kraju svake sesije.
- Roditeljski nadzor - omogućavanje roditeljskog nadzora i pružanje odgovarajućih informacija djetetu o tome. Ako internetska usluga omogućava roditelju ili skrbniku da prati aktivnosti svog djeteta na mreži ili da prati njegovu lokaciju, potrebno je dati očigledan znak djetetu kada ga roditelj/slrbnik promatrae.
- Profiliranje - dozvoliti profiliranje samo ako postoje odgovarajuće mjere za zaštitu djeteta od bilo kakvih štetnih učinaka (posebice sadržaja koji je štetan za njihovo zdravlje ili dobrobit).
- Tehnike "pritiska" - nisu prihvatljive tehnike "pritiska" usmjerene na poticanje ili ohrabrivanje djece da daju nepotrebne osobne podatke, oslabe ili da isključe zaštitu privatnosti.
- Povezane igračke i uređaji - povezivanje igračaka ili uređaja, trebalo bi da podrazumijeva uključivanje efikasnih alata za omogućavanje usklađenosti s ovim kodeksom.

- *Online* alati – istaknut i omogućen pristup alatima koji će pomoći djeci da ostvare svoja prava na zaštitu podataka i da prijave probleme.

Bijela knjiga *'Online Harms'* /Bijela knjiga o štetnim onlajn sadržajima

Odjel za kulturu, medije i sport Vlade Velike Britanije objavilo je u travnju 2019. godine Bijelu knjigu *'Online Harms'* koja bi u zakonu uspostavila novu obvezu skrbi prema korisnicima od strane platformi, koju će nadgledati neovisni regulator za sigurnost na internetu. Svojim sadržajem određuje mjere vlade za suzbijanje onlajn sadržaja ili aktivnosti koje štete pojedinim korisnicima, posebice djeci.

„Uz posebnu referencu na djecu koja pristupaju neprikladnom sadržaju, na primjer, neka od područja koja regulator treba uključiti u kodeks prakse su sljedeća:

- Koraci koje tvrtke trebaju poduzeti kako bi osigurale da je sigurnost integrirana u sam dizajn njihovih usluga. To može uključivati postojanje računa s različitim postavkama za djecu.
- Uvjeti pružanja usluge trebali bi razjasniti kakvo se ponašanje i aktivnost toleriraju kada je u pitanju korištenje usluge i postojeće mjere za sprječavanje djece da pristupe neprimjerenom sadržaju koje bi djeca i roditelji mogli lako razumjeti.
- Koraci koje poduzeća trebaju poduzeti kako bi osigurala da djeca ne mogu pristupiti neprikladnom sadržaju, uključujući upute za dobnu provjeru, upozorenja o sadržaju i mjere za filtriranje i blokiranje neprikladnog sadržaja.
- Mjere kojima se osigurava da su postupci prijavljivanja prikladni za postupanje u vezi sa štetnim sadržajem i da su jasni, vidljivi i jednostavni za djecu i roditelje. Korisnici bi trebali dobiti jasna objašnjenja donesenih odluka.
- Usluge imaju učinkovite i transparentne procese za moderiranje ove vrste sadržaja i aktivnosti. Korisnici su uvijek u tijeku s izvješćem o napretku,
- Koraci koje tvrtke trebaju poduzeti kako bi osigurale da se sporno pitanje štetnog materijala brzo rješava, poput uklanjanja sadržaja koji krši uslove pružanja usluge.
- Trebali bi postojati procesi unutar usluga kojima bi se osiguralo da se korisnici mogu žaliti na uklanjanje sadržaja ili neka druga vrsta odgovora kako bi se zaštitila prava korisnika na Internetu.
- Koraci za sprječavanje korisnika kojima je izrečena mjera zabrane da otvaraju nove račune kako bi nastavili kreirati neprikladni sadržaj koji krši uvjete pružanja usluge."[48]

Uloga javnih servisa u zaštiti djece na internetu

Primjeri dizajna primjerenog dobi uključuju posebne ponude nekih od velikih javnih servisa za određene dobn skupine. Tako, na primjer, njemački ARD (*Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland - Das Erste*) i *ZDF (Zweites Deutsches Fernsehen)* ciljaju svoju publiku počevši od 14 godine, nudeći prilagođeni sadržaj putem internet kanala funk.net.

BBC (*British Broadcasting Corporation*/ Britanska radiodifuzna korporacija) je pokrenuo *CBeebies* obrazovni televizijski kanal namijenjen djeci mlađoj od 6 godina. Ovaj kanal je osnovan s ciljem da unaprijedi učenje kroz igru u sigurnom okruženju i da obezbijedi kvalitetnu domaću produkciju. Kontinuirano nudi nove sadržaje namijenjene medijskoj publici ove dobi, obrazovnog i zabavnog karaktera. BBC je izradio i *CBeebies* edukativnu *web* stranicu. Sadržaj ove *web* stranice je posebno prilagođen odgovarajućim dobnim skupinama. Za sigurnost djece od 8 do 13 godina ponuđena je i mobilna aplikacija *Own IT.*

[48] Prema: Jean-François Furnémont (Wagner-Hatfield), Pregled odredbi Kodeksa o audiovizuelnim uslugama u vezi s zaštitom maloljetnika, 2020.

Također, Uredničke upute BBC-a predstavljaju opsežan dokument kojim su značajnim dijelom obuhvaćeni segmenti prvenstveno relevantni za zaštitu djece u digitalnom okruženju. Dokumentom su obuhvaćeni standardi i vrijednosti BBC-a, razrađeni kroz 18 odjeljaka/sekcija. U kontekstu zaštite interesa djeteta značajan je Odjeljak 9: Djeca i mladi kao suradnici, iako su i pojedinim ostalim odjeljcima također obuhvaćena načela važna u ovom kontekstu. U navedenom Odjeljku 9 posebno su razrađeni principi na kojima se temelji zaštita dobrobiti djece i mladih. Neki od njih su:

- da sva djeca i mladi imaju pravo na zaštitu od ozljeda i zlostavljanja;
- da informacije koje otkrivaju o djeci i mladima ne smiju ih izlagati riziku od ozljeda;
- da je zaštita djece i mladih na internetu zajednička je odgovornost za BBC, roditelje/staratelje i mlađe od 18 godina;
- da djeca i mladi imaju pravo glasa, ali i da ih ne smiju ohrabrivati da sudjeluju kao aktivni korisnici interneta kada su mlađi od propisane minimalne dobne granice;
- da je za pristup BBC online uslugama neophodan pristanak roditelja za određene aktivnosti;
- kada je izvjesno da će online sadržaj privući veliki broj djece i mladih da je potrebno ponuditi poveznice do relevantnih savjeta koji će im pomoći da razumiju i minimiziraju moguće rizike s kojima se mogu suočiti na mreži i da sigurnosne informacije trebaju biti istaknute, dostupne i jasne;
- da bi online prostori namijenjeni mlađim od 18 godina trebali biti prethodno moderirani;
- da je neophodna zaštita osobnih podataka djece i mladih i da ih treba koristiti u mjeri samo koliko je nužno, te da je podatke potrebno čuvati i pohranjivati sukladno BBC-jevom politikom zaštite podataka i dr.

Navedena načela sukladna su i sa BBC-jevim vodičem pod nazivom „Interakcija sa djecom i mladima na mreži". Upute su osmišljene da nude savjete proizvođačima onlajn sadržaja namijenjenih djeci i mladima. Bavi se pitanjima sigurnosti, privatnosti, pristanka i sl. Ukazuju na potrebu brzog djelovanja u situacijama koje uključuju bilo kakav oblik ugrožavnja djece i mladih u online prostoru. Vodič razrađuje i različite oblike iskorištavanja djece na internetu, kao što su vrbovanje (*grooming*), slanje eksplicitnih poruka (*sexting*), virtualno zlostavljanje (*cyber-bulling*) i druge vrste nasilnog ponašanja koje ugrožava prava djeteta.

Zakon o štetnim digitalnim komunikacijama (Novi Zeland)

Ovim zakonom iz 2015. godine *cyber* zlostavljanje je okarakterizirano kao posebno kazneno djelo i usmjereno je na širok raspon šteta, od *cyber* maltretiranja do pornografije iz osvete. Cilj mu je obeshrabriti, spriječiti i minimizirati štetnu digitalnu komunikaciju, čineći nezakonitim postavljanje digitalne komunikacije s namjerom da se izazove ozbiljna emocionalna tjeskoba kod druge osobe, i postavlja niz od deset načela komunikacije. Zakon omogućuje korisnicima da se žale neovisnoj organizaciji ako su ova načela prekršena. Prema zakonu, pojedinci mogu biti kažnjeni do 50.000 dolara ili osuđeni na dvije godine zatvora zbog namjernog napada na bilo koga s rasističkim, seksističkim, homofobnim ili vjerski netolerantnim komentarima.

Povjerenik eSafety (Australija)

Povjerenik *eSafety* je prva vladina agencija na svijetu koja se bavi sigurnošću na internetu. Osnovana 2015. godine, *eSafety* ima zakonsku ulogu da vodi, koordinira, obrazuje i savjetuje o pitanjima sigurnosti na internetu kako bi osigurala da svi Australijanci imaju sigurna i pozitivna iskustva na internetu.

eSafety upravlja istražnim programima koji se fokusiraju na čitav niz šteta, uključujući *cyber* maltretiranje djece, zlostavljanje utemeljeno na slikama i zabranjenim sadržajima. Ovlaštena je istraživati i poduzimati mjere radi rješavanja žalbi ili prijava koje uključuju ovakve vrste šteta - uključujući, u nekim slučajevima, ovlaštenja za izdavanje upozorenja pojedincima, te izdavanje naredbi pružateljima usluga na internetu za uklanjanje određenih sadržaja. Uz svoje istražne ovlasti, *eSafety* usvaja cjelovit

pristup zajednice koji se oslanja na socijalne, kulturne i tehnološke inicijative i intervencije. Preventivni, zaštitni i proaktivni napori *eSafety* agencije pružaju dobar i sustavan pristup sigurnosti na internetu.

Propisi u regiji

Sukladno primarnom cilju predmetne analize koji je usmjeren na utvrđivanje trenutne situacije u pogledu zaštite djece na internetu u BiH, u segmentu koji se odnosi na razinu korištenja mehanizama njihove zaštite od strane ISP-ova na ovom prostoru, kao korisno procijenjeno je analiziranje stanja u regiji. U tom kontekstu analizirani su mehanizmi regulacije ili samoregulacije koji djelomično ili u potpunsti normiraju ili samouređuju sferu zaštite djece na internetu. Ovaj dio analize omogućit će uvid u institucionalne i druge mehanizme, njihove potencijale i u tendencije usmjerene na ostvarivanje što sigurnijeg korištenja interneta u pjedinim zemljama regije.

Počevši od ustava kao najvišeg pravnog akta utvrđeno je da prema Ustavu Republike Srbije "dijete uživa ljudska prava pogodna za njihovu dob i stanje mentalne zrelosti" (članak 64). Ustav Crne Gore jamči djeci posebnu zaštitu od psiholoških, fizičkih, gospodarskih i drugih vrsta izrabljivanja i zlostavljanja. Stoga, pravo na sprječavanje i zaštitu djece od seksualnog iskorištavanja putem IKT-a jasno je istaknuto u ustavnim poveljama zemalja regije koje su obuhvaćene ovim istraživanjem. Obiteljski zakoni Republike Srbije i Crne Gore naglašavaju najbolji interes djeteta kao smjernicu za sve sudionike koje se bave aktivnostima vezanim za djecu, kao i obvezu države da poduzme sve potrebne mjere koje osiguravaju poštivanje, zaštitu i unaprjeđenje njihovih prava, i da ih zaštite od zanemarivanja, fizičkog i psihičkog zlostavljanja, i bilo kojeg drugog oblika iskorištavanja.

U narednim odjeljcima predstavljeni su dokumenti i mehanizmi koji jasnije i opsežnije normiraju zaštitu djece na internetu u zemljama obuhvaćenim analizom.

Srbija

Kazneni zakon Srbije

Kazneno djelo zlostavljanja i iskorištavanja dece i putem Interneta regulirano je Kaznenim zakonom. Članak 185b Kaznenog zakona (Iskorištavanje računačne mreže ili kominukacije drugim tehničkim sredstvima za izvršenje krivičnih djela protiv spolne slobode prema maloljetnoj osobi) navodi da izvršenje kaznenih djela Silovanja, Obljube nad nemoćnom osobom, Obljube nad djetetom, Obljube zlouporabom službenog položaja, Nedozvoljenim spolnim radnjama, Podvođenje ili omogućavanje vršenja spolnog odnosa, Posredovanja u vršenju prostiucije, Prikrivanje, pribavljanje i posjedovanje pornograskog materijala i iskorištavanje djece za pornografiju i poticanje maloljetnog lica na prisustvo spolnim radnjama, koristeći računalnu mrežu ili komunikaciju drugim tehničkim sredstvima da dogovori sa maloljetnikom sastanak i pojavi se na dogovorenom mjestu radi sastanka, bit će kažnjivo odgovarajućom zatvorskom kaznom. Ako je ovo djelo počinjeno prema djetetu zatvorska kazna je rigoroznija.

Nacionalni CERT Republike Srbije

Nacionalni centar za sprječavanje sigurnosnih rizika u IKT sustavima Republike Srbije osnovan je u okviru Regulatorne agencije za elektroničke komunikacije i poštanske usluge, sukladno Zakonu o informacijskoj sigurnosti. Primarna zaduženja Nacionalnog CERT-a su koordinacija prevencije i zaštite od sigurnosnih rizika u informacijsko-komunikacijskim sustavima(IKT sustavi) na nacionalnoj razini.

Nacionalni CERT prikuplja i razmjenjuje informacije o mogućim rizicima, a zatim informira, upozorava i savjetuje osobe koja upravljaju IKT sustavima, kao i javnost Republike Srbije. Nacionalni CERT prati prijavljene incidente na nacionalnoj razini i na temelju prikupljenih podataka analizira rizike i incidente sa ciljem podizanja svijesti, kako kod građana, tako i kod privrednih subjekata i tijela javne vlasti, o značaju informacijske sigurnosti.

Nacionalni CERT vodi evidenciju posebnih CERT-ova. Poseban CERT je tim koji obavlja poslove prevencije i zaštite sigurnosnih rizika u IKT sustavima unutar određene pravne osobe, skupine pravnih osoba ili oblasti poslovanja i slično. CERT ima i portal putem kojeg je moguće prijaviti odgovarajući sigurnosni incident. Nadzor nad radom Nacionalnog CERT-a u obavljanju poslova provodi Nadležno tijelo, odnosno Ministarstvo trgovine, turizma i telekomunikacija.

Uredba o sigurnosti i zaštiti djece pri korištenju informacijsko-komunikacijskih tehnologija

Uredbom o sigurnosti i zaštiti djece pri korištenju informacijsko-komunikacijskih tehnologija uređuju se preventivne mjere za sigurnost i zaštitu djece pri korištenju informacijsko-komunikacijskih tehnologija, odnosno na internetu i postupanje u slučaju povrede ili ugrožavanja sigurnosti djece na internetu. Ova uredba usvojena je na sjednici Vlade Republike Srbije 30.lipnja 2016. godine. Uredba je donesena na temelju članka 19a stavak 8. Zakona o informacionoj bezbednosti („Službeni glasnik RS", br. 6/16, 94/17 i 77/19) i članak 42. stavak 1. Zakona o Vladi („Službeni glasnik RS", br. 55/05, 71/05 – ispravka, 101/07, 65/08, 16/11, 68/12 – US, 72/12, 7/14 – US, 44/14 i 30/18 i dr. zakon).[49]

Cilj ove uredbe je da se:

- Podići razinu svijesti i znanja o prednostima i rizicima korištenja interneta i načinima sigurnog korištenja interneta,
- poboljšanje digitalne pismenosti djece, odnosno učenika, roditelja, odnosno skrbnika i nastavnika,
- poboljšati međuresorna suradnja u području sigurnosti i zaštite djece na internetu.

Ova uredba ne propisuje obveze pružatelja pristupa internetu u pogledu zaštite maloljetnika na internetu.

Nacionalni kontakt centar za sigurnost djece na internetu

Sukladno Uredbi o sigurnosti i zaštiti djece u korištenju informacijsko-komunikacijskoh tehnologija, 27. veljače 2017. godine formiran je Nacionalni kontakt centar za sigurnost djece na internetu. Kroz ovaj centar, resorno ministarstvo (Ministarstvo trgovine, turizma i telekomunikacija) provodi savjetovanje djece, roditelja, učenika i nastavnika, kao i svih ostalih građana, o prednostima i rizicima korištenja interneta i sigurnim načinima korištenja novih tehnologija kroz različite aktivnosti usmjerene na podizanje razine svijesti. Edukaciju o sigurnosti djece na internetu Nacionalni kontakt centar provodi i organiziranjem seminara, radionica, prezentacija i informiranjem tiskanim, elektroničkim i drugim medijima.

Centar je prvi, i za sada jedini, institucionalni mehanizam u regiji koji se bavi prevencijom i reagiranjem na ugrožavanje djece u digitalnom okruženju, pružajući mogućnost građanima da se besplatno obrate na broj telefona ili putem onlajn platforme „Pametno i bezbedno". Putem ove platforme omogućena je prijava štetnog, neprimjerenog i nelegalnog sadržaja i ponašanja na internetu, odnosno prijavljivanje ugroženosti prava i interesa djeteta.

Na osnovu prijave, Nacionalni kontakt centar poduzima sljedeće aktivnosti:

1. dostavlja obavijest o podnesenoj prijavi administratoru internet sajta u slučaju da navodi iz prijave ukazuju na neprimjeren ili štetan sadržaj,
2. prosljeđuje prijavu, ukoliko navodi iz prijave ukazuju na postojanje kaznenog djela, nadležnom državnom odvjetništvu, a informaciju o podnesenoj prijavi ministarstvu nadležnom za unutarnje poslove (Odjel za suzbijanje visokotehonološkog kriminaliteta), s ciljem informiranja i u svrhu borbe protiv visokotehološkog kriminala

[49] Član 19a Zakona o informacionoj bezbednosti jeste „Zaštita dece pri korišćenju informaciono-komunikacionih tehnologija": „Nadležni organ preduzima preventivne mere za bezbednost i zaštitu dece na internetu, kao aktivnosti od javnog interesa, putem edukacije i informisanja dece, roditelja i nastavnika o prednostima, rizicima i načinima bezbednog korištenja interneta, kao i putem jedinstvenog mesta za pružanje saveta i prijem prijava u vezi bezbednosti dece na internetu, i upućuje prijave nadležnim organima radi daljeg postupanja. Operator elektronskih komunikacija koji pruža javno dostupne telefonske usluge dužan je da omogući svim pretplatnicima uslugu besplatnog poziva prema jedinstvenom mestu za pružanje saveta i prijem prijava u vezi bezbednosti dece na internetu. U slučaju da navodi iz prijave upućuju na postojanje krivičnog dela, na povredu prava, zdravstvenog statusa, dobrobiti i/ili općeg integriteta deteta, na rizik stvaranja zavisnosti od korištenja interneta, prijava se prosleđuje nadležnom organu vlasti radi postupanja u skladu sa utvrđenim nadležnostima. Nadležni organ je ovlašćen da vrši obradu podataka o licu koje se obrati Nadležnom organu u skladu sa zakonom koji uređuje zaštitu podataka o ličnosti i drugim propisima (...)." https://www.paragraf.rs/propisi/zakon_o_informacionoj_bezbednosti.html

3. prosljeđuje prijavu nadležnom centru za socijalnu skrb u slučaju da navodi iz prijave ukazuju na povredu prava, zdravstvenog stanja, dobrobiti i/ili općeg integriteta djeteta, kao i obavijest nadležnom domu zdravlja o podnesenoj prijavi u slučaju da navodi iz prijave upućuju na rizik stvaranja ovisnosti od korištenja interneta
4. prosljeđuje prijavu inspekciji za informacijsku sigurnost u slučaju da navodi iz prijave upućuju na narušavanje sigurnosti ili neodgovarajuće postupanje operatera IKT sustava od posebne važnosti i obavještava podnositelja prijave o poduzetim aktivnostima u vezi sa zaprimanjem prijave.

Digitalni vodič „Deca i internet – pametno od početka"

Digitalni vodič „Djeca i internet – pametno od početka" je digitalni vodič na srpskom jeziku, namijenjen prvenstveno roditeljima/skrbnicima, odgajateljima i učiteljima djece dobi od 4-8 godina, ali i djeci i svima onima koji sudjeluju u vaspitanju i obrazovanju djece i žele da se informiraju o tome na koje načine mogu doprinijeti sigurnom i konstruktivnom korištenju digitalnih uređaja i interneta kod djece predškolskog i mlađeg školskog uzrasta.

Vodič sadrži tri odjeljka: Teme, Kviz za provjeru znanja o sigurnosti djece na internetu i Resursi, u kojima se nalaze crtići za djecu dobi 4-8 godina, rječnik za digitalno doba, brošura za roditelje, Vodič za sigurno i konstruktivno korištenje digitalne tehnologije i interneta i druge sadržaje.

Ovaj vodič nastao je 2019. godine u sklopu projekta UNICEF-a, u suradnji sa Ministarstvom prosvjete, nauke i tehnološkog razvoja i Užičkim centrom za prava djeteta, a uz potporu Telenora.

Crna Gora

Krivični zakonik Crne Gore

Kazneno zakonodavstvo Crne Gore kojim se regulira seksualno iskorištavanje djece na internetu uglavnom je usklađeno s međunarodnim standardima. Kazneni zakon Crne Gore definira veliki broj kaznenih djela u poglavlju „Kaznena djela protiv spolne slobode". Kaznenim zakonom propisane su kazne za seksualno iskorištavanje i zlouporabu djece na internetu i na drugi način. Postupanje prema djeci koja su žrtve i svjedoci zločina, ali i počinitelji, uređen je drugim zakonima, kao što je Zakon o postupanju prema maloljetnicima u kaznenom postupku, Zakon o kaznenom postupku i dr.

Kaznena djela spolnog zlostavljanja i iskorištavanja djece propisana su u Kaznenim zakonom Crne Gore, u članku 19 („Kaznena djela protiv spolne slobode").

Zakonodavstvo koje uređuje odgovornost davatelja internet usluga ili drugih tvrtki iz privatnog sektora da obavijeste policiju ako saznaju da se materijali o seksualnoj zlouporabi djece pohranjuju ili prenose putem njihovih mreža uključuje Zakon o elektroničkoj trgovini, koji obuhvaća davatelje internet usluga, i Zakon o odgovornosti pravnih osoba za kaznena djela, koji obuhvača ostale tvrtke iz privatnog sektora (članak 23).

Nacionalni tim za odgovor na sajber incidente (CIRT)

Nacionalni tim za odgovor na sajber incidente, koji djeluje unutar Ministarstva za informacijsko društvo i telekomunikacije, osnovan je 2011. godine. Tim je zadužen za reagiranje u slučaju visokotehnoloških napada na državna tijela, privredna društva i pojedince. Osim reagiranja na ove incidente, uloga tima je i obrazovna. Ovaj tim održava treninge i prezentacije u oblasti visokotehnološke sigunosti. Tim posjeduje i portal *(www.cirt.me)* zbog znatnog povećanja broja pritužbi i problema s kojima se građani suočavaju u ovom području.

Zakon o informacijskoj sigurnosti, između ostalog, definira ulogu Tima za odgovor na sajber incidente, kao tijela koje koordinira aktivnosti državnih tijela, tijela državne uprave i lokalne samouprave u provedbi mjera informacijske sigurnosti.

Elektronska linija za prijavljivanje ugroženih prava djece na internetu

U suradnji sa Ombudsmanom Crne Gore, Ministarstvo za informacijsko društvo i telekomunikacije otvorilo je elektroničku liniju za prijavljivanje nelegalnog sadržaja kojim se, na bilo koji način, ugrožavaju prava djece na internetu.

Hrvatska

Zakon o elektroničkim medijima (2021) i Agencija za elektroničke medije (AEM)

Sukladno odredbama Zakona o elektroničkim medijima u Hrvatskoj je osnovana Agencija za elektroničke medije (AEM), kojom upravlja nacionalni regulatorno tijelo Vijeće za elektroničke medije. AEM je neovisno regulatorno tijelo koje između ostalog promovira i potiče medijsku pismenost. Osim suradnje sa drugim javnim i državnim tijelima i suradnje na međunarodnoj razini, AEM ima članstvo u svim relevantnim međunarodnim regulatornim mrežama (ERGA, EPRA, MNRA, CERF). Sukladno Direktivi o adiovizuelnim medijskim uslugama Vijeće i Agencija aktivno sudjeluju u radu Opće uprave Europske komisije za komunikacijske mreže, sadržaj i tehnologiju (DG Connect).

Zakon o elektroničkim medijima revidran je 2021. godine, a njegova revizija podrazumijevala je i usklađenost sa Direktivom o adiovizuelnim medijskim uslugama (2018), čime je u hrvatsko zakonodavstvo uvrštena revidirana Direktiva (2018), kao akta EU. Promjene su, između ostalog, uključivale osiguravanje bolje zaštite maloljetnika od štetnog onlajn sadržaja na svim platformama. Zakonom o elektorničkim komunikacijama (2021) obuhvaćeni su i pružatelji platformi za razmjenu video sadržaja, tj. pravna ili fizička osoba koja pruža uslugu platforme za razmjenu videozapisa, a Članak 96 stavak (1) normira i određene mjere u pogledu zaštite „– maloljetnika od programa – videozapisa koji su generirali korisnici i audiovizualnih komercijalnih komunikacija koje bi mogle naštetiti fizičkom, mentalnom ili moralnom razvoju maloljetnika u skladu sa člankom 24. ovoga Zakona". Stavak (7) ovog članka, a u svrhu poduzimanja odgovarajućih mjera u pogledu zaštite maloljetnika obuhvaćenih stavkom (1) normirani su sljedeći aspekti:

- uspostave i primjene transparentnih mehanizama prilagođenih korisnicima kojima korisnici platforme za razmjenu videozapisa mogu prijaviti ili naznačiti relevantnom pružatelju usluge platforme za razmjenu videozapisa sadržaj iz stavka 1. ovoga članka pružen na njegovoj platformi
- osiguravanja sustava za roditeljsku kontrolu koji su pod kontrolom krajnjeg korisnika u pogledu sadržaja kojim bi se moglo naštetiti fizičkom, psihičkom ili moralnom razvoju maloljetnika
- predviđanja učinkovitih mjera i alata za razvoj medijske pismenosti i podizanje svijesti korisnika o tim mjerama i alatima.

Stavak (8) Članak 96 sadrži: „Osobni podaci maloljetnika koje su prikupili ili na drugi način dobili pružatelji usluga platformi za razmjenu videozapisa u skladu sa stavkom 7. podstavcima 6. i 8. ovoga članka ne smiju se obrađivati u komercijalne svrhe, kao što je izravni marketing, izrada profila i ciljano bihevioralno oglašavanje".

U suradnji sa AEM-om je provedeno Nacionalno istraživanje o sigurnosti djece internetu HR Kids online (Ciboci, Ćosić Pregrad, Kanižaj, Potočnik, Vinković, 2020). Istraživanje je provedeno u okviru međunarodnog projekta EU (Global) Kids Online. Riječ je o najvećem europskom projektu u području istraživanja odnosa djece i interneta. Kroz projekt se istražuju prednosti i rizici korištenja interneta među djecom u dobi od 9 do 16 godina (u nekim državama od 9 do 17 godina); izloženost djece elektroničkom nasilju, seksualno eksplicitnim sadržajima i ponudama; način i intenzitet korištenja interneta u zavisnosti od uzrasta i socioekonomskih obilježja, te uloga roditelja, učitelja i okoliša u zaštiti i edukaciji djece o opasnostima na internetu (Ciboci, Ćosić Pregrad, Kanižaj, Potočnik, Vinković, 2020: 4). Studijom su obuhvaćene sljedeće tematske cjeline: Internet u životima djece i roditelja; Društvene mreže i korištenje mobilnih aplikacija; Neželjena i uznemirujuća iskustva djece na internetu, Roditeljska medijacija; Korištenje interneta u obrazovne svrhe i Upute za roditelje.

Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM)

U kontekstu zaštite djece na internetu značajan je i angažman Hrvatske regulatorne agencija za mrežne djelatnosti (HAKOM). Na *web* stranici HAKOM-a navedeni su svajeti koji upućuju na način sigurnijeg krištenja interneta od strane djece. Za prijavljivanje ilegalnih i neprimjerenih sadržaja dostupna je stranica zastita-djece@hakom.hr . HAKOM je aktivan u podržavanju akcije „Sigurniji internet za djecu i mlade". U pogledu angažmana usmjerenog na podizanje razine zaštite djece na internetu značajane su i HAKOM-ove brošure koje sadrže praktične i korisne savjete u vezi sa opsanostima i sigurnosti na interentu, zaštitom privatnosti i ličnih podataka, načinu ponašanja i upotrebe društvenih mreža (Kako zaštiti dijete u svijetu interneta, mrežnih tehnologija i mobilnih telefona, 2016/2017; Kako zaštiti dijete u svijetu interneta, mrežnih tehnologija i mobilnih telefona, 2017/2018; Kako se zaštiti u svijetu interneta i mobilnih telefona, 2018/2019; Kako se zaštiti u svijetu interneta i mobilnih telefona, 2020; Kako se zaštiti u svijetu interneta i mobilnih telefona, 2021; Kako se zaštiti u svijetu interneta i mobilnih telefona, 2022).

Portal e-Građani

U Hrvatskoj je pokrenut portal e-Građani, na kojem su dostupne i informacije značajne u kontekstu zaštite djece na internetu. Između ostalog, na portalu su dostupne informacije o zabranjenim aktivnostima na internetu, a u vezi sa djecom. U Hrvatskoj je zabranjeno:

- predlaganje susreta djeci mlađoj od 15 godina putem interneta, elektroničke pošte i mobilnih telefona u svrhu stupanja u spolni odnos s djecom
- prikupljanje, davanje drugima i prijenos podataka o osobama mlađima od 15 godina radi stupanja u spolni odnos
- iskorištavanje djece za pornografiju, što uključuje i pristupanje takvim sadržajima na internetu i njihovo posjedovanje
- iznošenje ili prenošenje nečega iz osobnog ili obiteljskog života djece, objavljivanje njihovih fotografija ili otkrivanje njihovog identiteta, što bi kod djece izazvalo uznemirenost, porugu vršnjaka ili drugih osoba ili na drugi način ugrozilo njihovu dobrobit.

Ministartsvo unutrašnjih poslova (Red button, edukativni materijali, međunarodna saradnja)

Na portalu e-Građani dostupne su informacije i o aplikaciji Red button, koja je namijenjena svima, ali je posebno prilagođena djeci. Aplikacija omogućuje prijavljivanje sadržaja na internetu za koji njegovi korisnici sumnjaju da je nezakonit i da se odnosi na različite oblike iskorištavnja ili zlostavljanja djece. Aplikacija je dostupna na stranicama Ministarstva unutarnjih poslova. Na stranici ovog Ministartsva dostupni su različiti edukativni sadržaji o zlostavljanju putem interneta, seksualnom zlostavljanju, načinu prijavljivanja sadržaja objavljenom na društvenoj mreži/aplikaciji, rizicima online komunikacije sa nepoznatim osobama, kao i savjeti u pogledu sigurnosti djece na internetu, savjeti roditeljima, mjere koje plolicija može učiniti i sl. Posebna pozornost posvećena je seksualnom iskorištavanju djece putem interneta i polnom zlostavljanju:

On line seksualno iskorištavanje djece odnosi se na seksualno zlostavljanje osobe mlađe od 18 godina, kao i na neovlašteno snimanje, proizvodnju, nuđenje, činjenje dostupnim, distribuciju, širenje, uvoz, izvoz, pribavljanje za sebe ili drugoga, prodaju, davanje, prikazivanje, posjedovanje, svjesno pristupanje putem informacijsko komunikacijskih tehnologija, materijalima koji predstavljaju spolno zlostavljanje i iskorištavanje djece.

Modaliteti seksualnog iskorištavanje djece na internetu neprestano se razvijaju i oblikuju usporedno sa razvojem tehnologije. Mobilna povezanost, sve veća pokrivenost interneta u zemljama u razvoju, razvoj mogućnosti kolanja novca (oblika plaćanja) pružaju visoku anonimnost zlostavljačima/počiniteljima kaznenih djela, što pak omogućuje uzlazni trend komercijalizacije prijenosa uživo seksualnog zlostavljanja djece (eng. *live-streaming*).

Trend spolnog zlostavljanja djece može se definirati kroz nekoliko osnovnih oblika:

- ***Peer-to-peer*** (P2P) mreže i anonimni pristup poput mreži Darkneta (npr. Tor) - takav pristup predstavlja glavnu platformu za pregledavanje/dijeljenje materijala spolnog zlostavljanja i iskorištavanja djece,
- Prenos uživo seksualnog zlostavljanja djece - ovakav način zlostavljanja znatno je olakšan novim tehnologijama.

Novi trend ovakve zlostave je seksualno zlostavljanje djece u inostranstvu, uglavnom su naručitelji *zapadnjaci* koji plaćaju *on line* gledanje spolnog zlostavljanja uživo ispred kamera,

- ***On line*** pribavljanje materijala spolne zlostave djece i seksualne iznude - sve veći broj djece i tinejdžera koji posjeduju *pametne telefone* sami proizvode tkz. materijale spolne zlostave „prve-generacije" koje međusobno dobrovoljno ili dogovorno dijele. Takav i tako sačinjen materijal koji kreiraju same žrtve/djeca, često pronalazi svoj put do *sakupljača* (počinioca kaznenih djela), koji često dalje nastavljaju iskorištavati žrtvu, iznuđivati finansijska sredstva ili tražiti (iznuđivati) sačinjavanje/dostavljanje novih materijala spolne zlostave.[50]

U preventivne svrhe snimljen je kratak video film, preveden za sve jezike zemalja članica EU*: **Say no!*** Film upozorava djecu i mlade na opasnosti i posljedice izrađivanja i dijeljenja osobnih fotografija/video materijala, poznatim ili nepoznatim osobama putem Interneta.

Služba sajber sigurnosti aktivno surađuje sa EU institucijskim agencijama (EUROPOL, EUROJUST, CEPOL i dr.), međunarodnim organizacijama (INTERPOL), zemljama članicama EU i predstavnicima trećih zemalja u području suzbijanja spolnog zlostavljanja i iskorištavanja djece (eng. *Child Sexual Exploitation - Child Sexual Abuse*). Ovdje se apostrofira značaj preventivnog djelovanja u borbi protiv distribucije materijala polnog zlostavljanja djece *on line*, kao i međunarodne suradnje policije i građana. Također, skreće se pozornost na kampanju Europola *STOP CHILD ABUSE – TRACE AN OBJECT* koja je usmjerena na pomoć pri prepoznavanju objekata/ predmeta / interijera / eksterijera koji su vidljivi i dio su poznatih materijala koji predstavljaju polno zlostavljanje djece te tako doprinose identifikaciji djece žrtava i identifikaciji žrtava.

Nacionalni CERT (CERT.hr)

Nacionalni CERT (CERT.hr) je odjel Hrvatske akademske i istraživačke mreže – CARNET , a osnovan je u skladu sa Zakonom o informacionoj sigurnosti (NN 79/2007 od 30.07.2007. godine; 5. poglavlje) kao nacionalno tijelo za prevenciju i zaštitu od računalnih ugrožavnja sigurnosti javnih informacijskih sustava u Republici Hrvatskoj čiji je osnovni zadatak obrada računalnih sigurnosnih incidenata s ciljem očuvanja sajbersigurnosti u Republici Hrvatskoj.

U svrhu informiranja javnosti o važnosti sajber sigurnosti te poticanja odgovornog korištenja interneta, CARNET-ov Nacionalni CERT pokrenuo je nacionalnu kampanju "Veliki hrvatski naivci". Kampanja je dio projekta *„GrowCERT* – Jačanje kapaciteta Nacionalnog CERT-a i poboljšanje suradnje na nacionalnoj i europskoj razini" koji je sufinanciran sredstvima Europske komisije putem Instrumenta za povezivanje Europe (*CEF – Connecting Europe Facility*). U edukativne svrhe izrađene su i brošure: „Sigurnost bežičnih mreža", „Sigurnije na internetu", kao vodič za laike koji pomaže u prepoznavanju opasnosti na internetu i aktivnoj zaštiti (obuhvata društvene mreže – *Facebook* i dijeljenje podataka – *BitTorrent*, izbjegavanje prijevara, zaštitu osobnih i osjetljivih podataka), „Opasnosti *Facebooka*", „Zaštitite privatnost na *Facebooku*", koja upućuje na opasnosti kojima se korisnici ove društvene mreže izlažu postavljanjem osobnih podataka i sadržaja, i na način podešavanja profila koji će omogućiti zaštitu privatnosti. Osim navedenih dostupne su i druge brošure, koje svojim sadržajem ukazuju na opsanosti sa kojima se suočavaju i djeca prilikom korištenja interneta, kao i na mehanizme njihove zaštite.

Posebno je značajano sudjelovanje Nacionalnog CERT-a jeste u domenu Nacionalne strategije sajber sigurnosti i Akcijskog plana za provedbu nacionalne strategije sajber sigurnosti. Mjere u kojima CARNET, odnosno odjel za Nacionalni CERT, aktivno učestvuje kroz Nacionalnu strategiju sajber sigurnosti podrazumijevaju:

- razvoj međusektorske suradnje nacionalnih regulatornih tijela i tijela odgovornih za područje informacijske sigurnosti i politike zaštite podataka te uzajamnu koordinaciju i razmjenu iskustava u suradnji i zahtjevima koji proizlaze iz međunarodnih okvira,

[50] Preuzeto sa: https://policija.gov.hr/prevencija/racunalna-sigurnost/seksualno-iskoristavanje-djece-putem-interneta-i-spolno-zlostavljanje/461

- definiranje taksonomije (uključujući pojam značajnog incidenta), definiranje protokola za razmjenu anonimiranih podataka o značajnim sigurnosnim incidentima te uspostava platforme ili tehnologije za razmjenu podataka,
- razmjena ranije anonimiziranih podataka o incidentima između sektorski nadležnih tijela korištenjem definirane taksonomije i protokola;
- prikupljanje podataka o incidentima od dionika,
- izvješćivanje dionika unutar sektora o računalno-sigurnosnim incidentima te periodično izvješćivanje Nacionalnog vijeća za sajber sigurnost o trendovima, stanju i značajnim incidentima iz prethodnog razdoblja;
- izdavanje upozorenja o sigurnosnim ugrozama i trendovima te odgovarajućih preporuka za postupanje,
- edukaciju uposlenika na godišnjoj razini za potrebe ekspertize i specijalističke obuke,
- izrada i objavljivanje preporuka o minimalnim sigurnosnim zahtjevima za davatelje i korisnike različitih elektroničkih usluga, kao i javno i komercijalno dostupnih bežičnih mreža (Wi-Fi) koje postaju masovno korištene, s ciljem zaštite krajnjih korisnika takvih usluga koji su široko zastupljeni u svim sektorima društva;
- osmišljavanje i provođenje usklađene kampanje o podizanju svijesti svih korisnika, odnosno vlasnika javno dostupnih sustava u Republici Hrvatskoj, o značaju sajber sigurnosti.[51]

U pogledu normiranja i obezbjeđivanja sajber sigurnosti značajan je Zakon o sajber sigurnosti operatora ključnih usluga i davaoca digitalnih usluga koji je donesen 2018. godine. U Članku 1 obrazloženi su predmet i cilj ovog Zakona: (1) Ovim se Zakonom uređuju postupci i mjere za postizanje visoke zajedničke razine sajber sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, nadležnosti i ovlasti nadležnih sektorskih tijela, jedinstvene nacionalne kontaktne točke, tijela nadležnih za prevenciju i zaštitu od incidenata (u daljnjem tekstu: nadležni CSIRT) i tehničkog tijela za ocjenjivanje uskađenosti, nadzor nad operatorima ključnih usluga i davateljima digitalnih usluga u provedbi ovog Zakona i prekršajne odredbe. (2) Cilj je ovog Zakona osigurati provedbu mjera za postizanje visoke zajedničke razine sajber sigurnosti u davanju usluga koje su od posebne važnosti za odvijanje ključnih društvenih i gospodarskih aktivnosti, uključujući funkcioniranje digitalnog tržišta.

[51] Preuzeto sa: https://www.cert.hr/nacionalna-strategija

PREGLED REGULATIVE I MEHANIZAMA USMJERENIH NA ZAŠTITU DJECE NA INTERNETU U BIH

Važan preduvjet za revidiranje i modernizaciju zakonodavnog i regualtornog okvira BiH, kao i drugih mehanizama koji značajno mogu doprinijeti unaprjeđenju zaštite djece na internetu, jeste utvrđivanje postojećeg stanja u ovom pogledu. Na osnovu ovog segmenta analize bit će omogućeno kreiranje preporuka usmjerenih ka zadovoljavanju interesa, poštovanja prava i sloboda djeteta, ali i zaštite njegovih interesa, u smislu obezbjeđivanja što sigurnijeg i bezbjednijeg digitalnog okruženja, kao neizostavne sfere u savremenom informacijskom društvu.

Iz prethodnih dijelova analize primjeto je da je BiH na temelju članstva u pojedinim međunarodnim organizacijama i strateškog cilja usmjerenog ka stabilizaciji i pridruživanju EU, u obvezi da regulatorni okvir prilagodi relevantnim međunarodnim standardima, što se odnosi i na obavezu podizanja razine sigurnosti djece na internetu. U sljedećim dijelovima ovog poglavlja bit će predstavljeni dokumenti koji u bilo kom dijelu na određen način normiraju digitalnu sferu i zaštitu interesa djeteta u ovoj sferi. Polazeći od činjenice da „u BiH ne postoji zakonodavni ni regulatorni okvir koji izričito uređuje oblast zaštite djece na internetu, ne postoji udruga/asocijacija pružatelja internet usluga, ..." (Puharić, 2019: 9), cilj ovog poglavlja usmjeren je na identifikovanje regulatornih i institucionalnih mehanizama koji posjeduju potencijale za uređivanje ove oblasti. Važnost ovog segmenta analize proizilazi i iz činjenice da i javni i privatni ISP-ovi imaju važnu ulogu u oblasti zaštite na internetu i da je u tom smislu i na razini BiH nužan njihov angažman.

Normativni okvir BiH relevantan za zaštitu djece na internetu

Normativni okvir BiH sastoji se od pozitivnih pravnih propisa na različitim razinama, tj. na nacionalno-državnoj, entitetskoj, kantonalnoj i međunarodnoj razini, kroz norme međunarodnog prava koje su i formalno sastavni dio nacionalnog pravnog sustava.[52] Unutar nacionalno-državne, odnosno entitetske razine, izdvajaju se Ustav, kao najviši pravni akt, sistemski zakoni kojima se detaljno reguliraju i profiliraju različiti aspekti društvenog sustava i podzakonski akti.

Uvidom u sadržaj ustava BiH (Ustava Bosne i Hercegovine, Ustav Republike Srpske i Ustav Federacije Bosne i Hercegovine), primjetno je da se ustavno normiranje ljudskih prava i sloboda na sve tri razine zasniva na međunarodnim pravnim standardima, tj. na odredbama sadržanim u Europskoj konvenciji za zaštitu ljudskih prava i osnovnih sloboda.[53] Člankom II Ustava BiH normirana je sfera ljudskih prava i osnovnih sloboda, dok su 3. stavkom (Katalog prava) ovog članka, između ostalih, izdvojena i sljedeća prava: pravo na ličnu slobodu i sigurnost, pravo na privatni i obiteljski život, dom i prepisku i pravo na slobodu izražavanja. Ustav Federacije BiH, također normira oblast ljudskih prava i osnovnih sloboda (II LJUDSKA PRAVA I OSNOVNE SLOBODE), a Člankom 7 normirana je obvezna suradnja svih nadležnih tijela vlasti u Federacji sa svim međunarodnim nadzornim tijelima za ljudska prava uspostavljenim za BiH. Ljudska prava i slobode normirani su i Ustavom RS (II LJUDSKA PRAVA I OSNOVNE SLOBODE), gdje se između ostalog navodi da su sloboda i lična sigurnost čovjeka nepovredivi (Članak 12), te da su ljudsko dostojanstvo, tjelesni i duhovni integritet, čovjekova privatnost, osobni i obiteljski život, također, nepovredivi (Članak 13).

Odvojeni članci i odredbe Ustava doneseni na sve tri razine ukazuju na normativno prikladnu osnovu za ostvarivanje temeljnih sloboda i prava čovjeka. Iako ustavno normiranje nije dovoljno za ostvarivanje ovih vrijednosti, ipak ono u tom smislu predstavlja jedan od nužnih preduvjeta.

---

[52] „Kao članica Saveta Evrope (2002) i potpisnica Sporazuma o stabilizaciji i pridruživanju (2008), Bosna i Hercegovina je trasirala svoju stratešku evropsku orijentaciju i obavezala se na poštovanje definisanog okvira za implementaciju reformi kojima će se prilagoditi zahtevima Evropske unije" (Milutinović, 2017: 88).

[53] U Ustavu BiH u članku II („Ljudska prava i osnovne slobode") pod stavkom 1. se navodi: „Bosna i Hercegovina i oba entiteta će osigurati najvišu razinu međunarodno priznatih ljudskih prava i osnovnih sloboda", a pod stavkom 2. članka II: „Prava i slobode predviđeni u Europskoj konvenciji za zaštitu ljudskih prava i osnovnih sloboda i u njenim protokolima direktno se primjenjuju u Bosni i Hercegovini. Ovi akti imaju prioritet nad svim ostalim zakonima" (Ustav BiH, članak II, stavak 1. i stavak 2). U Aneksu Ustava Federacije BiH pod nazivom „Instrumenti za zaštitu ljudskih prava koji imaju pravnu snagu ustavnih odredaba" navodi se ukupno 21 međunarodna konvencija i deklaracija, među kojima su navedene i Univerzalna deklaracija o ljudskim pravima (UN), Europska konvencija za zaštitu ljudskih prava i osnovnih sloboda i Konvencija o pravima djeteta. U Ustavu RS nisu posebno navedene međunarodne konvencije, rezolucije i deklaracije.

Značajni u kontekstu zaštite i sigurnosti djece općenito, kao i na internetu, svakako su Kazneni zakoni doneseni na četiri razine (Kazneni zakon BiH, Kazneni zakon FBiH, Kazneni zakon RS i Kazneni zakon Brčko diskritka BiH). Opsežna i detaljna analiza sadržaja ovih zakona, a u kontekstu seksualnog iskorištavanja i zlostavljnja djece u digitalnom okruženju, kao jedne od najozbiljnijih prijetnji sigurnom i zaštićenom internetu, sadržana je u publikaciji pod nazivom „Upute za društveno odgovorne informacisjko-komunikacijske tvrtke u oblasti zaštite djece od seksualnog iskorištavanja i zlostavljanja" (2019), čiji je autor Predrag Puharić.[54] Publikacija je izrađena u suradnji sa RAK-om.

Sukladno odredbama Konvencije o kribernetičkom kriminalu, koju je Bosna i Hercegovina ratificirala 23. studenog 2001. godine, Bosna i Hercegovina je uspostavila pravni okvir kada su u pitanju kaznena djela koja se odnose na seksualno iskorištavanje i seksualnu zlouporabu djece, i zaštitu djece žrtava i svjedoka ovih krivičnih djela. Sukladno političko-upravnom uređenju BiH, četiri kaznena zakona inkriminiraju radnje seksualnog nasilja nad djecom: Kazneni zakon BiH, Kazneni zakon FBiH, Kazneni zakon RS-a i Kazneni zakon Brčko distrikta BiH. To jasno govori da je Bosna i Hercegovina prepoznala da seksualno iskorištavanje i zlostavljanje djeteta predstavlja iznimno težak oblik neprihvatljivog ponašanja, pa za njega predviđa kaznene sankcije i počinitelje progoni prema službenoj dužnosti. Definicije koje postoje u bh. propisima nisu precizne, te različito definiraju ovu materiju, što u praksi ima za posljedicu različito razumijevanje ovog kaznnog djela. U kaznenim zakonima u Bosni i Hercegovini na različite načine definirani su proizvodnja i prikazivanje materijala koji uključuju korištenje djece u seksualne svrhe, odnosno upoznavanje djeteta sa takvim sadržajem. Očito je da u Kaznenom zakonu Federacije Bosne i Hercegovine i Kaznenom zakonu Brčko distrikta ne postoji definicija niti objašnjenje pojma „dječije pornografije", za razliku od Kaznenog zakona Republike Srpske koji u članku 175. „Iskorištavanje djece za pornografiju" stavaku6. definira šta se smatra „dječijom pornografijom". Kazneni zakon Bosne i Hercegovine ne poznaje ovaj problem već se ona smatra oblikom trgovine ljudima, što je djelomično točno, budući da se eksploatacija djece dovodi u direktnu vezu sa trgovinom ljudima, ali ipak nema odgovarajuće definicije koja bi ukazivala na dječiju pornografiju (Muratbegović & Hasanović, Nasilje nad djecom putem informaciono - komunikacionih tehnologija (IKT), 2017). Ova problematika nije uređena Kaznenim zakonom Bosne i Hercegovine već se sve navedene inkriminacije nalaze u entitetskim kaznenim zakonima i Kazneom zakonu Brčko distrikta. Koja su to rješenja u materijalnom kaznenom zakonodavstvu BiH u vezi sa „dječijom pornografijom"? Kaznena djela koja se prvenstveno izravno odnose na seksualno iskorištavanje i zlostavljanje djece su:

- *„Iskorištavanje djeteta ili maloljetnika radi pornografije", članak 211. KZ FBiH, i članak 208. KZ BD – suštinski identičan tekst kao u čl. 211. KZ FbiH*
- *„Iskorištavanje djece za pornografiju" u KZ RS, članak 175.*
- *„Upoznavanje djeteta sa pornografijom", članak 212. KZ FBiH i članak 209. KZ BD – suštinski identičan tekst kao u čl. 212. KZ FbiH*
- *„Iskorištavanje djece za pornografske predstave", članak 176. KZ RS*
- *„Upoznavanje djece s pornografijom ", članak 177. KZ RS*
- *„Iskorištavanje kompjuterske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih djela seksualnog zlostavljanja ili iskorištavanja djeteta", članak 178. KZ RS*
- *„Neovlašteno snimanje slike", članak 189. stavak 3. KZFBiH i članak 186. stavak 3. KZ BD – suštinski identičan tekst kao u čl. 189. st. 3. KZ FBiH.*

Također, odmah se uočava da su ova krivična djela različita, kako po nazivu tako i po zakonskom opisu. Naime, inkriminacije u Federaciji Bosne i Hercegovine i Brčko distriktu su suštinski iste, dok razlike postoje ako se date inkriminacije iz KZ FBiH i KZ BD kompariraju sa inkriminacijama iz KZ RS. Isto tako, zakonodavac u Republici Srpskoj je u Kaznenom zakonu objavljenom u „Službenom glasniku RS", broj 64/17 inkriminirao kazneno djelo „Iskorištavanje računalne mreže ili komunikacije drugim teh-

[54]Ova publikacija izrađena je u okviru projekta „Zaustaviti nasilje nad djecom: Prevencija i rad na sprječavanju seksualnog iskorištavanja i zlostavljanja djece u digitalnom okruženju u Bosni i Hercegovini", čiju su realizaciju podržali Global Fund to End Violence Against Children i UNICEF. Izdavač publikacije je Save the Children in North West Balkans.

ničkim sredstvima za izvršenje krivičnih djela seksualnog zlostavljanja ili iskorištavanja djeteta" kojim se u kombinaciji sa drugim djelima iz iste glave mogu inkriminirati novi fenomenološki oblici. (Muratbegović & Hasanović, Nasilje nad djecom putem informaciono -komunikacionih tehnologija (IKT), 2017). Međutim, ne treba gubiti iz vida da neprijavljivanje saznanja o ovim kaznenim djelima također predstavlja kazneno djelo. To je još jedan od razloga zbog kojeg bi sve fizičke i pravne osobe trebale podržati otkrivanje i procesuiranje kaznenih djela seksualnog iskorištavanja i zlostavljanja. Ozbiljnost ovog problema i prijetnje za djecu potakla je i donošenje drugih specifičnih zakona. Tako je Narodna skupština Republike Srpske 29. ožujka 2018. godine donijela i Zakon o posebnom registru osoba pravosnažno osuđenih za kaznena djela seksualne zlouporabe i iskorištavanja djece. Cilj ovog zakona je spriječiti ponavljanje kaznenih djela na štetu djece od strane istih izvršitelja.[55]

U kontekstu zaštite osobnih podataka i pravnih propisa donesenih na nacionalnoj razini za Bosnu i Hercegovinu je najznačajnije donošenje Zakona o zaštiti osobnih podataka 2006. godine.[56] Donošenjem ovog zakona osnovana je i Agencija za zaštitu osobnih podataka u Bosni i Hercegovini. Kazneni zakoni doneseni na razini entiteta i na nacionalnoj razini, također, normiraju kaznena djela protiv privatnog života.[57] Kao kazneno djelo propisano je i neovlašteno korištenje osobnih podataka.

Na razini RS Zakonom o informacijskoj sigurnosti Republike Srpske („Službeni glasnik Republike Srpske", broj 70/11) i Uredbom o mjerama informacijske sigurnosti („Službeni glasnik Republike Srpske", broj 91/12) normirana je informacijska sigurnost, kao stanje povjerljivosti, cjelovitosti i dostupnosti podataka. Kao sinonimi za informacijsku sigurnost koriste se računarlna, kibernetička i sajber sigurnost. Narušavanje stanja informacijske sigurnosti naziva se računalno-sigurnosni incident. Rad na postizanju stanja informacijske sigurnosti i zaštiti informacijskih sustava podijeljen je na prevenciju, obradu i otklanjanje posljedica računalno-sigurnosnih incidenata. Prevencija je proaktivno djelovanje, dok se obrada i otklanjanje posljedica smatraju reaktivnim djelovanjem.[58] Zakon o informacijskoj sigurnosti iz 2011. godine definira nacionalni tim za odgovor na računalne bezbjednosne incidente i postavlja ga u Agenciju za informacijsko društvo Republike Srpske. CERT RS, kao organizaciona jedinica Agencije za informacijsko društvo, pod imenom Odjel za informacijsku sugurnost, počinje s radom 01.06.2015. godine. Donošenjem novog Zakona o republičkoj upravi („Službeni glasnik Republike Srpske", broj 115/18) CERT RS postaje organizaciona jedinica u Ministarstvu za naučnotehnološki razvoj, visoko obrazovanje i informacijsko društvo. CERT predstavlja posebnu organizacionu jedinicu za djelovanje u hitnim slučajevima, čiji je zadatak obrada računalnih bezbjednosnih incidenata, koordinacija prevencije i zaštite informacijskih sustava.[59]

Primaran sistemski zakon u kontekstu regulacije komunikacija na nivou BiH jeste Zakon o komunikacijama („Službeni glasnik BiH" br. 31/03), kojim se precizno normiraju pitanja u vezi sa radom regulatornog tijela (RAK) u BiH (član 1. stav 1). Kao nadležne institucije u oblasti komunikacija na nivou BiH zakonom su predviđeni Vijeće ministara, nadležan za kreiranje politike, i Agencija (RAK), nadležna za regulisanje oblasti komunikacija (član 3. stav 1). U članu 4. Zakona o komunikacijama u kojem se definišu regulatorni principi emitovanja i telekomunikacija također se navodi da oni obuhvataju „zaštitu slobode izražavanja i raznolikosti mišljenja poštujući općeprihavćene standarde ponašanja, nediskriminacije, pravičnosti, tačnosti i nepristrasnosti" (član 4. stav 1), te je u istom članu garantovan „pristup javnim telekomunikacionim uslugama za sve korisnike, na transparentnom, objektivnom i nediskriminatorskom osnovu (...)" (član 4. stav 2).

Posebice važan dio ovog zakona sadržan je u članku 46, koji normira izvršne ovlasti Agencije sukladno europskoj regulatornoj praksi. Njihovim normiranjem i preciziranjem omogućeno je ostvarivanje principa propisanih člankom 4. koji se odnose na zaštitu slobode izražavanja. Davanjem u nadležnost seta izvršnih mjera (članak 46) i pozicioniranjem Vijeća Agencije kao apelacionog tijela u odnosu na odluke Agencije i generalnog direktora (članak 39. stavak 1), „regulator je za kratko vrijeme postao jedna od najsnažnijih među sličnim institucijama u zemljama regije" (Kujundžić, 2015: 31). Zakon o komunikacijama regulira oblast komunikacija koje „uključuju telekomunikacije, radio, emitiranje (uključujući kabelsku televiziju), i usluge i sredstva koja su s tim u vezi" (članak 1. stavak 2) i „uspostavu i rad Regulatorne agencije za komunikacije Bosne i Hercegovine (...)" (članak 1. stavak 1).

---

[55] Puharić, Predrag (2019). „Upute za društveno odgovorne informaciono-komunikacijske kompanije u oblasti zaštite djece od seksualnog iskorištavanja i zlostavljanja". Save the Children in North West Balkans.

[5] Zakon o zaštiti osobnih podataka „Sl. glasnik BiH", br. 49/2006, 76/2011, 89/2011.

[57] Kazneni zakon Bosne i Hercegovine „Sl. glasnik BiH", br. 3/2003; Kazneni zakon Federacije Bosne i Hercrgovine „Sl. novine FbiH", br. 36/2003; Kazneni zakon Republike Srpske, „Sl.glasnik RS", br. 49/2003.

[58] https://www.vladars.net/sr-SP-Cyrl/Vlada/Ministarstva/mnk/rid/ib/Pages/default.aspx pristupljeno 10.03.2022. godine.

[59] https://www.vladars.net/sr-SP-Cyrl/Vlada/Ministarstva/mnk/cert/Pages/default.aspx pristupljeno 10.03.2022. godine.

Regulatorna agencija za komunikacije BiH (RAK)

Kada je riječ o regulaciji rada i sadržaja koje isporučuju i kreiraju ISP-ovi, RAK je jedina agencija koja je u određenim segmentima nadležna za ISP-ove i druge zakonom definirane učesnike na tržištu elektroničkih komunikacija.

> Agencija je regulator sa spojenim nadležnostima nastala po uzoru na slične procese u europskim zemljama i odražava spajanje tehnologija u telekomunikacijama i emitiranju, na način koji može da odgovori potrebama tržišta. Po ugledu na slične institucije u Europi, nadležnosti Agencije su zasnovane na principima neovisnosti, provedbi regulacije i monitoringu poštivanja zakona i pravila, i osiguranju tehničkih, financijskih i kadrovskih preduvjeta za učinkovito izvršavanje zadataka. U skladu sa Zakonom o komunikacijama BiH, nadležnosti Agencije su: kreiranje i promoviranje pravila u sektorima emitiranja i telekomunikacija, licenciranje operatora u sektorima emitiranja i telekomunikacija, planiranje, upravljanje i dodjeljivanje frekventnog spektra, primjenjivanje tehničkih i drugih standarda koji se tiču kvaliteta, te uspostava i održavanje sustava naknada za dozvole" (Puharić, 2019: 17).

U sektoru telekomunikacija, a u kontesktu predmetne analize i uzimajući u obzir izraženu tendenciju konveregencije usluga na tržištu telekomunikacija u pogledu telefonske usluge i usluge pristupa internetu, na razini RAK-a usluge pristupa internetu normirane su kroz dva pravila: Pravilo 60/2012 o obavljanju djelatnosti davatelja pristupa internetu i Pravilo 69/2013 o uslovima pružanja javnih telekomunikacijskih usluga i odnosima s krajnjim korisnicima. U Članku 8 (Ponuda usluge) Pravila 60/2012 je navedeno da internet usluga mora omogućiti krajnjem korisniku neometan pristup svim javno raspoloživim sadržajima i uslugama koji se nude na Internetu, te da izuzetak čine sadržaji ili usluge čije bi korištenje zasnovalo izričitu protivpravnost ili krivično djelo. Ovim člankom normirane su i precizirane dužnosti ISP-ova u pogledu postupanja sa štetnim i nezakonitim sadržajima. U tom kontekstu članak 8, stavak (2) kaže da je ISP dužan da na temelju posebnih propisa ili odluke nadležne institucije u Bosni i Hercegovini kojom se određeni sadržaji oglašavaju nezakonitim, primjenom pogodnih tehničkih mjera onemogućiti pristup internet adresama za koje je takvim posebnim propisima ili odlukama nadležnih institucija u Bosni i Hercegovini utvrđeno da su štetni i protuzakoniti, a posebice ukoliko se tim sadržajima širi dječija pornografija i slični štetni sadržaji, omogućava protuzakonito on-line kockanje, šire računalni virusi ili opasni programi, nezakonito pribavljaju osobni podaci, ugrožava opća sigurnost, javni red i mir, omogućava protupravna uporaba računalnih programa i aplikacija, kao i druge opasnosti po sigurno korištenje Interneta. Člankom 36 (Zaštita maloljetnih lica) Pravila 69/2013 izričito je normirana dužnost operatera javnih telekomunikacijskih usluga u uspostavljanju i primjenjivanju odgovarajućih mjera za zaštitu maloljetnih lica (stavak 1), a stavokm (2) istog članka normirano je pravo Agencije da može donijeti posebne propise za zaštitu maloljetnih lica.

U sektoru emitiranja, kao relevantne dokumente za zaštitu maloljetnika, naročito u kontekstu ograničavanja njihovog pristupa i izlaganja neprikladnim sadržajima, moguće je izdvojiti dva kodeksa: Kodeks o audiovizuelnim medijskim uslugama i medijskim uslugama radija i Kodeks o komercijalnim komunikacijama. Ovi kodeksi predstavljaju dokumente sa snažim potencijalima i za zaštitu djece u digitalnom okruženju, naročito u kontekstu njihovog revidiranja usmjerenog ka usklađivanju sa revidiranom Direktivom o audiovizuelnim medijskim uslugama (2018), čiji je sadržaj prethodno elaboriran.

Aktivnosti, upute i strategije RAK- a usmjerene na zaštitu djece u medijskom/digitalnom okruženju

Dosadašnjom analizom utvrđeno je da je RAK kontinuirano angažovan na različite načine u cilju obezbjeđivanja sigurnijeg digitalnog okruženja za djecu. Angažman regulatornog tijela se, između ostalog, ogleda u brojnim aktivnostima usmjerenim na izradu različitih strategija o IKT sigurnosti na razini BiH.

Posebice važan u kontekstu predmetne analize jeste angažman Vijeća ministara BiH i RAK-a u pogledu Akcionog plana za zaštitu djece i sprječavanje nasilja nad djecom putem informaciono-komunikacijskih tehnologija u Bosni i Hercegovini za razdoblje 2014-2015, koji je sačinjen u skladu sa Strategijom suprostavljanja trgovini ljudima u Bosni i Hercegovini (2013-2015) usvojenom na 43. sjednici Vijeća ministara Bosne i Hercegovine održanoj 26.03.2013. godine. Strateški cilj 4. (Proaktivna zaštita) sadrži Stratešku mjeru D.6. „Poboljšanje sistema zaštite od dječije pornografije i pedofilije" kojom se planira „Osigurati efikasne mehanizme zaštite od dječije pornografije i drugih oblika seksualnog iskorištavanja, te zlouporabe djece putem informacijskih i komunikacijskih tehnologija." Takav plan, Strategija obrazlaže na sljedeći način:

> Neograničeni „*cyber* prostor" i dostupnost informacija u svakom trenu iz bilo koje točke planete zasigurno predstavlja krucijalni beneft civilizacije. Međutim, ovakvo stanje ima i svoje negativne trendove i posljedice. Naime, upravo ovaj neograničeni prostor, dostupnost i djelomična anonimnost omogućava devijacije različitih formi na koje službe formalne socijalne kontrole i službe za provedbu zakona nisu navilke u svakodnevnim aktivnostima. Djeca kao „znatiželjna kategorija" stanovništva svake zemlje vrlo često dolaze u opasnost da postanu žrtve različitih zlouporaba upravo pomenutog „*cyber* prostora". Stoga je potrebno defnirati posebnu mjeru u okviru ove Stretegije.[60]

Akcioni plan za provedbu Strategijom suprostavljanja trgovini ljudima u Bosni i Hercegovini (2013-2015) kao aktivnost D.6.3. predvidio je Usvajanje Akcionog plana za zaštitu djece i sprječavanje nasilja nad djecom putem informaciono-komunikacijkih tehnologija.

Ovaj dokument pruža korisne i relevantne upute za podizanje razine zaštite i sigurnosti djece na internetu, uvažavajući sve prednosti IKT-a, kao i neophodnost njihovog slobodnog, ali i bezbjednijeg korištenja od strane djece. Akcionim planom obuhvaćeni su svi aspekti primarno značajni za obezbjeđivanje sigurnijeg digitalnog okruženja za djecu: zakonodavstvo, institucionalni kapaciteti i suradnja i prevencija. Ovim dokumentom, između ostalog predviđena je i izgradnja kapaciteta internet servis „provajdera" (ISP) i suradnja sa agencijama za provođenje zakona i pravosudnim institucijama (B.4.).

U ovom smislu također značajan dokument je Upute za strateški okvir *cyber* sigurnosti u BiH (2019), na čijoj izradi je bio angažovan i RAK. Upute su izrađene uz potporu misije OSCE-a u BiH. U dokumentu je prije svega jasno određena vizija Strateškog okvira za *cyber* sigurnost u BiH:

> Vizija Strateškog okvira za *cyber* sigurnost u Bosni i Hercegovini je da se, sukladno realnim potrebama, potencijalnim prijetnjama, kao i međunarodnim obvezama i standardima u oblasti *cyber* sigurnosti, te sukladno nadležnostima, osigura strateški i zakonski okvir, te unaprijede procedure i tehnike u cilju zaštite informaciono-komunikacijskih sustava i krajnjih korisnika u *cyber* prostoru. Ostvarenjem vizije postiže se smanjenje rizika, uz uvažavanje privatnosti, te istovremeno promoviraju tehničke inovacije, olakšava komunikacija, gospodarski razvoj i transparentnost, kao i sigurnost sveukupnog društva.[61]

Ovim dokumentom definiran je minimalan broj ciljeva i aktivnosti koji će dovesti do efikasnog i provodivog strateškog okvira, odnosno do konkretnih i mjerljivih rezultata upravljanja sustavom *cyber* sigurnosti, iz čega proizilazi postavljanje općeg cilja koji se odnosi na unaprjeđenje sigurnosti *cyber* prostora u funkciji napretka društva u cjelini, koje se ostvaruje jačanjem kapaciteta i razvojem mehanizama za prvenciju, detekciju i sigurnosne izazove. Kao strateški ciljevi izdvojeni su sljedeći:

A. Osiguran sustavni pristup usklađivanju i izradi zakonodavstva u području *cyber* sigurnosti;

B. Zaštićeni informaciono-komunikacijski sustavi za pružanje ključnih usluga;

C. Podizanje razine svijesti i znanja o *cyber* sigurnosti;

D. Uspostava tijela zadužena za osiguranje, jačanje i poboljšanje *cyber* sigurnosti;

E. Poboljšana sigurnost i otpornost informaciono-komunikacijskih sustava;

F. Ojačani kapaciteti za borbu protiv *cyber* kriminala;

G. Uspostava učinkovite suradnja u oblasti *cyber* sigurnosti u međunarodnim, regionalnim i domaćim okvirima;

H. Izgrađeni kapaciteti za adekvatan odgovor na krizne situacije;

I. Uspostava javno-privatno partnerstvo[62]

Jedan od rezultata ove vrste angažmana jesu i „Upute o korištenju medija, informacijsko-komunikacijskih tehnologija i vremenu koje djeca provode pred ekranom" (2021), čiji su izdavači RAK i Fondacija za razvoj medija i civilnog društva "Mediacentar". Polazeći od kompleksnosti medijskog okruženja u kojem djeca odrastaju procijenjeno je da, kako je navedeno u uvodnom dijelu

---

[60] Akcioni plan za zaštitu djece i sprječavanje nasilja nad djecom putem informaciono-komunikacijskih tehnologija u Bosni i Hercegovini za period 2014-2015, str. 5.
[61] Smjernice za strateški okvir cyber sigurnosti u BiH (2019), str. 4. Dostupno na: https://www.osce.org/bs/mission-to-bosnia-and-herzegovina/438386
[62] Isto, str 9.

ove publikacije, „roditeljima i stručnjacima iz različitih područja koji rade s djecom, potrebna je pomoć i potpora kako bi osigurali uživanje prava djeteta i maksimalno iskoristili pozitivni potencijal medija i IKT za razvoj djeteta, ali u isto vrijeme i osigurali odgovarajuću zaštitu djeteta od potencijalnih rizika".[63]

Posebice važan je angažman RAK-a u pogledu podizanja razine svijesti građana o značaju posjedovanja kompetencija koje se stiču medijskim i informacijskim opismenjavanjem jeste pokretanje zajedničke web-stranice RAK-a i UNESCO-a kao bosanskohercegovačkog portala posvećenog medijskoj i informacijskoj pismenosti, medijskapismenost.ba. Stranica je prvenstveno namijenjena djeci školske dobi od 6 do 18 godina , zatim roditeljima i nastavnicima, kao i stručnoj javnosti angažovanoj na polju medijske i informacijske pismenosti. „Stranica je formirana u cilju promoviranja i unaprjeđenja medijske i informacijske pismenosti (MIP) građana BiH i posvećena je informiranju javnosti o inicijativama, istraživanjima i projektima i razvijenim materijalima različitih formata brojnih organizacija i institucija aktivnih u oblasti MIP u BiH. Ova stranica je i dio regionalne UNESCO-ve stranice posvećene ovoj temi SeeMIL."[64]

Pokretanje ove stranice predstavlja jedan od indikatora koji upućuje na usklađenost angažmana regulatornog tijela BiH sa praksom europskih regulatora u domenu medijske i informacijske pismenosti. Naime, posjedovanjem vještina stečenih medijskim i informacijskim opismenjavanjem i podizanjem svijesti o njihovom značajnu, uveliko se može doprinijeti suzbijanju negativinih efekata koje sa sobom donosi suvremeno digitalno okruženje i adekvatnom korištenju suvremenih IKT, koje istovremeno podrazumijeva podizanje razine sigurnosti, naročito djece i mladih.[65] Na ovoj stranici su dostupna brojna istraživanja, analize i strategije, a u kontekstu zaštite djece na internetu naročito je značajna kategorija pod nazivom „Bolji i sigurniji internet", koja sadrži edukativne materijale o opasnim i neprimjernim sadržajima, zaštiti privatnosti, neželjenom kontaktu i sl.

RAK ima veoma važnu ulogu u ostvarivanju komunikacijskih prava djece. Zaštita maloljetnika smatra se jednim od najznačajnijih zadataka medijskog reguliranja i pitanjem od izuzetnog javnog interesa. U medijskoj regulativi postoje dva osnovna aspekta zaštite maloljetnika: zaštita maloljetnika kada su predmet medijskih sadržaja i zaštita maloljetnika od medijskih sadržaja. U kontekstu zaštite maloljetnika kada su predmet/dio medijskih sadržaja, primarno su relevantne odredbe sadržane u Kodeksu o audiovizuelnim medijskim uslugama i medijskim uslugama radija koje se odnose na učešće maloljetnika u programima, na različite aspekte zaštite privatnosti maloljetnika, zaštitu maloljetnika u medijskom izvještavanju o izborima i izvještavanju o maloljetnicima u vezi sa kaznenim djelima i postupcima itd. U pogledu zaštite maloljetnika od medijskih sadržaja, navedenim kodeksom predviđa se dvostupanjski sustav reguliranja. Sadržaji se, pri tome, dijele na dvije kategorije potencijalno štetnog sadržaja za maloljetnike: sadržaj koji može ozbiljno naškoditi i sadržaj koji će vjerovatno naškoditi njihovom fizičkom, mentalnom ili moralnom razvoju. U kodeksu je razrađen sustav klasificiranja sadržaja za koje je vjerovatno da bi mogli ugroziti fizički, psihički ili moralni razvoj maloljetnika, a koji predviđa tri kategorije 12+, 16+ i 18+ uz odgovarajuće termine emitiraja sadržaja iz kategorije 16+ i 18+. U Kodeksu o komercijalnim komunikacijama sadržane su i odredbe koje garantuju zaštitu maloljetnika kao potrošača, imajući u vidu njihovu posebnu ranjivost u tom pogledu. Osim navedenih ingerencija RAK ima zadatak da osigura zastupljenost različitih vrsta programa, pa tako i dječijeg programa u zemlji. RAK također poduzima aktivnosti u oblasti digitalne sigurnosti maloljetnika, samostalno kao i u suradnji s brojim partnerima.

Između ostalog, učestvuje u obilježavanju Dana sigurnijeg interneta[66], surađuje sa Konzorcijem za zaštitu djece od nasilja u digitalnom okruženju, te je organizirala i kampanju s ciljem podizanja svijesti javnosti o sigurnosti djece na internetu.

---

[63] „Upute o korištenju medija, informaciono-komunikacijskih tehnologija i vremenu koje djeca provode pred ekranom" (2021).

[64] https://medijskapismenost.ba/o-nama/

[65] U oktobru 2019. godine Agencija je formirala poseban odsjek za sadržaj i medijsku pismenost, što je rezultiralo povećanim aktivnostima na tom polju. Uspostavljena je neformalna mreža relevantnih institucija, organizacija i pojedinaca aktivnih na polju MIP, pokrenuta je Facebook stranica *„Medijska i informacijska pismenost u Bosni i Hercegovini"* kao i Facebook zatvorena grupa *„Medijska i informacijska pismenost – grupa eksperata u BiH"*. Cilj ovih aktivnosti je informiranje šire javnosti o raznim temama iz domena MIP, generiranje i razmjena materijala unutar članica MIP mreže, organizacija *Dana medijske pismenosti*, te obilježavanje UNESCO-ve *Globalne sedmice MIP*-a. https://medijskapismenost.ba/o-nama/

[66] Dan sigurnijeg interneta (Safer Internet Day – SID) je međunarodni dan koji se na inicijativu Europske komisije globalno obilježava već godinama. Tom prilikom brojni akteri iz oblasti obrazovanja, zaštite djece, medijske politike i telekomunikacionog sektora promovišu sigurno i odgovorno korištenje interneta i digitalnih tehnologija. U Bosni i Hercegovini se ovaj dan obilježava od 2011. godine na inicijativu udruženja „Međunarodni forum solidarnosti – EMMAUS" (MFS-EMMAUS), u organizaciji Centra za sigurni internet u BiH u cilju podržavanja aktivnosti u oblasti sprječavanja zloupotrebe djece i mladih u digitalnom okruženju. Inicijativu također podržava Ministarstvo sigurnosti BiH, Regulatorna agencija za komunikacije BiH, kao i BiH Konzorcij za zaštitu djece koji uz MFS-EMMAUS čine organizacije UNICEF i Save the Children. Preuzeto sa: https://www.sigurnodijete.ba/blog/dan-sigurnijeg-interneta-safer-internet-day-sid

U cilju podizanja svijesti o uticaju televizijskih sadržaja na djecu i maloljetnike, kao i potrebi aktivnijeg praćenja njihovih medijskih navika, RAK je izradila i spot koji je prvenstveno namijenjen roditeljima, skrbnicima i drugim licima koja brinu o maloljetnicima. Zatim, izrađen je spot primarno usmjeren na korištenje interneta, koji ukazuje na moguće opasnosti za djecu i maloljetnike na internetu, kao što su nasilje i pornografski sadržaji, te kontakti sa pedofilima i radikalnim grupama u društvu. Spot Gdje je Buco ima za cilj promociju medijske pismenosti i zaštitu djece i maloljetnika od potencijalno štetnih sadržaja na internetu.

Kako bi pomogla pružateljima medijskih usluga, ali i široj javnosti, da dodatno shvate mogući utjecaj medijskih sadržaja na djecu, inicirala je i izradu dokumenta koji se bavi utjecajem televizije na djecu i maloljetnike – stručni elaborat Utjecaj televizije na djecu i maloljetnike i u suradnji s UNICEF-om Upute za klasificiranje televizijskih sadržaja. Ovi dokumenti nude detaljan uvid u način na koji maloljetnici doživljavaju televizijske sadržaje u različitim fazama razvoja, te ukazuju na utjecaj koji ovakvi sadržaji mogu imati na njihov razvoj. U toku 2019. godine pokrenuta je i kampanja u cilju podizanja svijesti o utjecaju televizijskih sadržaja na djecu i maloljetnike, kao i o potrebi aktivnijeg praćenja njihovih medijskih navika. U okviru kampanje, emitiran je televizijski spot namijenjen roditeljima, skrbnicima i drugim osobma koje brinu o maloljetnicima, te izrađena brošura o zaštiti maloljetnika. Od posebne koristi za roditelje, ali i druge koji se brinu o djeci, kao što su odgajatelji, učitelji, nastavnici, pedagozi, psiholozi i pedijatri su Upute za korištenje medija, IKT i vremenu koje djeca provode pred ekranom koje je izradila multidisciplinarna grupa stručnjaka pod vodstvom RAK-a i Mediacentra Sarajevo.[67]

Agencija sarađuje i sa ITU, a jedan od rezultata njihove suradnje jeste promocija uputa i edukativnih materijala o *online* sigurnosti djece pod nazivom"Sigurnost djece online". Promocija je organizirana u vidu *online* prezentacije u okviru koje su predstavljene nove upute i edukativni materijali o sigurnosti djece *online* koje je izradio ITU 2020. godine i koje sadrže sveobuhvatan set preporuka za djecu, roditelje i edukatore, industriju i kreatore politika o tome kako doprinijeti razvoju sigurnog i osnaženog *online* okruženja za djecu i mlade. Ovim materijalima obuhvaćeni su sljedeći aspekti značajni u kontekstu *online* sigurnosti djece:

- Upute za roditelje i edukatore o zaštiti djece online,
- Upute za kreatore politika za zaštitu djece na internetu,
- Upute za industriju za zaštitu djece online,
- Slikovnica za djecu,
- Radna knjiga za djecu,
- Vodič za nastavnike,
- Tvrtka za društvene mreže za tinejdžere.

Evidentno je da RAK kontinuirano surađuje sa relevantnim međunarodnim organizacijama, poput UNICEF-a, UNESCO-a, Vijeća Evrope, ITU-a, potom sa BiH Konzorcijom za zaštitu djece koji uz MFS-EMMAUS čine organizacije UNICEF i *Save the Children*, Centrom za sigurni internet BiH, i drugim organizacijama i institucijama. Suradnja je, između ostalog, usmjerna na promociju MIP-a, koja uključuje istraživanja, publikacije, prezentacije i druge aktivnosti iz ove oblasti.

Kontinuirana saradnja RAK-a sa navedenim međunarodnim organizacijama rezultirala je i publikacijama poput finalnog izvješć „Medijske navike odraslih u BiH" (2021). Studija je izrađena uz potporu Vijeća Europe i projekta Medijska i informacisjka pismenost: za ljudska prava i demokratiju, u okviru Akcionog plana za Bosnu i Hercegovinu 2018-2021. Potom, publikacijom u formi finalnog izvješća „Medijske navike djece i stavovi roditelja" (2020), u suradnji sa UNICEF-om. RAK je, također, surađivao u izradi veoma značajne publikacije, posebice u kontekstu predmetne analize, pod nazivom „Upute za društveno odgovorne informaciono-komunikacijske tvrtke u oblasti zaštite djece od seksualnog iskorištavanja i zlostavljanja" (2019).

Naime, očigledan je angažman regulatornog tijela u BiH u pogledu podizanja razine sigurnosti djece na internetu, naročito u vidu preventivnog, proaktivong i konsturktivnog djelovanja.

---

[67] Sadržaj o navedenim aktivnostima RAK-a preuzet je sa web stranice: https://medijskapismenost.ba/komunikacijska-prava-djece/

Aktivnosti i programi usmjereni na podizanje nivoa sigurnosti djece na internetu u BiH

Osim ranije navedenog značajnog angažmana RAK- a u pogledu promoviranja i edukacije usmjerene ka medijskom opismenjavanju građana i građanki BiH, a naročito djece, tokom izrade ove analize uočene su značajne aktivnosti koje u velikoj mjeri mogu doprinijeti sticanju kompetencija neophodnih za adekvatno korištenje medija i IKT tehnologija. To je svakako potreban preduvjet za bezbjednije ponašanje djece u digitalnom okruženju, jer djeca koja posjeduju višu razinu medijske pismenosti, tj. više kompetencija koje se stiču medijskim opismenjavanjem manje su izložena rizicima koje sa sobom nosi gotovo svakodnevno korištenje interneta.

U navedenom kontekstu značajan je program obuka za nastavnike i saradnike u osnovnim školama u oblasti medijske pismenosti. Obuke se realizuju u okviru projekta „Jačanje medijske pismenosti kod djece u Republici Srpskoj", a provodi ih Ministarstvo prometa i veza RS, uz podršku Ministarstva prosvjete i kulture i Republičkog pedagoškog zavoda. Cilj obuka je jačanje kapaciteta osnovnih škola u smislu pružanja dodatnih znanja za rad sa učenicima u oblasti medijske i informacijske pismenosti kroz redoviti, postojeći nastavni plan i program. Realiziranje obuka počelo je u listopadu 2021. godine.

Poseban značaj ovih obuka proizilazi i iz toga što je u osnovnim školama u RS od školske 2021/22. godine za učenike drugih razreda u postojeći nastavni plan i program uveden novi predmet prilagođen savremenom digitalnom okruženju u kojem djeca neminovno odrastaju pod nazivom „Digitalni svijet".

Također, u pogledu proaktivnog djelovanja u domenu podizanja razine zaštite maloljetnika na interentu značajne su aktivnosti Ministarstva sigurnosti BiH. Ministarstvo je kontinuirano angažovano u izradi strateškog i zakonskog okvira za *cyber* sigurnost i na unaprjeđenju procedura i tehnika u cilju zaštite informaciono-komunikacijskih sustava i krajnjih korisnika u *cyber* prostoru u BiH. Jedan od značajnih angažmana u ovom smislu jeste i osnivanje Centra za sigurni internet u cilju sprječavanja seksualnog iskorištavanja i zlostavljanja djece u digitalnom okruženju i obezbjeđivanja informacija i alata za sigurno i odgovorno korištenje informacijskih i komunikacijskih tehnologija. Centar je uspostavljen 2018. godine, a čine ga Informativni centar, *Helpline, Hotline* (član međunarodne mreže INHOPE) sa jasno definiranim mehanizmima djelovanja:

- Informativni centar - aktivnosti su usmjerene na podizanje svijesti i razumijevanje pitanja sigurnosti na internetu i aktuelnih trendova, te ima za cilj realiziranje javnih tvrtki u cilju obezbjeđivanja vještina, znanja i strategija za djecu, mlade, roditelje, nastavni kadar i druge profesionalce, da sigurno koriste internet i prednosti koje pružaju informacijske i komunikacijske tehnologije;
- SOS linija za potporu putem besplatne telefonske linije pruža informacije, profesionalne savjete i potporu psihologa djeci, omladini i roditeljima kako da postupaju sa štetnim sadržajima, kontaktima i postupcima online;
- SOS linija za prijavu je uspostavljena 2010. godine i omogućava anonimnu prijavu nelegalnih i neprimjerenih online sadržaja, koje se potom proslijeđuju relevantnim agencijama koje mogu djelovati u ovoj oblasti (agencije za provedbu zakona ili INHOPE članica/Hotline u odgovarajućoj državi).

Osim Centra za sigurni internet/sigurno dijete u BiH je uspostavljena i savjetodavna linija za djecu i mlade Plavi telefon, uz potporu Mtela, zahvaljujući kojoj sva djeca iz BiH mogu dobiti pomoć putem besplatne savjetodavne linije bez obzira na mrežu iz koje zovu. Linija je prvenstveno namijenjena djeci koja osjećaju da ih neko iz njihovog okoliša na bilo koji način zlostavlja (tuče, vrijeđa, naziva pogrdnim imenima, prilazi im na seksualno neprihvatljiv način..) ili zanemaruje i za one koji znaju ili su vidjeli da je neko dijete zlostavljano i zanemareno. Pored problema nasilja, linija je otvorena za sve probleme koje djeca imaju, a o kojima nemaju sa kim razgovarati i od koga da zatraže potporu i pomoć. Ova vrsta potpore namijenjena je i za prijavljivanje zlostavljanja u onlajn okruženju, kao i za sve sve probleme u ovoj sferi.

Brojne aktivnosti RAK-a, kao i navedenih institucija i međunarodnih organizacija na prostoru BiH, upućuju na prisutnost tendencija veoma važnih u kontekstu podizanja razine svijesti građana o značaju posjedovanja kompetencija koje se stiču medijskim opismenjavanjem i koje su neophodne za sigurno korištenje digitalnih medija, društvenih mreža, različitih aplikacija

i sl. Osim toga, u ovom pogledu primjetne su konkretne aktivnosti koje omogućuju sticanje medijskih kompetencija i koje značajno doprinose zaštiti djece na internetu. Međutim, osim ovih angažmana, potrebna je primjena i drugih mehanizama, kao i angažman ostalih institucija i subjekata, usmjeren na zaštitu interesa djeteta, njegovih prava i sloboda, koji su u suvremenom informacijskom društvu izloženi brojnim i veoma problematičnim izazovima.

PREPORUKE

Na osnovu analize različitih praksi regulatornih i samoregulatornih mehanizama usmjerenih na zaštitu djece na Internetu na međunarodnoj i nacionalnoj razini, kao i rezultata istraživanja koje je bilo usmjereno na utvrđivanje razine primjene različitih tehničkih potencijala i preventivnih mehanizama od strane ISP-ova, koji značajno mogu doprinijeti sigurnijem digitalnom okruženju za djecu, potrebno je izdvajanje ključnih preporuka. Posebnu pozornost je posvetiti specifičnostima trenutne raspodjele nadležnosti i zakonodavno-pravne arhitekture BiH, koja podrazumijeva sinhrono i aktivno uključivanje više pravnih i društvenih subjekata, na horizontalnoj i vertikalnoj razini suradnje.

Preporuke koje slijede obuhvataju dvije razine: suradnju institucija i stvaranje mreže društvenih aktera, i jasnije pozicioniranje i naglašavanje podzakonske regulative koja tretira ovu oblast:

- **Kreiranje mreže društvene i institucionalne suradnje.** Uspostava funkcionalne mreže institucija, akademske zajednice, organizacija i udruga, koja podrazumijeva aktivno sudjelovanje regulatornog tijela i svih nositelja dozvola za ISP u BiH, sa ciljem analitičkog tretiranja pojava nasilja nad djecom putem informaciono-komunikacijskih tehnologija.
- **Definiranje mehanizma institucionalnog postupanja.** Počevši od postojećih zakonskih nadležnosti, putem jedinstvene radne platforme, uspostaviti funkcionalnu suradnju između policijskih direkcija, pravosudnih tijela, nositelja dozvola za ISP i regulatornog tijela, sa ciljem definiranja jasne procedure registrovanja svih slučajeva zloupotrebe djece na Internetu, i institucionalne koordinacije u tom pogledu, kao i unutarinstiitucionalnih procedura. Institucionalna suradnja treba da obuhvati kreiranje jedinstvenih uputa o postupanju ISP-ova u slučaju detektiraja spornih internet stranica, kao i ostvarivanje uvjeta za formiranje *„blacklist" web* stranica/domena, koje sadrže različite materijale sa svim oblicima nasilja nad djecom putem informaciono-komunikacijskih tehnologija.
- **Uspostava koregulacije kao sustava udruženog djelovanja mehanizma regulacije i samoregulacije.** Iako je uočljiva tendencija ka uspostavljanju mehanizma samoregulacije u domenu zaštite djece na Internetu od strane IKT tvrtki, kao učinkovitiji za BiH može se predložiti sustav koregulacije u ovoj oblasti, imajući u vidu činjenicu da je regulatorno tijelo, u sadašnjim zakonskim okvirima, nadležno za definiranje tehničkih uvjeta prilikom izdavanja dozvola za ISP. Preduvjet za funkcionalno definiranje sustava koregulacije specifično za ovu oblast jeste uspostava jedinstvene organizacije/asocijacije koja bi uključila sve nositelje dozvola za ISP, kao referentnu adresu za institucionalni pristup ostalim akterima koji treba da definiraju mehanizam institucionalnog postupanja.
- **Korištenje mehanizma podzakonske regulative, pravila i propisa regulatornog tijela.** Ne prejudicirajući šire promjene zakonskog okvira, u potpunosti je neophodno iskoristiti mogućnosti koje pruža sadašnja podzakonska regulativa na razini regulatornog tijela, a posebice Pravilo 60/2012 o obavljanju djelatnosti davatelja pristupa Internetu, kao i Pravilo 69/2013 o uvjetima pružanja javnih telekomunikacijskih usluga i odnosima s krajnjim korisnicima. Za učinkovitu primjenu članka 8. stavak (2) Pravila 60/2012 neophodno je jasnije definiranje mehanizma za prijavu štetnih sadržaja koji se odnose na iskorištavanje i zlostavljanje djece, kao i za uspostavljanje procedura za utvrđivanje, proglašavanje i blokiranje štetnih sadržaja na Internetu. Nadalje, članak 36. Pravila 69/2013 (Zaštita maloljetnih lica) omogućava donošenje posebnih propisa regulatornog tijela, za zaštitu maloljetnih lica.
- **Revizija stanja u oblasti zaštite djece na Internetu.** Sa ciljem boljeg povezivanja mreže institucionalnih učesnika, na polugodišnjoj ili godišnjoj osnovi, a na inicijativu nadležnog regulatornog tijela u BiH, neophodno je pregledati i/ili revidirati ukupno stanje u ovoj oblasti, sa konkretnim prijedlozima poboljšanja postojeće regulative i pregledom provedbe postojećih zakonskih i podzakonskih rješenja koja tretiraju i oblast regulacije, pravosuđa i rad policijskih direkcija. Revidiranje stanja na periodičnoj osnovi služila bi kao osnov resornom ministarstvu u procesu izrade Akcionog plana za zaštitu djece i sprječavanje nasilja nad djecom putem IKT u BiH, a zasnivala bi se, pored ostalog, na općim smjernicama Međunarodne unije za telekomunikacije (ITU). Značajno je donošenje zakonskih i podzakonskih akata koji

[68] *Blacklist*-e su metod koji se koristi za filtriranje IP adresa / DNS imena sa kojih dolaze nelegitimni ili zlonamjerni sadržaji. *Blacklist*-e sadrže opsege ili pojedinačne IP adrese i DNS imena koje je potrebno blokirati, a koriste ih različiti uređaji i alati za filtriranje saobraćaja.

će, u skladu sa međunarodnim standardima, regulisati ovu sferu na konkretniji način, prilagođen društvenom kontekstu, te kontinuirano ažuriranje zakonske regulative sukladno veoma dinamičnom tehnološkom razvoju i izraženoj penetraciji korisnika interneta, naročito djece i mladih. Iz analize različitih mehanizama regulacije zaštite djece na internetu proizilazi preporuka o neophodnosti donošenja zakona koji bi na nacionalnoj razini značajno doprinio zaštiti djece na internetu.

U izvješću Europske komisije o napretku BiH (2016), navedeno je da: „Bosna i Hercegovina nema sveobuhvatni strateški pristup za rješavanje pitanja prijetnji u oblasti *cyber* kriminala i *cyber* sigurnosti." U Izvješću je apostrofirana potreba za osnaživanjem reagovanja na prijetnje u oblasti *cyber* sigurnosti, postojećih kapaciteta za borbu protiv *cyber* kriminala, kao i kapaciteta timova za prevenciju i zaštitu od *cyber* incidenata i prijetnji sigurnosti javnih informacijskih sustava (CERT/CSIRT). Na osnovu analize angažmana CERT-ova u različitim zemljama evidento je da njihove aktivnosti zaista mogu značajano doprinijeti osveštavanju javnosti o važnosti *cyber* sigurnosti te poticanju odgovornog korištenja interneta. Kako je CERT tim formiran na razini RS, razmotriti mogućnost formiranja dodatnih CERT timova, kao i CERT i na ostalim razinama. Pored toga, veoma je važno da se stvore potrebni uvjeti koji će obezbijediti da CERT timovi raspolažu dovoljnim brojem stručnog osoblja.

- **Uspostavljanje i promoviranje programa edukacije djece i roditelja – RAK, obrazovni sistem, javni servisi i mediji, IKT tvrtke (ISP i dr.), vlade, nevladin sektor, onlajn platforme** – Realiziranje aktivnosti usmjerenih na podizanju rzine svijesti građana o značaju posjedovanja kompetencija koje se stiču medijskim i informacijskim opismenjavanjem i na značaj uspješne realizacije edukativnih programa koji će mladima, djeci, roditeljima, prosvjetnim radnicima i dr. omogućiti posjedovanje vještina i znanja neophodnih za sigurno korištenje digitalnih medija i iskorištavanje njihovih potencijala, uz svođenje rizika na minimum.

  Analizom aktuelnog stanja u BiH u ovom pogledu uočeni su značajni proaktivni i konstruktivni vidovi djelovanja, kao i intenziviranje realizacije različitih promotivnih aktivnosti, izrada edukativnih sadržaja (Uputa za korištenje medija, IKT i vremenu koje djeca provode pred ekranom, Sigurnost djece online i dr), osnivanje Centra za sigurni internet, uspostava savjetodavne linije za djecu i mlade Plavi telefon i sl. U ovom smislu uočen je značajan angažman RAK-a. Međutim, u kontekstu preporuke koja upućuje na uspostavljanje multisektorskog i sinhronizovanog djelovanja, i u ovom domenu bilo bi korisno da se i ostale relevantne institucije i organizacije aktivnije uključe u promotivne aktivnosti i izradu edukativnih materijala usmjerenih na zaštitu djece na internetu. U ovom smislu preporuka je da se intenzivinije angažiraju i medijske organizacije, naročito one koje čine Javni radio-televizijski sustav u BiH i javne radio i TV stanice, kao i veći angažman ISP-ova. Kampanje sigurnosti/bezbjednosti djece na internetu uglavnom organiziraju ISP-ovi sa velikim brojem korisnika, što je svakako ohrabrujuće, ali ne isključuje potrebu za ovakvom vrstom angažmana i drugih ISP-ova sa manjim brojem korisnika.

- **Unaprjeđenje suradnje između odjea za visokotehnološki kriminalitet** – Odjeli za visokotehnološki kriminalitet policijskih agencija kontinuirano rade na uklanjanju spornih sadržaja sa interneta, prvenstveno sa različitih *web* platformi. Ove aktivnosti se provode uglavnom putem direktnog kontakta sa vlasnicima ovih platformi, bez obzira na to da li se platforme nalaze u zemlji ili inostranstvu. Kako bi se ove i slične aktivnosti mogle provoditi još uspješnije potrebno je obezbijediti direktnu suradnju između odjela za visokotehnološki kriminalitet u policijskim agencijama.

- **Normiranje tehničkih aspekta – Obveze i preporuke za ISP-ove**:

  - Obvezna provedba sustava za filtriranje web prometa ili na strani ISP-eva ili na strani krajnjih korisnika (pretplatnika), jer maloljetnici pristup internetu ostvaruju najčešće putem web-a;
  - Neophodnost obezbjeđivanja usluga/paketa filtriranja prometa na strani ISP-eva ili na strani krajnjih korisnika (pretplatnika), pri čemu je moguće da te usluge/paketi budu ponuđeni krajnjim korisnicima i na komercijalnoj osnovi;
  - Neophodnost obezbjeđivanja tehničkih preduvjeta za filtriranje prometa koje se primjenjuje na sve oblike povezivanja koje ISP nudi;
  - Provedba i upraba sustavaza blokiranje pristupa baziranih na listama malicioznih URL adresa;

- Provedba sustava koji omogućuju krajnjim korisnicima da na jednostavan način uključe uslugu filtriranja prometa;
- Provedba potpore za izradu različitih profila za filtriranje prometa i njihovu primjenu na različite uređaje u mreži pretplatnika;
- Provedba potpore za odgovarajuće sustave zaštite u slučaju kada su pretplatnici obrazovne institucije, a posebno u slučajevima kada se radi o osnovnim i srednjim školama. Ovdje se preporučuje obvezno filtriranje eksplicitnih sadržaja poput pornografije, gambling sadržaja i sl.;
- Neophodnost obveznog redovitog ažuriranja i testiranja ispravnosti primjene pravila za filtriranje prometa na uređajima ISP-ova;
- Provedba sustava koji omogućava uvid krajnjim korisnicima u blokirani web promet;
- Kreiranje usluga/paketa koje ISP-ovi nude, a koji se odnose na filtriranje prometa koji je nepoželjan za djecu.
- Neophodna je integracija prava djeteta u korporativne politike, što bi podrazumijevalo da ove tvrtke sve raspoložive tehničke resurse, koji pritom ne dovode u pitanje njihovu gospodarsku održivost, koliko je moguće usmjere na zaštitu djece na internetu. U tom kontekstu je primarno bavljenje informatičkom sigurnosti, te sudjelovanje u radu organizacija koje se bave sigurnosti djece na internetu.

KORIŠTENI IZVORI

- Agencija Europske unije za kibernetičku sigurnost/European Union Agency for Cybersecurity (ENISA). Dostupno na: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/enisa_hr
- Agencija za zaštitu osobnih podataka u Bosni i Hercegovini. [online]. [2021-01-18]. Dostupno na:http://azlp.ba/GDPR_Menu/Sta_je_GDPR/default.aspx?id=2373&langTag=bsBA&template_id=149&pageIndex=1
- Akcioni plan za zaštitu djece i sprječavanje nasilja nad djecom putem informaciono-komunikacijskih tehnologija u Bosni i Hercegovini za period 2014-2015. Vijeće ministara Bosna i Hercegovina.
- Dostupno na: http://msb.gov.ba/PDF/140605_Nasilje_bosnanski_SG_ver2.pdf
- Bogdan-Martin, D.(2020). Smjernice za IKT tvrtke u pogledu sigurnosti djece na intrenetu. Međunarodna unija za telekomunikacije. Dostupno na: http://telrad.net/download/22.pdf.
- Ciboci, L., Ćosić Pregrad, I., Kanižaj, I., Potočnik, D. i Vinković, D. (2020). Nacionalno istraživanje o sigurnosti djece internetu HR Kids online. Dostupno na: http://hrkids.online/prez/EUKidsOnlineHRfinal.pdf .
- CSIRTs Network (engl. Computer Security Incident Response Team). Dostupno na: https://www.enisa.europa.eu/topics/csirts-in-europe .
- Čengić, L., Dokić Mrša, S., Kafedžić, L., Grahovac, N., Zečević, I., Trninić, D., Sivrić, I., Krajina, S., Romčević Šukalo, J., Risojević, S., Džaferović, A. (2021). Smjernice o korištenju medija, informacijsko-komunikacijskih tehnologija i vremenu koje djeca provode pred ekranom. Sarajevo: Regulatorna agencija za komunikacije BiH i Fondacija za razvoj medija i civilnog društva "Mediacentar". Dostupno na: https://docs.rak.ba/articles/470200ce-f648-4dee-b6f6-2535bd295e37.pdf .
- Digitalni vodič „Deca i internet – pametno od početka". Dostupno na: https://digitalni-vodic.ucpd.rs/ .
- Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća o mjerama za visoki zajednički nivo sigurnosti mrežnih i informacijskih sustava (NIS direktiva - EU Network and Information Security Directive). Dostupno na: https://www.enisa.europa.eu/topics/nis-directive .
- Direktiva o audiovizuelnim medijskim uslugama (2018/1808). Europski parlament i Vijeće Europe.
- Dječje dostojanstvo u digitalnom svijetu, Savez za dostojanstvo djeteta: Izvješće radne grupe za tehnologiju. Dostupno na: https://www.sigurnodijete.ba/blog/svjetski-kongres-dostojanstvo-djeteta-u-digitalnom-svijetu/ .
- Europska konvencija za zaštitu ljudskih prava i osnovnih sloboda (1953). Vijeće Evrope. Dostupno na: https://www.echr.coe.int/documents/convention_bos.pdf .
- Furnémont (Wagner-Hatfield), J. F. (2020). „Pregled odredbi Kodeksa o audiovizuelnim uslugama u vezi s zaštitom maloljetnika". Izvješće za: Regulatorna agencija za komunikacije BiH. Vijeće Evrope.
- General Data Protection Regulation (GDPR) (2016). Evropski parlament. Dostupno na: https://gdpr-info.eu/ .
- Godišnje izvješće Regulatorne agencije za komunikacije za 2020. godinu. Dostupno na: https://docs.rak.ba//documents/f71db1bf-2b1d-4f26-84d8-0905e7619849.pdf
- Hasanagić, S., Papović, M. i Kovačević, S. (2020). Medijske navike djece i stavovi roditelja. Regulatorna agencija za komunikacije BiH i UNICEF. Dostupno na: https://www.unicef.org/bih/izvje%C5%A1taji/medijske-navike-djece-i-stavovi-roditelja .
- Hasanagić, S., Papović, M. i Lević, E. (2021). Medijske navike odraslih u BiH. Regulatorna agencija za komunikacije

i Vijeće Evrope. Dostupno na: https://medijskapismenost.ba/wp-content/uploads/2021/10/Medijske-navike-odraslih-u-BiH.pdf .

- Kako zaštiti dijete u svijetu interneta, mrežnih tehnologija i mobilnih telefona (2016/2017). Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM). Dostupno na:https://www.hakom.hr/UserDocsImages/2016/dokumenti/HAKOM_BROSURA_FIN.pdf?vel=3826397 .
- Kako zaštiti dijete u svijetu interneta, mrežnih tehnologija i mobilnih telefona (2017/2018). Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM). Dostupno na:https://www.hakom.hr/UserDocsImages/2018/dokumenti/HAKOM_BROSURAmala.pdf?vel=1730420 .
- Kako se zaštiti u svijetu interneta i mobilnih telefona. Kratki vodič za djecu i roditelje (i sve koji žele znati više u digitalnom dobu) (2018/2019). Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM). Dostupno na: https://www.hakom.hr/UserDocsImages/2019/dokumenti/HAKOM_BROSURA_2018.pdf?vel=2677470 .
- Kako se zaštiti u svijetu interneta i mobilnih telefona. Kratki vodič za roditelje (i sve koji žele znati više u digitalnom dobu) (2020). Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM). Dostupno na: https://www.hakom.hr/UserDocsImages/2020/Hakom%202019_brosura_kako%20se%20zastititi%20u%20svijetu%20interneta.pdf?vel=1440144 .
- Kako se zaštiti u svijetu interneta i mobilnih telefona. Kratki vodič za roditelje (i sve koji žele znati više u digitalnom dobu) (2021). Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM). Dostupno na: https://www.hakom.hr/UserDocsImages/2020/dokumenti/HAKOMova%20bro%C5%A1ura%20%20Kako%20se%20za%C5%A1tititi%20u%20svijetu%20interneta%20i%20mobilnih%20telefona.pdf?vel=14464818
- Kako se zaštiti u svijetu interneta i mobilnih telefona. Kratki vodič za roditelje (i sve koji žele znati više u digitalnom dobu) (2022). Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM). Dostupno na: https://www.hakom.hr/UserDocsImages/2022/dokumenti/Bro%C5%A1uraKako%20se%20za%C5%A1tititi%20u%20svijetu%20interneta%20i%20mobilnih%20ure%C4%91aja_2022.pdf?vel=18464276
- Kodeks o audiovizuelnim medijskim uslugama i medijskim uslugama radija, RAK. Dostupno na: https://docs.rak.ba//articles/7f0a56a6-6c7d-423b-8ff9-b50bed88bc52.pdf
- Kodeks o komercijalnim komunikacijama, RAK. Dostupno na: https://docs.rak.ba//articles/12903551-ca2a-47b0-99ac-4264e199c2bf.pdf .
- Kodeks za dizajniranje prilagođeno uzrastu/Introduction to the Age appropriate design code, ICO./Information commissioner's Office UK. Dostupno na: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/
- Konvencija o kibernetičkom kriminalu (2001). Vijeće Evrope. Dostupno na: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa401 .
- Konvencija o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja. Dostupno na: https://rm.coe.int/168046e1d1 .
- Konvencija UN-a o pravima djeteta (1989). Generalna skupština Ujedinjenih naroda. Dostupno na: https://www.unicef.org/bih/media/676/file/Konvencija%20o%20pravima%20djeteta.pdf?fbclid=IwAR0CMNHt4iz3GL1pX4OgswiM4xY_n3DBgvt1sBO0jj6Nd5Xv67lSKQdcysc .
- Konvencija Vijeća Europe o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja (2007). Dostupno na: https://rm.coe.int/168046e1d1 .

- Konvencija za zaštitu pojedinaca u vezi sa automatskom obradom ličnih podataka (Konvencija 108)/ Konvencija 108+ (Modernizovana konvencija) (2018). Vijeće Evrope. Dostupno na: https://www.poverenik.rs/sr-yu/међународни-документи6/савет-европе/3457-модернизована-конвенција-о-заштити-лица-у-односу-на-аутоматску-обраду-личних-података-конвенција-108.html .
- Korać, N., Zečević, I. i Bajraktarević, J. (2009). Utjecaj televizije na djecu i maloljetnike. Sarajevo: RAK. Dostupno na: https://docs.rak.ba//articles/962a5448-464a-4827-9337-a84f7220fbba.pdf
- Krivični zakon Bosne i Hercegovine „Sl. glasnik BiH", br. 3/2003. Dostupno na: https://www.paragraf.ba/propisi/bih/krivicni-zakon-bosne-i-hercegovine.html
- Kazneni zakon Brčko diskritka BiH, „Sl. glasnik Brčko distrikta BiH", br. 19/2020. Dostupno na: https://www.paragraf.ba/propisi/brcko/krivicni-zakon-brcko-distrikta-bosne-i-hercegovine.html
- Kazneni zakon Federacije Bosne i Hercrgovine „Sl. novine FbiH", br. 36/2003. Dostupno na: https://www.paragraf.ba/propisi/fbih/krivicni-zakon-federacije-bosne-i-hercegovine.html .
- Kazneni zakon Republike Srpske, „Sl.glasnik RS", br. 49/2003. Dostupno na: https://www.paragraf.ba/propisi/republika-srpska/krivicni-zakon-republike-srpske-t.html .
- Kazneni zakon Crne Gore "Sl. list RCG", br. 70/2003, 13/2004 - ispr. i 47/2006 i "Sl. list CG", br. 40/2008, 25/2010, 32/2011, 64/2011 - dr. zakon, 40/2013, 56/2013 - ispr., 14/2015, 42/2015, 58/2015 - dr. zakon, 44/2017, 49/2018 i 3/2020). Dostupno na: https://www.paragraf.me/propisi-crnegore/krivicni-zakonik-crne-gore.html .
- Kazneni zakon Srbije "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. Dostupno na: https://www.paragraf.rs/propisi/krivicni-zakonik-2019.html
- Kujundžić, B. (2015). Četvrta grana vlasti/ misija i put neovisnog regulatora u Bosni i Hercegovini. Sarajevo: Friedrich Ebert Stiftung.
- Livingstone, S. i dr. (2009). "EU Kids Online: Završni izvješće". Londonska škola ekonomije.
- LOI n° 2022-300 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à internet (NOR : ECOX2137360L). Dostupno na: https://www.legifrance.gouv.fr/download/pdf?id=LIhsICgDpYJsCxxsL1_RUt_gRqcUA3qn9Cpuf_2cwJA=
- Milanović, Z. i Radovanović, R. (2020). Informaciona bezbednost ključni problem savremene organizacije. Interni projekat TRANZICIJA I EKONOMSKI KRIMINAL II - TEMATSKI ZBORNIK RADOVA, ISBN 978-86-7020-305-1, Kriminalističko-policijska akademija, Beograd, 2014. str. 135-149. Dostupno na: https://www.researchgate.net/publication/345005347_INFORMACIONA_BEZBEDNOST_KLUCNI_PROBLEM_SAVREMENE_ORGANIZACIJE
- Milutinović, I. (2017). Medijski sistem i nacionalni interes u kontekstu evrointegracija: stanje i perspektive Republike Srpske. Nacionalni interes: časopis za nacionalna i državna pitanja, Beograd: Institut za političke studije, godina HIII, vol. 28, broj 1, 87–104.
- Nacionalna strategija kibernetičke sigurnosti. Nacionalni CERT, Republika Hrvatska. Dostupno na: https://www.cert.hr/nacionalna-strategija .
- Non-Violent Childhoods : Action Plan for the Prevention of Violence against Children 2020–2025. Publications of the Ministry of Social Affairs and Health 2020:34. Dostupno na:https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162554/STM_2020_34_J.pdf
- Odluka o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti (NN 108/2015). Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2015_10_108_2106.html .

- Opasnosti Facebooka. Hrvatska akademska istraživačka mreža CARNet/Nacionalni CERT, Republika Hrvatska. Dostupno na: https://www.cert.hr/wp-content/uploads/2018/02/Opasnosti-Facebooka.pdf .
- Opći komentar br. 25 (2021) o pravima djeteta u vezi sa digitalnim okruženjem. Komitet za prava djeteta UN. Dostupno na: https://cpd.org.rs/wpcontent/uploads/2021/08/Op%C5%A1ti-komentar-br-25-Prava-deteta-u-digitalnom-okru%C5%BEenju.pdf
- Praktičan vodič za kompanije koji im pomaže da razumiju i poboljšaju svoj uticaj na dečija prava. Specijalni vodič za kompanije „Deca su svima važna" (2013), UNICEF. Dostupno na: https://api.pks.rs/storage/assets/Deca-su-svima-vazna.pdf .
- Pravilo 60/2012 o obavljanju djelatnosti davaoca pristupa internetu, RAK. Dostupno na: https://docs.rak.ba/articles/0c5876db-760a-4bb3-82ce-71bc9b92988a.pdf .
- Pravilo 69/2013 o uslovima pružanja javnih telekomunikacijskih usluga i odnosima s krajnjim korisnicima, RAK. Dostupno na: https://docs.rak.ba//articles/16232d73-7be2-4b5e-a026-b7ec6ed01988.pdf .
- Prensky, M. (2005). Digitalni urođenici, digitalne pridošlice. Edupoint časopis, časopis o primjeni informacijskih tehnologija u obrazovanju, godište V / ISSN 1333-5987. Dostupno na: http://edupoint.carnet.hr/casopis/40/clanci/3.html .
- Preporuka ECD-a u pogledu bezbjednosti djece na internetu (eng. Recommendation of the Council on Children in the Digital Environment), (2012, ažurirana 2021). Dostupno na: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389 .
- Prilike i izazovi za djecu i IKT industriju (2019), UNICEF. Dostupno na: http://telrad.net/download/22.pdf .
- Puharić, P. (2019). Upute za društveno odgovorne informacijsko-komunikacijske kompanije u oblasti zaštite djce od seksualnog iskorištavanja i zlostavljanja. Save the Children in North West Balkans. Dostupno na: https://nwb.savethechildren.net/sites/nwb.savethechildren.net/files/library/Smjernice-za-drustveno-odgovorne-informacijsko-komunikacijske-kompanije-u-oblasti-zastite-djece-od-seksualnog-iskoristavanja-i-zlostavljanja-lat.pdf .
- Regionalna publikacija "Regulatorne agencije za medije i zaštita maloljetnih osoba" (2019). Vijeće Evrope. Dostupno na: https://rm.coe.int/regulatorne-agencije-za-medije-i-zastita-maloljetnih-osoba-bos-/1680a3351b .
- Seksualno iskorištavanje djece putem Interneta i spolno zlostavljanje. Ministarstvo unutarnjih poslova, Republika Hrvatska. Dostupno na: https://policija.gov.hr/prevencija/racunalna-sigurnost/seksualno-iskoristavanje-djece putem-interneta-i-spolno-zlostavljanje/461 .
- Sigurnost bežičnih mreža. Nacionalni CERT, Republika Hrvatska. Dostupno na: https://www.cert.hr/wp-content/uploads/2019/03/Sigurnost-bezicnih-mreza.pdf .
- Sigurnije na internetu (drugo izdanje). Hrvatska akademska istraživačka mreža CARNet/Nacionalni CERT, Republika Hrvatska. Dostupno na: https://www.cert.hr/wp-content/uploads/2018/02/Sigurnije_na_internetu.pdf
- Upute OECD-a za davaoce digitalnih usluga (eng. OECD guidelines for digital service providers), (2021). Dostupno na: https://www.oecd.org/mcm/OECD%20Guidelines%20for%20Digital%20Service%20Providers.pdf .
- Upute za IKT tvrtke u pogledu bezbjednosti djece na intrenetu. Međunarodna unija za telekomunikacije. Dostupno na: http://telrad.net/download/22.pdf.
- Upute za kreatore politika o zaštiti djece na internetu (2020). Međunarodna unija za telekomunikacije. Dostupno na: https://docs.rak.ba/articles/80657572-ac8f-43f1-8212-00025ce117b8.pdf .

- Upute za strateški okvir cyber sigurnosti u Bosni i Hercegovini (2019). OSCE. Dostupno na: https://www.osce.org/files/f/documents/4/8/438386.pdf .
- Telekomunikacijski indikatori BiH u 2020. godini, Regulatorna agencija za komunikacije BiH. Dostupno na: https://rak.ba/bs-Latn-BA/telecom-market-analysis
- Trninić, D. i Kuprešanin Vukelić, A. (2021). Privacy On The Internet Concerning Generation Z In Bosnia And Herzegovina. „Media Literacy and Academic Research", Vol. 4, No. 1, april, 180-198. https://www.mlar.sk/wpcontent/uploads/2021/04/12_Trninic_Vukelic.pdf
- Uredničke smjernice BBC-a/Editorial Guidelines BBC. Dostupno na: https://www.bbc.com/editorialguidelines/guidelines .
- UREDBA (EU) 2021/1232 EUROPSKOG PARLAMENTA I VIJEĆA od 14. srpnja 2021. o privremenom odstupanju od određenih odredbi Direktive 2002/58/EZ u pogledu tehnologija koje pružatelji brojevno neovisnih interpersonalnih komunikacijskih usluga upotrebljavaju za obradu osobnih i drugih podataka u svrhu borbe protiv seksualnog zlostavljanja djece na internetu. Dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32021R1232&from=EN .
- UREDBA (EZ) br. 460/2004 EUROPSKOG PARLAMENTA I VIJEĆA od 10. ožujka 2004. o osnivanju Europske agencije za mrežnu i informacijsku sigurnost. Dostupno na:
- https://eur-lex.europa.eu/legalcontent/HR/TXT/PDF/?uri=CELEX:32004R0460&from=HR
- Uredba o bezbednosti i zaštiti djece pri korišćenju informaciono-komunikacionih tehnologija. Dostupno na: http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2020/13/4/reg
- Ustav Bosne i Hercegovine Aneks IV Općeg okvirnog sporazuma za mir u Bosni i Hercegovini i "Sl. glasnik BiH", br. 25/2009 - Amandman I. Dostupno na: https://www.paragraf.ba/propisi/bih/ustav-bosne-i-hercegovine.html .
- Ustav Crne Gore "Sl. list CG", br. 1/2007 i 38/2013 - Amandmani I-XVI. Dostupno na: https://www.paragraf.me/propisi-crnegore/ustav-crne-gore.html .
- Ustav Federacije Bosne i Hercegovine Sl. novine FBiH", br. 1/1994 i Amandmani. Dostupno na: https://www.paragraf.ba/propisi/fbih/ustav-federacije-bosne-i-hercegovine.html
- Ustav Republike Srbije „Sl. glasnik RS", br. 98/2006 i 115/2021. Dostupno na: https://www.paragraf.rs/propisi/ustav_republike_srbije.html .
- Ustav Republike Srpske "Sl. glasnik RS", br. 21/1992 i Amandmani. Dostupno na: https://www.paragraf.ba/propisi/republika-srpska/ustav-republike-srpske.html .
- Vodič: Interakcija sa djecom i mladima na mreži/Guidance: Interacting with children and young people online, BBC. Dostupno na: https://www.bbc.com/editorialguidelines/guidance/children-young-people-online/ .
- Zakon o digitalnim uslugama (2022). Evropski parlament. Dostupno na: https://www.europarl.europa.eu/doceo/document/A-9-2020-0172_HR.html .
- Zakon o informacionoj bezbednosti "Sl. glasnik RS", br. 6/2016, 94/2017 i 77/2019. https://www.paragraf.rs/propisi/zakon_o_informacionoj_bezbednosti.html .
- Zakon o informacionoj bezbjednosti „Sl. glasnik RS", br. 70/2011. Dostupno na:
- https://izis.org/wpcontent/uploads/2020/09/IZIS_080UPP_110ZAK_Zakon_o_informacionoj_bezbjednosti.pdf .
- Zakon o komunikacijama „Službeni glasnik BiH", br. 31/03. Dostupno na: https://docs.rak.ba//articles/da724391-4a61-429b-885914d77fbfbf43.pdf .

- Zakon o zaštiti ličnih podataka „Sl. glasnik BiH", br. 49/2006, 76/2011, 89/2011. Dostupno na: https://www.paragraf.ba/propisi/bih/zakon-o-zastiti-licnih-podataka.html .
- Zakon o elektroničkim medijima „Urbroj: 71-10-01/1-21-2. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2021_10_111_1942.html .
- Zakon o informacijskoj sigurnosti (NN 79/2007). Dostupno na: https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti .
- Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018). Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_07_64_1305.html .
- Zakon o izmjenama i dopunama Zakona o zaštiti mladih (eng. Second Act amending the German Youth Protection Act) (2021). Dostupno na: https://www.bundesrat.de/SharedDocs/beratungsvorgaenge/2021/0101-0200/0195-21.html .
- Zaštitite privatnost na Facebooku, verzija 3/10/2015. Hrvatska akademska istraživačka mreža CARNet/ Nacionalni CERT, Republika Hrvatska. Dostupno na: https://www.cert.hr/wp-content/uploads/2019/04/BrosuraPrivatnost_2015_0.pdf
- Zečević, I. (2010). Smjernice za klasifikaciju televizijskih sadržaja. RAK i UNICEF. Dostupno na: https://docs.rak.ba//documents/14ebe2c5-9cfa-4a54-8d40 d07a99e4f07a.pdf

PRIVITKE

Privitak 1: Upitnik upućen pružateljima pristupa internetu u BiH o temi Zaštite djece na Internetu u sustavima korisnika dozvola RAK-a

Projekt „Zaštita djece na Internetu u sustavima korisnika dozvola Regulatorne agencije za komunikacije" - Pitanja za ISP

Naziv operatora:	
Datum:	

1. Da li postoje tehnički uvjeti i za filtriranje prometa po različitim protokolima (HTTP, SMTP, ...) na strani ISP-a?

    a. Ako postoje, navedite o kojim protokolima se radi.
    b. Koje sve uređaje/servise koristite za filtriranje prometa (navesti tačan naziv uređaja / servisa koji se koristi)?

2. Da li postoji filtriranje neželjenog prometa bez znanja krajnjih korisnika (pretplatnika) koje se radi na strani ISP-a?

    a. Ako postoji, navedite o kojim vrstama prometa se radi.
    b. Koje sve urađaje/servise koristite za ovu namjenu (navesti tačan naziv uređaja / servisa koji se koristi)?

3. Da li postoji mogućnost kupovine usluge filtriranja prometa na strani ISP-a?

    a. Ako postoji, navedite o kojim uslugama (i paketima usluga) se radi i na koje protokole se primjenjuje (npr. HTTP - filtriranje potencijalno malicioznih web sajtova).
    b. Da li se registracija za ovu uslugu radi online ili putem šaltera?
    c. Da li su pretplatniku informacije o filtriranju prometa dostupne u toku registracije?
    d. Da li postoje detaljne informacije o tome koje vrste prometa su blokirane, sa odgovarajućim primjerima takvog prometa?
    e. Dostavite cjenik usluga/paketa filtriranja prometa.

3. Da li se filtriranje prometa primjenjuje na sve oblike povezivanja koje ISP nudi (ADSL, kabelska, optička veza, mobilni internet, itd.)?

    a. Ako to nije slučaj, navedite sve oblike povezivanja koje ISP nudi, a za koje se vrši filtriranje prometa, kao i sve oblike povezivanja koje ISP nudi, a za koje se ne vrši filtriranje prometa.

5. Da li postoje pretplatnici za koje se ne vrši filtriranje prometa na strani ISP-a?

    a. Ako postoje, da li je njihov saobraćaj evidentiran?
    b. Ako jeste, da li se evidentira na način koji povezuje promet sa pretplatnikom?

6. Da li postoji mogućnost inspekcije enkriptovanog prometa na strani ISP-a?

    a. Ako postoji, navedite o kojim se vrstama prometa radi (npr. inspekcija HTTPS prometa).

7. Da li pretplatnici samostalno mogu da uključuju/isključuju opcije filtriranja prometa na strani ISP-a?

    a. Ako to jeste slučaj, na koji način pretplatnici to mogu da urade (npr. putem određenog web interfejsa/aplikacije) i sa kojom razinom detaljnosti (da li je npr. moguće deblokirati pristup određenim sajtovima)?

8. Da li postoji mogućnost filtriranja prometa na strani pretplatnika, a na opremi koju pretplatniku isporučuje ISP?

    a. Ako postoji, da li ISP koristi ove mogućnosti?
    b. Ako postoji i ako ISP koristi ove mogućnosti, da li korisnik ima pristup ovoj opremi i da li je može kontrolirati, te npr. isključiti opciju filtriranja prometa?
    c. Da li postoji mogućnost kreiranja različitih profila za filtriranje prometa i primijeniti ih na različite uređaje u mreži pretplatnika (npr. poseban profil za filtriranje prometa za uređaj koji koristi dijete)?

9. Da li postoje razlike po pitanju filtriranja prometa ako su pretplatnici obrazovne institucije, posebno ako se radi o osnovnim i srednjim školama?
    a. Ako postoje, navedite koje.

10. Da li ste provodili testiranja ispravnosti primjene pravila za filtriranje prometa?

    a. Ako je odgovor potvrdan, na koji način i koliko često se ova testiranja provode?
    b. Ako odgovor nije potvrdan, da li postoje planovi za redovne provjere efikasnosti i kvaliteta filtriranja prometa?
    c. Ako se postoje, kolika je točnost primijenjenih mehanizama za filtriranje prometa?

11. Kada je pristup nekom resursu blokiran, da li se i koje informacije o tome dostavljaju pretplatniku?

    a. Da li se ove informacije čuvaju na strani ISP-a i koliko dugo?
    b. Da li pretplatnik ima mogućnost da prijavi nepravilno blokiranje prometa i na koji način?

12. Da li postoje usluge/paketi koji se odnose na filtriranje prometa, a koji je nepoželjan za djecu?

    a. Ako postoje, o kojim uslugama/paketima se radi?
    b. Ako postoje da li se ovo filtriranje radi na strani ISP-a, na strani pretplatnika ili na obe strane??

Privitak 2: Upitnik o temi sigurnost/bezbjednost djece na Internetu

(odgovore boldirati/markirati/podvući, opisne navesti u tekst box)

1. Da li ste upoznati sa smjernicama za IKT kompanije u pogledu sigurnosti/ bezbjednosti djece na Internetu?

- Da
- Ne

2. Možete li navesti koje ste konkretne aktivnosti poduzeli o temi sigurnosti/ bezbjednosti djece na Internetu?

3. Da li ste član domaćih i/ili međunarodnih udruženja/zajednica/stručnih skupina sigurnosti/bezbjednosti djece na Internetu?

- Da
- Ne
- (Ako je odgovor Da, navesti naziv):

4. Da li u okviru svoje tvrtke realizirate kampanje sigurnosti/bezbjednosti djece na Internetu?

- Da
- Ne
- (Ako je odgovor Da, navesti naziv):

5. Da li putem svojih web stranica promovirate sigurnost/bezbjednost djece na Internetu?

- Da
- Ne

6. Po vašem mišljenju i vašim iskustvima, na skali od 1 do 5, ocijenite važnost sigurnosti/ bezbjednosti djece na Internetu (1 najniže, 5 najviše):

- 1
- 2
- 3
- 4
- 5

7. Da li u okviru svoje tvrtke imate posebnu organizacionu jedinicu ili osobu koja se isključivo bavi sajber sigurnosti?

- Da
- Ne

8. Koji čimbenik najviše utječe na razvoj sajber sigurnosti u vašoj tvrtki?

- Regulacija
- Zahtjevi/potražnja korisnika
- Politika/strategija kompanije
- Tržišni uvjeti
- Drugo (Navesti):

9. Da li ste u zadnju godinu dana imali službene zahtjeve policije ili drugog nadležnog organa za dostavu podatka o svojim korisnicima i njihovim aktivnostima na Internetu?

- Da
- Ne

10. Koliko dugo čuvate podatke (logove) svojih korisnika?

- 6 mjeseci
- 1 godinu
- 2 godine
- Drugo (Navesti):

11. Po vašem mišljenju i vašim iskustvima, preko kojih servisa djeca najlakše mogu biti ugrožena na Internetu? (možete izabrati više odgovora)

- Aplikacije za razmjenu poruka (Viber, WhatsApp, Facebook Messenger...)
- Društvene mreže (Facebook, Instagram, TikTok...)
- Aplikacije za live streaming (Faccebook live, You Tube live, Twitch live...)
- Drugo (Navesti):

12. Po vašem mišljenju i vašim iskustvima, koji od navedenih mehanizama roditeljskog nadzora je najučinkovitiji za zaštitu djece na Internetu? (možete izabrati više odgovora)

- Liste za blokiranje/dozvola pristupa
- Filteri sadržaja
- Nadzor upotrebe
- Vremenska ograničenja
- Upravljanje kontaktima
- Drugo (Navesti):

13. Da li u okviru svoje ponude imate posebnu uslugu/paket za djecu sa odgovarajućim sigurnosnim mehanizmima?

- Da
- Ne
- (Ako je odgovor Da, navesti naziv i link):

14. Da li u okviru svoje ponude imate posebnu uslugu roditeljska kontrola/nadzor koja omogućava neki od mehanizama roditeljske kotrole/nadzora kao što su liste za blokiranje, filtriranje sadražaja, nadzor upotrebe, vremenska ograničenja uporabe i drugo?

- Da
- Ne
- (Ako je odgovor Da, navesti naziv i link):

15. Da li u okviru svoje tvrtke razvijate mehanizme kao što su softver za roditeljsku kontrolu/nadzor i drugi alati koji omogućavaju roditeljima da upravljaju pristupom Interneta djeci?

- Da
- Ne

16. Da li u okviru svoje ponude imate rutere koji omogućavaju funkciju roditeljske kontole/nadzora na svim uređajima u koji su povezani sa njim?

- Da
- Ne

17. Da li ste imali zahtjeve ustanova i organizacija koji su vaši korisnici (npr. škole, fakulteti, bolnice i sl.), a koji u svojim prostorijma daju mogućnost otvorenog pristupa Internetu preko wifi mreže, za blokiranje nekih stranica na Internetu za koje se zna da im je sadržaj neprikladan za široku publiku?

- Da
- Ne

18. Da li promovirate alate i aplikacije roditeljske kontrole/nadzora djece na Internetu razvijene od strane tvrtke koje se bave zaštitom i sigurnošću na Internetu?

- Da
- Ne
- (Ako je odgovor Da, navesti naziv i link):

19. Po vašem mišljenju i vašim iskustvima, da li kampanja sigurnosti/bezbjednosti djece na Internetu realizirana u okviru vaše tvrtke, kroz razvijanje sopstvenih mehanizama roditeljske kontrole/nadzora, promoviranje već postojećih aplikacija i alata za zaštitu djece na Internetu, objavljivanja edukativnih sadržaja o zaštiti djece na Internetu i dr., u javnosti stvara pozitivnu sliku vaše tvrtke te na taj način privlači pozornost potencijalnih korisnika vaših usluga?

- Da
- Ne

20. Da li imate ideje/prijedloge za dopunu/izmjenu propisa, a u cilju učinkovitijeg djelovanja o temi sigurnost/bezbjednost djece na Internetu?

- Da
- Ne
- (Ako je odgovor Da, navesti koje):

21. Da li želite nešto dodati što nije obuhvaćeno navedenim pitanjima, a smatrate bitnim za temu sigurnost/bezbjednost djece na Internetu?