

ZAŠTITA PRAVA DJECE U DIGITALNOM OKRUŽENJU

Sažetak: Progresivan razvoj informacijskih tehnologija donosi nove rizike i ugroze za zaštitu prava djece te postaje tema koja sve više zaokuplja znanstvene i stručne rasprave. Države su, prema Preporukama Vijeća Europe i Smjernicama o pravosuđu naklonjenom djeci, dužne osigurati djelotvorna pravna sredstva u slučaju povrede njihovih ljudskih prava i temeljnih sloboda u digitalnom okruženju. Pritom ključnu ulogu igra i sama prevencija i edukacija o zaštiti djece te njihovom pristupu virtualnom okruženju. Sukladno navedenom, autorice će u ovom radu dati prikaz mjera zaštite djece na internetu uz naglasak na djelotvorna pravna sredstva temeljena na aktualnom zakonodavnom okviru.

Ključne riječi: djeca, digitalno okruženje, kaznena djela, pravna sredstva, sigurnost.

1. Uvodna riječ: Mediji i pravo na privatnost u digitalnom okruženju

U suvremenom, informacijskom društvu informacije postaju temeljem procesa javnog informiranja, sastavnog dijela demokratskih i političkih procesa. Informacije postaju važan element slobode i prava na širenje informacija koji u velikoj mjeri ovisi upravo o legitimnosti i mogućnosti upravljanja zbirkama podataka. Razvidno je da sa postupak širenja informacija, njihovog tiskanja, objavljivanja ili emitiranja u medijima podliježe njihovom pogrešnom interpretiranju. Logično, jedno od ustavnopravnih i diferencirajućih sredstava ograničavanja slobode javnog informiranja radi zaštite prava ličnosti jest pravo na ispravak informacije. Sam Ustav Republike Hrvatske (»Narodne novine« br. 56/90, 135/97, 8/98 –pročišćeni tekst, 113/2000,124/2000 – pročišćeni tekst, 28/2001, 41/2001 –pročišćeni tekst, 85/2010-pročišćeni tekst, 05/14 – u daljnjem tekstu Ustav RH) jamči pravo na ispravak svakomu kome je javnom viješću povrijeđeno Ustavom i Zakonom utvrđeno pravo (Ustava RH čl. 38.). Sam postupak širenja informacija, njihovog tiskanja, objavljivanja ili prikazivanja uređuje pravna regulativa javnog informiranja. U Republici Hrvatskoj informiranje se ostvaruje putem medija koji su podložni nacionalnom zakonodavstvu odnosno Zakonu o medijima¹, („Narodne novine“, br. 59/04., 84/11, 81/13 - dalje –ZM).

1 Mediji su: novine i drugi tisak, radijski i televizijski programi, programi novinskih agencija, elektroničke publikacije, teletekst i ostali oblici dnevnog ili periodičnog objavljivanja urednički oblikovanih programskih sadržaja prijenosom zapisa, glasa, zvuka ili slike. Mediji nisu knjige, udžbenici, bilteni, katalozi ili drugi nositelji objavljivanja informacija koji su namijenjeni isključivo obrazovnom, znanstvenom i kulturnom procesu, oglašavanju, poslovnoj komunikaciji, radu trgovačkih društava, zavoda i ustanova, udruga, političkih stranaka, vjerskih i ostalih organizacija, školska glasila, »Narodne novine« Republike Hrvatske, službena glasila jedinica lokalne i područne (regionalne) samouprave i ostala službena priopćenja, plakati, letci, prospekti i transparenti, te video stranice bez žive slike i druge besplatne obavijesti, osim ako ovim Zakonom nije drukčije propisano. (ZM, čl.2. st. 1.)

Pravno gledano, zanimljivo je stajalište ispravka informacije koje predstavlja jedno od logičkih, ustavnopravnih i diferencirajućih sredstava ograničavanja slobode javnog informiranja radi zaštite prava ličnosti. ZM daje pravo pravnoj i fizičkoj osobi da u roku od 30 dana od objave neistinite ili nepotpune informacije od glavnog urednika zahtijeva objavu ispravka o obavijesti kojom su povrijeđena njena prava i interesi². Ispravak se mora objaviti u prvom, a ako stigne prekasno, u drugom programskom sadržaju nakon primitka; bez promjena i dopuna; na istom ili istovrijednom mjestu programskog prostora; na isti ili istovrijedan način na koji je objavljena informacija; u programima radija i televizije objavljuje se čitanjem u istom programu i terminu ili u istoj vrsti programa istovjetne gledanosti.³ Zakon također uređuje pravila sudskog postupka ako glavni urednik odbije objaviti ispravak ili ga ne objavi u roku i na način propisan zakonom. Sagledavajući bit slobode javnog informiranja u pravnu slobodu izvješćivanja, pobornici logičkih ograničenja slobode tiska u ispravku informacije vide sredstvo kojim se podupire načelo dužnosti istine, tj. prenošenja samo istine u izvješćivanju. Za pobornike ustavnopravnog ograničavanja slobode javnog informiranja granice javnog informiranja izvode se iz zaštite osobne časti, te iz načela jednakosti građana. Za teoriju diferencirajućih razgraničenja ispravak informacije služi obrani određenih konstitucionaliziranih i „povlaštenih“ (ustavom i zakonom) utvrđenih prava. Ustav Republike Hrvatske jamči „pravo na ispravak svakome kome je javnom viješću povrijeđeno ustavom i zakonom utvrđeno pravo“. (Ustav RH čl. 38 st. 5)

Putem sredstva javnog informiranja ostvaruje se ustavno pravo na slobodu izražavanja misli. Ostvarivanje tog prava zahtijeva slobodu tiska i drugih sredstava javnog informiranja, slobodno osnivanje svih ustanova javnog informiranja, zabranu cenzure i pravo novinara na slobodu izvještavanja i pristupa informaciji. U Republici Hrvatskoj jamči se sloboda izražavanja i sloboda medija koja obuhvaća osobito slobodu izražavanja misli, prikupljanja, istraživanja, objavljivanja i širenja informacija, tiskanja i raspačavanja tiska, protoka informacija, otvorenost medija, pluralizam i raznovrsnost medija, dostupnost javnim informacijama, proizvodnju i emitiranje radijskog i televizijskog programa, slobodu osnivanja pravnih osoba za obavljanje djelatnosti javnog informiranja (ZM čl. 3. st. 1. i 2.). No, sloboda informiranja može dovesti do objavljivanja neistinitih i uvredljivih informacija kao i prouzročiti povredu privatnosti. (ZM čl. 7 st. 1.) Stoga se pravno jamči pravo na ispravak i odgovor te pravo na naknadu prouzročene štete.⁴ S druge pak strane, sprječavanje tiskanja, raspačavanja tiskanih stvari i emitiranja predstavlja kazneno djelo.

Također, pravo novinara, glavnog urednika, urednika i autora objavljenih priloga da odbije dati podatke o izvoru objavljene informacije ili informacije koju

2 Prema ZM svatko ima pravo od glavnog urednika zahtijevati da bez naknade objavi ispravak objavljene informacije kojom su bila povrijeđena njegova prava ili interesi. Pravo na ispravak imaju i pravne osobe i druge organizacije i tijela, ako su informacijom bila povrijeđena njihova prava i interesi. Svrha ispravaka je ispravljanje netočne ili nepotpune informacije. Objava ispravka može se zahtijevati u roku od 30 dana od objave informacije. (ZM, čl. 40, st. 1. i 2.)

3 O tome vidi ZLATOVIĆ, D., „Pravo na ispravak i odgovor prema novom Zakonu o medijima“, Pravo i porezi, br. 3., ožujak 2007., str. 38 – 42.

4 Vidi šire u KOVAČIĆ, T., „Odgovornost za štetu zbog povrede prava osobnosti pravne osobe objavom informacije u medijima (I.)“, Pravo i porezi, br. 8., kolovoz 2008., str. 40 - 45

ima namjeru objaviti, štiti se prema ZM na specifičan način. Naime, „novinarska tajna“, termin koji je uvriježen za takav oblik čuvanja informacija, razlikuje se od profesionalnih tajni po tome što je ona samo pravo, ali ne i obveza. Dakle, novinar može odbiti odati izvor informacija, ali nema pravnu obvezu čuvanja tajnost navedenih podataka. (ZM čl. 30 st. 1) Sud će zahtjev za odavanjem izvora usvojiti ako je to nužno radi zaštite javnog interesa u posebno važnim i ozbiljnim okolnostima, a nema razumne alternativne mjere otkrivanju tih podataka, te ako interes javnosti za otkrivanje podataka o izvoru jasno prevladava nad interesom njegove zaštite⁵. Prema tumačenju Zakona o kaznenom postupku (Zakon o kaznenom postupku (»Narodne novine«, NN 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17, 126/19, 126/19 - dalje ZKP) novinar se oslobađa dužnosti svjedočenja o izvorima informacija za koje je saznao u obavljanju svog zanimanja, osim u kaznenom postupku zbog kaznenih djela protiv časti i ugleda počinjenih sredstvima javnog priopćavanja (ZKP čl. 285 st. 1. t. 6)⁶

Ipak, ostaje pitanje može li se zaista sudskim sporom nadoknaditi počinjena šteta samom objavom ispravka netočne informacije? Iako se sudski sporovi vezani uz objavu i ispravku informacije rješavaju po hitnom postupku, ostaje otvoren problem nadoknade i zaštite osobnih podataka i osobne informacijske sigurnosti s ciljem prevencije zadiranja u ove temelje ljudskih prava i dostojanstva. Nadalje, ipak ostaje pitanje „nepopravljive“ štete kojom je povrijeđeno pravo osobnosti, njena čast, ugled, dostojanstvo, nečija privatna i intimna sfera, ime, lik ili pak djelo.

Budući da živimo u digitalnom okruženju naprednih informacijskih tehnologija jedan od osnovnih parametara koje vežemo uz (ne)sigurnost su umreženi sustavi.⁷ Umrežavanje sustava, bilo da se radi o računalima u kućnoj uporabi ili da je riječ o višoj razini – umrežavanja informacijskih sustava u području financijskih sustava, banaka, itd. koji sadrže niz povjerljivih podataka- povećava se rizik pristupa informacijama i podacima. Samim time informacijska sigurnost postaje ključna tema suvremenog informacijskog društva, a mjere i standardi informacijske sigurnosti utvrđuju se u skladu s mjerama i standardima zakonom propisanim za zaštitu osobnih podataka

5 Prema . čl. 262 st. 1 t.5 ZKP-a u kaznenom postupku privremenom oduzimanju ne podliježu zapisi o činjenicama koje su sastavili novinari i urednici u sredstvima javnog priopćavanja o izvorima obavijesti i podataka za koje su saznali u obavljanju svoga zanimanja i koji su uporabljeni prilikom uređivanja sredstava javnog priopćavanja, a koji se nalaze u njihovom posjedu ili u uredništvu u kojem su zaposleni.

6 Prema članku 285. st. 1. ZKP-a : „*Oslobodeni su obveze svjedočenja: 1) osoba s kojom je okrivljenik u braku ili izvanbračnoj zajednici, 2) srodnici okrivljenika u ravnoj lozi, rođaci u pobočnoj lozi do trećega stupnja zaključno te srodnici po tazbini do drugoga stupnja zaključno, 3) posvojenik i posvojitelj okrivljenika, 4) javni bilježnici, porezni savjetnici, u okviru zakonske obveze čuvanja tajne, 5) odvjetnici, liječnici, zubari, psiholozi i socijalni radnici o onome što su u obavljanju svoga zanimanja saznali od okrivljenika, 6) novinari i urednici u sredstvima javnog priopćavanja o izvorima obavijesti i podataka za koje su saznali u obavljanju svoga zanimanja i koji su uporabljeni prilikom uređivanja sredstava javnog priopćavanja, osim u postupku zbog kaznenih djela protiv časti i ugleda počinjenih putem sredstava javnog priopćavanja i u slučaju propisanom posebnim zakonom.*

7 Nakon implementacije jedne funkcionalne računalne mreže i njene umreženosti sa ostalim sustavima, postavlja se pitanje sigurnosti i zaštite od raznih oblika “napada” i “ometanja” iz okoline sustava. Činjenica jest da brzirazvojtehnologijatražikonstantnopraćenjeteimplementacijusveboljihibrž ihrješnja u području sigurnosti upravo umreženih sustava. Šire o tome KIZZA, J. M., „*Computer Network Security*“, Springer Science+Business Media, Inc., 2005., str. 49.

građana. U smislu rizika pristupa podacima, s naglaskom na osobne podatke građana, promatrati će se Internet kako temeljnu poveznicu umreženih sustava, iako tek jedna od mreža, ali ipak najrasprostranjenija i u najširoj uporabi.

Rađanje i eksponencijski rast te razvoj globalne informacijsko-komunikacijske mreže–Interneta⁸–praćen naglim porastom količine informacija i novim, interaktivnim načinom komuniciranja koji ne poznaje teritorijalne granice, korjenito mijenja tradicionalni način rada i života.⁹ Također, pojavom elektroničkog bankarstva¹⁰ i virtualnog novca, elektroničke pošte i telefonije te sve bržim uvođenjem i prelaskom na elektroničko poslovanje¹¹, pitanje efikasne i cjelovite zaštite osobnih podataka (privatnosti) i informacijskih sustava dobiva sve više na važnosti i postaje primarnim interesom kako pojedinca tako i zajednice u cjelini. mreža razvijena u okviru vojne

8 Internet je globalni komunikacijski sustav koji povezuje i spaja računalne mreže pojedinih zemalja i organizacija, te tako omogućava posjednicima računala diljem svijeta da putem svojih lokalnih mreža i telefonskih mreža međusobno komuniciraju, razmjenjuju informacije i koriste brojne druge usluge. U fizičkom smislu, to je niz međusobno povezanih računalnih mreža, organiziranih na jedinstven način, sa zajedničkim komunikacijskim protokolima i mrežnim uslugama. Za razliku od ostalih informacijskih sustava, informacijsko-komunikacijski sustavi bave se prikupljanjem, obradom i distribucijom različitih informacijskih sadržajnih formi u cjelokupnom fizičkom komunikacijskom prostoru. Fizički komunikacijski prostor i sukomunikacijske mreže koje omogućavaju pretraživanje bilo koje lokacije u mreži s bilo koje druge lokacije u istoj mreži. Tako i šire GRBAVAC, V., PLENKOVIĆ, M., „Komunikacijski sustavi na prijelazu u 21. stoljeće“, Informatologija, br. 27., 1995, str. 1

9 Početci razvoja Interneta vezani su uz ARPANET, računalnu mrežu koju je uspostavila ARPA (Advanced Research Projects Agency) 1969 godine, nakon višegodišnjih istraživanja i razvoja, a u cilju postizanja vojne i tehnološke premoći nad tadašnjim Sovjetskim Savezom. Dizajn mreže zasnivao se na višeslojnoj, decentraliziranoj arhitekturi i otvorenim komunikacijskim protokolima koji otvaraju nove načine komuniciranja. Svojom pojavom uvelike je promijenila svijet računala i komunikacija. Razvijen je TCP/IP (Transmission Control Protokol- skup komunikacijskih protokola koji računala koriste pri radu i komuniciranju putem Interneta) protokol, MODEM, operacijski sustav UNIX (koji je u početcima bio temeljni operacijski sustav mreže), elektronička pošta, itd. U devedesetima su se počeli koristiti hipertekstualni sustavi koji su se razvili u World Wide Web tehnologiju. Prvi Web server i korisnička računala izgrađeni su 1990. godine u CERN-u. Time je obilježen početak Internet revolucije koja se preko znanstvenih institucija proširila na poduzeća i širi krug korisnika, pa se 1995. godina uglavnom prihvaća kao godina stvaranja Weba. Detaljniji opis nastanka i razvoja Interneta dali su oni koji su u tome i neposredno sudjelovali LEINER, B. M., CERF, V. G., CLARK, D. D., KAHN, R. E., KLERINROCK, L., LYNCH, D. C., POSTEL, J., ROBERTS, L. G., WOLF, S., u članku: „A Brief History of the Internet“, - dostupno na <http://www.isoc.org/internet/history/brief.shtml> (05. 02. 2021.)

10 O tome vidi *Elektroničko bankarstvo: nezaustavljiv trend*, Privredni vjesnik, 31. kolovoza 1998.

11 „Elektroničko poslovanje (u daljem tekstu -EP) je oblik organizacije rada u obradi i razmjeni poslovnih informacija koji koristi i suvremenu elektroničku tehnologiju. EP znatno povećava učinkovitost u radu, skraćuje vrijeme obrade i time smanjuje troškove. Većina je uz taj pojam povezivala Internet, kupovinu na Internetu ili pak elektroničku novčarku. Zaboravljali su da je potrošač samo jedan sudionik u lancu poslovanja. Elektroničko poslovanje integrira čitav poslovni proces, od nabave do prodaje i omogućuje razmjenu dokumenata, automatizaciju obrade, marketing, bankarstvo bez šaltera, automatizaciju opskrbnog lanca, just-in-time dopremu sirovina...“

industrije¹², a za potrebe suradnje akademske zajednice¹³ danas je dostupna i običnim građanima.

Suvremeni način poslovanja i komuniciranja putem globalnih informacijskih mreža doveo je do sve veće povezanosti ne samo ljudi već i informacijskih sustava. Uz sve svoje blagodati takav način rada nosi u sebi i brojne opasnosti po sigurnost svih sudionika, kao i samih informacijskih sustava. Podaci i informacije, koji se unutar takvih sustava obrađuju, memoriraju i distribuiraju, kao i tehnička osnovica koja to omogućuje, sve su češće cilje takvih zloupotreba, pa se zato i postavlja kao osnovni zadatak zahtjev za njihovom efikasnom i cjelovitom zaštitom.

Sve veća povezanost i upućenost informacijskih sustava na uključivanje u globalne informacijske mreže, u prvom redu Internet, ali i na neke druge koje su nastale logičkim slijedom vremena ali na istim principima (WLAN, primjerice), doveli su do toga da se njihova zaštita više ne može promatrati i rješavati izolirano, već samo kao dio tog sustava. Takva otvorenost informacijskih sustava prema sve većem broju korisnika dodatno je oslabila njihovu sigurnost. Zato je nužno da se pitanjima zaštite pristupi s jednog šireg, globalnog aspekta – aspekta globalnih informacijskih mreža koje ih sve više objedinjuju. Dakle, pitanja sigurnosti i zaštite Interneta postaje jedno od osnovnih pitanja kako za same informacijske sustave i njihove korisnike tako i za cijelu međunarodnu zajednicu.

Intenzivan razvoj i brzina nastanka i primjene informacijskih tehnologija premašile su očekivanja, namjere i ideje čak i njihovih tvoraca. Poznato je stajalište da je navedeni trend cijena napretka u svijetu u kojemu dobro i zlo idu zajedno s istim pojavama i procesima te ih je nemoguće unaprijed predvidjeti i na vrijeme spriječiti.¹⁴ Na žalost sve su brojnije zlouporabe koje izlaze iz tih okvira pa negativne prateće posljedice postaju neizbježnim suputnikom suvremenog razvoja“.

Najugroženiji aspekt i posljedica informacionalističkog razvoja jest ugrožavanje

12 Prvotno nastao kao dio ARPANET pri Ministarstvu obrane SAD, Internet se iz sigurnosnih razloga izdvaja u MILNET (engl. *MILitary NETwork* – vojna mreža) i po prvi put se javlja naziv *Internet*. Godine 1989. ARPANET i službeno postaje Internet i prestaje biti vladin znanstveni projekt i postaje otvorena za druge korisnike. O tome vidi šire DRAGIČEVIĆ, D., „*Kompjutorski kriminalitet i informacijski sustavi*“, Informator, 1999., str. 31

13 S pravom se ističe da je Internet najvažnija suvremena globalna infrastruktura za obrazovanje, informiranje, istraživanje i razvoj u javnim djelatnostima i gospodarstvu. U tom je sustavu i *Hrvatska akademska i istraživačka mreža* – CARNET, nastala 1991. godine kao projekt Ministarstva znanosti i tehnologije Republike Hrvatske. U ožujku 1995. godine Vlada Republike Hrvatske donosi Uredbu o osnivanju ustanove CARNet sa svrhom pospešivanja napretka, kako pojedinca tako i društva u cjelini pomoću novih informacijskih tehnologija. Riječ CARNet je skraćenica od engleskog naziva ustanove (Croatian Academic and Research Network). Uz 96 zaposlenih, CARNet ima oko 20 vanjskih suradnika, a djelatnici više ustanova i tvrtki sudjeluju u različitim projektnim timovima. Najvažniji CARNetovi partneri su Sveučilišni računski centar - Srce i Fakultet elektrotehnike i računarstva u Zagrebu. CARNetove aktivnosti mogu se podijeliti u tri osnovna područja: pružanje Internet usluga, poticanje razvoja informacijskog društva i obrazovanje za novo doba. Sustavnim organiziranjem tečajeva namijenjenih krajnjim korisnicima, program ima obrazovanja budućih predavača i inženjera računalnih sustava te posebnim programima poput CISCO akademije mrežnih tehnologija CARNet nastoji pomoći svojim korisnicima u svladavanju i primjeni informacijskih tehnologija u svakodnevnom životu i radu te ih na taj način pripremiti za informacijsko društvo. Vidi šire http://www.carnet.hr/o_carnetu/o_nama (05. 12. 2018.)

14 Op. cit., DRAGIČEVIĆ, A., DRAGIČEVIĆ, D., str. 417

privatnosti pojedinca i ograničavanje slobode izražavanja. Samim time, povlači se pitanje zaštite od negativnog utjecaja informacionalizma na zaštitu nacionalne sigurnosti, zaštitu maloljetnika, zaštitu ljudskog dostojanstva, zaštitu ljudske časti i ugleda te zaštitu intelektualnog vlasništva. Uz sve prednosti koje nam donose nove tehnologije i tehnološki napredak, očekivana je pojava i negativnih posljedica. Veliko otvaranje naših lokalnih i nacionalnih okolina utjecajima iz raznih dijelova svijeta ponekad ostavlja osjećaj nemoći i gubitka kontrole nad vlastitom okolinom i događanjima. Ključni negativan utjecaj u kontekstu globalizacije i ICT-a jest usko definirani razvoj - kao ekonomski razvoj - koji nije uključivao kulturnu dimenziju, doveo je do gubitka identiteta i osjećaja pripadnosti zajednici. Stoga ne čudi da je kulturni identitet postao važna tema istraživanja i rasprava.¹⁵

Postoji mišljenje da negativne posljedice proizlaze iz, osim iz već spomenutog: 1. brzine u selektivnosti širenja informacijske tehnologije; 2. informacijskog stresa i informacijskog onečišćenja; 3. računalnog i kibernetičkog kriminaliteta; 4. informacijskog ratovanja i kibernetičkog terorizma¹⁶. Ključno pitanje, koje se samim time nameće, jest zapravo kako postići „kontrolirani razvoj“, odnosno kako osigurati da se ekspanzivni tehnološki razvoj kreće unutar uvriježenih etičkih, pravnih i kulturoloških okvira za dobrobit ljudskoga društva?

Nove informacijske i komunikacijske tehnologije umrežile su već stotine milijuna ljudi. Vijesti se, putem masovnih medija, šire velikom brzinom i dolaze do svih kutaka zemlje, pa tako nekada posve nepoznata mjesta ulaze u svakodnevni rječnik udaljenih zajednica¹⁷. Imati pravu informaciju u pravo vrijeme na pravom mjestu – postaje poput oružja što dovodi do jednog od najopasnijih negativnih suputnika informacionalističkog razvoja - kibernetičkog terorizma. Povreda zaštite privatnosti i zlouporaba osobnih podataka u ovom aspektu terorizma dovodi u pitanje nacionalnu sigurnost te osobnu i fizičku zaštitu osoba. Aktivnim kriptiranim pristupom podacima prenose se informacije kojima se planira ugrožavanje života građana i otvara se sasvim nova era- era informacijskog ratovanja.

2. Zaštita djece na internetu

Internet je u relativno kratkom razdoblju postao najpopularniji medij među djecom i mladima. Suvremena „digitalna generacija“ u okruženju digitalnih tehnologija od najranije dobi je informatički pismena i stoga je podložna utjecaju novog medija, što se i jasno vidi kroz porast broja kaznenih djela i kibernetičkog

15 Mreža CULTURELINK je u proteklih deset godina objavila brojne priloge o temi kulturnog identiteta te je organizirala nekoliko konferencija i seminara na tu temu: međunarodni tečajevi - Redefining Cultural Identities: Cultural Industries and Technological Convergence; Redefining Cultural Identities: Southeastern Europe, Redefining Cultural Identities: The Multicultural Contexts of the Central European and Mediterranean Regions i međunarodne konferencije - The Mediterranean: Cultural Identity and Prospects for Intercultural Dialogue, i Europe of Cultures: Cultural Identity of Central Europe. Rezultati s tih skupova publicirani u zbornicima radova pod istim nazivom. Izvor: www.culturelink.org, (05. 10. 2018.)

16 Op. cit. DRAGIČEVIĆ, A., DRAGIČEVIĆ, D, str. 417

17 Više o tome LÉVY P., *Collective intelligence: mankind's emerging world in cyberspace*, Plenum Trade, 1997., str. 60

kriminala na štetu djece kao i u porastu maloljetničke delikvencije.¹⁸ Mladi ljudi sve više vremena provode na Internetu, što je nažalost rezultiralo i pojavom nove bolesti – ovisnosti o Internetu.

2.1. Osvrt na aktualno stanje u Europi i svijetu

Instagram, Facebook, Twitter, samo su neke od najpopularnijih društvenih mreža. Prema Sari Kiesler, autorici knjige *Culture of the Internet* ključna je engleska izreka „you are who you pretend to be“ (u prijevodu: „ti si onaj koji se pretvaraš da jesi“) koja ističe kako nas Internet ne ograničava našom prošlošću, već možemo makar virtualno započeti život ispočetka i stvoriti novi identitet.¹⁹ Mladi ljudi daju prednost virtualnoj komunikaciji i sve više vremena provode na društvenim mrežama razmjenjujući s nepoznatim ljudima informacije o sebi, svojoj intimi, kao i fotografije bez ikakve svijesti o opasnostima koje im takvo ponašanje donosi.²⁰ Razvoj novih tehnologija s jedne strane omogućava brži protok informacija i otvara ove mogućnosti dok s druge strane donosi nove rizike koje možemo rješavati isključivo edukacijom djece – upoznavanjem s rizicima, prednostima i manama od najranije dobi.

Osobito zabrinjavajuća jest činjenica da djeca kao korisnici Interneta nepoznatim ljudima povjeravaju veoma privatne stvari, poput svog stvarnog imena, adrese, broja telefona, godina i ostalih stvari pomoću kojeg nepoznata osoba može bez lakoće doći do djeteta i u realnom svijetu. Stoga jedna od važnih tema edukacije prvenstveno mora biti i upozorenje djece, ali i njihovim roditeljima²¹ da ne dijele svoju intimu s drugim ljudima iz sigurnosnih razloga.

Nažalost, društvene mreže se koriste i za promoviranje nasilja. Štoviše, učenici osnovnih i srednjih škola „zakazuju tuče“ putem Facebooka. Stoga su predstavnici Europske komisije i 17 društvenih mreža (poput Facebooka i Instagrama i drugih) potpisali ugovor prema kojem će zajedničkim snagama štititi djecu i mlade od cyber-bullyinga i nasilja na Internetu.

Europske zemlje nisu jednoglasne po pitanju ograničenja na Internetu. Organizacije poput OSCE, Reporteri bez granica, UNESCO, zalažu se za potpunu slobodu novog medija. Naravno, po njihovom mišljenju, Internet se ne smije koristiti u kriminalne svrhe, ali ipak se protive ograničenjima, jer postoji mogućnost da će korisnici Interneta izgubiti povjerenje u njega. Postoje provedena istraživanja koja ističu kako većina europskih korisnika interneta smatra da je zatvaranje „nedoličnih“ web stranica predstavljalo povreda prava potrošača.²² Ali, treba posebno naglasiti da

18 Vidi McCABE, K., *The Role of Internet Service Providers in Cases of Child Pornography and Child-Prostitution*, *Social Science Computer Review*, 26 (2008) 2, 248, <http://ssc.sagepub.com/cgi/content/refs/26/2/247> (27. 03. 2019)

19 Prema KIESLER, S., *Culture of the Internet*, Mahwah, Lawrence Erlbaum Associates, 1997, str. 147

20 Tako i šire RUŽIĆ, N., *Zaštita djece na internetu*, Nova prisutnost 9 (2011) 1, 155-170

21 Vidi MADDEN, M., *What are parents doing to protect teens online?*, Pew Internet, <http://www.pewinternet.org/Commentary/2007/July/What-are-parents-doing-to-protect-teens-online.aspx> (10.02.2021.)

22 CHIH, W., *Internet Censorship in the United States stumbling blocks to the Information Age*, *IFLA Journal*, 29 (2003) 2, 4,5, URL: <http://ifl.sagepub.com/cgi/content/refs/29/3/213> (02.02.2021)

neprimjereni sadržaji nemaju nikakve veze sa slobodom Interneta niti sa cenzurom interneta na koju se u istraživanju pozivaju. Pod slobodom ne podrazumijevamo podržavanje kriminalnih djela radi unaprjeđenja demokracije. Sama pojava dječje pornografije koja predstavlja kazneno djelo upravo je činjenica koja potkrepljuje potrebu veće kontrole „internetskih prava“ djece. Niti jedan medij ne može i ne smije biti iznad zakona, poglavito kaznenog zakona bilo koje zemlje.

Najlakša meta na Internetu su djeca, stoga ih je potrebno zaštititi ne samo od cyber-bullyinga, već ne dozvoliti da budu žrtve cyber-kriminala. Na forumu upravljanja Internetom pri OUN-u predstavnik Francuske, Bernard Benamu, izjavio je da su sudionici foruma imali različita mišljenja što se tiče kontrole Interneta, ali su se složili u jednom: da moraju zaštititi djecu od Internet-predatora. Predstavnik Brazila izjavio je da treba naučiti upravljati Internetom

– kako bi donosio samo korist ljudima.

2.2. Zaštita djece na internetu i utjecaj Opće uredbe o zaštiti podataka (GDPR)

Opća uredba o zaštiti podataka (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (GDPR) koja se primjenjuje od 25. svibnja 2018. godine u Europskoj uniji postrožila je pravila u obradi osobnih podataka djece i zamijenila zakone u području zaštite osobnih podataka u cijeloj Europskoj uniji od svibnja prošle godine. Bespredmetno je raspravljati o zakonskim okvirima koji su, s razlogom, sigurnost djece na internetu uistinu postaje sve značajnija tema a Uredba je regulirala obradu osobnih podataka djece kao posebno štićenu kategoriju s posebnim naglaskom na usluge informacijskog društva. Posebna su kategorija upravo osobni podaci djece gdje je ponajprije postavljena dobna granica 16 godina ali i mogućnost predviđanja niže dobne granice za davanje privole za obradu osobnih podataka djece i do 13 godina što su države članice Europske unije regulirale zakonima o provedbi GDPR-a. Sukladno čl. 8. GDPR-a pod nazivom Uvjeti koji se primjenjuju na privolu djeteta u odnosu na usluge informacijskog društva u st. 1. „Kada se primjenjuje članak 6. stavak 1. točka (a), u pogledu nuđenja usluga informacijskog društva izravno djetetu, obrada osobnih podataka djeteta zakonita je ako dijete ima najmanje 16 godina. Ako je dijete ispod dobne granice od 16 godina takva je obrada zakonita samo ako i u mjeri u kojoj je privolu dao ili odobrio nositelj roditeljske odgovornosti nad djetetom.“ (Čl. 8 st. 1. GDPR)²³ U tom slučaju, sukladno Uredbi, „Voditelj obrade mora uložiti razumne napore u provjeru je li privolu u takvim slučajevima dao ili odobrio nositelj roditeljske odgovornosti nad djetetom, uzimajući u obzir dostupnu tehnologiju.“ (čl. 8. st. 3. GDPR) Države članice mogu u te svrhe zakonom predvidjeti nižu dobnu granicu, pod uvjetom da takva niža dobna granica nije niža od 13 godina. (GDPR, čl. 8. st. 1.) Postoje dodatni uvjeti koje treba zadovoljiti kada se zahtjev za brisanje odnosi na osobne podatke djece, osobito u mrežnom okruženju. Osobito je važan element “privole” – kada je osoba kao dijete dala privolu za obradu podataka, no

23 Tako i šire Boban, M., Zaštita osobnih podataka i nova EU uredba o zaštiti podataka, Bilten HDMI, 2018; 24(1):26-40

nakon nekoliko godina je zatražila brisanje. Osoba ima opravdani razlog za brisanje podataka, jer kao dijete, tijekom davanja privole, nije mogla biti u potpunosti biti svjesna rizika koji su uključeni u proces obrade. Ovo se osobito odnosi na društvene mreže i internetske forume.

2.3. Uloga obrazovanja u zaštiti djece na internetu

Zakonodavni okvir Republike Hrvatske predstavlja temeljni mehanizam u smislu zaštite prava djece na digitalnom okruženju ali se sam po sebi ne može smatrati dovoljnim. Na prvom mjestu ističem edukaciju i ulogu obrazovanja koji u ovom trenutku u Hrvatskoj prevladava kroz izradu kurikularne reforme i reforme sustava odgoja i obrazovanja u cijelosti. Također, radionice i predavanja u organizaciji školskih kurikuluma predstavljaju dobre primjere u praksi ali ne samo ona namijenjena djeci već i roditeljima koji također trebaju edukaciju.²⁴ U proteklih nekoliko godina podignuta je razina osviještenosti o zaštiti prava djece u digitalnom okruženju ali još uvijek ne postoji strukturirana strateška aktivnost u smislu nacionalne strategije koja bi se bavila ovim pitanje uz aktivnosti koje bi bile definirane. Ipak, pomaci su vidljivi upravo u školstvu i moram pohvaliti ravnatelje osnovnih i srednjih škola koji su uistinu prepoznali potrebu uključivanja tema o zaštiti prava djece u školske kurikulume kao i prijave projekata financiranih iz europskih fondova.²⁵

Kako bi zaštitili privatnost djece roditeljima se svakako preporučuje nadzor nad djetetovim aktivnostima ali ne i isključive zabrane već odgojnu i edukativnu komunikaciju kojoj je cilj upoznati dijete s opasnostima i upozoriti na moguće posljedice jer same zabrane nikako ne mogu spriječiti dijete da pristupi sadržajima s obzirom na svakodnevnu uporabu mobilnih uređaja i računala te dostupnosti wireless tehnologija. Upoznavanje s rizicima i edukacija uvijek su se pokazali boljim rješenjem! Na tom tragu ključan dio problematike zaštite djece jest i razina (ne)znanja samih roditelja (odnosno skrbnika) i nepoznavanje funkcioniranja društvenih mreža i internetskih pretraživača kao javnih mreža. I sami roditelji od, koji prema GDPR-u daju privole za korištenje osobnih podataka djece od trećih osoba, moraju biti upoznati s rizicima što nažalost često nije slučaj pa samim time dovode i djecu u nepovoljan položaj, kao

24 “Sve ono što se ranije događalo u realnom prostoru, sada se prebacilo u virtualnu stvarnost u kojoj je puno teže reagirati. Novi zakoni su doneseni, novi uvjeti, a sve se treba uskladiti s GDPR-om, te donijeti preporuke kako ćemo to primijeniti u praksi. Ono čime su djeca najviše ugrožena je pravo na privatnost, ali i izloženost raznim sadržajima kojima dijete ima pristup. Nisu bitne zabrane, već edukacija, jednako kako smo djecu nekada upozoravali da ne ulaze u automobile s nepoznatim osobama sada ih upozoravamo da ne razgovaraju s nepoznatima preko društvenih mreža. Treba ih naučiti o opasnostima, a ne im nametati zabrane” Sigurnost i zaštita djece na internetu i poglavito u okruženju novih tehnologija koje predstavljaju svakodnevnicu, ključna je tema u trenutku svih akademskih i stručnih rasprava na europskoj i globalnoj razini. Prema izjavi iz intervjua Boban. M. u okviru stručnog seminara “Zaštita prava djece u digitalnom okruženju” u organizaciji Hrvatske udruge ravnatelja osnovnih škola – ogranka Splitsko-dalmatinske županije, dostupno na Splitski dnevnik, <https://splitskidnevnik.rtl.hr/vijesti/grad/nekada-se-djecu-upozoravalo-da-ne-ulaze-u-automobile-s-nepoznatima-a-sada-da-ne-razgovaraju-s-njima-preko-drustvenih-mreza/> (08. 04. 2019.)

25 Tako i šire A&S Adria online izdanje časopisa, Važnost zaštite privatnih podataka djece na internetu, (objavljeno 7. 3. 2019.) <https://www.asadria.com/vaznost-zastite-privatnih-podataka-djece-na-internetu/> (20. 02. 2021.)

u primjerice situaciji kada objave fotografije maloljetne djece kod prvog dana škole uz objavu lokacije škole, uz javnu vidljivost ili vidljivost prijateljima prijatelja i to u realnom vremenu.²⁶ Uistinu je pitanje koliko su svjesni rizika javnosti takvih objava. Najnoviji podaci pokazuju da danas sve mlađa djeca imaju pristup internetu. Svjesni smo da se granice svakim danom sve više snižavanju budući da današnji aktualni projekt „Škola za život“ uvodi „tablet“ kao pomagalo u nastavi već u nižim razredima osnovne škole. Ipak, uvodi ga uz prateće obrazovanje i edukaciju što je nužni preduvjet kako bi se dijete razvijalo sukladno s tehnologijom koja ga svakodnevno okružuje. Stoga, nameće se zaključak da Internet postaje sastavni dio nastave još od osnovne škole ali isključivo uz praćenje i nadzor te edukaciju roditelja i nastavnika. Tu svakako treba staviti i predloženu granicu pristupa internetu budući da do početka osnovne škole dijete nema osnovnu potrebu za pristup internetskom sadržaju bez nadzora roditelja što naravno podrazumijeva i niže razrede osnovne škole. Česta pogreška roditelja je kupovina pametnih telefona djetetu već od prvog razreda osnovne škole a sam pametni telefon omogućava im neograničen pristup svim sadržajima te se svakako preporučuje oprez i u tom pogledu. Stoga, praćenje razvoja djeteta i nadzor nad aktivnostima na internetu postaju svakodnevica u odgoju djeteta uključujući aktivnu komunikaciju o opasnostima kako bi i samo dijete postalo svjesno kako prednosti tako i rizika internetskih tehnologija. Samim time-edukacija je na prvom mjestu!

2.4. Zaštita djece na internetu u kaznenom zakonodavstvu Republike Hrvatske i Bosne i Hercegovine

Iako digitalna tehnologija i inovacije mogu otvoriti vrata prema boljoj budućnosti pružajući djeci lakši pristup učenju, interesnim zajednicama i druge pogodnosti koje im mogu pomoći u ispunjavanju njihovih potencijala, ipak digitalno okruženje i interaktivnost predstavljaju i značajne rizike za sigurnost djeteta, za djetetovu privatnost i dobrobit. Tehnološke kompanije, imaju ključnu ulogu u dijeljenju digitalnih alata, znanja i stručnosti s agencijama za provođenje zakona radi zaštite djece na mreži. Jedan od preduvjeta zaštite djece od nasilja putem informaciono-komunikacionih tehnologija svakako je cjelovit, jasan i učinkovit međunarodni i nacionalni pravni okvir. Međunarodni dokumenti koje je ratificirala BiH dio su pravnog sustava ove države i samim tim dio Ustava BiH²⁷, a pored ustava, različiti zakoni i podzakonski akti zahtijevaju od organa vlasti da osiguraju odgovarajuću zaštitu prava i interesa djeteta kao i njihovu zaštitu od različitih oblika iskorištavanja i zloupotreba putem informaciono-komunikacionih tehnologija. Najvažniji nacionalni dokumenti zaštite djece od potencijalnih kaznenih djela uz

²⁶ Ibidem.

²⁷ Time i Ustava Federacije BiH i Ustava Republike Srpske, te dio Statuta Brčko Distrikta BiH

Ustav su Kazneni zakon²⁸, Zakon o kaznenom postupku²⁹, te Zakon o zaštiti i postupanju s djecom i maloljetnicima u kaznenom postupku³⁰. Međutim, u Bosni i Hercegovini ne postoji zakonodavni ni regulatorni okvir koji eksplicitno uređuje oblast zaštite djece na internetu, ne postoji udruženje/asocijacija pružatelja internet usluga, niti je evidentna organizirana pripadnost međunarodnim udruženjima koja se tiču zaštite djece na internetu³¹. Nacionalni pravni okvir propisuje u kaznenom zakonodavstvu moguća ponašanja na štetu djece koja mogu biti počinjena i putem informacijsko komunikacijskih tehnologija.

Obzirom na činjenicu da seksualno zlostavljanje djece i maloljetnika putem informaciono-komunikacionih sredstava, osobito putem društvenih mreža, kao takvo predstavlja globalnu kriminalnu aktivnost, uzevši u obzir težinu i ozbiljnost posljedica koje pogađaju žrtvu, kaznenim zakonima entiteta i Brčko Distrikta BiH u glavama „Kaznena djela protiv spolnog integriteta i morala“ i „Kaznena djela protiv braka i obitelji“, kao i u Kaznenom zakonu RH u glavi „Kaznena djela spolnog zlostavljanja i iskorištavanja djeteta“³², propisana su sljedeće kaznena

djela koja mogu biti počinjena ili se korištenjem informacijsko komunikacijskih tehnologija može omogućiti počinjenje sljedećih kaznenih djela:

- povreda privatnosti djeteta³³ (čl. 189. st.2. KZ RS, čl. 178. KZ RH) Povreda privatnosti djece posebno je ugrožena u vrijeme digitalizacije, pa je kaznenopravno normiranje načina počinjenja povrede nužnost. U Bosni u Hercegovini je normirana samo u Republici Srpskoj, pa bi u tom pravcu trebalo raditi izmjene i dopune federalnog i Kaznenog zakona BD BiH.

- neovlašteno optičko snimanje (čl. 189. st.3. KZ F BiH, čl. 186. KZ BD BiH)

28 Kazni zakon BiH, Službeni glasnik BiH br. 3/2003, 32/2003 - ispr., 37/2003, 54/2004, 61/2004, 30/2005, 53/2006, 55/2006, 8/2010, 47/2014, 22/2015, 40/2015 i 35/2018 (u daljnjem tekstu KZ BiH); Kazneni zakon F BiH, Sl. novine F BiH br. 36/2003, 21/2004 - ispr., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 i 75/2017. (dalje KZ FBiH); Kazneni Zakon RS, Sl. glasnik RS br. 64/17, 15/21.; Kazneni zakon Brčko Distrikta BiH, Sl. glasnik BD BiH br. 10/03, 45/04, 06/05, 21/10, 52/11.26/16, 13/17., 50/18.

29 Zakon o kaznenom postupku BiH, Sl. glasnik BiH br. 3/03, 32/03 - ispr., 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 29/07, 53/07, 58/08, 12/09, 16/09, 93/09, 72/13, 65/18 (u daljnjem tekstu ZKP BiH), Zakon o kaznenom postupku F BiH, Sl. novine FBiH br. 35/03, 56/03 - ispr., 78/04, 28/05, 55/06, 27/07, 53/07, 9/09, 12/10, 8/13, 59/14, 74/20 (dalje ZKP FBiH), Zakon o kaznenom postupku RS, Sl. glasnik RS br. 53/12, 91/17, 66/18, 15/21. Zakon o kaznenom postupku BD BiH, Sl. glasnik BD BiH br. 10/03, 48/04, 06/05, 12/07, 14/07, 21/07, 27/14, 3/19 (dalje KZ BD BiH)

30 Službene novine FBiH br. 7/14, 74/20; Sl. glasnik RS br. 13/10, 61/13, 68/20; Službeni glasnik Brčko distrikta BiH, broj 44/11

31 Smjernice za društveno odgovorne informacijsko-komunikacijske kompanije u oblasti zaštite djece od seksualnog iskorištavanja i zlostavljanja, Save the Children in North West Balkans, 2019.

32 NN RH br. NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19.

33 (1) Tko iznese ili pronese nešto iz ličnog ili porodičnog života djeteta ili suprotno propisima objavi djetetovu fotografiju ili otkrije identitet djeteta i time kod djeteta stvori stanje uznemirenosti ili ga izloži poruzi vršnjaka ili drugih lica ili na neki drugi način ugrozi sigurnost djeteta, kaznit će se novčanom kaznom ili kaznom zatvora do jedne godine. (2) Tko djelo iz stava 1. ovoga člana izvrši putem sredstava masovne komunikacije, kompjuterskog sistema ili mreže, na javnom skupu ili na drugi način, zbog čega je ono postalo pristupačno većem broju lica, kaznit će se novčanom kaznom ili kaznom zatvora do dvije godine.

(3) Tko djelo iz st. 1. i 2. ovoga člana izvrši kao službeno lice ili u obavljanju profesionalne djelatnosti, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

Dispozicija ovog kaznenog djela propisanog st. 3. u potpunosti je jednaka st. 1. čl.211 KZ FBiH, pa bi, radi jasnoće zakona trebalo taj stavak iz čl. 189. KZ FBiH brisati, jer bi time bila postavljena jasna distinkcija kaznenog djela Neovlašteno optičko snimanje od kaznenog djela Iskorištavanje djeteta ili maloljetnika radi pornografije.;

- zadovoljavanje pohote pred djetetom ili maloljetnikom³⁴ (čl. 209. KZ F BiH, čl. 179 KZ RS, čl.160. KZ RH). Dok kazneno zakonodavstvo BiH uopćeno propisuje počinjenje kaznenog djela prema djetetu, KZ RH propisuje kažnjavanje ako djelo počinjeno prema djetetu mlađem od 15 godina³⁵. Kao oblik počinjenja kaznenog djela zadovoljenja pohote pred djetetom KZ RH navodi i počinjenje kaznenih djela Silovanja, Bludnih radnji i Teških kaznenih djela protiv spolne slobode. Kazneni zakon RH propisuje i kažnjavanje za sami pokušaj ovog kaznenog djela.

- navođenje na prostituciju (KZ FBiH čl.210 st. 4; KZ RS 169; KZ BD BiH čl. 207);

- trgovina djecom (KZ RS čl. 145.) i trgovina ljudima (KZ FBiH čl. 210a; KZ BD BiH čl. 207a);

- iskorištavanje djeteta ili maloljetnika za pornografiju (KZ F BiH čl.211; KZ BD BiH čl.208, KZ RH čl.163) i iskorištavanje djece za pornografske predstave (KZ RS čl. 176 st.3, čl. 164 KZ RH) KZ RH opisu bića kaznenog djela eksplicitno navodi način počinjenja ovog kaznenog djela "Tko dijete namamljuje, vrbuje ili potičena sudjelovanje u snimanju dječje pornografije ili tko organizira ili omogućiti snimanje...", te bi u tom smislu bilo uputno napraviti izmjene i u zakonodavstvu BiH, jer bi time decidno i jasno bilo definirano što podrazumijeva dječja pornografija. Za razliku od bosanskohercegovačkog kaznenog zakonodavstva u KZ RH je jasno normirano da dijete neće biti kažnjeno za proizvodnju i posjedovanje pornografskog materijala³⁶;

- upoznavanje djeteta s pornografijom (KZ F BiH čl.212; KZ BD BiH čl.209,

34 DelegeferendauKZFBiHučl.209imaprostorazanadopunuopisakaznenogdjelaZadovoljenjepohote pred djetetom ili maloljetnikom, gdje bi se izmjenom propisa mogla samo dodati kvalifikacija počinjenja putem informacijsko komunikacijskih tehnologija. više u Stipanović, I.: Issues in Proving Criminal Offenses of Violence against Children through Information and Communication Technologies in Bosnia and Herzegovina, SoftCom, 2019.

35 Kazneni zakon RH posebnim člankom zakona (čl. 158. i 159.) propisuje spolnu zlouporabu djeteta mlađeg i starijeg od petnaest godina, što u kaznenom zakonodavstvu BiH nije slučaj.

36 Kaznom iz stavka 1. ovoga članka kaznit će se tko neovlašteno snima, proizvodi, nudi, čini dostupnim, distribuirati, širi, uvozi, izvozi, pribavlja za sebe ili drugoga, prodaje, daje, prikazuje ili posjeduje dječju pornografiju ili joj svjesno pristupa putem informacijsko komunikacijskih tehnologija.

(3)Tko dijete silom ili prijetnjom, obmanom, prijevarom, zlouporabom ovlasti ili teškog položaja ili odnosa ovisnosti, prisili ili navede na snimanje dječje pornografije, kaznit će se kaznom zatvora od tri do dvanaest godina. (4)Posebne naprave, sredstva, računalni programi ili podaci namijenjeni, prilagođeni ili uporabljeni za počinjenje ili olakšavanje počinjenja kaznenog djela iz stavka 1., 2. i 3. ovoga članka će se oduzeti, a pornografski materijal koji je nastao počinjenjem kaznenog djela iz stavka 1., 2. i 3. ovoga članka će se i uništiti. (5)Dijete se neće kazniti za proizvodnju i posjedovanje pornografskog materijala koji prikazuje njega samog ili njega i drugo dijete ako su oni sami taj materijal proizveli i posjeduju ga uz pristanak svakog od njih i isključivo za njihovu osobnu upotrebu. (6)Dječja pornografija je materijal koji vizualno ili na drugi način prikazuje pravo dijete ili realno prikazano nepostojeće dijete ili osobu koja izgleda kao dijete, u pravom ili simuliranom spolno eksplicitnom ponašanju ili koji prikazuje spolne organe djece u spolne svrhe. Materijali koji imaju umjetnički, medicinski, znanstveni, informativni ili sličan značaj ne smatraju se pornografijom u smislu ovoga članka .

KZ RS čl.177. st.1., čl. 165. KZ RH) Dok kazneni zakoni u BiH uopćeno propisuju "Tko djetetu proda, prikaže ili javnim izlaganjem ili na drugi način učini pristupačnim spise, slike, audiovizuelne i druge predmete pornografskog sadržaja ili mu prikaže pornografsku predstavu" KZ RH uz taj dio navodi i počinjenje "posredstvom računalnog sustava, mreže ili medija za pohranu računalnih podataka." KZ RH propisuje i strožu sankciju za počinjeno kazneno djelo i to do pet godina, a kazneni zakoni u BiH od jedne godine (KZ FBiH) do tri godine (KZ RS);

- Iskorištavanje kompjuterske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje kaznenih djela seksualnog zlostavljanja ili iskorištavanja djeteta (čl. 178 KZ RS).³⁷ Kazneni zakon Republike Hrvatske propisao je kazneno djelo Mamljenje djece za zadovoljenje spolnih potreba u čl. 161.st.1. koje definira na način da punoljetna osoba koja osobi mlađoj od petnaest godina, u namjeri da ona ili druga osoba nad njom počinu kazneno djelo spolne zloporabe djeteta mlađeg od petnaest godina, putem informacijsko komunikacijskih tehnologija ili na drugi način predloži susret s njom ili drugom osobom koja poduzme mjere da do tog susreta dođe kaznit će se kaznom od šest mjeseci do pet godina.

Definiranje kaznenih djela počinjenih nad djecom u Bosni i Hercegovini, osobito djela s elementom nasilja, potrebno je potpuno uskladiti s međunarodnim standardima i konvencijama, što je u Republici Hrvatskoj učinjeno, pa se kao primjer dobre prakse može koristiti. Trenutno je zakonodavstvo Republike Srpske dobrim dijelom uskladilo odredbe materijalnog kaznenog prava s propisanim međunarodnim standardima zaštite djece, osobito Lanzarote konvencijom³⁸.

Djeca, ali i odrasle osobe, nažalost nisu svjesni činjenice da biti prisutan na društvenim mrežama poput Facebook-a ne znači samo mogućnost stjecanja novih prijateljstava, nego može biti izvor potrebnih informacija počiniteljima različitih vrsta kaznenih djela³⁹. Isto tako, digitalno opismenjavanje roditelja nužno je za zaštitu djece i maloljetnika kako u praćenju aktivnosti djeteta na društvenim mrežama, tako i u dijeljenju sadržaja o svojoj djeci bez svjesnosti o mogućim rizicima koje objavljivanje sadržaja o vlastitoj djeci može imati.⁴⁰

Djeci se treba osigurati pravo na informiranost i imati podršku tijekom pokretanja sudskog ili drugog postupka na način primjeren razvojnim sposobnostima djeteta. Nužno je usklađivanje specijaliziranih kaznenih postupaka ispitivanja i saslušanja djece s međunarodnim standardima kako bi odredbe relevantnih zakonskih propisa

37 Kazneni zakon Republike Srpske je prvi eksplicitno inkriminirao korištenje informacijsko komunikacijske tehnologije kao posrednog sredstva omogućavanja počinjenja kaznenog djela: (1) Tko sa djetetom starijim od petnaest godina, koristeći kompjutersku mrežu ili komunikaciju drugim tehničkim sredstvima, dogovori sastanak radi vršenja obljube ili sa njom izjednačene spolne radnje, ili radi proizvodnje pornografskog materijala, ili radi drugih oblika seksualnog iskorištavanja i pojavi se na dogovorenom mjestu radi sastanka, kaznit će se kaznom zatvora od jedne do pet godina.

(2) Ako je djelo iz stava 1. ovog člana izvršeno prema djetetu mlađem od petnaest godina, počinitelj će se kazniti kaznom zatvora od dvije do osam godina.

38 Konvencija Vijeća Europe o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja (Usvojio Odbor ministara 12. srpnja 2007. na 1002. sastanku zamjenika ministara)

39 Report of The Philippine National Police Anti-Kidnapping Group, <https://technology.inquirer.net/39521/kidnappers-scanning-social-networks-for-potential-victims-pnp>, 30.3.2021.

40 više u Grmuša, T., Tomulić, A.M., Anđelić, V.: Zaštita privatnosti djece i maloljetnika na društvenoj mreži Facebook: navike i iskustva roditelja, dostupno na https://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=326233, 25.3.2021.

bile primijenjene na odgovarajući način u skladu s najboljim interesima djeteta.

Škole, predstavnici organa unutarnjih poslova, institucije socijalne skrbi naglašavaju potrebu donošenja jasnih internih procedura za postupanje s pritužbama djece na određena potencijalno protupravna ponašanja kojima su izložena. Značajni izazovi za otkrivanje i procesuiranje počinitelja kaznenih djela prema djeci u digitalnom okruženju svakako su i značajno ograničeni tehnički kapaciteti policijskih agencija kao i, za ovu oblast, niska kadrovska osposobljenost organa kaznenog pravosuđa⁴¹. Jedini zakonom propisan učinkovit

mehanizam kojim se trenutno može doći do tragova i dokaza u slučaju počinjenja kaznenog djela prema djetetu u digitalnom okruženju jesu posebne istražne radnje. Primjenom posebnih istražnih radnji povećava se učinkovitost kaznenog postupka u otkrivanju specifičnih kaznenih djela. S druge strane, primjena posebnih istražnih radnji može se promatrati i kroz aspekt narušavanja prava i sloboda građana, posebice prava na privatnost i zaštitu obiteljskog života. Upravo zbog toga ZKP propisuje primjenu posebnih istražnih radnji protiv osobe za koju postoje osnovi sumnje da je sama ili s drugim osobama sudjelovala ili sudjeluje u počinjenju kaznenih djela iz članka 131.⁴² ZKP FBiH, članka 235⁴³. ZKP RS, članka 117⁴⁴. ZKP BD BiH mogu se

41 Vujović, S.: Seksualno iskorištavanje i zlostavljanje djece u digitalnom okruženju: Intenzitet rizika, težina posljedice i adekvatna reakcija u BiH (Policy brief), July 2019, DOI: [10.13140/RG.2.2.11391.15528](https://doi.org/10.13140/RG.2.2.11391.15528)

42 Posebne istražne radnje iz člana 130. stav (2) ovog zakona mogu se odrediti za krivična djela:

a) Unošenje opasnih materija u Federaciju (član 160.), Izazivanje narodnosne, rasne i vjerske mržnje, razdora ili netrpeljivosti (član 163.), Protupravno lišenje slobode (član 179.), Neovlašćeno prisluškivanje i zvučno snimanje (član 188.), Neovlašćeno optičko snimanje (član 189.), Povreda slobode odlučivanja birača (član 195.), Oduzimanje djeteta ili maloljetnika (član 217.), Nedozvoljeno presađivanje dijelova ljudskog tijela (član 231.), Oštećenje, uništenje i nedozvoljeni izvoz spomenika kulture i zaštićenih objekata prirode (član 321.), Nedozvoljeno obavljanje istraživačkih radova i prisvajanje spomenika kulture (član 322.), Udruživanje radi činjenja krivičnih djela (član 340.), Prinuda prema osobi koja vrši pravosudnu funkciju (član 359a.), Uništenje ili prikrivanje arhivske građe (član 368.), Davanje dara i drugih oblika koristi (član 381.), Oštećenje računalnih podataka i programa (član 393.), Računalno krivotvorenje (član 394.), Računalna prijevarama (član 395.), Ometanje rada sustava i mreže elektronske obrade podataka (član 396.), Neovlašćeni pristup zaštićenom sustavu i mreži elektronske obrade podataka (član 397.).

b) za druga krivična djela za koja se može izreći kazna zatvora pet godina ili teža kazna

43 Radnje iz člana 234. stav 2. ovog zakona mogu se odrediti za kaznena djela:

a) protiv ustavnog uređenja i bezbjednosti Republike Srpske,

b) protiv čovječnosti i vrijednosti zaštićenih međunarodnim pravom,

v) terorizma i

g) za koja se prema Kaznenom zakoniku može izreći kazna zatvora od pet godina ili teža kazna.

44 Istražne radnje iz člana 116 stava 2 ovog zakona mogu se odrediti za kaznena djela:

a) protiv države (glava XV),

b) terorizma (glava XVIII),

c) Otmica (član 177); Iskorištavanje djeteta ili maloljetnika radi pornografije (član 208); Neovlašćena proizvodnja i stavljanje u promet opojnih droga (član 232); Pranje novca (član 265); Udruživanje radi počinjenja krivičnih djela (334); Organizirani kriminal (336); Primanje dara i drugih oblika koristi (član 374); Davanje poklona i drugih oblika koristi (član 375); Primanje nagrade ili drugog oblika koristi za trgovinu uticajem (član 376); Davanje nagrade ili drugog oblika koristi za trgovinu utjecajem (član 376a); Zloupotreba položaja ili ovlaštenja (član 377); Nezakonito pogodovanje (377a); Oštećenje računalnih podataka i programa (387); Računarska prevara (389) i Računarska sabotaza (392),

d) kaznena djela za koje je propisana kazna zatvora najmanje pet godina ili teža kazna.

odrediti posebne istražne radnje ako se na drugi način ne mogu pribaviti dokazi ili bi njihovo pribavljanje bilo povezano s nerazmjernim teškoćama.

Iako je dijapazon kaznenih djela za koja se mogu izreći posebne istražne radnje dosta širok, kada se govori o povredi prava djece mogućnost primjene navedenih radnji je dosta ograničena. Tako se izrijeком posebne istražne radnje mogu prijeniti samo za kaznena djela iskorištavanje djeteta ili maloljetnika radi pornografije (čl. 208 KZ BD BiH) i neovlašteno optičko snimanje (čl. 189 ZKP F BiH), te ako je propisana sankcija viša od pet godina. Dakle, posebne istražne radnje ne mogu se provoditi u cilju otkrivanja, istraživanja i dokazivanja svih kaznenih djela, premda bi to vjerojatno umnogome olakšalo istražnu djelatnost tijela kaznenog progona, već se mogu poduzeti samo za ona kaznena djela kod kojih se radi o ugrožavanju ili povredi zaštićenog dobra veće vrijednosti ili u većem obimu, koji slijedom toga opravdavaju ograničavanje prava i sloboda pojedinaca i skupina osumnjičenih za njihovo (po)činjenje.⁴⁵

Zakoni o kaznenom postupku propisuju listu prikrivenih istražnih radnji kojima se za potrebe suzbijanja kriminaliteta privremeno ograničavaju temeljna prava i slobode čovjeka, i to: - nadzor i tehničko snimanje telekomunikacija; - pristup kompjutorskim sustavima i kompjutorsko sravnjenje podataka; - nadzor i tehničko snimanje prostorija; - tajno praćenje i tehničko snimanje osoba, transportnih sredstava i predmeta koji stoje u vezi sa njima, - korištenje prikrivenih istražitelja i korištenje informatora; - simulirani i kontrolirani otkup predmeta i simulirano davanje potkupnine i - nadzirani prijevoz i isporuka predmeta kaznenog djela (čl. 116. st. 2. ZKP BiH)⁴⁶. Izbor najpodesnije istražne radnje predložiti će tužitelj u suradnji s organima unutarnjih poslova, a provođenje radnji nalogom odobrava sudac za prethodni postupak. Zbog specifičnih okolnosti kojima mogu biti povrijeđena prava djeteta u digitalnom okruženju, najvjerojatnije je da će tužitelj predložiti Nadzorom i tehničkim snimanjem telekomunikacija ili eventualno prikrivenog istražitelja ili informatora.

Nadzor i tehničko snimanje telekomunikacija odnosi se na sva tehnička sredstva (npr., stacionirana, mobilna, digitalna, tonska, slikovna i sl.), koja se koriste preko poduzeća za održavanje usluga u telekomunikacijskom prometu uključujući i elektroničku poštu (e-mail), kao i druge oblike komuniciranja koji se odvijaju preko kompjutorskih uređaja i drugih sustava informacijske tehnologije⁴⁷. Prikriveni istražitelj je posebno osposobljena ovlaštena službena osoba koja istražuje pod izmijenjenim identitetom. Iako može pod izmijenjenim identitetom nastupati u pravnom prometu, prikriveni istražitelj ne smije poticati na počinjenje kaznenog djela, u protivnom ako poduzme radnje poticanja, ta okolnost isključuje kazneno gonjenje poticane osobe. Vrijednost primjene instituta prikrivenog istražitelja očituje se u usmjeravanju procesnih i kriminalističkih aktivnosti.⁴⁸ Maksimalno trajanje posebnih istražnih radnji u inicijalnoj fazi je mjesec dana. Moguće ih je produžavati za dalje intervale od po maksimalno mjesec dana, a dužina njihovog ukupnog trajanja ovisi o vrsti svake pojedine radnje, kao i o kaznenom djelu za koje se određuju.

45 Sijerčić-Čolić, H.(ur.) i sur.: Priručnik o posebnim istražnim radnjama, DCAF, 2020. str.23

46 Čl. 130. st. 2. ZKP F BiH; čl. 116. st.2. ZKP BD BiH; čl. 234. st. 2. ZKP RS

47 Sijerčić-Čolić, H. (ur) i sur., op. cit., str.20.

48 Petrović, B: Kriminalistika, Pravni fakultet Univerziteta u Sarajevu, Sarajevo, 2016., str. 289.

3. Zaključak

Potrebno je naglasiti važnost educiranja djece o svim pravima koja imaju sukladno međunarodnom i nacionalnom zakonodavnom okviru, ali svakako i o rizicima koji ih kao osjetljivu kategoriju prate kako u svakodnevnom realnom svijetu, tako još i više u digitalnom okruženju. Stoga je potreba da države uspostave eksplicitne, jasne zakonske okvire i lako primjenjive procedure kojima će osigurati upoznavanje djece s pravima, dostupnim pravnim lijekovima i mogućnošću obeštećenja za čitav niz povreda njihovih prava.

Povreda prava djece zloupotrebom digitalnog okruženja može se dogoditi svakom djetetu koje ima pristup tehnologiji. Nove informacijske i komunikacijske tehnologije umrežile su već stotine milijuna ljudi. Upravo tu činjenicu treba koristiti u svrhu promoviranja i podržavanja njihove uloge i uloge medija općenito u podizanju svijesti djece o njihovim pravima, ali i o svim potencijalnim rizicima digitalnog okruženja. Virtualni prostor, koji je moguća najveća prijetnja sigurnosti djece danas, moguće je takvim pristupom pretvoriti u oružje primarne prevencije, ali i sredstva jačanja povjerenja djece u pravosudne institucije ističući uspješne primjere sudske prakse u zaštiti prava djece. Svjesni toga, moramo uvidjeti i potrebu multidisciplinarnog koordiniranog pristupa zaštite djece u virtualnom okruženju, a to možemo postići suradnjom svih izravno ili neizravno uključenih subjekata u zaštiti prava djece, počevši od roditelja, staratelja, odgajatelja, predstavnika sektora sigurnosti i pravosudnog sektora, ali svakako i predstavnika sektora informacijsko komunikacijskih tehnologija.

Marija Boban, Ph. D., Associate Professor
Faculty of Law, University of Split

Ivana Stipanović, Ph.D., Assistant Professor
Faculty of Law, University of Mostar

PROTECTION OF CHILDREN'S RIGHTS IN THE DIGITAL ENVIRONMENT

Summary: The progressive development of information technologies brought new risks and threats to the protection of children's rights and it has become a topic that increasingly preoccupied scientific and professional discussions. According to the Guidelines of the Committee of Ministers of the Council of Europe on child-friendly justice, States have the obligation to provide effective remedies in the case of a violation of their human rights and fundamental freedoms in the digital environment. Prevention and education on the protection of children and their access to the virtual environment also has a key role. In accordance with the above, the authors will present an overview of measures for the protection of children on the Internet, with an emphasis on effective legal remedies based on the current legislative framework.

Key words: children, digital environment, criminal offenses, legal remedies, security.