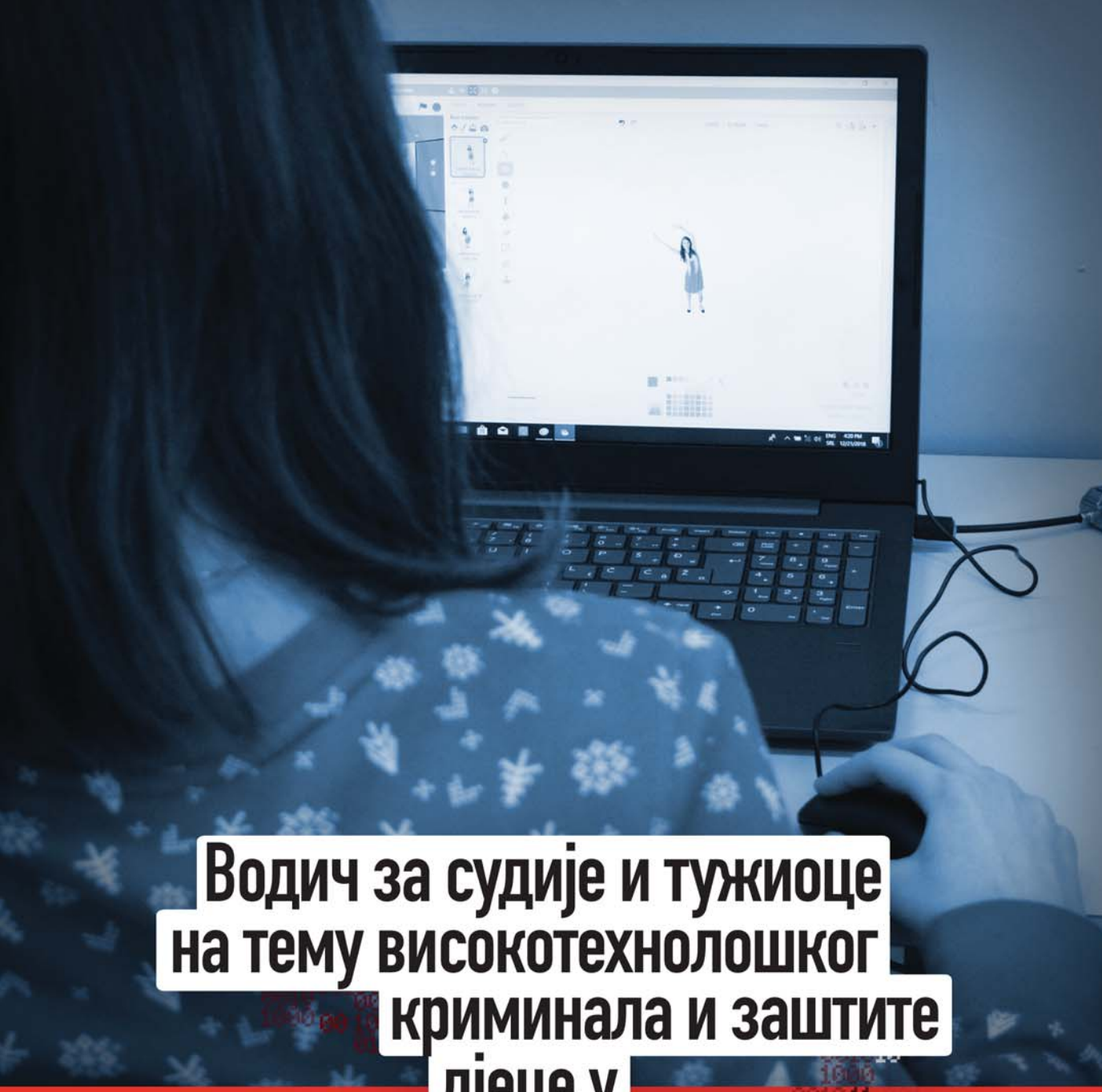


Водич за судије и тужиоце на тему високотехнолошког криминала и заштите дјеце у Босни и Херцеговини

Save the Children
100 YEARS

MEĐUNARODNI FORUM SOLIDARNOSTI - EMMAUS
BOSNA I HERCEGOVINA

unicef
za svako dijete

BOSNA I HERCEGOVINA – БОСНА И ХЕРЦЕГОВИНА – BOSNIA AND HERZEGOVINA
REPUBLIKA SRPSKA – РЕПУБЛИКА СРПСКА
FEDERACIJA BOSNE I HERCEGOVINE – ФЕДЕРАЦИЈА БОСНЕ И ХЕРЦЕГОВИНЕ

ЈАВНА УСТАНОВА ЦЕНТАР ЗА ЕДУКАЦИЈУ СУДИЈА И ЈАВНИХ ТУЖИЛАЦА У РС
JAVNA USTANOVA CENTAR ZA EDUKACIJU SUDIJA I TUŽILACA U FBiH
JAVNA USTANOVA CENTAR ZA EDUKACIJU SUDACA I TUŽITELJA U FBiH
PUBLIC INSTITUTIONS CENTRES FOR JUDICIAL AND PROSECUTORIAL TRAINING
OF THE RS AND THE FBiH

Водич за судије и тужиоце на тему високотехнолошког криминала и заштите дјеце у Босни и Херцеговини

Аутори:

Бранко Стаменковић
Саша Живановић
Бојана Пауновић
Ивана Стевановић

Сарајево, 2021. године

ИМПРЕСУМ

Save the Children вјерује да свако дијете заслужује будућност. У земљама сјеверозападног Балкана радимо сваки дан како бисмо за дјецу осигурали здрав почетак живота, прилику за учење и заштиту од насиља. Дајемо све од себе за дјецу – сваки дан и у вријеме криза – мијењајући њихове животе и будућност која је пред нама.

Издавач: Save the Children

Аутори: Бранко Стаменковић, Саша Живановић, Бојана Пауновић, Ивана Стевановић

Текст прилагодили контексту БиХ: проф. др. Елмедин Муратбеговић и
проф. др. Харис Халиловић

Текст одобрили: Центар за едукацију судија и тужилаца Федерације БиХ и
Центар за едукација судија и јавних тужилаца Републике Српске

Графички дизајн: КОМИТЕТ Сарајево

Штампа: Графика Шаран, Сарајево

Тираж: 150

Ова публикација израђена је у оквиру пројекта „Зауставити насиље над дјецом: Превенција и рад на спречавању сексуалног искоришћавања и злостављања дјеце у дигиталном окружењу у Босни и Херцеговини“, чију су реализацију подржали Global Fund to End Violence Against Children и УНИЦЕФ.

ЦИП - Каталогизација у публикацији
Национална и универзитетска библиотека Босне и Херцеговине, Сарајево

343.62-053.2:004.738.5(036)

ВОДИЧ за судије и тужиоце на тему високотехнолошког криминала и заштите дјеце у Босни и Херцеговини / Бранко Стаменковић ... [et al.]. - Сарајево : Save the Children, 2021.- 92. стр.

Ћир. - Библиографија: стр. 89-92 ; библиографске и друге билјешке уз текст.

ISBN 978-9926-462-29-1

1. Стаменковић, Бранко

COBISS.BH-ID 42627846

САДРЖАЈ

Предговор **5**

Увод у високотехнолошки криминал и савремени трендови у извршењу кривичних дјела из ове области 7

1. Увод **7**

2. Међународни значај рачунарског криминала **8**

3. Развој рачунарског криминала у Босни и Херцеговини **9**

4. Конвенција Вијећа Европе о високотехнолошком (кибернетичком) криминалу (CETS 185) **11**

4.1. Циљ и структура Конвенције Вијећа Европе о високотехнолошком криминалу 12

4.2. Појмовна одређења 13

4.3. Пружалац услуга 15

4.4. Подаци о саобраћају 15

4.5. Кривична дјела 16

4.6. Процесно право 18

4.7. Међународна сарадња 23

5. Директива 2013/40/EU **26**

6. Нормативни и институционални оквир у Босни и Херцеговини **28**

6.1. Конвенције, протоколи и законски оквир у Босни и Херцеговини 28

6.2. Подзаконски акти 31

7. Институционални оквир **31**

8. Савремени трендови **32**

8.1. Рачунарски криминал на мобилним платформама 33

8.2. Интензивно кориштење банкарских малвера и тројанаца 33

8.3. „Хактивизам“ и злоупотреба рачунарских мрежа 34

8.4. Савремене повреде права интелектуалне својине 34

8.5. Пораст циљаних напада – Advanced Persistent Threat („APT“) 35

8.6. Појава и злоупотреба криптовалута (Bitcoin, Ethereum, Ripple итд.) 35

8.7. Појава и злоупотреба интернета ствари (*IoT*, *Internet of Things*) 36

Прво реаговање на електронске доказе 37

1. Увод **37**

2. Стратегија за прикупљање дигиталних доказа **37**

2.1. Системи видео надзора 38

2.2. Подаци из отвореног интернетског извора 38

2.3. Онлајн кориснички налози за складиштење података 38

2.4. Електронска евиденција и комуникациони подаци (задржани подаци) 38

2.5. Подаци с уређаја крајњег корисника 39

2.5.1. Осигурање несталих доказа 39

2.5.2. Електронско трагање 39

2.5.3. Претрес и запљена 40

2.5.4. Рачунарско-дигитално вјештачење 40

3. Општи принципи **40**

4. Осигурање доказа са система видеонадзора **41**

5. Евиденције и подаци пружалаца комуникационих услуга **42**

5.1. Добивање података о комуникацији 42

5.2. Добијање садржаја комуникације....42
5.3. Добијање података од других онлајн услуга у Босни и Херцеговини....43
5.4. Добијање података из иноземства....43
6. Подаци из отворених интернетских извора....44
7. Онлајн кориснички налози и онлајн складиштење података....45
8. Уређаји крајњег корисника (оштећени/свједоци)....45
8.1. Професионални свједоци....46
9. Електронско трагање....46
9.1. Онлајн идентификатор....46
9.2. Адреса интернетског протокола (IP)....47
9.3. Утврђивање онлајн идентификатора....47
10. Савјет о претресању....48
10.1. Прије претреса....48
10.2. Брифинг....48
10.3. Припрема за претрес....49
10.4. Претресање мјеста извршења кривичног дјела....49

Високотехнолошки криминал као кривично дјело у домаћем законодавству с посебним освртом на cyberbullying i grooming....57
1. Увод....57
2. Кривични закони, појмовна одређења и заштита дјеце и малољетника....58
3. Заштита дјеце од сексуалног злостављања и искориштавања у Босни и Херцеговини....60
3.1. Република Српска....60
3.1.1. Кривично дјело искориштавање дјеце за порнографију (чл. 175. КЗ-а РС)....61
3.1.2. Искориштавање дјеце за порнографске представе (чл. 176. КЗ-а РС)....62
3.1.3. Упознавање дјеце с порнографијом (чл. 177. КЗ-а РС)....62
3.1.4. Искориштавање компјутерске мреже или комуникације другим техничким средствима за извршење кривичних дјела сексуалног злостављања или искориштавања дјетета (чл. 178. КЗ-а РС)....63
3.2. Федерација Босне и Херцеговине....63
3.2.1. Искориштавање дјетета или малољетника ради порнографије (чл. 211. КЗ-а ФБиХ)....63
3.2.2. Упознавање дјетета с порнографијом (чл. 212. КЗ-а ФБиХ)....64
3.2.3. Неовлаштено оптичко снимање (чл. 189. ст. 3. КЗ-а ФБиХ)....64
3.3. Брчко дистрикт Босне и Херцеговине....65
3.4. Сексуално, односно сполно узнемиравање....65
4. Grooming – поглавље прилагођено рјешењима у Босни и Херцеговини....66
5. Виртуелно злостављање (Cyberbullying)....68

Опће мјере заштите и исказ дјетета у кривичном поступку....78
1. Увод....78
2. Опће мјере заштите дјетета оштећеног/свједока у кривичном поступку....78
3. Поштовање принципа најбољег интереса дјетета и права на партиципацију у кривичним поступцима....81
3.1. Кривичноправни систем и уважавање принципа најбољег интереса дјетета и права на партиципацију у кривичним поступцима у Босни и Херцеговини....83

Препоручена литература....87

Препоручени интернетски ресурси....89

Предговор

Поштовани читаоци,

пред вама се налази документ под називом *Водич за судије и тужиоце на тему високотехнолошког криминала и заштите дјеце у Босни и Херцеговини*, који је првенствено намијењен за подршку у реализацији основних обука за судије и тужиоце који раде или се желе едуковати за рад на предметима високотехнолошког криминалитета у којем се дјеца јављају као починиоци, жртве или свједоци. Први документ, под готово идентичним називом (*Водич за судије и тужиоце на тему високотехнолошког криминала и заштите малољетних особа у Републици Србији)* израђен је 2017. године, а намијењен је тужиоцима и судијама полазницима Основног програма обуке Правосудне академије у Републици Србији. У том смислу водич прати развијени и усвојени Курикулум од Програмског одбора ове институције, која је овлаштена за реализацију специјализованих програма обуке за судије и тужиоце носиоце цертификата за рад с малољетницима као починиоцима кривичних дјела, односно малољетним оштећеним особама, тј. жртвама кривичних дјела. С обзиром на садржај таквог документа, он се може примијенити на различитим локацијама, па је у сарадњи с професорима Универзитета у Сарајеву извршено његово прилагођавање правном оквиру у Босни и Херцеговини. Стога се ова верзија документа сматра прилагођеном и корисном за обуке судија и тужилаца у Босни и Херцеговини, у оквиру програма Центара за едукацију судија и тужилаца у Ф БиХ и РС кроз сарадњу са Save the Children.

Аутори водича првенствено имају у виду да је информатичка револуција донијела квалитативни напредак у животима свих људи, толико јак да је практично више немогуће замислити цивилизацију без информатичке подршке у свим својим облицима коју нам пружају информационе технологије, али да је с друге стране овакав експлозиван развој неумитно произвео и одређене пратеће посљедице негативног карактера. Из тог разлога у Водичу се посебна пажња управо поклања основним појмовима високотехнолошког криминала, указује на његове појавне облике, даје приказ савремених трендова у извршењу кривичних дјела из ове области и анализира нормативни оквир који регулише ову област у Босни и Херцеговини, првенствено у сфери кривичноправне реакције.

Такође, уважена је и чињеница да је у посљедњих неколико деценија нарочита пажња на међународном плану посвећена успостављању дјелотворне заштите дјеце жртава савремених облика криминалитета, посебно имајући у виду неопходност подузимања законодавних и других мјера за спречавање свих видова сексуалне експлоатације и сексуалног злостављања дјеце, као и потребу њихове заштите, уважавајући да најбољи интереси дјетета и право дјетета да се његово мишљење чује и узме у разматрање представљају један од основних принципа у остваривању, поштовању и заштити њихових права. Државе уговорнице, свјесне обима и карактера ових појава, посебно повећане међународне трговине дјецом, искоришћавања дјеце у проституцији и порнографији, односно све израженије злоупотребе рачунарских система и мрежа у циљу регрутовања дјеце у споменуте сврхе, поред осталог реаговале су и успостављањем нових норми и стандарда који ће бити посебно истакнути и дале су јасна упутства за њихову непосредну примјену од носилаца правосудних функција.

Водич садржи и јасна упутства за поступање у случајевима кривичних дјела на штету дјеце и малољетника у дјелу злоупотреба на интернету (односно у сфери злоупотреба савремених

технологија), начин реаговања на електронске доказе и детаљне информације о одузимању, руковању и испитивању електронских уређаја и уређаја повезаним с њима. Посебна пажња посвећена је и практичним примјерима из области високотехнолошког криминала уз нагласак на неопходност унапређења међународне и међуресорне сарадње свих актерима у сфери заштите дјеце и ојачавања система.

Све наведено аутори су уобличили у четири тематске цјелине:

- Увод у високотехнолошки криминал и савремени трендови у извршењу кривичних дјела из ове области (Бранко Стаменковић, Посебни тужилац за високотехнолошки криминал);
- Прво реаговање на електронске доказе (Саша Живановић, начелник Одјељења за високотехнолошки криминал УКП МУП Републике Србије);
- Високотехнолошки криминал као кривично дјело у домаћем законодавству с посебним освртом на тзв. *cyberbullying* и *grooming* (Бојана Пауновић, Судија Апелационог суда у Београду;
- Опће мјере заштите и исказ дјетета у кривичном поступку (др. Ивана Стевановић, Виши научни сарадник Института за криминолошка и социолошка истраживања).

Поштоване колегице и колеге, поштовани читаоци, надамо се да ће Водич бити од користи за боље разумијевање сложене проблематике о којој смо писали и представљати још један корак напријед ка успостављању „правосуђа по мјери дјетета" у Босни и Херцеговини.[1]

"Правосуђе по мјери дјетета" означава правосудни систем који јамчи поштовање и дјелотворно спровођење свих права дјетета на највишем могућем нивоу… То је прије свега правосуђе које је доступно, примјерено узрасту, ефикасно, прилагођено потребама и правима дјетета и усредсређено на те потребе и права, уз поштовање права дјетета, укључујући право на поступак у складу са законом, право да учествује у поступку и да разумије поступак, на поштовање приватног и породичног живота и на интегритет и достојанство. Остваривање „правосуђа по мјери дјетета подразумијева правосуђе прилагођено на начин да буде примјереније дјетету и ефикасне поступке доступне дјеци уз осигурање неопходне независне правне репрезентације. На овај начин се омогућава дјеци да када дођу у контакт с правосудним системом, било као свједоци, жртве (оштећени) или као починиоци кривичних дјела, тужиоци и подносиоци притужби буду у могућности да на адекватан начин заштите своја права и интересе.

Прилагођавање правосуђа да буде примјереније дјеци у Европи дио је Агенде Европске уније о правима дјетета[2] *и представља један од најважнијих стандарда у области права дјетета. Уважавање основних начела „правосуђа (правде) по мјери дјетета" подразумијева примјену основних принципа: принципа партиципације, уважавање најбољих интереса дјетета, поштовање достојанства дјетета, заштиту од дискриминације и владавину права (Смјернице Комитета министара Вијећа Европе о правосуђу по мјери дјетета – III Основна начела – од А до Е).*

Уважавање наведених принципа од посебне је важности у свјетлу заштите малољетних особа као оштећених/свједока савремених облика криминалитета од посљедица секундарне виктимизације у кривичном поступку.

[1] *Смјернице Комитета министара Вијећа Европе о правосуђу по мјери дјетета*, усвојене 17. новембра 2010. на 1.098. засједању замјеника министара Вијећа Европе Редигована верзија од 31. маја 2011.

[2] *Агенда Европске уније о правима дјетета* усвојена од Европске комисије Европске уније 52011DC0060 од 15. фебруара 2011. године 52011DC0060, (52011DC0060, 15. фебруар 2011. године).

Увод у високотехнолошки криминал и савремени трендови у извршењу кривичних дјела из ове области

1. Увод

Револуција у информационим технологијама је суштински промијенила друштво и настављат ће га мијењати и убудуће. Многи послови су постали једноставнији за обављање. Доскора и у само одређеним дијеловима друштва ради рационализације радних процедура коришћене су информационе технологије у свакодневном раду. Данас је тешко замислити било који дио друштва без утјецаја примјене рачунара и рачунарских система. Информационе технологије су на свеобухватан начин данас умијешане и искоришћене у сваком аспекту људске активности.

Овакав развој је директно утјецао на до сада невиђени економски напредак, али и друштвене промјене које су у оквиру свог настанка и постојања дошле и у контакт с тамнијом страном људске природе. Настајање нових типова и врста криминала, као и извршење традиционалних кривичних дјела употребом нових технологија постало је стандардни дио реалности државних органа који поступају у овој области.

Штавише, посљедице извршења кривичних дјела и понашања извршилаца данас много више и дубље обухватају ткиво сваког друштва, па и наших, с обзиром на то да данас не постоје географске ни националне границе када говоримо о употреби информационих технологија и извршењу кривичних дјела.

Нове технологије постављају изазов пред постојеће правне концепте. Ток информација и комуникација данас је на планетарном нивоу у потпуности олакшан. Границе више нису границе за овакву врсту размјене. Криминалци су све више лоцирани на мјестима одакле њихове радње могу произвести значајнији ефект, тј. посљедицу не само по њих већ и по друге.

Ипак, домаћи је законодавни оквир генерално ограничена територија националног законодавства. Из тих разлога проблеми у овој области морали су се ријешити на међународном нивоу кроз међународни правни оквир који је изњедрио усвајање адекватних међународних правних инструмената. Данас такав инструмент представља Конвенције о кибернетичком криминалу Вијећа Европе (CETS 185)[3], чији је циљ да се супротстави овој врсти изазова, уз дужно поштовање људских права у новом информатичком и постинформатичком друштву.

[3] Будимпешта, 23.11.2001. године, ступила на снагу 01.07.2004. године, ступила на снагу у односу на БиХ 01.09.2006. године; објава „Службени гласник БиХ“ – Међународни уговори број: 06/2006

2. Међународни значај рачунарског криминала

Према неким изворима[4] који прате глобални тренд извршења кривичних дјела у области рачунарског, то јест кибернетичког криминала, мотивацију која стоји иза извршења овог, али и других облика противправног друштвеног понашања, могуће је подијелити на пет главних група, и то као мотивацију уперену ка:

- рачунарским – високотехнолошким кривичним дјелима (кибернетичком криминалитету),
- „хактивизму“,
- кибернетичкој шпијунажи,
- кибернетичком ратовању,
- осталим облицима санкционисаног или неприхватљивог понашања.

У том смислу, интересантно је да подаци из наведених јавних извора указују на то да на годишњем нивоу долази до значајних промјена у односу између ових група, што је могуће видјети већ на упоредном приказу података који су обрађени у јуну 2015. и новембру 2016. године и који указују на то да простор који захвата рачунарски криминал расте из године у годину значајном стопом. Тако, нпр., 2015. године процијењени је удио рачунарског, то јест високотехнолошког криминала у односу на друге групе износио 59,5%, док је већ у 2016. години тај удио порастао на 82,7%. Највећи пад су доживјеле активности које припадају тзв. „xaktivizmu“, о чему ће бити више ријечи детаљније у даљем тексту, док су групе којима припадају кибернетичка шпијунажа и ратовање, као и остали облици извршења ових дјела или догађаја остали на приближно истим нивоима.

Што се праваца извршења ових кривичних дјела тиче, примијећено је да је доста присутно увјерење да су жртве, тј. оштећени у овој области понајвише физичке особе. Ипак, подаци говоре другачије и указују на то да уствари највећу групу оштећених чине правне особе, тј. подузећа која обављају комерцијалну дјелатност. Одмах из ове групе и то с врло сличним процентом (око 21%), долазе државни органи као мете и жртве кибернетичких напада. Тек након ове двије групе (које заједно заузимају скоро 44% од укупног броја извршења ових кривичних дјела) долази група која припада физичким особама, и то с процијењеним процентом од око 12% од укупног броја. Након ове три главне групе мета напада (уједно и жртава) скоро равномјерно распоређено долазе разне организације, образовне институције, финансијски сектор итд.

Приликом анализе података који се односе на средства и правце који су искориштени за извршење ових кривичних дјела, као и догађаја који можда немају одмах кривичноправну конотацију, интересантно је примијетити да највећи удио од скоро једне четвртине припада средствима која су непозната, тј. да трагови извршења дјела нису са сигурношћу могли указати на то који је малициозни софтвер конкретно коришћен у одређеној прилици.

Што се препознатих средстава и праваца тиче, највећи дио припада разним облицима малициозног софтвера који је коришћен за нападе на комерцијалне услуге које пружају разне правне особе с намјером остваривања зараде. Након малициозног софтвера појављује се тзв. „отимање налога“, тј. неовлаштено преузимање корисничких налога на разним платформама, укључујући оне које припадају друштвеним мрежама, електронској пошти, банкарским услугама и сл. За овим категоријама слиједе специфични облици као што су SQL

[4] www.hackmageddon.com

ињекције, Дистрибуисани DoS напади, измјена насловних страна одређених интернетских презентација (*defacement*) и сл.

Када говоримо о штети која настаје противправним понашањем путем кориштења рачунара и рачунарских мрежа, а посебно кривичних дјела која се могу означити као високотехнолошка, треба имати на уму процјену одређених јавних извора[5] да штета која на овај начин настаје на глобалном годишњем нивоу може досећи износ од преко 388 милијарди USD. Овај износ представља збир стварне штете која је настала извршењем наведених дјела као и новчаних и материјалних средстава која су физичке и правне особе уложиле у отклањање штете и додатну превентивну заштиту након оваквих догађаја. Стварна штета процијењена је на износ од 114 милијарди USD, док је отклањање штете и подизање нивоа сигурности коштало 274 милијарди USD.

Поређења ради, свјетска трговина најпопуларнијим нелегалним наркотицима, тј. опојним дрогама, као што су марихуана, кокаин и хероин, процијењена је на годишњем нивоу на износ од 288 милијарди USD, док је укупна свјетска трговина нелегалним наркотицима процијењена збирно на износ од 411 милијарди USD.

Из једноставног поређења износа процијењене штете од рачунарског криминала и вриједности трговине опојним дрогама произилази јасан закључак да трговина потоњим тек за неких 23 милијарде USD премашује претходни износ, што у свјетским размјерама заиста не представља значајну бројку. Овај податак је значајнији тим прије што извршење кривичних дјела које за свој објекат имају опојне дроге подразумијева присуство изузетног ризика по извршиоце ових кривичних дјела у виду реакције државних органа како појединачних земаља, тако и координисани наступ и сарадњу ових органа на свјетском нивоу ради сузбијања ове врсте криминалитета, који у великом броју случајева подразумијева и употребу физичке силе и ватреног оружја.

С друге стране, у свом највећем дијелу извршење кривичних дјела тзв. кибернетичког криминала подразумијева управо супротно, тј. још увијек постоји одсуство значајнијег ангажовања државних органа као и, скоро сигурно, одсуство примјене јаких мјера репресивне државне силе.

Наведени примјери уствари додатно појашњавају присутни тренд који се креће у правцу помјерања активности припадника криминогених средина из области високо ризичних кривичних дјела која су до сада имала високе приносе противправне имовинске користи у разним облицима у област високотехнолошког криминала, који уз значајно мање улагање и сигурно мање присутну опасност по физички интегритет доноси практично исту, ако не у одређеним случајевима и већу противправну имовинску корист извршиоцима. Овај је тренд уочен како на глобалном, тако и локалном нивоу.

3. Развој рачунарског криминала у Босни и Херцеговини

Несумњиво је да је високотехнолошки криминал у Босни и Херцеговини много старији од његовог инкриминисања и имплементације законских описа ових кривичних дјела у домаће кривичноправне прописе. Као зачетак у процесу инкриминисања високотехнолошког криминала у Босни и Херцеговини можемо сматрати реформу кривичног законодавства из

[5] http://resources.infosecinstitute.com

2003. године, која је обухватила како материјално, тако и процесно кривично право. На подручју материјалног кривичног права то је значило увођење нових кривичних дјела у законске прописе, док је на подручју кривичног процесног права то значило дефинисање појмова високотехнолошког криминала како би се олакшало процесуирање ових кривичних дјела, посебно у дијелу који се односио на радње доказивања. Ипак, значења појмова „компјутерски систем" и „компјутерски податак" у циљу адекватнијег супротстављања овом виду криминала бивају имплементирана у законске прописе на подручју кривичног поступања тек 2009. године. Без икакве дилеме, а пратећи развој информатичких технологија, којем смо у посљедњих скоро три деценије могли и лично посвједочити, можемо утврдити како се прописивање ових кривичних дјела као и појмова с овог подручја у Босни и Херцеговини догађа прилично касно. Једно од проведених истраживања на тему понашања дјеце на интернету резултирало је закључком да се дјеца од девет до 17 година у Босни и Херцеговини готово без изузетка користе савременим информационо-комуникацијским технологијама, и што је врло релевантно, корисници су интернета.[6]

Данашњи статистички показатељи о обиму ових кривичних дјела воде ка закључку како она не представљају већу друштвену опасност, с чиме бисмо се међутим тешко могли сложити. Можда је прије ријеч о томе да откривање, а потом и адекватно процесуирање ове врсте кривичних дјела још није на нивоу који бисмо могли сматрати задовољавајућим. Наводимо неке од тих показатеља:

Осуђени пунољетни починиоци кривичних дјела против система електронске обраде података у Федерацији БиХ за период 2010–2017.[7]

Година	2010.	2011.	2012.	2013.	2014.	2015.	2016.	2017.	**УКУПНО**
Број осуђених пунољетних починилаца	10	18	22	4	-	5	8	4	**60**

Осуђени пунољетни починиоци кривичних дјела против сигурности рачунарских података у Републици Српској за период 2011–2017.[8]

Година	2011.	2012.	2013.	2014.	2015.	2016.	2017.	**УКУПНО**
Број осуђених пунољетних починилаца	-	2	2	-	2	-	2	**8**

[6] Муратбеговић, Е., Кобајица, С. и Вујовић, С. (2016). *Насиље над дјецом путем информационо-комуникаијских технологија у Босни и Херцеговини*, CPRC, Save the Children, Сарајево, стр. 149.

[7] Статистика правосуђа 2017, Статистички билтен бр. 272/2018, Босна и Херцеговина, Федерални завод за статистику, Сарајево, 2018.

[8] Правосуђе, Статистички годишњак Републике Српске, Република Српска, Републички завод за статистику, Бања Лука, 2018., 2017., 2016, 2015., 2014., 2013. и 2012.

У вези с динамиком настанка и развоја феномена високотехнолошког криминала у Босни и Херцеговини, између осталих, посебно се истичу сљедеће карактеристике и околности:[9]

1. законодавни проблеми;
2. социо-економска ситуација;
3. отвореност граница;
4. пораст броја корисника компјутера.

Свака од наведених околности као и све заједно у својој укупности доприносе отежавању сузбијања високотехнолошког криминала у нашој држави. За очекивати је да ће босанкохерцеговачко друштво у времену које слиједи ипак пронаћи начина да адекватније одговори оваквом виду криминалног понашања које ће сигурно из мноштва разлога, па и оних посве баналних, као што је континуирано повећање броја корисника овог вида технологија, довести и до већег степена њихове злоупотребе. У том смислу бит ће потребно подузети мноштво мјера, не само у виду прописивања нових инкриминација или пуком преузимању различитих појмова из међународних докумената да би се само номинално испуниле међународне обавезе већ конкретних мјера на едукацији специјализованог особља, као и мјера на успостави посебних организацијских јединица у оквиру правосуђа и полицијских агенција специјализованих за откривање и процесуирање ове врсте кривичних дјела.

4. Конвенција Вијећа Европе о високотехнолошком (кибернетичком) криминалу (CETS 185)

Конвенција о високотехнолошком (кибернетичком) криминалу Вијећа Европе је први међународни споразум, тј. правни акт, који регулише материјални, процесни и међународни правни оквир за кривична дјела која су извршена путем рачунара, рачунарских мрежа, као и коришћењем интернета и других рачунарских мрежа међународног или локалног карактера.

Конвенција поставља основе правних норми које се тичу кршења права интелектуалне својине, превара извршених коришћењем рачунара, злоупотребе малољетника у порнографске сврхе, противправног приступа заштићеном рачунару и рачунарској мрежи, пресретању података итд. Овом конвенцијом су прописане и радње и мјере како материјално, тако и процесно-правне природе, које су усмјерене ка негативном санкционисању друштвено штетног понашања у овој области и које примјењују савремене истражне методе приликом откривања и гоњења извршилаца кривичних дјела, као што су претрага рачунарских мрежа и пресретање рачунарских података, чији је главни циљ гоњење извршилаца кривичних дјела и успостављање заједничке кривично правне политике која је усмјерена ка заштити друштва од свих облика високотехнолошког, тј. кибернетичког криминала, посебно кроз усвајање одговарајућих правних норми и успостављање оперативне међународне сарадње у овој области.

Конвенција о кибернетичком криминалу Вијећа Европе је након вишегодишњег периода усаглашавања изворног текста отворена за потписивање од стране чланица Вијећа Европе 23. новембра 2001. године, као и за потписивање од стране земаља које нису чланице ове

[9] В. Будимлић, М. и Пухарић, П. (2009) *Компјутерски криминалитет: криминолошки, кривичноправни, криминалистички и сигурносни аспекти, Факултет за криминалистику, криминологију и сигурносне студије*, Сарајево стр. 47–48.

организације, а које имају интерес да примјењују одредбе Конвенције и да учествују у међународној сарадњи.

Чињеница је да ова конвенција тренутно представља једини међународно правно признати и континентално раширени правни инструмент у области високотехнолошког криминала, који у свом тексту обједињује прецизно одређене и, што је још битније, употребљиве савремене методе поступања државних органа, али не само њих већ и других институција и организација у овој области, све у циљу успостављања дјелотворног међународног механизма, који је састављен од више органских цјелина на нивоу појединих земаља које су потписале или ратификовале ову конвенцију.

Ове земље кроз на тај начин успостављену планетарну мрежу за прво као и рано реаговање, те вођење даљих преткривичних и кривичних поступака, имају могућност да на одговарајући начин, у складу са својим техничким могућностима, одговоре на изазове високотехнолошког, тј. кибернетичког криминала, које пред њих стављају извршиоци ових кривичних дјела.

До 1. јула 2017. године више од 59 земаља ратификовало је ову конвенцију, затражило приступање овој конвенцији или ју је потписало. Осам земаља нису чланице Вијећа Европе. У те земље спадају Аустралија, Канада, Чиле, Доминиканска Република, Израел, Јапан, Маурицијус, Јужноафричка Република, Панама, Сенегал, Шри Ланка, Тонга и Сједињене Америчке Државе.

Од земаља чланица Европске уније, којих је укупно 28 у овом тренутку, само Република Ирска и Шведска нису и ратификовале ову конвенцију, али је јесу потписале, док су све остале земље чланице Европске уније Конвенцију и ратификовале, те се она у складу с унутрашњим правним порецима земаља потписница активно примјењује кроз унутрашње материјално, процесно и међународноправне одредбе.

4.1. Циљ и структура Конвенције Вијећа Европе о високотехнолошком криминалу

Конвенција Вијећа Европе о високотехнолошком криминалу за свој циљ има на првом мјесту хармонизацију домаћих материјалних кривичноправних одредби у области рачунарског криминала, омогућавање домаћем кривичном процесно-правном оквиру да надлежним државним органима пружи овлаштења која су неопходна за ефектно откривање и гоњење извршилаца ових кривичних дјела, као и успостављање брзог и ефективног оквира међународне сарадње у овој области.

Имајући наведено у виду, Конвенција се састоји из четири главе и то:

I. Употреба термина,

II. Мјере које се требају подузети на домаћем нивоу – материјално и процесно право,

III. Међународна сарадња и

IV. Завршне одредбе.

Први одјељак друге главе предвиђа одредбе о санкционисању криминала који је извршен помоћу рачунара и рачунарских мрежа и који одређује девет општих кривичних дјела која су подијељена у четири различите категорије.

Кривична дјела која су одређена конвенцијом су:

1. **неовлаштени (противправни) приступ,**
2. **неовлаштено (противправно) пресретање,**
3. **ометање тока података,**
4. **ометање рачунарског система,**
5. **злоупотреба уређаја,**
6. **фалсификовање извршено помоћу рачунара,**
7. **превара извршена помоћу рачунара,**
8. **кривична дјела дјечије порнографије и**
9. **кривична дјела ауторских и сродних права.**

У одјељку 2 друге Главе, када говоримо о процесним одредбама, предвиђено је:

1. **хитно чување похрањених података,**
2. **хитно чување и дјелимично откривање података о саобраћају,**
3. **наредба за достављање,**
4. **претрага и запљена рачунарских података,**
5. **прикупљање података о саобраћају у реалном времену,**
6. **пресретање података о саобраћају.**

У трећем одјељку конвенција садржи одредбе које се односе на традиционалне и рачунарски повезане правне инструменте међусобне сарадње, тј. међународне сарадње у кривичном праву, као и правила за изручење. Поглавље говори о традиционалној међународној сарадњи у кривичној материји у двије ситуације:

- када не постоји правна основа у виду споразума, реципроцитета итд. између страна потписница конвенције, у којем се случају примјењују одредбе саме конвенције, као и у случајевима када таква основа постоји,
- када се примјењују одредбе тих правних оквира уз помоћ примјене саме конвенције.

Такође, у глави III су садржане одредбе о посебним облицима прекограничног приступа похрањеним рачунарским подацима који не захтијевају поступак међународне правне помоћи, као и успостављање такозване „24/7“ мреже за хитно реаговање, ради омогућавања брзе и ефективне сарадње између надлежних органа страна потписница.

4.2. Појмовна одређења

У оквиру поглавља 1 Конвенција на општи начин дефинише појмове као што су рачунарски систем, рачунарски подаци, пружалац услуга, подаци о саобраћају итд., што је пренесено у значајном обиму и у домаће законодавство.

Имајући наведено у виду, Конвенција у ширем смислу дефинише рачунарски систем као уређај који се састоји од хардвера, тј. физичких уређаја и софтвера, тј. рачунарских програма, који се заједно користе за аутоматско процесуирање дигиталних података.

Наведени збирни уређај може укључити улазне и излазне уређаје, као и уређаје за похрањивање. Такође, он може бити сачињен као самосталан уређај који није повезан на рачунарску мрежу или као уређај који је повезан на мрежу с другим сличним уређајима.

Под аутоматском обрадом података сматра се обрада података без непосредне, тј. директне људске интервенције, док се процесуирање података описује као скуп података у компјутерском систему који се користи кроз извршавање одређеног компјутерског програма.

Надаље, рачунарски програм је сет инструкција који може бити извршен од рачунара ради постизања одређених тј. жељених резултата. Рачунари могу користити различите програме.

Рачунарски систем обично се састоји од различитих уређаја који се међусобно разликују као обрађивачи или централне обрађивачке јединице уз употребу такозваних периферијских јединица. Периферијска јединица је уређај који може обавити одређене специфичне функције у сарадњи с главном процесорском јединицом, као што су штампачи, видеобимови, CD/DVD читачи и писачи и други слични уређаји.

У смислу конвенције, рачунарску мрежу представљају два или више међусобно повезана рачунарска система. Међусобна повезаност може бити земаљска, тј. путем жице или кабла, бежична (путем радио, инфрацрвеног или сателитског емитовања) или коришћењем оба начина. Мрежа може географски бити ограничена на малу област (локална мрежа) или се може пружати преко велике територијалне области (као што су такозване „WAN“ мреже). Овакве мреже такође могу бити међусобно повезане на описане начине.

Интернет представља глобалну мрежу која се састоји од мноштва међусобно повезаних мрежа које све користе исти комуникациони протокол, тј. начин комуникације. Други типови мрежа такође постоје, без обзира на то јесу ли или нису повезане на интернет и међусобно су оспособљене да комуницирају размјеном рачунарских података између рачунарских система.

Појединачни рачунари или рачунарски системи могу бити повезани на мрежу као завршне тачке комуникације или могу у оквиру таквих мрежа служити као помоћ у прослеђивању података између других рачунара и рачунарских система. Оно што је есенцијално битно је то да подаци употребом оваквих система могу и јесу размијењени путем мреже, тј. међусобне повезаности.

Конвенција се приликом дефинисања рачунарских података ослања на дефиницију таквих података према такозваним ИСО-стандардима. Ова дефиниција садржи изразе који су погодни за процесуирање, тј. коришћење. Ово значи да су подаци да би имали квалитет рачунарских састављени у таквој форми да могу бити директно обрађени – процесуирани од рачунарског система.

Да би било потпуно јасно да подаци на које се односи Конвенција требају бити подведени под податке у електронској или у другој форми која је подобна за рачунарско процесуирање, израз „рачунарски подаци“ уведен је и дефинисан.

На основу ове дефиниције рачунарски подаци су они подаци који су у смислу кривичноправног законодавства аутоматски процесуирани и могу бити мета, тј. предмет извршења кривичних дјела која су дефинисана наведеном Конвенцијом, као и објекат примјене неке од истражних мјера које су њоме предвиђене.

4.3. Пружалац услуга

Термин пружалац интернетских услуга тј. *Internet service provider* („ISP“), обухвата широку категорију физичких и правних особа које имају одређене улоге у односу на комуникацију или процесуирање података у рачунарским системима. Под овом дефиницијом јасно је наведено да како јавни, тако и приватни субјекти који пружају овакву врсту услуга јесу и морају бити укључени у кривичноправни законодавни оквир земаља потписница Конвенције.

Према томе, небитно је да ли корисници међусобно формирају тј. чине затворену групу која не пружа овакву врсту услуга према спољашности, да ли такозвани „провајдер услуга“ своје услуге пружа ка јавности, као и да ли је ово пружање услуга бесплатно или уз накнаду. Примјер затворене групе могу бити запослени у оквиру приватног подузећа којима је оваква врста комуникације омогућена од компанијске мреже.

У оквиру ове дефиниције јасно је да се израз пружалац услуга такође односи и на оне ентитете, тј. субјекте који похрањују или на други начин обрађују податке у име и за рачун претходно наведених субјеката. Надаље, израз обухвата и оне субјекте који похрањују или на други начин процесуирају податке у име и за рачун корисника сервиса који су споменути под овом дефиницијом.

Напримјер, у оквиру ове дефиниције пружалац услуга обухвата подједнако услуге такозваног „хостинга“ и „кешинга“, тј. трајнијег или привременог чувања података и услуга, као и услуге које омогућавају повезивање на одређену мрежу. Ипак, обичан пружалац услуга презентовања одређеног садржаја, као што је напримјер особа која склопи уговор с компанијом за такозвано „web-хостовање“ ради „хостовања“, тј. чувања и приказивања његове/њене web-странице – презентације, није обухваћан овом дефиницијом, уколико ентитет код кога се наведени садржај налази такође не пружа комуникационе или обрађивачке услуге података.

4.4. Подаци о саобраћају

Појам података о саобраћају дефинисан је у члану 1. Конвенције, у оквиру става Д, и представља категорију рачунарских података који су предмет посебног правног режима. Ову врсту података генерисао је - створио рачунар (компјутер) у тзв. „ланцу комуникације“, ради усмјеравања комуникације од свог мјеста настанка до крајње дестинације. У том смислу подаци о саобраћају представљају помоћно средство самој комуникацији.

У случају вођења истраге за кривично дјело које је извршено у вези с рачунаром или рачунарским системом, подаци о саобраћају су неопходни ради праћења извора комуникације као почетна тачка за прикупљање даљих доказа, као дио самог доказног материјала у прилог постојања основане сумње да је извршено кривично дјело, или, у каснијем току кривичног поступка, ради доказивања постојања кривичног дјела и кривичноправне одговорности његовог извршиоца. Због своје природе, која се огледа у врло кратком трајању, подаци о саобраћају захтијевају да буду сачувани - осигурани на најбржи могући начин.

Посљедично, њихово брзо откривање може бити од кључне важности за лоцирање комуникационог правца ради даљег прикупљања доказа, за које постоји опасност да ће бити избрисани, или који могу послужити за откривање идентитета извршиоца кривичног дјела.

С тим у вези, уобичајене процедуре, радње и мјере које у стандардном вођењу кривичног поступка од надлежног органа откривања или гоњења бивају подузете ради утврђивања постојања кривичног дјела и евентуалне кривичноправне одговорности његовог извршиоца, могу се у овом случају показати као недовољне. Штавише, упоредна правна пракса како редовних тако и специјализованих органа откривања и гоњења, тј. служби и јединица Министарства унутрашњих послова као и надлежних државних, тј. јавних тужилаштава, управо показује да временски оквири који прате примјену стандардних истражних метода могу представљати једну од кључних препрека за успјешно гоњење у овој кривичноправној области.

Конвенција таксативно набраја категорије података о саобраћају и то у виду поријекла - извора комуникације, њеног одредишта, пута, времена, датума, величине, трајања и врсте услуге која је пружена. Вриједно је споменути да неће све ове категорије бити увијек технички доступне, посебно када имамо у виду разноликост техничке опремљености и обученост запослених у разним подузећима која се баве услугом пружања приступа интернету или омогућавању кориштења одређених категорија услуга које су везане за кориштење рачунарских мрежа, како међународних тако и локалних, јавних и приватних.

Поријекло комуникације се односи на број телефона, адресу интернетског протокола или сличну идентификацију комуникационе опреме којој пружалац интернетских услуга пружа услуге.

Одредиште представља упоредиву индикацију о уређајима који служе за комуникацију и како је сама комуникација (тј. подаци) усмјерена, пренесена или испоручена.

Појам врсте сервиса односи се на врсту услуге која се користи унутар саме мреже и може се остварити кроз размјену тзв. фајлова, електронску пошту или размјену инстант-порука.

Дефиниција на овај начин описана оставља националним законодавствима могућност да примијене у датим оквирима различит приступ правној заштити података о саобраћају, у складу с њиховом осјетљивошћу. У овом смислу, у члану 15. Конвенције постоји обавеза страна потписница да пруже увјете и гаранције ради адекватне заштите људских права и слобода.

У том смислу материјалноправне одредбе као и процесноправне одредбе које се примјењују или могу бити примијењене могу бити различите, тј. варирати у односу на осјетљивост самих података.

4.5. Кривична дјела

Конвенција у другој Глави у оквиру трећег дијела регулише материјалноправни оквир и то у члановима од 2. до 13., процесноправни оквир од чланова 14. до 21., као и надлежност у члану 22.

Циљ прописивања материјалноправног оквира Конвенцијом у сваком случају лежи у унапређењу законских одредби ради спречавања као и гоњења специфичног облика, тј. врсте криминалитета који се извршава помоћу рачунара и у рачунарском окружењу уз кориштење рачунарских мрежа.

Успостављањем заједничког минималног стандарда у прописивању кривичних дјела и њихових битних обиљежја, постиже се хармонизација међународног кривичног права, која је посебно значајна у овој области криминалитета, имајући у виду његову експоненцијалну

криву раста и развоја, а које би требало подразумијевати хармонизацију како на националном, тако и на међународном нивоу.

Уколико би оваква хармонизација материјалноправних кривичних одредби изостала, примјена других међународно правних инструмената, као што је напримјер Палермо конвенција или Конвенција о пружању међународне правне помоћи у кривичним стварима из 1959. године, била би доведена у питање, у смислу да било знатно отежано, ако не и немогуће, да се одредбе тих других конвенција примјењују јединствено на територији и у оквиру правних поредака земаља које су их ратификовале и које основано желе да своје унутрашње правне поретке и органе који те поретке спроводе доведу у такво стање оперативности и сарадње које би гарантовало успјешно гоњење извршилаца кривичних дјела.

Основни постулат пружања међународне правне помоћи у кривичним стварима је постојање кажњивости у кривичноправном смислу одређеног људског понашања, које мора бити прописано како материјалноправним одредбама кривичног законодавства земље молиоца, као и замољене земље. У случају недостатка хармонизације материјалноправних прописа у овој области, као и у свакој другој области кривичноправог прогона неумитно би довело до нежељеног исхода у виду немогућности подузимања радњи које су на располагању органима откривања и гоњења, а тиме и ефективног онемогућавања санкционисања такве врсте противправног понашања. То би на крају довело до немогућности да се друштвена заједница сваке од тих земаља заштити на одговарајући начин и гарантује сигурност људи и њихове имовине.

Кривична дјела која су наведена Конвенцијом кибернетичког криминала Вијећа Европе представљају минимум регулисања и прописивања кривичноправне норме у домаћим законодавствима земаља које су је ратификовале и која у сваком случају не искључује њихову додатну разраду у оквиру кривичних законика тих земаља.

Комитет наведене Конвенције под називом T-CY, који је састављен од националних представника земаља које су ратификовале Конвенцију, као и биро наведеног Комитета, у периоду који је данас већ дужи од једне декаде активно је радио и ради на осавремењивању тумачења и метода примјене основних одредби саме Конвенције кроз тзв. „упутства“ (*Guidelines*), која би требале детаљније појаснити могућност примјене одређених одредби Конвенције у савременом животу као и у савременом откривању и гоњењу кривичних дјела из ове области.

Ипак, може се одати признање творцима текста овог међународноправног акта, који су у другој половини 90-тих година XX вијека успјели скоро у потпуности дефинисати, прописати и предвидјети преовлађујуће облике тзв. кибернетичког криминалитета те их уткати у ткиво Конвенције, која и послије скоро 20 година од настанка првобитног текста, уз мање корекције, доношењем додатног протокола и издавањем претходно споменутих упутстава успијева у свијету који се скоро дневно мијења, као што је свијет информационо-комуникационих технологија и социјалног умрежавања користећем тих технологија, одговорити на изазове који се налазе пред оним припадницима друштва којима је дата уставна и законска надлежност да то штите од штетних друштвених појава.

Криминализација тих понашања у виду противправног приступа, противправног пресретања, ометања података, ометања система и злоупотребе уређаја, као и кривичних дјела као што су рачунарски фалсификат, рачунарска превара, злоупотреба малољетника у порнографске сврхе (дјечија порнографија), као и кривична дјела која се односе на повреду ауторских и других сродних права, како у свом основном облику извршења, тако и кроз саучесништво у виду саизвршилаштва, подстрекавања и помагања, уз дефинисање

кривичноправне одговорности правних особа у овој области, указује на то да и поред протека већ наведеног периода и брзе промјене наведених технологија, у својој бити извршење кривичних дјела, укључујући и њихове нове облике и нове начине извршења у тзв. кибернетичком свијету, могу се успјешно предвидјети, дефинисати и санкционисати.

Тиме се отвара пут да примјеном алата генералне и специјалне кривичноправне превенције ови облици криминалитета буду, у најбољем случају, искоријењени или сведени на онај ниво који не представља или не би представљао значајну или значајнију друштвену опасност.

Чињеница је да овом циљу теже скоро сва кривичноправна законодавства земаља свијета данашњице, а која представљају главни покретачки мотив поступања службених особа које се налазе у систему кривичноправне заштите и који су посвећени борби против свих облика криминалитета.

Треба имати у виду да се у овој области поред редовног сета вјештина с којима припадници ових органа морају располагати, подразумијева да полицајци, тужиоци и судије морају располагати и додатним знањима и вјештинама, често техничког и технолошког карактера, како би били у могућности да правовремено, квалитетно и успјешно одговоре изазовима овог криминалитета.

4.6. Процесно право

Технолошка револуција, а посебно револуционарни развој информационих технологија, која свој посебан успон доживљава од почетка XXI вијека и у оквиру тога незапамћени развој друштвених заједница које су у свом настанку и развоју користиле услуге интернетских протокола и интернетских технологија, међусобно су повезане кроз подјелу заједничких ресурса на локалном и на глобалном нивоу, чиме неминовно долазе у контакт и с криминогеним срединама, често бивајући отворене или рањиве за злоупотребу од друштвених елемената који нису спремни да се придржавају законом прописаних оквира друштвено прихватљивог понашања.

Комуникационе мреже које се стално шире на сваки могући замисливи начин како територијално тако и технолошки отварају практично свакодневно нова врата за криминалне активности како у погледу традиционалних, тј. стандардних кривичних дјела, тако и кривичних дјела која су специфична за употребу информационих технологија. С тим у вези, није довољно да само материјално кривично право буде у корак с оваквим развојем друштвене стварности и њеним злоупотребама већ и процесно право с истражним техникама које су прописане и неопходне за успјешно поступање у овој области такође мора бити, чак и више него материјално право, у складу са ИКТ (информационо-комуникационом технологијама), па чак при томе покушавајући да буде и корак испред савремених технолошких збивања.

Наравно, заштитне мјере које постоје или су предвиђене да буду контролни механизам за нарастајућа овлаштења државних институција такође морају бити у корак с развојем технологије и кривичноправног материјалног и процесног оквира.

Један од највећих изазова у борби против високотехнолошког криминала у мрежном окружењу је потешкоћа идентификације извршиоца кривичног дјела и процјена обима штете коју извршење таквог кривичног дјела изазива. Један од повезаних проблема је осјетљивост електронских података који могу бити врло лако измијењени, помјерени или избрисани у неколико секунди. Например, корисник који има могућност контроле података

може искористити рачунарски систем или рачунар да избрише те податке, а који јесу и могу бити предмет интересовања кривичне истраге, чиме практично приступа уништавању доказног материјала.

Брзина и понекад тајност поступања, врло често су од виталног значаја за успех истрага у овој специфичној области криминала.

У том смислу Конвенција о високотехнолошком криминалу Вијећа Европе прилагођава традиционалне процесне мјере као што су претресање стана и просторија новом техничком окружењу. С тим у вези, могу се креирати и употријебити нове мјере и радње, као што су убрзано чување података у циљу осигуравања да традиционалне мјере и радње могу остати и даље употребљиве у врло осјетљивом технолошком окружењу.

С обзиром на то да ново технолошко окружење није увијек статично, већ може бити врло флуидно у смислу процесуирања комуникација и њиховог тока, друге стандардне кривично-правне процедуре које служе за прикупљање доказног материјала и које су од значаја за информационо-комуникациону технологију, као што су прикупљање података о саобраћају у реалном времену и пресретање садржаја комуникације, такође могу и јесу прилагођене новим околностима у намјери да дозволе прикупљање електронских података који настају или су саставни дио процеса комуникације.

Овом приликом напомињемо да су неке од ових мјера наведене и у препоруци Вијећа Европе број P (95) 13 у вези с проблемом кривичнопроцесног права који је у вези с информационим технологијама.

Кривичноправне материјалне и процесне одредбе се у свом општем облику односе на све типове података, укључујући и три специфична типа рачунарских података који се могу подијелити на:

1. **податке о претплатнику (*basic subscriber information* ili *BSI*),**
2. **податке о саобраћају (*traffic data*),**
3. **податке о садржини комуникације (*content data*).**

Наведени подаци могу постојати у своја два збирна подоблика и то у:

1. **похрањеном облику и**
2. **у облику кориштења у реалном времену у току комуникације.**

Конвенција предвиђа дефиниције ових израза у својим члановима 1. и 18. Примјењивост одређене процедуре за одређени тип или врсту електронских података зависи од природе и облика података, као и природе процедуре, што је посебно описано у наведеним члановима Конвенције.

У току адаптације традиционалних процесних одредби закона новом технолошком окружењу поставило се питање употребе одговарајуће терминологије у односу на процесноправне инструменте. Главно питање се односи и усмјерено је ка укључивању и одржавању традиционалног рјечника који је познат у законицима о кривичном поступку, као што је „претрес стана и просторија“, „одузимање предмета“ итд., у односу на кориш-тење нових и више технолошких оријентисаних рачунарских термина као што је „приступ“ и „копирање“, који су данас већ стандардно укључени у текстове међународног окружења у вези с овим питањима.

Чини нам се да би један флексибилнији приступ који би омогућио поступајућим органима да поред стандардних користе и нове термине, посебно у одређивању и примјени одређених процесних радњи и техника у сваком случају био користан за успјешно вођење кривичног поступка.

Такође, појам надлежних органа је посебно у земљама окружења у посљедњих десет година значајно промијењен, у смислу да су овлаштења у истражном поступку значајно или у потпуности пренесена на државна тужилаштва, у ком смислу је као *суи генерис* овлаштење судске власти остало старање о институтима којима се ограничавају људска права и слободе, тј. институтима чије је одређивање неопходно ради успјешног вођења преткривичног и кривичног поступка, као што су тајне мјере надзора комуникације, прикупљање података о садржају комуникације итд.

Обухват процесних одредби, када говоримо о рачунарском криминалу и "Будимпештанској конвенцији" тј. Конвенцији о кибернетичком криминалу Вијеће Европе, подразумијева да ће све земље које су ратификовале ову Конвенцију усвојити такав нормативни оквир који ће даље дати овлаштења надлежним државним органима да успјешно откривају и гоне кривична дјела која су предвиђена Конвенцијом, друга кривична дјела која су извршена путем рачунарских система, као и прикупљање доказа у електронској форми ради вођења поступка за извршење ових кривичног дјела.

С друге стране, успостављање и примјена овакве врсте овлаштења кроз процесне одредбе треба се пажљиво посматрати и усмјерити ка могућности увјетовања и контроле које су предвиђене у оквиру домаћег законодавстава. Другачије речено, земље које су ратификовале Конвенцију су у обавези да донесу одређене процесноправне норме ради успостављања и примјене ових овлаштења како у опћим, тако и у посебним случајевима, а чије ће прописивање бити у складу с домаћим правним оквиром. Ове одредбе могу укључивати и такву врсту заштитних одредби које су на домаћем националном нивоу предвиђене у оквиру Устава, правног поретка, судског и јавнотужилачког система и слично.

Битно је нагласити да успостављање уравнотеженог система подразумијева да такав приступ захтијева усклађеност потребе и захтјева органа откривања, тј. припадника Министарства унутрашњих послова и сигурносних агенција да поступају у складу с одредбама Конвенције и других међународних и правних аката, којима се осигурава одређена заштита људских права и слобода.

У том смислу Конвенција изричито наводи и тиме уважава да државе које су је ратификовале потјечу из различитих правних система и култура те да није могуће таксативно навести као и конкретно одредити јасно примјењиве увјете и заштитне одредбе за свако могуће овлаштење или процедуру у свакој појединачној земљи. С тим у вези, ипак постоји заједнички минимум стандарда које Конвенција предвиђа. Овај минимум стандарда проистиче из обавеза сваке земље која ју је ратификовала да примијени међународне инструменте који су донесени у овој области и који укључују Европску конвенцију о заштити људских права и основних слобода из 1950. године са својим додатним протоколима број 1, 4, 6, 7 и 12, као и Међународну конвенцију о грађанским и политичким правима из 1960. године, не искључујући у одређеним правним системима и географским дијеловима планете примјену Америчке конвенције о људским правима из 1960. године, као и Афричку повељу о људским правима и слободама народа из 1981. године.

Не ограничавајући врсте и увјете за успостављање ових механизама Конвенција специфично захтијева да се такви увјети који се сматрају одговарајућим у смислу одредби процесних законодавстава, односе на правосудне или друге независне органе надзора, који

у оквирима својих овлаштења могу одобрити на одређени начин кривичноправне процесне алате у смислу вођења кривичних поступака, као и њихово евентуално ограничавање ради осигуравања и поштовања људских права и слобода.

Имајући раније наведено у виду у смислу процесних одредби, Конвенција подразумијева такве механизме и алате који подразумијевају хитно чување похрањених рачунарских података, који су прописани члановима 16. и 17. Конвенције, и који се односе на податке који су већ прикупљени и сачувани од држаоца података, као што су напримјер пружаоци интернетских сервиса. Ове одредбе се не односе на прикупљање података у реалном времену, прикупљање података о будућем саобраћају или приступ комуникацијама у реалном времену. Мјере које су описане у овом члану се односе само на податке који већ постоје и који су похрањени.

Треба нагласити да се чување података мора разликовати од похрањивања података. Иако су на први поглед ови појмови слични, постоји битна разлика између ових термина у односу на њихово коришћење када су рачунари у питању.

„**Презервација/очување података**“ означава чување података који већ постоје у похрањеној форми, који су заштићени од било чега што може утјецати на њихов квалитет или увјете у којима би они евентуално били измијењени или оштећени.

„**Ретенција података**“ означава чување података који се тренутно производе - генеришу у нечијем посједу од садашњег момента ка будућности. Ретенција података даље означава акумулацију података у садашњости и њихово чување за будуће и у будућем периоду. Ретенција података је уствари поступак одлагања података, док је презервација података активност која означава чување података на сигурном и осигураном мјесту.

Чланови 16. и 17. Конвенције односе се на тзв. презервацију података, а не на ретенцију. Они не одређују колекцију и ретенцију свих или неких података који су прикупљени од пружалаца интернетских сервиса или другог ентитета, тј. привредног субјекта у току обављања њихових послова. Презервација/очување података се односи и примјењује на рачунарске податке који су похрањени од стране средстава рачунарског система, што претходно подразумијева да ти подаци већ постоје, тј. да су били прикупљени и одложени.

Конвенција у својим наредним члановима одређује и дефинише процесне инструменте као што су:

- **хитно чување похрањених рачунарских података** (члан 16.),
- **хитно чување и дјелимично похрањивање података о саобраћају** (члан 17.),
- **наредбу о достављању података** (члан 18.),
- **претрагу и запљену похрањених рачунарских података** (члан 19.),
- **прикупљање података у реалном времену**,
- **прикупљање података о саобраћају у реалном времену** (члан 20.),
- **пресретање података о садржини комуникације** (члан 21.).

Од наведених мјера посебно је интересантно осврнути се на тзв. „наредбу о пружању података“, која представља флексибилну мјеру коју би припадници органа откривања могли примијенити у различитим случајевима, посебно у оним моментима када друге врсте мјера, као што су наредбе о претресу, запљени, пресретању комуникација и слично, захтијевају испуњавање значајнијих и захтјевнијих правних и техничких увјета.

Примјена овог процедуралног механизама посебно је корисна и може се односити на рачунарске податке или податке о претплатнику који се налазе у посједу или контроли одређене особе или пружаоца. Наравно, ова је мјера примјењива уколико особа или пружалац сервиса такву врсту података чува. *Треба бити свјестан да у појединим земљама у свијету не постоји обавеза пружаоца интернетског сервиса да овакве врсте података чувају, тј. похрањују.*

Посебно треба нагласити да имајући у виду посебни правни режим прибављања података о саобраћају, података о садржини саобраћаја, подаци о претплатнику су дефинисани на такав начин да се односе на било коју информацију која је задржана од пружаоца сервиса и која се односи на претплатника њихових услуга. Претплатнички подаци могу се чувати у било којој форми од електронске до папирне.

Такође, појам претплатника укључује широки појам клијената пружалаца сервиса, од особа које су на основу уговорног односа корисници услуга тог подузећа, до оних који су повремени претплатници само за одређену прилику и у одређеном ограниченом временском трајању, па све до оних који услуге одређеног пружаоца користе без надокнаде.

У току кривичне истраге претплатничка информација ће се највероватније затражити у двије ситуације, тј. примјера. У првом примјеру претплатничка информација потребна је ради идентификације које је сервисе и техничке мјере одређена особа користила или их још користи, а та је особа претплатник, као што су тип телефонског сервиса (је ли мобилна или фиксна линија), тип других придружених сервиса тј. услуга (као што је, напримјер, просљеђивање позива, говорна пошта итд.), телефонски број или техничка адреса (IP-адреса, е-маил адреса).

У другом примјеру, када је техничка адреса позната, претплатничка информација ће се затражити и бит ће потребна ради установљавања идентитета особе у питању.

Друге претплатничке информације, као што су комерцијалне информације о наплати, тј. увјетима плаћања које претплатник има, такође могу бити од значаја за вођење кривичне истраге, посебно у случајевима када се истрага води ради утврђивања кривичног дјела и одговорности за рачунарску превару за "класично" кривично дјело преваре, као и друга кривична дјела која су усмјерена против имовине особе, платног промета и привреде.

Такође, подаци о претплатнику нису ограничени само на информације које се односе на директну употребу комуникационих сервиса. Оне такође могу подразумијевати било коју информацију, осим информација о саобраћају или о садржају саобраћаја, на основу којих се може установити идентитет одређене особе, поштанска или географска адреса, телефонски или други број или адреса, информације о наплати и плаћању које су прикупљене и засноване на основу уговора о претплатничком односу итд.

Наведене информације такође могу обухватити и податке гдје је одређена комуникациона опрема инсталирана (кабловски модем, напримјер), а та је информација на располагању на основу уговора о заснивању претплатничког односа и инсталацији наведеног уређаја од овлаштене сервисне особе пружаоца интернетског сервиса, тј. подузећа.

Поред информације о мјесту и адреси гдје је наведена опрема инсталирана, оваква врста информације је такође битна са становишта утврђивања чињенице да таква врста опреме није лако покретна, већ да је на основу техничких показатеља у оквиру рада наведеног подузећа – пружаоца интернетског сервиса, потврђено да је таква врста опреме функционална на адреси на којој је и инсталирана од овлаштених особа, сходно чему је јасно да подаци који се налазе у уговору о заснивању претплатничког односа одговарају реалном стању ствари.

Треба нагласити да су ова овлаштења везана с одредбама чланова 14. и 15. Конвенције о високотехнолошком криминалу Вијећа Европе, које остављају националним законодавствима успостављање система контроле и заштите људских права у овој области.

Национална законодавства, уколико сматрају за потребно, могу прописати да се за овакве врсте радњи по свим елементима или само у некима за које се може сматрати да су осјетљиви са становишта заштите личних података, може тражити контрола правосудних или других самосталних и независних органа.

4.7. Међународна сарадња

Конвенција о високотехнолошком криминалу Вијећа Европе у свом трећем поглављу регулише у члановима од 23. до 35. међународну правну помоћ у кривичним стварима у области тзв. кибернетичког криминалитета. Конвенција у наведеним члановима, а посебно у уводним, наглашава и подвлачи неопходност проширења међународне сарадње на најшири и најобухватнији могући начин. Практично, Конвенција кроз успостављање принципа међународне сарадње омогућава успостављање интензивне и екстензивне међусобне сарадње држава и њених органа и покушава умањити сваки негативни утјецај на брз и неометан проток информација и доказа у међународном окружењу.

Такође, међународна сарадња би требала бити усмјерена и обухватати и сва кривична дјела која се односе на рачунаре и рачунарске системе као и податке који су генерисани од рачунара, који су употријебљени или на други начин искоришћени у току рачунарске комуникације као и прикупљање доказа у електронској форми у вези с извршењем кривичних дјела. Ово значи да, без обзира на то је ли кривично дјело извршено употребом рачунара, рачунарског система или се ради о уобичајеном вршењу кривичног дјела које није извршено путем рачунара, али укључује електронске доказе, чланови Конвенције у овој Глави могу и требају бити примијењени.

Ипак, треба нагласити да чланови 24. - екстрадиција, 33. - међународна сарадња у односу на прикупљање у реалном времену података о саобраћају и члан 34. - међународна помоћ у односу на пресретање садржаја комуникације, дозвољава земљама које су ратификовале ову конвенцију да путем резерви или на други начин пруже другачији приступ и обухват примјене ових мјера, када се ради о међународној сарадњи.

Посебно је битно нагласити да међународна сарадња у области кибернетичког криминала треба бити у складу с одредбама ове главе и кроз примјер, али и кроз примјену свих релевантних међународних споразума у вези с међународном сарадњом у кривичним предметима, других прописаних облика међународне сарадње који су омогућени на основу реципроцитета, као и на основу домаћег законодавства.

Ово стога што одредбе Конвенције у овом поглављу не надјачавају одредбе међународних споразума о међународној помоћи у кривичним стварима, екстрадицији, реципроцитету, као и одредбе националних законодавстава које регулишу међународну сарадњу.

Потребно је у овом контексту још једном нагласити да су рачунарски подаци врло осјетљиви те да уз неколико притисака на рачунарску тастатуру или усљед извршења аутоматског програма, наведени подаци могу бити избрисани или на други начин трајно уништени, чиме би идентификација извршиоца кривичног дјела или употреба можда критичног дјела доказног материјала којим би се доказало постојање кривичног дјела и

кривичноправна одговорност његовог починиоца била онемогућена. Неки облици рачунарских података похране се само у врло кратком периоду прије него што се обришу, тј. учине на други начин трајно недоступним. У другим случајевима значајна штета може се причинити како људима, тако и имовини, уколико се ова врста доказа не прикупи врло брзо.

У таквим хитним случајевима не само слање захтјева на хитан начин већ и одговор на хитан начин морају се омогућити и извршити. Из тог разлога од круцијалне је важности омогућавање убрзавања процеса остваривања међународне правне помоћи у кривичним стварима, управо у циљу избјегавања губитака критичних информација или доказа, који би, уколико се оваква врста и начин поступања и извршења не би преузели, били изложени опасности брисања, тј. неповратног губитка.

Чињеница је да кроз тзв. традиционални начин пружања међународне правне помоћи комуникација између надлежних државних органа, чак и у реалности информатичког или постинформатичког друштва данашњице и даље доста споро тече те да је у највећем броју случајева размјена писмене документације или документације кроз дипломатске канале или поштански систем врло спора те да захтијева коришћење сложених међународних процедура. Овакав начин пружања међународне правне помоћи у области високотехнолошког криминала практично представља једну од главних, ако не и главну препреку успјешном кривичном гоњењу у овој области криминалитета.

Из тих разлога се истиче неопходност пружања међународне правне помоћи на начин као што је то наведено, тј. омогућавање да се она врло брзо постигне кроз примјену таквих мјера које ће бити предвиђене не само кроз саму Конвенцију већ и кроз билатералне и мултилатералне споразуме о кривичноправној сарадњи, домаће законодавство, као и кроз друге облике регулисања правне помоћи у овој области.

Из тих разлога се коришћење модерних средстава комуникације, као што су електронска пошта, факс, VOIP-комуникација, видеоконференције, употреба директне комуникације и размјене података путем мобилних уређаја који користе интернетско окружење итд. поставља као увјет без којег се не може постићи жељени циљ.Посебно је битно нагласити неопходност праћења развоја информационо-комуникационих технологија и њихово искоришћавање ради што брже размјене података и комуницирања приликом остваривање међународне сарадње, посебно имајући у виду чињеницу да ће извршиоци кривичних дјела, у сваком случају, имати довољно мотива и енергије да управо најсавременије облике информационо-комуникацкионих технологија искористе за извршење кривичних дјела.

У оквиру регулисања међународне правне помоћи у кривичним стварима, а које се односе на борбу против високотехнолошког криминала, посебну улогу заузима постојање тзв. „24/7 мреже“, која представља мрежу тачака контакта међу земљама које су ратификовале Конвенцију и које се у највећем броју случајева налазе при министарствима унутрашњих послова и јавним тужилаштвима, а рјеђе у министарствима правде одређених земаља. С тим у вези, јасно је да ова мрежа представља брзи одговор на претходно наведену потребу за ефективном борбом против кривичних дјела која су почињена коришћењем рачунарских система и рачунара као и ефективно прикупљање доказа у електронској форми.

Битно је имати у виду да радње које ми подузимамо за тастатуром нашег рачунара у току, напримјер, радног времена, скоро тренутно имају посљедице и на рачунарима који се налазе можда десетинама хиљада километара далеко и у различитим временским зонама.

Из ових разлога постојање већ наведене класичне тј. стандардне сарадње и модалитета сарадње у међународноправној помоћи у кривичним стварима захтијева додатне канале комуникације и сарадње управо ради давања одговора свим овим изазовима које доноси информатичко и постинформатичко доба. Добра искуства групе „Г-8“, која је такође за потребе сарадње те групе земаља формирала сличну „24/7 мрежу“ контаката и сарадње, указала су на могућност успостављања таквог модалитета директне сарадње у хитним случајевима на основу, као и у оквирима ове конвенције Вијећа Европе.

Чланом 35. ове конвенције свака земља која ју је ратификовала има обавезу да одреди тачку контакта која ће бити на располагању 24 сата дневно, седам дана у седмици, током цијеле године, ради омогућавања хитног, тј. тренутног одговора и помоћи у истрагама, као и процедурама међународне правне помоћи. Земље које су ратификовале Конвенцију сложиле су се да успостављање овакве врсте повезивања, тј. мреже, представља један од најбитнијих елемената по својој важности у смислу средстава која су на располагању земљама ради примјене Конвенције и омогућавања ефективног одговора органа откривања, органа гоњења и судова на изазове које нам доноси савремени рачунарски криминалитет.

С тим у вези тачке контакта „24/7“, морају бити оспособљене да директно и самостално или директно уз сарадњу других надлежних органа земље чланице пруже технички савјет, чување и прибављање података, прибављање доказа, давање правних информација, као и идентификацију и локацију на којој се налази осумњичена особа.

Земље које су ратификовале Конвенцију задржавају слободу да одреде гдје ће се наведена тачка контакта успоставити. Најбоље резултате у оквиру до сада успостављене праксе пружају контактне тачке које су на првом мјесту успостављене у јавним/државним тужилаштвима, а након тога и у министарствима унутрашњих послова, а тек на крају контактне тачке при другим агенцијама или министарствима правде.

Разлог успјешности сарадње државних, тј. јавних тужилаштава лежи у томе што се у скоро свим земљама које су сада ратификовале ову Конвенцију примјењују одредбе Законика о кривичном поступку, које омогућавају државним тужиоцима вођење тзв. „тужилачке истраге“, која мијења класични концепт истраге и спровођење истраге од истражног одјељења/истражног судије суда, чиме се знатно с једне стране убрзава вођење кривичне истраге, док с друге стране, имајући у виду квалитет државних тужилаштава у смислу њиховог аутономног или независног положаја у оквиру правосудне гране власти, омогућава да тужилаштва кроз своје радње контролишу радње и мјере које припадници министарстава унутрашњих послова примјењују.

Ово је посебно стога што се у ставу 2. члана 35. Конвенције наводи да је један од кључних задатака које контактне тачке ове мреже требају испунити управо могућност успостављања брзог извршења оних функција и задатака који су неопходни ради брзог поступања у овој кривичноправној материји. Например, уколико је тачка контакта „24/7“ одређена полицијска јединица, она мора имати могућност да брзо координира рад са свим другим релевантним и надлежним органима у оквиру кривичноправног система своје земље, као што су, например, овлаштено министарство за извршавање међународне правне помоћи, јавно тужилаштво итд., ради постизања правовремене и правилне реакције на одређени међународни захтјев који може бити испостављен у било које доба дана или ноћи. Такође, не треба занемарити ни потребу да тачка контакта има такав капацитет да на најбржи могући начин изврши комуникацију с другим чланицама, тј. другим контактним тачкама ове мреже на најбржи могући начин.

5. Директива 2013/40/EU

Директиву 2013/40/EU донио је Европски парламент 20. августа 2013. године и односи се на нападе усмјерене против информационих система. Директива мијења оквирну одлуку Вијећа 2005/222/ЈНА и представља саставни дио тзв. *Acqui communautaire* – заједничког правног оквира земаља чланица Европске уније.

Циљ Директиве је да приближи кривичним законодавствима земаља чланица уније област напада против информационих система успостављањем минималних правила који се односе на дефиницију кривичних дјела и одговарајућих кривичноправних санкција, као и унапређење сарадње између надлежних органа који укључују припаднике полиције и других специјализованих агенција за спровођење закона чланица Уније, као и надлежних специјализованих агенција и тијела саме Европске уније као што су EUROJUST, EUROPOL и његов Европски центар за рачунарски криминал (EC 3), као и укључивање у рад Европске агенције за мрежну и информатичку сигурност (ENISA).

Информациони системи у оквиру ове директиве су идентификовани као кључни елемент политичке, друштвене и економске интеракције у самој унији. Друштва су тренутно веома, а у блиској будућности ће још више бити, у односу зависности од коришћења наведених система. Неометана употреба, као и њихова сигурност у оквиру земаља чланица уније, од виталног је интереса за развој како интерних тржишта тако као и модерне, иновативне и компетитивне тржишне економије. Овакве врсте напада представљају пријетњу постизању циља сигурнијег информатичког друштва те пријетњу и области слобода, сигурности и правде. Из тих разлога захтијевају одговор на нивоу Европске уније кроз унапређење сарадње и координације на међународном нивоу.

Чињеница је да постоји велики број објеката у свом физичком или софтверском облику који представљају дијелове критичне инфраструктуре те би прекидање рада или уништење овакве врсте инфраструктуре имало за посљедицу наношење значајне штете како директно становницима Европске уније, тако и њиховој имовини. Постало је јасно да постоји потреба да се критична инфраструктура дефинише као средство, систем или дио средстава из система, који су од есенцијалне важности за одржавање виталних друштвених функција, као што су здравље, сигурност, економска или друштвена добробит народа. Системи као што су електране, транспортне мреже или мреже комуникација у служби влада држава, чије би нарушавање или уништење довело до, врло је могуће, катастрофалних посљедица.

Постоје докази који указују на тенденцију растуће опасности и понављања напада у великом обиму и снази који су усмјерени против информатичких система, а који су од критичног значаја за земље чланице уније. Ова тенденција је попраћена и развојем софистицираних метода као што су производња и коришћења тзв. *бот нетова*, који укључују неколико нивоа извршења кривичног дјела, гдје сваки од тих нивоа може представљати значајан ризик за јавни интерес.

Ова директива између осталог уводи кривичне санкције за ново кривично дјело у виду прављења и коришћења *бот нетова*, као чин успостављања удаљене контроле над значајним бројем рачунара путем њиховог инфицирања кроз инсталацију малициозног софтвера, а кроз прецизно усмјерене кибернетичке нападе. Једном кад се таква мрежа креира, она конституише *бот нет* који може бити активиран без знања и пристанка власника тј. корисника рачунара ради отпочињања напада у широком обиму и захвату, који обично има такав капацитет, тј. могућност и снагу да изазове знатну штету на начин као што је то описано у Директиви.

Овакве врсте великих и широких напада могу изазвати значајну економску штету, како кроз прекидање рада информационих система и комуникација, тако и кроз губитак или измјену комерцијално битних повјерљивих информација и података. Посебна пажња треба се усмјерити ка подизању свијести малих и средњих подузећа у циљу идентификације овакве врсте опасности, као и рањивости тих подузећа у овом смислу, а кроз њихову растућу зависност од коришћења информационих система. Битно је такође нагласити да ова директива прописује висину кривичних санкција, тј. барем за она кривична дјела која се не сматрају као мање друштвено опасна.

Државе чланице уније могу прописати шта представља мање друштвено опасна дјела у складу с њиховим националним законодавствима и праксом. Напримјер, кривично дјело у том смислу може бити наношење штете интегритету рачунара, рачунарских система и података у таквој мјери и на такав начин који не прелази одређени праг кривичноправне одговорности која захтијева реакцију органа откривања и гоњења у оквиру кривичног поступка.

С друге стране директива, посебно у области напада против информационих система, захтијева ефективно, пропорционално и довољно одвраћајуће кривичноправне санкције и њихову висину, као и унапређење сарадње међу правосудним и другим надлежним органима, а што се све не може постићи само од појединачних земаља чланица, већ би се требало постићи на нивоу саме Европске уније, из којих разлога унија може остварити такве врсте мјера које су у складу с принципом супсидијаритета које је прописано чланом 5. Уговора о Европској унији.

Директива 2013/40/EU у свом члану 2. даје значење појмова и израза:

- „**Правна особа**“ представља ентитет који има статус правне особе под примјењивим законом, али не укључује државе, тј. државне или јавне органе, институције или тијела која поступају у име државе, као ни јавне међународне организације.
- „**Без права**“ означава поступак на који се односи дио Директиве који укључује приступ, ометање или пресретање који није овлаштен од власника или другог овлаштеног носиоца одређеног права на систему или његовом дијелу, или није дозвољено на основу домаћег законодавства.

У свом даљем тексту Директива даје елементе бића кривичних дјела као што су неовлаштени приступ информационом систему, неовлаштено ометање система, неовлаштено ометање података, коришћење средстава за извршење ових кривичних дјела.

Посебно је потребно нагласити да у члану 9., који се односи на врсту и висину санкција, Директива обавезује земље чланице Европске уније да у оквиру својих домаћих законодавстава морају увести такве врсте кривичних санкција за наведена кривична дјела које ће бити ефективне, пропорционалне и довољно одвраћајуће у односу на извршиоце кривичних дјела.

С тим у вези, Директива предвиђа обавезу да се за наведена кривична дјела запријети казна затвора с најдужим роком трајања од најмање двије године и то за кривична дјела која се не сматрају мање друштвено опасним.

Такође, кривична дјела неовлаштеног ометања система и неовлаштеног ометања података када су учињена с умишљајем, морају бити запријећена с максимумом од најмање три године, када је дошло до значајнијег оштећења информационог система и њиховог броја кроз коришћење алата на које се односи члан 7. Директиве, тј. уређаја и програма који су дизајнирани или адаптирани првенствено у ту сврху.

Такође, за кривична дјела из чланова 4. и 5. Директива предвиђа да треба бити запријећена, тј. прописана највиша казна од најмање пет година затвора у случајевима:

- када су оваква кривична дјела извршена од криминалне организације дефинисане кроз оквирну одлуку 2008/841/ЈНА, без обзира на казну која је прописана за саму организацију;
- уколико је извршење кривичног дјела начинило озбиљну штету или
- уколико је кривично дјело извршено против информационог система критичне инфраструктуре.

У свом члану 17. Директива је обавезала Европску Комисију да до 4. септембра 2017. године поднесе извјештај Европском парламенту и Вијећу у оквиру којег ће постојати процјена примјене ове директиве од земаља чланица, у смислу јесу ли подузеле неопходне мјере ради поштовања Директиве и, уколико је то потребно, достављање законодавних предлога. Комисија ће такође узети у обзир и технички и правни развој у области кибернетичког криминала, посебно имајући у виду обухват ове директиве.

6. Нормативни и институционални оквир у Босни и Херцеговини

6.1. Конвенције, протоколи и законски оквир у Босни и Херцеговини[10]

Одлука о ратификацији Конвенције о кибернетичком криминалу из 2006. године.[11] Потврђивањем наведене Конвенције Босна и Херцеговина се обавезала на усвајање појмова у вези с компјутерским криминалом установљених Конвенцијом, усклађивање свог материјалног и процесног кривичног права као и међународну сарадњу на пољу сузбијања компјутерског криминала.

Одлука о ратификацији Додатног протокола уз Конвенцију о кибернетичком криминалу, а у вези с кажњавањем дјела расистичке и ксенофобичне природе учињених путем компјутерских система такође из 2006. године.[12] Наведеним протоколом је предвиђено инкриминисање дјела расистичке и ксенофобичне природе учињених путем компјутерских система која нису била обухваћена претходно донесеном Конвенцијом.

Одлука о ратификацији Факултативног протокола уз Конвенцију о правима дјетета који се односи на продају дјеце, дјечију проституцију и дјечију порнографију из 2002. године.[13] Наведеним Протоколом предвиђа се, између осталог, обавеза имплементације мјера заштите права дјетета у кривичном поступку, мјера којима би се осигурала одговарајућа обука за особе које раде са жртвама протуправних радњи забрањених према овом Протоколу и прописује обавезу установљавања мјера како би се заштитила сигурност и интегритет особа и/или организација укључених у спречавање и/или заштиту и рехабилитацију жртава таквих незаконитих радњи.

[10] Законодавни оквир ближе ће бити разматран у такстовима који слиједе.
[11] „Службени гласник БиХ" – Међународни уговори, бр. 6/06
[12] „Службени гласник БиХ" – Међународни уговори, бр. 6/06
[13] „Службени гласник БиХ" – Међународни уговори, бр. 2/05

Одлука о ратификацији Конвенције Вијећа Европе о заштити дјеце од сексуалног искоришћавања и сексуалне злоупотребе из 2012. године[14], која за циљ има сузбијање сексуалног искоришћавања и сексуалног злостављања дјеце, заштиту права дјеце жртава сексуалног искоришћавања и сексуалног злостављања те унапређење националне и међународне сарадње у борби против сексуалног искоришћавања и сексуалног злостављања дјеце.

Кривични закон Босне и Херцеговине[15] не дефинише изразе од важности за компјутерски криминал. У овом закону нису прописана кривична дјела високотехнолошког, односно компјутерског криминала осим што поједини законски описи кривичних дјела користе појмове рачунарски програм и сл. (в. нпр. кривично дјело Недозвољено коришћење ауторских права чл. 243. ст. 3.).

Кривични закон Федерације Босне и Херцеговине[16] прописује кривична дјела из домена компјутерског криминала у Глави XXXII под називом „Кривична дјела против система електронске обраде података" чл. 393 398. Кривично гоњење се врши по службеној дужности. Он, међутим, не дефинише значење израза од важности за компјутерски криминал.

Кривични законик Републике Српске[17] прописује кривична дјела компјутерског криминалитета, такође у Глави XXXII под називом „Кривична дјела против сигурности компјутерских података". Осим ове групе кривичних дјела високотехнлошки криминал је дијелом и других инкриминација из овог закона, а због његове посебне важности издвајамо кривично дјело из чл. 178. Искоришћавање компјутерске мреже или комуникације другим техничким средствима за извршење кривичних дјела сексуалног злостављања или искоришћавања дјетета. Кривично гоњење за ова дјела се врши по службеној дужности осим за дјело из чл. 413. Неовлаштено коришћење компјутера или компјутерске мреже које се врши на приједлог оштећеног. Наведени Закон само дјелимично дефинише значење израза од важности за компјутерски криминал. У том смислу видјети нпр. чл. 123. ст. 18., у оквиру којег се под покретном ствари има подразумијевати и сваки регистровани податак који је резултат електронске обраде података (компјутерски податак или програм).

Кривични закон Дистрикта Брчко Босне и Херцеговине[18] као и претходна два закона такође прописује кривична дјела високотехнолошког криминала. Инкриминисана су Глави XXXII као „Кривична дјела против система електроничке обраде података". Кривично гоњење за ова кривична дјела подузима се по службеној дужности, а наведени закон не дефинише значење израза од важности за ово подручје.

Закон о кривичном поступку Босне и Херцеговине[19] у складу с начелом законитости кривичног поступања утврђује правила чији је циљ да нико невин не буде осуђен, а да се починиоцу кривичног дјела у законито проведеном поступку изрекне кривичноправна санкција под увјетима које прописује Кривични закон БиХ, али и други закони у Босни и Херцеговини којима су прописана кривична дјела. Закон о кривичном поступку БиХ као и други закони о кривичном поступку који су на снази у Босни и Херцеговини представљају темељне правне изворе у регулирању процесуирања починилаца кривичних дјела, па тако и оних с подручја компјутерског криминала. Поред прописивања права и дужности процесних

[14] „Службени гласник БиХ" – Међународни уговори, бр. 11/12
[15] „Службени гласник БиХ", бр. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07, 8/10, 47/14, 22/15, 40/15 и 35/18
[16] „Службене новине ФБиХ", бр. 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14, 46/16 и 75/17
[17] „Службени гласник РС", бр. 64/17 и 104/2018 – Одлука УС
[18] „Службени гласник Дистрикта Брчко БиХ", бр. 10/03, 45/04, 05/05, 21/10, 52/11, 9/13 и 50/18
[19] „Службени гласник БиХ", бр. 3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09, 72/13 и 65/18

субјеката те форми радњи које се подузимају у поступку, вриједи напоменути да закон посебно прописује одговарајући оквир радњи доказивања те посебних истражних радњи које су од изнимне важности за доказивање, а тиме и адекватно процесуирање свих кривичних дјела, укључујући ту дакако и дјела високотехнолошког криминала. Законом су дефинисани и изрази од важности за високотехнолошки криминал. У том смислу видјети одредбе чл. 20. у) и в), којима су одређени појмови „компјутерски систем" и „компјутерски податак".

Закон о кривичном поступку Федерације Босне и Херцеговине.[20] Све изнесено у вези с ЗКП БиХ вриједи и за ЗКП ФБиХ.

Закон о кривичном поступку Републике Српске.[21] Претходно изнесено у вези с ЗКП БиХ и ЗКП ФБиХ вриједи и за ЗКП РС.

Закон кривичном поступку Дистрикта Брчко Босне и Херцеговине.[22] Исто тако, видјети изнесено уз ЗКП БиХ те ентитетске законе.

Закон о заштити и поступању с дјецом и малољетницима у кривичном поступку Федерације Босне и Херцеговине из 2014. године.[23] Наведеним законом прописана су посебна правила поступања с дјецом која су у сукобу са законом, млађим пунољетним особама и дјецом на чију је штету почињено кривично дјело, односно која се појављују као свједоци у поступку.

Закон о заштити и поступању с дјецом и малољетницима у кривичном поступку Републике Српске из 2010. године.[24] Наведено у погледу одредби Закона о заштити и поступању с дјецом и малољетницима у кривичном поступку Ф БиХ вриједи и за Закон Републике Српске уз напомену да је Закон о заштити и поступању с дјецом и малољетницима у кривичном поступку РС заправо и први закон на подручју малољетничког преступништва који је донесен у Босни и Херцеговини.

Закон о заштити и поступању с дјецом и малољетницима у кривичном поступку Дистрикта Брчко Босне и Херцеговине из 2011. године.[25] Све напријед наведено у погледу Федерације БиХ и Републике Српске вриједи и за Закон Дистрикта Брчко БиХ.

Закон о међународној правној помоћи у кривичним стварима из 2009. године.[26] Наведеним се законом уређује начин и поступак пружања међународне правне помоћи у кривичним стварима уколико међународним уговором није другачије уређено.

Закон о комуникацијама Босне и Херцеговине из 2003. године[27], којим се уређује област комуникација у Босни и Херцеговини те успоставља и регулише рад Регулаторне агенције за комуникације Босне и Херцеговине (РАК) у складу с Уставом Босне и Херцеговине, који предвиђа успостављање и функционисање заједничких и међународних комуникацијских средстава.

[20] „Службене новине ФБиХ", бр. 35/03, 37/03, 56/03, 78/04, 28/05, 55/06, 27/07, 53/07, 09/09, 12/10, 08/13 и 59/14
[21] „Службени гласник РС", бр. 53/12, 91/17 и 66/18
[22] „Службени гласник Дистрикта Брчко БиХ", бр. 10/03, 48/04, 06/05, 12/07, 14/07, 21/07 и 27/14
[23] „Службене новине ФБиХ", бр. 7/14
[24] „Службени гласник РС", бр. 13/2010, 61/2013 и 68/20
[25] "Службени гласник Дистрикта Брчко БиХ", бр. 44/11
[26] „Службени гласник БиХ", бр. 53/2009 и 58/2013
[27] "Службени гласник БиХ", бр. 31/03, 75/06, 32/10 и 98/12

6.2. Подзаконски акти

Правило 69/2013 о увјетима пружања јавних телекомуникацијских услуга и односима с крајњим корисницима Регулаторне агенције за комуникације Босне и Херцеговине[28], којим се одређују основни принципи пружања јавних телекомуникацијских услуга, обавезе оператера јавних телекомуникацијских услуга у погледу односа с крајњим корисницима те се поближе одређују обавезе прописане посебним прописима.

Одлука о посебним обавезама правних и физичких особа које пружају телекомуникацијске услуге, администрирају телекомуникацијске мреже и врше телекомукацијске дјелатности у погледу обезбјеђења и одржавања капацитета који ће омогућити овлаштеним агенцијама да врше законито пресретање телекомуникација, као и капацитета за чување и обезбјеђивање телекомукацијских података[29] **те њена Одлука о измјенама и допунама**[30], којом се уређује подручје законитог пресретања у Босни и Херцеговини у складу с резолуцијом Вијећа Европске уније о законитом пресретању телекомуникација од 17. јануара 1995. (OJ 96/C 329/01) и одговарајућим стандардима и препорукама Европског института за телекомуникацијске норме (ETSI). Одлука има изузетан значај и за дефинисање низа појмова у вези са законитим пресретањем телекомуникација.

Правилник о провођењу одредби Закона о заштити личних података у Регулаторној агенцији за комуникације[31], којим се уређују увјети прикупљања, обраде и објављивања личних података у складу са Законом.

7. Институционални оквир

У Босни и Херцеговини не постоји нити на једној од законодавних разина посебно тијело које би искључиво било надлежно за гоњење кривичних дјела високотехнолошког криминала као што је то случај нпр. с Републиком Србијом и Посебним тужилаштвом за борбу против високотехнолошког криминала. У складу с тим кривични прогон за ова кривична дјела или у вези с њима врше одговарајуће тужилачке институције на нивоима ентитета Федерације БиХ и Републике Српске те Дистрикта Брчко БиХ које су општенито надлежне и за гоњење свих других кривичних дјела. Од полицијских агенција у Босни и Херцеговини једино је у оквиру МУП-а Републике Српске успостављено одјељење за борбу против високотехнолошког криминала. Несумњиво да и у оквиру осталих полицијских агенција на свим разинама у Босни и Херцеговини постоје истражиоци унутар различитих криминалистичко-истражних одјела едуцирани управо за ову врсту криминала, ипак без постојања посебно устројеног организацијског одјела специјализованог за ову врсту кривичних дјела може се поставити питање ефикасности њиховог рада. Ово све посебно имајући у виду да се ради о форми криминала која ће *pro futuro* само добивати на свом обиму. Са стајалишта пресуђења, такође не постоји посебно одређен суд или судови који би у оквирима своје надлежности поступали у предметима високотехнолошког криминала. Дакле, поступају судови опће надлежности.

[28] Регулаторна агенција за комуникације Босне и Херцеговине, бр. 01-02-929-1/13 од 01.04.2013. године.
[29] "Службени гласник БиХ", бр. 104/06
[30] "Службени гласник БиХ", бр. 58/07
[31] Регулаторна агенција за комуникације Босне и Херцеговине, бр. 01-02-3-2364-1/15 од 25.09.2015. године.

Треба напоменути да значајну улогу на подручју уређења система пружања комукацијских, односно телекомуникацијских услуга у Босни и Херцеговини, а тиме и становитог вида превенције високотехнолошког криминала имају и Министарство комуникација и саобраћаја Босне и Херцеговине те Регулаторна агенција за комуникације (РАК). **Министарство комуникација и саобраћаја Босне и Херцеговине** врши активности на изради и предлагању законских прописа на подручју комуникација, односно телекомуникација, праћењу примјене закона и других прописа, активностима на међународној сарадњи и сл. **Регулаторна агенција за комуникације**, с друге стране, као функционално независна и непрофитна институција са статусом правне особе према законима Босне и Херцеговине обавља своје дужности у складу с циљевима и регулаторним принципима као што су регулисање емитерских и јавних телекомуникационих мрежа и услуга, укључујући издавање дозвола, утврђивање цијена, међуповезивање и дефинисање основних увјета за осигуравање заједничких и међународних комуникацијских средстава и др.

8. Савремени трендови

Поред свих специфичности које рачунарски криминал садржи због своје уске повезаности с технолошком садржаоцем, још један аспект га додатно чини разноврснијим и сложенијим у односу на стандарде облике криминогеног понашања. Наиме, за разлику од „класичних" кривичиних дјела, код којих начин извршења остаје у највећем броју случајева исти кроз дужи период, или се врло тешко мијења, рачунарски криминал у врло кратком периоду, практично из године у годину, може доживјети врло драстичне промјене не само начина извршења појединих дјела већ и потпуну измјену саме супстанце која чини кривична дјела садашњице или блиске будућности.

Приликом кратког осврта на почетке рачунарског криминалитета у Републици Србији констатовали смо да је исти више од 40 година присутан и да је у деценијама које су слиједиле скоро декадно доживљавао одређене измјене како у мотивацији, тако и у начину извршења. Чини се да се законитости „Муровог закона" („*број транзистора у интегрисаном рачунарском колу сваке двије године бива дуплиран*") скоро могу примијенити у одређеном смислу и на свијет рачунарских кривичних дјела. Наиме, за разлику од ранијег периода, у посљедњих неколико година трендови извршења кривичних дјела се значајно чешће мијењају како у својим основним, тако и у својим пратећим облицима, слиједећи понајвише пут којим свјетска технологија и економија иду.

Имајући наведено у виду, чини се да је брзина развоја рачунарских и комуникационих технологија као и економских кретања директно пропорционална развоју, тренду и обиму извршења кривичних дјела рачунарског, тј. кибернетичког криминала.

Трендови извршења кривичних дјела у посљедњих неколико година на свјетском и домаћем нивоу могли су се подијелити у седам главних праваца:

1. **Рачунарски криминал на мобилним платформама;**
2. **Интензивно коришћење банкарских малвера и тројанаца;**
3. **„Хактивизам" и злоупотреба друштвених мрежа;**
4. **Савремене повреде права интелектуалне својине;**
5. **Пораст циљаних напада (*APT – Advanced Persistent Threat*);**

6. **Појава и злоупотреба криптовалута (Bitcoin, Ethereum, Ripple);**
7. **Појава и злоупотреба Интернета ствари (*IoT*, *Internet of Things*).**

8.1. Рачунарски криминал на мобилним платформама

Омасовљење употребе мобилних рачунарских платформи има своју узлазну путању још од појаве првих мобилних рачунара током седамдесетих и осамдесетих година прошлог вијека у виду тзв. „laptop", „notebook", „handheld", „palmtop" и других варијанти мањих рачунарских уређаја који су могли бити лако транспортовани, врло често и у џеповима одјеће. Права експлозија присуства и коришћења оваквих уређаја настаје појавом првог паметног телефона у виду Apple Inc. iPhone мобилног телефонског уређаја, који у исто вријеме има и значајне рачунарске капацитете. Свијет данашњице се практично не може замислити без присуства паметних мобилних телефона, који су уствари мали рачунарски уређаји који се првенствено користе за рачунарску, а мање оригиналну намјену, тј. обављање телефонских разговора.

Овакав тренд, наравно, није остао незапажен у криминогеним срединама, па су тако забиљежени значајни продори извршења и разнородних кривичних дјела путем коришћења ових мобилних уређаја на различите начине. Посебно треба нагласити постојање разних врста малициозног софтвера (вируса, тројанаца, вормова итд.), који се могу инсталирати на оперативним системима модерних мобилних телефона и који имају различите функције: од простог копирања бројних база података које оштећени посједују на својим уређајима (листа телефонских контаката, електронска пошта, смс, фотографије, видеозаписи, поруке на друштвеним мрежама итд.), праћења кретања корисника уређаја у реалном времену и посматрања путем злоупотребе камере и микрофона окружења у којем се апарат, тј. корисник налазе, до утјецаја на новчане трансакције које оштећени путем тзв. „мобилних апликације" чине помоћу свог уређаја.

8.2. Интензивно коришћење банкарских малвера и тројанаца

Рачунари и мобилни рачунарски уређаји постали су саставни дио пословања правних и физичких особа данашњице. Скоро је немогуће замислити бављење или обављање многих послова без употребе рачунара. Ово је посебно видљиво када говоримо о области у којој су рачунару „домаћи", тј. у области рачунања математичких израза, а који су даље саставни дио пословања финансијских институција у јавном и приватном сектору. Наравно, имајући у виду значајан потенцијал за стјецање противправне добити, ово поље коришћења рачунара је постало једно од омиљених и за криминалну злоупотребу.

Zeus, Citadel, SpyEye, WannaCry и сл., само су неки од назива различитих малвера који су настали посљедњих година због њиховог инсталирања без знања корисника рачунара на њихове уређаје у циљу прибављања финансијских података и њихове злоупотребе противправним преузимањем контроле над банкарским рачунима оштећених и новчаним трансакцијама у корист извршилаца кривичних дјела. Посљедњи примјери случајева тзв. „BEC – Business E-mail Compromise", у којима су стотине хиљада, па и милиони еура преусмјерени на преварне рачуне под контролом криминалаца ради остваривања енормних криминалних профита, указују на даљи правац развоја економских кривичних дјела и све већу употребу информационих технологија ради њиховог извршења.

8.3. „Хактивизам“ и злоупотреба рачунарских мрежа

Према слободним изворима “**хактивизам**”[32] представља субверзивну употреба рачунара и рачунарских мрежа за промовисање политичке агенде или социјалних промјена.
С коријенима у култури хакера и хакерској етици, његови циљеви су често повезани са слободом говора, људским правима или покретима који промовишу слободан проток информација. Термин је ушао у употребу 1994. године. Примјетно је да постоје разлике у ближем одређивању ове врсте активизима на интернету. Док неке дефиниције подразумијевају акте кибернетичког тероризма (*Anonymous*), друге покушавају да дају оправдање употреби неовлаштеног приступа рачунарима да би се извршиле друштвене промјене.

Ипак, хактивизам у највећем броју случајева представља радње усмјерене на злонамјерне и деструктивне радње појединаца које уствари подривају сигурност интернета као техничке, економске и друштвене платформе.

Злоупотребе рачунарских мрежа у протеклих неколико година су добиле своје ново тежиште на такозваним друштвеним мрежама, тј. стално активним глобалним рачунарским програмима који омогућавају директну комуникацију корисника путем размјене порука, фото и видеоматеријала, гласа итд. Пораст злоупотребе ових мрежа с циљем застрашивања, изнуђивања жељеног понашања, као и злоупотребе у порнографске сврхе, поприма забрињавајуће размјере у нашој земљи, о чему ће бити детаљније ријечи у тексту овог приручника.

8.4. Савремене повреде права интелектуалне својине

Повреде права интелектуалне својине спадају у кривичноправном смислу у групу кривичних дјела која су добро позната јавним тужиоцима, замјеницима јавних тужилаца и судијама. Може се слободно констатовати да је управо извршење ових кривичних дјела током деведесетих година прошлог и почетком овог вијека, посебно кроз злоупотребу рачунара и рачунарских технологија за масовно копирање и нелегалну продају ауторских садржаја као што су филмови, музика и рачунарских програми и довело до почетка озбиљнијег посвећивања пажње рачунарском криминалитету.

Ипак, према процјенама Америчке привредне коморе[33] у Републици Србији до 2015. године забиљежен је пад неовлаштене употребе ауторских права у области рачунарских програма до процента од 67%. Наравно, тај процент никако није задовољавајући, имајући у виду да у земљама Европске уније износи око 29% и обавезује на даље дјеловање државних органа.

Посебну пажњу треба скренути на продају путем интернета фалсификованих лијекова и медицинских препарата. Тренд куповине ових производа путем рачунарких мрежа је у узлазној линији, али су забиљежени значајни случајеви продаје нелегалних копија медикамената путем интернетског оглашавања и достављања на кућну адресу. У неким од ових случајева је дошло и до животног угрожавања особа које су конзумирале ове препарате усљед дјеловања на организам супстанци од којих су исти били направљени.

[32] https://en.wikipedia.org/wiki/Hacktivism
[33] https://www.amcham.rs

Нажалост, у свијету су забиљежни и смртни случајеви усљед оваквог прибављања и конзумације.

8.5. Пораст циљаних напада – Advanced Persistent Threat („APT“)

Циљани напади представљају нови облик извршења кривичних дјела у чијој се основи налази такозвани „социјални“ тј. друштвени инжењеринг. Главне одлике извршења ових кривичних дјела су да њихови извршиоци на свом располагању имају широки спектар програмских алата и злонамјерних програма путем којих се инфилтрирају и преузимају контролу над циљаним рачунаром и мрежом, или врше присмотру тих система ради прибављања података који нису јавни. Такође, циљани напади се могу окарактерисати и као упорни из разлога што једном остварен увид и контрола над рачунарским процесима мете/жртве, не напушта се већ користи до момента откривања. Понекад се користи и додатни атрибут ових напада у смислу пријетње коју они стварају, имајући у виду постојање специфичног циља, обуке, мотивисаности, организованости и постојања извора финансирања.

Тренутно најприсутнији начини извршења овакве организоване криминалне акције се могу видјети у раније споменутим предметима „БЕЦ“ превара, гдје циљ представља пресретање и контрола пословних комуникација између два и/или више пословних ентитета ради преусмјеравања процеса плаћања на преварне рачуне.

8.6. Појава и злоупотреба криптовалута (Bitcoin, Ethereum, Ripple итд.)

Криптовалуте представљају рачунарско програмско дигитално средство дизајнирано ради употребе као средство плаћања или размјене добара и услуга, користећи криптографију ради осигурања трансакција и контроле стварања додатних јединица валуте. Криптовалуте су класификоване као подскуп дигиталних и алтернативних валута. *Bitcoin* представља прву познату криптовалуту која је настала 2009. године. *Bitcoin* и његови деривати користе децентрализовану контролу насупрот централизованим електронским новчаним и банкарским системима. Наиме, криптовалуте не представљају новац који издаје централна банкарска институција одређене земље, већ рачунарски податак који се ствара коришћењем одређених програма који се користе на интернету и који се чува у искључиво електронском облику пролазећи кроз низ различитиих провјера корисника интернета који учествују у тим трансакција, с обзиром на то да ове врсте валута не постоје у "правом", тј. штампаном или кованом облику.

Криптовалуте се користе на различите начине и данас је могуће електронским путем купити велики број добара и услуга на интернету коришћењем овог "кибернетичког новца". Ипак, битно је нагласити да и поред јаке промоције ових валута од "бораца за слободе и приватност интернета" криминалци и криминалне групе од самог њиховог настанка интензивно користе овакав вид плаћања имајући у виду потешкоће с којим се државни органи суочавају приликом праћења ових трансакција и запљене криптовалута. Посебно треба споменути да на мање приступачним дијеловима интернета, као што су *Deep* или *Dark Web* коришћење ових валута представља правило приликом купопродаје наркотика, ватреног оружја, трговине људима и дјечијом порнографијом, па чак и приликом наручивања убистава.

8.7. Појава и злоупотреба интернета ствари (IoT, Internet of Things)

Интернет ствари представља међуумрежавање физичких објеката, возила (што се односи и на „повезане" и „паметне уређаје"), зграда и других ствари с уграђеном електроником, програмима, сензорима који омогућавају предметима да размјењују податке с произвођачем, оператером и/или другим повезаним уређајима. *Global Standards Initiative on Internet of Things* (*IoT-GSI*) дефинисала је IoT као „глобалну инфраструктуру информатичког друштва која омогућава напредне услуге (физичким и виртуалним) умрежавањем ствари, притом се заснивајући на постојећим и интероперабилним информационим и комуникационим технологијама у развоју". У ту сврху термин ствар представља „предмет физичког свијета (физичких ствари) информација или ријеч (виртуалне ствари), који је могуће идентификовати и који може бити интегрисан у комуникационим мрежама".

IoT омогућава да објекти буду опажени и контролисани даљински путем постојеће мрежне инфраструктуре, стварајући тако прилику за директнију интеграцију физичког свијета и рачунарских система, што резултује повећањем ефикасности, тачности и економске користи, уз смањење људске интервенције. Сваку ствар је могуће јединствено идентификовати кроз уграђен рачунарски систем и свака ствар је интероперабилна у оквиру постојеће интернетске инфраструктуре. Стручњаци процјењују да ће IoT до 2020. године имати између 26 и 30 милијарди предмета.

У контексту овог приручника ова област кориштења рачунара и рачунарских мрежа представља заиста будућност криминала која је на помолу. Начини злоупотребе могу бити значајни и примјери који су већ сада забиљежени у виду, напримјер, даљинске контроле моторних возила од хакера, активирања и контроле кућних уређаја који су повезани на интернет, и то оних чијом се злоупотребом може надгледати, па и утјецати на догађаје који се одвијају у одређеном простору, у овом случају приватном, указују на то да се посебна пажња мора посветити овој наступајућој опасности као и новим облицима извршења кривичних дјела који ће представљати директни производ овог развоја технологије.

Прво реаговање на електронске доказе

1. Увод

У оквиру пројеката "Спојени и сигурни – у сусрет кибернетичкој средини која је сигурна за дјецу'' створила се потреба за додатним усавршавањем те је извршена едукација носилаца правосудних функција у циљу упознавања за прво реаговање на електронске доказе[34], која је од виталног значаја да припадници полиције и тужилаштва имају алатке за ефикасно спречавање и откривање високотехнолошког криминала, што представља нови изазов који се умногоме разликује од конвенционалних кривичних истрага.

Савремена тенденција прикупљања електронских доказних радњи приликом поступања полицијских службеника како у традиционалним кривичним дјелима, тако и у кривичним дјелима високотехнолошког криминала током привременог одузимања предмета иницирала је доношење „Обавезне инструкције о прикупљању и осигурању електронских доказа'', којом се утврђује методологија за прикупљање електронских доказа тј. њихово откривање, осигурање, прикупљање и евидентирање у циљу јединственог поступања полицијских службеника Министарства унутрашњих послова Републике Србије с електронским доказима. Наведена инструкција представља стандард за правилно руковање електронским доказима с циљем спречавања њиховог оштећења, губитка, модификације, транспорта и осигурања аутентичности електронских доказа неопходних да се осигура проглашење осумњиченог кривим. Оваква инструкција не постоји тренутно у Босни и Херцеговини.

2. Стратегија за прикупљање дигиталних доказа

У ово доба технолошке револуције скоро да је немогуће замислити сценариј гдје не би било могуће да доказ или обавјештајни податак нису снимљени у неком електронском тј. дигиталном облику. Имајући то на уму, полицијски службеници који с тужилаштвом истражују кривична дјела требали би увијек узети у обзир стратегију за прикупљање електронских доказа од почетка свих својих упита. Најчешћи уређаји који могу садржати електронске доказе су: системи видеонадзора, рачунарски системи, таблет-уређаји, уређаји за складиштење података (хард дискови и Solid state дискови SDD, меморијске картице, USB-уређаји за похрану података, оптички компакт-дискови, траке за похрану података и др.), дигитални фотоапарати и видеокамере, дигитални аудиоснимачи, дигитални видеорекордери с меморијским модулима, играчке конзоле, MP3 и MP4 плејери, GPS уређаји, рутери, паметни кућни апарати попут паметног ТВ-а, медиа плејера, уређаји set top box

[34] Електронски доказ је било која информација генерисана, обрађена, ускладиштена или пренесена у дигиталном облику на коју се суд може ослонити као мјеродавном, тј. свака бинарна информација састављена од дигиталних 1и 0, ускладиштена или пренесена у дигиталној форми, као и друге могуће копије оригиналне дигиталне информације које имају доказну вриједност и на које се суд може ослонити у контексту форензичке аквизиције, анализе и презентације, што је сагласно с чл. 112. ст. 17. и ст. 26. Кривичног законика Републике Србије ("Сл. гласник РС", бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 и 94/2016).

и др. Такође, веома је битно и да се прикупе информације у погледу дужине власништва над рачунарском опремом, умрежених рачунара, кориштеним оперативним системима, ко су све власници и корисници рачунарске опреме, онлајн корисничких налога за складиштење података тј. налога електронске поште, података који се односе на криптографску заштиту, даваоце интернетских услуга и кориштења рачунарских мрежа, складиштења електронских података на другом локалитету и скривених уређаја за похрањивање података.

2.1. Системи видеонадзора

Системи видеонадзора сада преовладавају на већини јавних мјеста. За сва мјеста извршења кривичног дјела, укључујући њихове приступне и одступне путање, требало би провјерити постоје ли сигурносне камере. Већина система видеонадзора ће сачувати снимке само ограничен период. Да би се избјегао губитак доказа, полицијски службеници морају подузети кораке како би осигурали доказе са система видеонадзора што је могуће прије.

2.2. Подаци из отвореног интернетског извора

Информације које су важне за истрагу могу се објавити на интернету. Ови се подаци могу изгубити уколико полицијски службеник не дјелује брзо како би их сачувао. Разлог губитка не мора бити евентуално уклањање електронских доказа тј. података од извршиоца или неке друге особе, они могу нестати због временског ограничења трајања одређеног интернетског домена или другом криминалном активношћу трећих особа нпр. убацивањем малициозних програма тзв. ransomvera[35], који шифрују податке на серверима, рачунарима и другим уређајима.

2.3. Онлајн кориснички налози за складиштење података

Данас је постало уобичајено да људи складиште своје електронске податке онлајн (*free file hosting sites*, *cloud computing*[36]), што им даје могућност да им приступе с било ког рачунара или другог уређаја. Често се копије ових података не чувају на локалним рачунарима. Електронска пошта, текстуални документи и фајлови с мултимедијалним садржајима (слике, музика и видеоснимци) су типични примјери. Приступање овим подацима полицијским службеницима често може представљати изазов у смислу прибављања електронских доказа који се не налазе на физичкој локацији на којој се обавља рачунарско претраживање електронских података.

2.4. Електронска евиденција и комуникациони подаци (задржани подаци)

Интернет, телекомуникациона индустрија и друге онлајн организације производе током пословања разну електронску евиденцију која се биљежи кроз задржане податке као што су

[35] *Ransomware* (у појединим случајевима тај тип малвера означава се и као криптовирус, криптотројани или криптоцрв) обухвата класу малвареа која ограничава приступ рачунарским системима које инфицира те захтијева плаћање откупнине (уцјене) креаторима малициозних програма како би се ограничење уклонило. Извор: http://www.nod32.com.hr/ThreatCenter/ThreatTest/tabid/2556/Default.aspx#ransomware

[36] Тако например Европска унија у свом стратешком документу „Ослобађање потенцијала клауд компјутинга у Европи“ наводи да: „Клауд компјутинг (*Cloud Computing*) у поједностављеном смислу може схватити као чување, обрађивање и кориштење података који се налазе на удаљеним рачунарима и којима се може приступити преко интернета“. Извор: http://pravoikt.org/racunarstvo-u-oblacima-cloud-computing-sta-je-i-sto-nas-treba-da-bude-briga/

адреса интернетског протокола, подаци о саобраћају, подаци о локацији и др. Ова евиденција може бити од непроцјењиве важности за полицијског службеника и као доказ и у смислу обавјештајних података. У неким случајевима то ће бити једине информације које повезују осумњиченог с кривичним дјелом. Овакве евиденције у складу са чл.128. Закона о електронским комуникацијама ("Сл. гласник РС", бр. 44/2010, 60/2013 - одлука УС и 62/2014) чувају се 12 мјесеци од дана обављене комуникације, а у чл. 129. наведеног закона дефинисане су врсте задржаних података. Стога је потребно да полицијски службеници реагују брзо да не би изгубили доказе.

2.5. Подаци с уређаја крајњег корисника

„Уређај крајњег корисника" је опћи назив за сваки кориснички производ који се користи за обраду или складиштење електронских података. Као што је наведено, доступно је много различитих врста уређаја крајњег корисника као што су: рачунари, мобилни телефони, видеокамере, музички плејери, Sat-Nav, GPS, оптички дискови и меморијски стикови и др. Сви ови уређаји ће имати могућност да пруже витalне доказе, али се мора поштовати строга процедура када се њима рукује.

Стратегија за прикупљање дигиталних доказа би требала узети у обзир четири фазе у наставку описане.

2.5.1. Осигурање несталих доказа

Што се тиче електронских доказа, прво што би полицијски службеници морали имати на уму је да сачувају несталне доказе:

- могуће је наснимити нешто преко снимака система видеонадзора;
- могуће је да податке објављене на интернету уклони њихов аутор или администратор;
- могуће је да евиденција комуникације буде прочишћена или преко ње нешто наснимљено;
- подаци на уређајима крајњег корисника могу бити случајно или намјерно измијењени, обрисани или да се преко њих нешто насними;
- очување се може осигурати одузимањем уређаја који садржи првобитне податке, узимањем копије тих података или захтијевајући од треће особе да их сачува за каснију потребу.

Полицијски службеник мора бити упознат с опћим принципима одузимања електронских доказа (уврштених у овај приручник) како би се осигурало да оно што подузме не угрози доказну вјеродостојност података.

2.5.2. Електронско трагање

Постоје два аспекта електронског трагања:

- утврђивање поријекла сваке електронске информације,
- трагање за осумњиченим(а) преко њихових електронских отисака.

Локардов основни принцип форензике "Сваки контакт оставља траг." истинит је када су у питању рачунари и интернет. Заправо у сваком тренутку креирање, модификовање или брисање електронских података моћи ће се довести у везу с одређеним рачунаром и корисничким налогом.

У већини случајева ово ће значити идентификовање аутора или креатора електронских података преко интернетског протокола тј. IP-адресе рачунара који је кориштен. За ово ће вам бити потребни и тачан датум и вријеме (укључујући временске зоне) да је информација забиљежена. Ова информација може бити достављена пружаоцима услуга кориштења интернетских мрежа (интернетским пружаоцима сервиса ISP), који ће утврдити име особе која је користила тај интернетски налог. Традиционалне полицијске вјештине ће и даље бити неопходне како би се осумњичени довео у везу с идентификованим рачунаром или интернетским налогом.

2.5.3. Претрес и запљена

Када се идентификује осумњичени, вероватно ће бити потребно да се претресе и одузме електронски доказ који је код њега. Овај приручник пружа свеобухватан водич за националну најбољу праксу приликом претресања и одузимања електронских података. Приручник истиче кључне ствари које би тужилаштво и полицијски службеници требали имати на уму приликом сваког процеса претресања и одузимања.

2.5.4. Рачунарско-дигитално вјештачење

Када се одузму уређаји крајњег корисника, потребно је да иду на дигитално форензичко вјештачење како би се извукли сви електронски докази у облику који је прихватљив за судове. Бит ће потребно да се електронски докази прикупљени током истраге протумаче и представе тако да они који нису познаваоци технике или нису претходно били упознати са случајем могу једноставно схватити повезаност тих доказа са случајем. Ово је поступак за који су потребни специјалистичке вјештине и знања.

3. Опћи принципи

Овај водич између осталог пружа најбољу праксу у раду с електронским доказима. Постоје четири опћа принципа којих се полицијски службеници морају придржавати како би се очувала вјеродостојност доказа.

Први принцип

Никаква акција коју подузму полицијске службе не би требала измијенити датум на рачунару или уређају за складиштење података на шта би накнадно могло да се рачуна на суду. Стога, потребно је извршити планирање претреса електронских доказа, прикупити информације о осумњиченом, локацијама и процјени људских капацитета и потребне опреме.

Други принцип

У случају да полицијски службеник сматра да је неопходно да приступи првобитном датуму на рачунару или уређају за складиштење података, он мора бити компетентан за то и способан да пружи доказ уз објашњење зашто је то релевантно и на шта указује тај њихов поступак.

Трећи принцип

Требало би направити и сачувати траг ревизије или неку другу евиденцију свих поступака примијењених на електронске доказе с рачунара ии другог уређаја. Независна трећа страна би требала прегледати ове поступке и добити исти резултат.

Четврти принцип

Полицијски службеник задужен за истрагу (надлежан за тај предмет) у потпуности је одговоран да осигура да се поступа по закону и овим принципима.

4. Осигурање доказа са система видеонадзора

У области сигурности и праћења системи видеонадзора су мало стандардизовани, тако да се мноштво различите опреме разликује по квалитету слике и користи различите форме записа и њиховог складиштења.

Када утврди положај система видеонадзора, полицијски службеник би се требао повезати с оператером система и затражи од њега да сарађује у осигурању одговарајућих снимака.

Типично за старе аналогне системе је да снимају на VHS или SVHS видеокасете, што даје могућност полицијском службенику да привремено одузме касете на одређени период.

Новији дигитални системи обично снимају на интерни хард диск преко чега ће након одређеног периода аутоматски бити наснимљен нови снимак. Овај период ће зависити од величине хард диска и конфигурације система видеонадзора. Полицијски службеник би требао тражити од оператера на систему видеонадзора да набави копију тражених снимака. Већина система ће имати опцију за копирање података на екстерни уређај (DVD, CD, USB).

У случајевима када је доказ осигуран на самом уређају система видеонадзора и уколико га није могуће копирати на екстерни уређај или оптички компакт диск, полицијски службеник би требао у складу са Законником о кривичном поступку привремено одузети такав уређај.

Након што се осигурају подаци са система видеонадзора, потребно је да се предоче на уобичајен начин, а потом предају полицијској јединици за обраду видеоматеријала. Они ће похранити оригинални примјерак и припремити доказне копије података у облику који је погодан за потребе суда.

5. Евиденције и подаци пружалаца комуникационих услуга

5.1. Добивање података о комуникацији

Одлуком Вијећа министара Босне и Херцеговине о посебним обавезама правних и физичких особа које пружају телекомуникацијске услуге, администрирају телекомуникацијске мреже и врше телекомуникацијске дјелатности, у погледу осигурања и одржавања капацитета који ће омогућити овлаштеним агенцијама да врше законито пресретање телекомуникација, као и капацитета за чување и осигурање телекомуникацијских података и Одлуком о измјени те одлуке, успостављени су центри интерфејса за законито пресретање за потребе полицијских органа и Обавјештајно-сигурносне агенције (у даљњем тексту: ОСА-е). Центар за законито пресретање интерфејса имат ће директан електронски приступ систему за управљање пресретањем код оператера телекомуникација, мрежних оператера, давалаца услуга и давалаца приступа у Босни и Херцеговини, као и системе којима ће се осигурати достављање садржаја телекомуникације и информација у вези с пресретањем центрима за снимање и мониторинг полицијских органа и ОСА-е (чл.. 7).

У складу са чл. 8. Одлуке оператери телекомуникација, мрежни оператери, даваоци услуга и даваоци приступа обавезни су осигурати неопходне техничке и организацијске предувјете, из властитих ресурса и о властитом трошку, да би омогућили да се законито пресретање телекомуникацијских услуга и активности проводи од центра интерфејса за законито пресретање.

Обавезе оператера телекомуникација, мрежних оператера, давалаца услуга и давалаца приступа су:

- *уградња опреме за законито пресретање и интерфејса за фиксну мрежу, мобилну мрежу и интернетску мрежу у складу са ETSI или другим стандардима;*
- *уградња неопходне телекомуникацијске опреме и инфраструктуре те техничких рјешења у домену управљања телекомуникацијским мрежама, којима се омогућује управљање достављањем циљаних телекомуникација од центра интерфејса за законито пресретање;*
- *достава садржаја, као и података у вези с пресретањем свих циљаних телекомуникација с цијелог простора који покрива оператер центру интерфејса за законито пресретање уз употребу минималног броја конекција довољног капацитета;*
- *процедуре и стручни кадар којима се осигурава достава пресретаних циљаних телекомуникација центру интерфејса за законито пресретање у складу с гарантованим IoS стандардима (чл. 9.).*

5.2. Добијање садржаја комуникације

"Законито пресретање" је наведеном Одлуком одређено као пресретање и достављање циљаних телекомуникација у току њиховог преноса тако да, осим за пошиљаоца или циљаног примаоца телекомуникације, дио или цијели садржај телекомуникације и с њом повезаних телекомуникацијских података постане доступан и овлаштеној агенцији, како је

то одређено за посебне истражне или обавјештајне радње, а у складу с одредбама закона у Босни и Херцеговини (чл. 3. т).

Оператери телекомуникација, мрежни оператери, даваоци услуга и даваоци приступа смију користити податке у вези с пресретањем и сигнале, али не и садржај телекомуникација добијен примјеном функције законитог пресретања, и то само за потребе одржавања функције законитог пресретања и само на начин који предвиди или одобри Заједнички управни одбор (чл. 13. ст. 2.).

У складу с чланом 14. Одлуке функција законитог пресретања састоји се од пресретања телекомуникација у току њиховог преноса, испоруке садржаја и информација у вези с пресретањем и осталих захтјева.

Са стајалишта кривичног поступања за провођења радњи које имају карактер законитог пресретања потребна је наредба судије за претходни поступак. Ово се односи на примјену посебних истражних радњи као незаобилазног вида прикупљања доказа у савременим увјетима. Одређени видови законитог пресретања у хитним околностима могући су и темељем наредбе тужиоца. Овдје мислимо на наредбу оператеру телекомуникација или другој правној особи која врши пружање телекомуникационих услуга да достави податке о кориштењу телекомуникационих услуга те особе, ако би такви подаци могли бити доказ у кривичном поступку или послужити прикупљању информација које могу бити од користи у кривичном поступку.

5.3. Добијање података од других онлајн услуга у Босни и Херцеговини

Из анализе доступних прописа за Босну и Херцеговину није било могуће утврдити на који начин се законито добивају подаци од других онлајн услуга. Нема сумње да би и у таквим околностима требало поступити у складу с већ наведеним одредбама закона о кривичном поступку које се односе на посебне истражне радње те привремено одузимање предмета у смислу достављања података о кориштењу телекомуникацијских услуга особе у погледу које постоје основи сумње на почињење кривичног дјела.

5.4. Добијање података из иностранства

Постоји много онлајн услуга које пружају организације које се налазе изван Босне и Херцеговине и међународне организације које своје податке држе изван Босне и Херцеговине. У том случају је можда неопходна помоћ стране полицијске службе. Ови упити су често спор поступак. Да би се спријечио губитак података док траје поступак међународних упита, препоручује се да се власнику података (пружаоцу интернетског сервиса и др.) изда Захтјев за очување података, којим се он обавјештава о томе које информације се траже. Ово омогућује да се подаци очувају док се чека добијање одговарајућег правног документа тј. међународне замолнице за пружање правне помоћи. Захтјеви за очување података требали би се упућивати преко контакт-тачке 24/7 при Одјељењу за борбу против високотехнолошког криминала или Посебног тужилаштва за борбу против високотехнолошког криминала.

Такође, велики пружаоци интернетских услуга попут сервиса Facebook, Google, Yahoo и др. остварују непосредну комуникацију с надлежним институцијама задуженим за вођење

преткривичног поступка. Примјера ради, компанија Facebook ауторизованим институцијама за спровођење закона у складу са својом пословном политиком и примјењивим законом на образложени захтјев надлежног тужилаштва доставља задржане податке о својим корисницима (интернетски протокол и електронске адресе и др.).

Више информација о сарадњи у кривичним истрагама с компанијом Facebook можете наћи на интернетској страници друштвене мреже Facebook[37], која даје детаљна правна упутства попут информација за полицијске службе, захтјева на основу судских рјешења у САД, података о налогу које откривају искључиво у складу са својим увјетима кориштења услуге и важећим законом, укључујући савезни Закон о сачуваној комуникацији (*Stored Communications Act*, *SCA*), 18. том Кодекса САД (U.S.C.), одјељци 2701–2712., захтјева на основу међународних судских решења, чувања налога, захтјева у хитним случајевима, питања везана за сигурност дјеце, задржавања и доступности података, облику захтјева, пристанку корисника налога (ако припадник полицијске службе тражи информације о кориснику Facebooka који је пристао на то да тај припадник полиције приступи подацима о налогу корисника или да их добије, кориснику треба препоручити да сам преузме те информације с налога), обавјештавање корисника налога чија се провјера тражи (политика компаније Facebook налаже да људе који користе њихову услугу обавијесте о захтјевима за приступ њиховим информацијама прије него што те информације открију, осим када им закон то забрањује или у изузетним околностима, као што су случајеви експлоатације дјеце, хитни случајеви или случајеви у којима би обавјештење било контрапродуктивно), вјештачења, надокнаде трошкова и подношења захтјева с адресом.

Сви захтјеви надлежног тужилаштва морају садржавати детаљне информације о траженим подацима, као и сљедеће ставке:

- назив органа који га је издао (навести надлежно тужилаштво), број значке/ идентификационог документа задуженог полицијског службеника, е-адресу с домена полицијске службе и директан број телефона за контакт.
- е-адресу, идентификациони број корисника (http://www.facebook.com/profile.php?id=1000000XXXXXXXX) или његово корисничко име (http://www.facebook.com/username) са профила на Facebooku.

6. Подаци из отворених интернетских извора

Информација из отвореног извора се дефинише као: "Свака информација која није означена као повјерљива, у било којем средству информисања, која је опће доступна јавности, чак и у случају да је дистрибуција ограничена или могућа само уз плаћање".

На интернету постоји значајан број информација из отвореног извора које се могу употријебити као доказ или обавјештајни податак у прилог случају који се обрађује, као нпр. идентификациони подаци о особи које можемо увезати с неким електронским налогом или фотографијом, кућна адреса, телефонски број, имовина, географски подаци тј. локације, пословање и финансијски подаци, повезаност особа по различитим основама, интересовања и много других података на основу којих је могуће извршити квалитетну анализу и профилисање особа.

[37] https://www.facebook.com/safety/groups/law/guidelines

7. Онлајн кориснички налози и онлајн складиштење података

Како се технологија развија, постаје уобичајено да људи рутински складиште своје електронске податке онлајн. То им омогућује да својим фајловима приступе с било којег рачунара који има приступ интернету, укључујући мобилне уређаје као што су лаптоп рачунари, таблети, ''паметни'' телефони и др. Овакав приступ обради, складиштењу и поновном проналажењу података се често назива „рачунарство у облацима". У многим случајевима копије ових фајлова неће се чувати на личном рачунару неке особе, већ ће се ти онлајн подаци вјероватно чувати у шифрованом облику на серверима изван територије Босне и Херцеговине. Најчешће врсте фајлова који се у данашње вријеме складиште онлајн су електронске поруке, разни документи у различитим форматима и мултимедијални фајлови (фотографије, музика и видеозаписи). Приступ овим подацима често може бити изазов за полицијске службенике.

Оштећени и свједоци

Када су електронски докази доступни оштећеној особи или свједоку преко онлајн налога, требало би од њих захтијевати да доставе копију тих података који се могу предочити на уобичајен начин. Уколико је могуће, те податке би требало копирати на оптички компакт диск (CD/DVD) како би се сачувао њихов првобитни облик. Уколико то није могуће, полицијски службеник мора размотрити одговарајуће алтернативно решење. Могуће опције би могле бити да сачини штампану копију, пренесе податке на USB-уређај или их пошаље електронском поштом.

Осумњичени

Када се обавља разговор с осумњиченима, важно је питати их имају ли приступ било којем онлајн налогу гдје се могу похранити електронски подаци. Када се утврди да осумњичени има налог, требало би га упитати жели ли добровољно пристати да полицијски службеник приступи тим налозима и копира све податке које сматра битним за случај који се истражује и привремено преузме такав налог у смислу одредби чл. 147. ст. 3 у вези са ст. 1 Законика о кривичном поступку, уз уредно издату потврду о привремено одузетим предметима у којој је неопходно констатовати да је особа добровољно предала своја корисничка имена и шифре за своје електронске налоге полицијским службеницима.

8. Уређаји крајњег корисника (оштећени/свједоци)

Када се обавља разговор с оштећеном особом или свједоком, важно је утврдити да ли посједује или контролише било какав уређај који може садржати електронске доказе. Осјетљивост електронских података је таква да лако могу бити оштећени или уништени. Стога је потребно подузети мјере да се сачува њихова доказна вјеродостојност.

Уколико је могуће, полицијски службеник би требао од оштећене особе или свједока тражити да сарађује и пристане осигурати уређај како би се вјештачењем могло доћи до било каквих доказа.

Водич пружа детаљне информације о одузимању, руковању и испитивању електронских уређаја и уређаја повезаним с њима. У одјељку Водича Претресање и одузимање наведене су кључне ствари које треба запамтити.

У случају да се не може добити пристанак, полицијски службеник мора размотрити је ли одговарајући корак да привремено одузме уређај по основу чл. 147. ст. 3. у вези са ст. 1. Законика о кривичном поступку.

Када се по основу закона налази у неким просторијама, полицијски службеник може одузети сваки предмет за који верује да постоји основана сумња да је доказ кривичног дјела и да је одузимање неопходно како би се спријечило да уређај буде сакривен, изгубљен, измијењен, оштећен или уништен.

Када полицајски службеник има овлаштење да одузме било који материјал у електронском облику, он може захтијевати да тај материјал сачини у облику који се може понијети, да је јасан и читак.

8.1. Професионални свједоци

У раду с професионалним свједоцима који држе електронске доказе као дио евиденције коју прикупљају у пословању или пружању услуга кроз одређене интернетске презентације, као што су пружаоци интернетских сервиса, пружаоци услуга мобилне телефоније и администратори интернетских презентација, полицијски службеник би требао поступити по сљедећим одјељцима овог приручника:

- Евиденција и подаци пружалаца комуникационих услуга,
- Специјалне процедуре на основу најбоље праксе које не утјечу на измјену електронских доказа.

9. Електронско трагање

Постоје два аспекта електронског трагања:

- утврђивање правог идентитета неке особе путем онлајн идентификатора,
- утврђивање ко је аутор одређене електронске информације на основу адресе интернетског протокола.

9.1. Онлајн идентификатор

Скоро сваки пружалац услуга преко интернета који дозвољава интеракцију корисника (више од самог прегледања објављених садржаја) захтијева да се креира кориснички налог. Ови налози служе да се осигура извјестан степен одговорности и ревизорске функционалности пружаоцу услуга. Степен верификације идентитета који се односе на онлајн налоге се у великој мјери разликује међу пружаоцима. У неким случајевима се тражи веома мало личних података да би се отворио налог и ништа од наведених података се не провјерава. У тим случајевима наведени подаци се не могу са сигурношћу сматрати тачним. С друге стране

постоје налози у вези с којима се примјењују знатне сигурносне мјере како би се потврдио тачан идентитет особе која отвара налог или му приступа. Када је лични идентитет садржан у онлајн налогу, дужност је полицијског службеника да утврди његово поријекло прије него што поступи по тој информацији.

9.2. Адреса интернетског протокола (IP)

Рачунари повезани с интернетом између себе комуницирају користећи интернетски протокол (IP). Сваки рачунар повезан с интернетом мора имати јединствену IP-адресу преко које се може идентификовати. IP-адреса рачунара се може сматрати „бројем телефона“ за телефонску мрежу или „поштанском шифром“ за поштанске услуге. То је јединствен идентификатор који омогућује да се пошаљу информације. Очита разлика између аналогија телефона и поштанске услуге с IP-адресирањем је у томе што су им јединствени идентификатори додијељени за стално док IP-адресе често додјељује пружалац интернетског сервиса (ISP) својим клијентима (претплатницима) у виду краткорочног закупа и те адресе називамо динамичким. Из тог разлога полицијски службеник обавезно мора утврдити тачан датум и вријеме (укључујући временску зону) за које је заинтересован у вези с датом IP-адресом. То дозвољава да пружалац интернетског сервиса провјери своју евиденцију и утврди којем претплатнику је додијељена посебна IP-адреса у било које вријеме, како би се идентификовао аутор одређене електронске информације. Међутим, ISP чува ову евиденцију само током ограниченог периода. У већини случајева је то период од 12 мјесеци. Полицијски службеник мора дјеловати брзо како би осигурао да се не изгубе подаци који су од кључног значаја за улажење у траг осумњиченом.

Примјер IP-адресе: 176.221.75.99 (IP-адреса Републичког јавног тужилаштва тј. www.rjt.gov.rs)

Постоје одређене IP-адресе које су резервисане за приватне мреже. Ово омогућује да рачунари у оквиру неке мреже могу међусобно комуницирати, али не директно с интернетом. Уколико рачунари с приватне мреже имају приступ интернету, то се одвија преко одређеног рачунара познатог као *gateway* (капија).

Распон приватне (интерне) IP-адресе:

- 10.xxx.xxx.xxx [xxx = вриједност између 0 и 255]
- 192.168.xxx.xxx [xxx = вриједност између 0 и 255]
- 172.yy.xxx.xxx [yy = распон између 16 и 31][xxx = распон између 0 и 255]

Уколико полицијски службеник током истрага добије приватну IP-адресу, из те информације неће бити могуће идентификовати одређену приватну мрежу или рачунар. Важно је да прво идентификује интернетску капију (*gateway*), што потом води идентификацији приватне мреже.

9.3. Утврђивање онлајн идентификатора

Без обзира на то покушавате ли идентификовати особу иза неког „онлајн идентитета“ или приписујете интернетски садржај одређеној особи, методологија ће бити иста. Полицијски службеник мора тражити податке од пружаоца интернетског сервиса или оних који

посједују податке тј. евиденције о корисничким приступима. Уз верификоване налоге то може бити довољно информација за дјеловање. У другим случајевима може бити неопходно да се захтијева историјат логовања одређеног налога или тражи IP-адреса која је повезана с одређеном информацијом или трансакцијом (немојте заборавити вријеме и датум). Напредак у интернетским упитима како би се добиле најквалитетније информације које је могуће верификовати је вјештина која се развија искључиво праксом. Полицијски службеници и тужиоци се охрабрују да у свом раду упућују упите који се тичу интернета јер ће то неизоставно проширити њихове истражне вјештине. Интернетски упити о корисницима опсега IP-адреса који се налазе код једног од пет свјетских регионалних интернетских регистара *Whois* база података (***African Network Information Centre***, ***American Registry for Internet Numbers***, ***Asia-Pacific Network Information Centre***, ***Latin America and Caribbean Network Information Centre***, ***RIPE Network Coordination Centre***)[38] **најчешће се врше преко сљедећих онлајн интернетских сервиса: хттпс://централопс.нет, хттп://www.инфоснипер.нет и др.**

Након што се утврди IP-адреса, требало би бити могуће да се она повеже с налогом претплатника преко одговарајућег пружаоца интернетског сервиса.

Запамтите да сви захтјеви које се тичу IP-адреса и других упита упућених операторима телекомуникација и пружаоцима интернетских сервиса подлијежу Законику о кривичном поступку и Закону о електронским комуникацијама.

10. Савјет о претресању

10.1. Прије претреса

Потрудите се да прикупите што више информација о врсти, мјесту и конекцији сваког рачунарског система. Уколико планирате претресање пословне просторије гдје постоје корпоративне мреже, потребно је да се за савјет обратите Посебном тужилаштву за борбу против високотехнолошког криминала или Одјељењу за борбу против високотехнолошког криминала.[39]

10.2. Брифинг

Веома је важно да сви службеници који присуствују мјесту претресања буду адекватно информисани. У овој фази би требало дати савјет о томе како да се сигурно прибави сваки доказ с рачунара. Требало би дати строга упозорења како би необучени службеници били спријечени да приступају рачунарима и носачима меморија. Тимове за претресање би требало посавјетовати да се за савјет обрате Посебном тужилаштву за борбу против високотехнолошког криминала прије него што одузму било који рачунар који је дио корпоративне мреже.

[38] Извор: https://en.wikiversity.org/wiki/Whois/IP_address

[39] Наглашавамо да у оквиру организације тужилаштава у Босни и Херцеговини, односно ентитетима Федерација БиХ и Република Српска, као и у Брчко дистрикту БиХ нема посебно установљене тужилачке институције која би била надлежна за процесуирање ове врсте кривичних дјела.

10.3. Припрема за претрес

Провјерите да ли опрема за претресање мјеста извршења кривичног дјела садржи одговарајући материјал за одузимање рачунара, уређаја за похрањивање електронских података и сваки други доказ који има везе с тим.

Шта понијети:

- фотоапарат и/или камеру за снимање лица мјеста и информација на екрану,
- рукавице за једнократну употребу (за све службенике који врше претрес),
- алатке (батеријску лампу, маказе, шарафцигер, клијешта и резаче жица),
- наљепнице за доказни материјал,
- кесе за заштиту од неовлаштених измјена доказног материјала (разних величина),
- провидне пластичне кесе за доказни материјал (разних величина) и печате за кесе
- папирне кесе за доказни материјал (разних величина) и селотејп,
- фломастере у боји за обиљежавање шифри и назива предмета који су узети,
- кутије на склапање.

10.4. Претресање мјеста извршења кривичног дјела

При доласку на мјесто извршења кривичног дјела или током претресања просторија гдје постоји могућност да се налази електронски доказ на рачунару, полицијски службеник би требао преузети контролу над тим мјестом побринувши се да се особе одмакну од рачунара или других уређаја на којима би могли утјецати на доказ.

Након што се осигура просторија, требало би је снимити камером или фотографисати прије почетка претреса. Нарочито би требало обратити пажњу на радно мјесто у рачунарским системима и око њих те утврдити да ли има DVD/CD медија у уређају.

Уколико су рачунари искључени, немојте их укључити. Уколико су укључени, немојте пасти у искушење да вршите претрагу на њима тражећи доказе. За претрагу рачунара је потребна посебна вјештина. Приступање рачунару без примјене одговарајуће процедуре вјештачења ће измијенити податке и компромитовати доказе.

Што се тиче лаптопа, имајте на уму да се неки могу аутоматски укључити самим подизањем поклопца. Укључивањем рачунара промијенит ће се датум у оперативном систему, што може компромитовати вјеродостојност доказа на њему.

Увијек се придржавајте савјета о одузимању рачунара наведених у „Обавезној инструкцији о прикупљању и осигурању електронских доказа", донесеној 26.02. 2013. године и заведеној под број: 01-1000/13-12. (УКП бр.03/4 1633/13 од 01.03.2013.).

Сјетите се да потражите лозинке које су често забиљежене у дневницима или биљешкама око рачунара.

Потражите приручнике с упутствима за софтвер или одузете уређаје. То може бити корисно вјештаку када спроводи анализу.

Потражите све повезане уређаје за складиштење електронских података. Многи уређаји имају опције за одвојено складиштење података. Доказ који тражите можда је већ пренесен на тај одвојени дио и више није доступан на уређају. Уређај за складиштење може физички бити веома мали, а да може похранити велику количину података, па је неопходна темељна претрага.

Сви одузети предмети би требали бити пажљиво запаковани и приложени на уобичајен начин. Предмети би требали бити приложени појединачно, осим у случају веће количине сличних предмета пронађених на истом мјесту. Например, сви компакт дискови пронађени на радном столу могу се приложити заједно, док се сви хард дискови могу приложити као слеђећи доказ. Међутим, ове двије врсте предмета не би требало измијешати у један доказни предмет.

Све доказне предмете чувајте даље од магнета и радиоодашиљача.

Све доказне материјале би требало евидентирати као списак доказних материјала у потврдама о привремено одузетим предметима и записницима и залијепити на њих наљепнице на којима је наведено мјесто одузимања и мјесто за складиштење.

Како одузети рачунар (када је искључен)

- Немојте укључивати рачунар.
- Имајте на уму да се лаптопи могу укључити самим подизањем поклопца.
- Немојте дозволити осумњиченима да приступе уређају.
- Фотографишите рачунар и радни сто/мјесто гдје се налази.
- Фотографишите каблове који иду до/од рачунара.
- Искључите кабел за струју из задњег дијела рачунара, а не из зида.
- Нацртајте дијаграм и означите каблове за касније распознавање повезаних уређаја.
- Посебно погледајте постоји ли било каква интернетска конекција.
- Искључите све каблове и уређаје из рачунара.
- Пажљиво спакујте и означите предмете који се одузимају као доказни материјал.
- Одузмите све уређаје за складиштење електронских података који се налазе на том мјесту.
- Одузмите све приручнике за употребу тих уређаја.
- Одузмите све биљешке у близини рачунара.
- Документујте све што сте радили.

Лаптоп

Имајте на уму да се лаптопи могу укључити самим подизањем поклопца.

Да бисте осигурали да се лаптоп случајно не укључи, препоручује се да извадите батерију.

Како одузети рачунар (када је укључен)

- Осигурајте област гдје се налази компјутерска опрема.
- Удаљите људе од рачунара и напајања за струју.
- Немојте дозволити да осумњичени прилазе било којим уређајима.
- Немојте користити рачунар нити претраживати по њему тражећи доказе.
- Евидентирајте оно што је на екрану (фотографија и биљешке).
- Немојте користити тастатуру.
- Ако је активан чувар заслона, покрет миша би га требао склонити, користите миш да прелазите преко отворених прозора с *task bara*.
- Уколико нека апликација брише податке – одмах искључите рачунар извлачећи кабел за струју из задњег дијела рачунара. Појединим врстама података би могло бити немогуће поново приступити након што би се искључио рачунар. Уколико сумњате да нека од отворених апликација можда садржи доказе, прије него што наставите требали бисте се обратити за савјет Одјељењу за ВТК или Служби за специјалне истражне методе ради евентуалног креирања форензичке копије RAM[40] меморије.
- Размислите о томе да питате корисника о било којој од отворених апликација.
- Водите писану евиденцију о свему што сте подузели.
- Пустите да сви штампачи заврше штампање.
- Фотографишите рачунар и радни сто/мјесто гдје се налази.
- Извадите кабел за напајање струјом из задњег дијела рачунара (не из зида) без искључивања било ког програма или искључите рачунар по уобичајеном поступку.
- Фотографишите каблове који воде до/од рачунара.
- Нацртајте дијаграм и означите каблове за касније распознавање повезаних уређаја.
- Посебно погледајте постоји ли било каква интернетска конекција.
- Искључите све каблове и уређаје из рачунара.
- Пажљиво спакујте и означите предмете који се одузимају као доказни материјал.
- Одузмите све уређаје за складиштење електронских података који се налазе на том мјесту.
- Одузмите све приручнике за употребу софтвера и одузетих уређаја.
- Одузмите све биљешке у близини рачунара.
- Пустите да се опрема охлади прије премјештања.
- Документујте све кораке подузете у поступку одузимања.

[40] Особина RAM-меморије је да се сваком њеном бајту може слободно приступити независно од претходне меморијске локације, с тим да се у њу подаци могу и уписивати (***write***) и очитавати (***read***) из ње. Сваким уписом податка у неку локацију њен претходни садржај се аутоматски губи. Друга важна особина RAM-меморије је да она податке који се у њој налазе задржава (чува) само док постоји напон напајања на њој. Чим нестане напона напајања, комплетан садржај меморије се губи и приликом поновног доласка напона напајања (при сљедећем укључењу рачунара) она је потпуно празна.

Лаптопи

Скидање кабла с лаптопа вјероватно га неће искључити јер ће се пребацити на батеријско напајање. Да бисте га искључили, притисните и држите дугме *on/off* пет до десет секунди (док се не искључи). Потом извадите батерију.

Уколико су отворене неке апликације (као што су шифроване), можда би било боље да лаптоп оставите укључен на батеријском пуњењу и пренесете га директно у Управу криминалистичке полиције, Службу за специјалне истражне методе, уколико је то могуће. То би могло смањити ризик од губитка тих података када се рачунар искључи.

Кућне мреже – шта имати на уму

Данас се домаћи *Broadband* приступ интернету може остварити од куће користећи један од сљедећа два начина:

- ADSL Broadband (нпр. БТ телефонска линија)[41],
- оптички кабел (нпр. SBB SOLUTIONS кабловски интернет).

Обично пружалац интернетског сервиса испоручује интернетску услугу Broadband преко модема који је физички повезан с телефонском линијом корисника. Модем је једноставан електронски уређај који конвертује дигиталне податке с рачунара тако да се могу пренијети преко телефонске мреже. Модем може бити конектован директно на рачунар или на рутер. Рутер је електронски уређај који омогућује да више рачунара буде повезано како би размјењивали податке и средства (као што су штампачи и интернетске конекције). Рутери дају једнаку могућност рачунарима да буду повезани физички (Ethernet Cable) или бежично (WiFi). У пракси није неуобичајено да се модем и рутер комбинују у једном уређају који је повезан каблом и бежичним путем за приступ *Broadband* интернету. Модем/рутер пружа приступ интернету једном или више рачунара. Они могу бити повезани кабловима (*Ethernet Cables*) или бежично. Требали бисте имати на уму да поред десктоп рачунара и лаптопа, и други портабл уређаји могу пружити приступ интернету, попут паметних телефона, PDA уређаја, играчких конзола, таблет рачунара, ТВ-а који у себи садрже меморијске јединице и др.

Кућне мреже – шта узети у обзир при претресању и привременом одузимању предмета

- Осигурајте област гдје се налази рачунарска опрема.
- Удаљите људе од свих рачунара и напајања за струју.
- Немојте дозволити да осумњичени прилазе било којим уређајима.
- Утврдите гдје је модем/рутер и искључите га из телефона и напајања.
- Утврдите гдје су уређаји крајњег корисника (рачунари, телефони, персонални дигитални асистент - PDA итд.).

[41] Широкопојасни приступ интернету који омогућује велике брзине преноса података коришћењем телефонске инфраструктуре, док ВТ телефонска линија подразумијева више телефонских линија кроз један прикључак.

- Обрадите сваки уређај (одредите приоритете у одузимању): је ли уређај укључен (дајте му предност у односу на искључене), бришу ли се подаци (извуците кабел за струју да бисте га искључили).
- Немојте користити рачунаре нити покушавати вршити претраге на њима тражећи доказе.
- Систематски се позабавите сваким рачунаром као што је горе наведено.

Одузимање модема и рутера

Од природе ваше истраге ће зависити да ли бисте требали одузети интернетски модем/рутер. Ови уређаји се не користе за складиштење личних фајлова, али могу садржавати фајлове о логовању и информације о конфигурацијама који могу помоћи при идентификацији уређаја који су преко њих конектовани на интернет. Неки од ових уређаја ће изгубити ове информације ако се искључе. Уколико мислите да информације с модема/рутера могу бити од користи за ваше истраге, онда вас молимо да се додатно посавјетујете с Одјељењем за борбу против ВТК (бит ће вам потребни детаљи и модел модема/рутера).

Алтернативне методе приступа интернету

Требали бисте имати на уму чињеницу да поред конвенционалних интернетских услуга које се пружају преко кућног фиксног телефона, постоје и алтернативне методе приступа интернету, преко уређаја као што су: Broadband Dongle, MiFi (Mobile Internet Hub), WiFi hotspot-ова, дијељење мреже преко паметних телефона, таблет рачунара и сл.

Такође је могуће да се неко конектује преко несигурног бежичног рутера неког у комшилуку (са или без његовог знања о томе) или у неком ресторану, хотелу, интернет-кафеу и сл.

Мрежни сервери и пословне мреже

Када се сусретнете с пословном мрежом и сервером сложене инфраструктуре, прије него што било шта подузмете, морате се обратити за даљу помоћ некоме из Службе за специјалне истражне методе.

Утврдите ко је мрежни или системски администратор како би припадници Службе за специјалне истражне методе могли с њим разговарати о могућим начинима да се осигурају докази.

Имајте на уму да би та особа могла бити осумњичена у одређеним случајевима.

Осигурајте то мјесто и немојте дозволити да било ко користи било који од рачунарских система док се не добију одговарајуће смјернице.

УПОЗОРЕЊЕ

Извлачење утикача могло би:

- озбиљно оштетити систем,
- изазвати губитак кључних доказа,
- омести законито пословање,

- створити могућност за подузимање законите радње; уколико је неопходно, привремено одузети сервер након завршетка рачунарског претраживања података на основу наредбе надлежног судије за претходни поступак, имајући у виду чињеницу прекид функционисања рада сервера, нпр. уколико се на серверу налазе искључиво недозвољени и штетни садржаји, као и други незаконити подаци.

Мобилни телефони и остали дигитални уређаји крајњег корисника

Мобилни телефони могу ускладиштити доказне податке директно на интерну меморију, СИМ-картицу или додатну меморијску картицу. У даљем тексту је детаљно наведено како правилно одузети и сачувати ове уређаје и с њима повезане додатне дијелове.

- Ако је уређај искључен, немојте га укључити.
- Ако је уређај укључен:
  - фотографишите или забиљежите све што је на екрану,
  - обратите пажњу на то који датум и вријеме су на екрану, а који су стварни датум и вријеме.
- За уобичајен случај одузимања искључите телефон.
- За случај опасности по живот оставите уређај укључен.
- Не падајте у искушење да претражујете по уређају тражећи доказе.
- Уколико га посједујете, ставите телефон у торбу с ефектом Фарадејевог кавеза[42].
- Питајте власника жели ли добровољно предати PIN или лозинке.
- Одузмите све каблове (укључујући оне за напајање струјом) и држите их с уређајем.
- Одузмите све уређаје за складиштење (меморијске картице).
- Документујте све кораке које сте подузели при одузимању уређаја и компонената.

Ови уређаји имају сигурносну особину даљинског брисања података за случај крађе уређаја. Да бисте спријечили активирање ове особине, извадите SIM-картицу и ставите уређај у торбу с ефектом Фарадејевог кавеза.

Обавјештење

Искључивање мобилног телефона могло би накнадно активирати тражење лозинке или ПИН-кода, чиме се одлаже или спречава каснији приступ доказима уколико не знамо ту информацију или је не можемо лако добити. Међутим, уколико би мобилни телефон остао укључен, постоји ризик да се подаци могу измијенити или преко њих наснимити нови од долазећих позива и текстуалних порука. Полицијски службеници ће морати сами проценити шта је најбоље да ураде у датој ситуацији.

[42] Фарадејев кавез или Фарадејев штит представља простор ограничен неким проводљивим материјалом или мрежом направљеном од таквог материјала. Такав простор има особину да блокира ванјско статичко електрично поље.

Поред рачунара и мобилних телефона постоје многи други дигитални или електронски уређаји крајњих корисника који имају могућност да пруже доказне податке. Неки од уобичајених примјера су: персонални дигитални асистенти (PDA), дигиталне камере, MP3 музички плејери, глобални системи за одређивање положаја (GPS) и системи за сателитску навигацију (Sat-Nav) и др. Ови уређаји могу складиштити податке користећи интерну меморију или додатне дијелове. У даљем тексту су наведена упутства за одузимање носивих уређаја крајњег корисника и с њима повезаних додатних дијелова.

- Ако је уређај искључен, немојте га укључивати.
- Ако је уређај укључен:
- фотографишите или забиљежите све што је на екрану о PDA оставите укљученим (Погледајте савјет о PDA). Остале уређаје искључите.
- Покупите све каблове (укључујући оне за напајање струјом и кућишта уређаја).
- Одузмите све додатне уређаје за складиштење (меморијске картице).
- Питајте власника жели ли добровољно рећи лозинке.
- Документујте све кораке које сте подузели при одузимању уређаја и компонената.

Савјет о PDA

Искључивање персоналног дигиталног асистента (PDA) би могло активирати тражење лозинке, што спречава или одгађа приступ доказима. Већина ових уређаја има интерну батерију која је од кључног значаја за чување личних података корисника (познате као „нестална меморија“). Важно је да ова батерија увијек буде напуњена, иначе докази могу бити изгубљени. Уколико је то могуће, ставите овај уређај на пуњење док вршите претрес и поново када се вратите у полицијску станицу. Чим је то могуће, однесите уређај у Службу за специјалне истражне методе, гдје се може похранити и прегледати на одговарајући начин.

Рачунарско вјештачење

Полицијски службеници никада не би требали пасти у искушење да укључе или претражују садржаје било којих рачунара, мобилних телефона, осталих електронских уређаја крајњег корисника или с њима повезаних уређаја када постоји могућност да имају доказну вриједност. Рачунарска тријажа је процес који користи технологију аутоматске претраге како би се открио специфичан доказ на рачунарима или уређајима за складиштење података. Технички је погоднија да потврди постојање доказа на уређају него да докаже да нема доказа. Стога тријажу никако не би требало сматрати замјеном за темељно вјештачење рачунара. Међутим, то је користан поступак за утврђивање је ли одузет прави уређај или да се одреди приоритет у испитивању одузетих предмета.

- Савјет о томе је ли неки случај погодан за тријажу потражите од Службе за специјалне истражне методе.
- Испитивање рачунара, мобилних телефона и других дигиталних уређаја крајњег корисника захтијева вјештине специјалисте за дигитално форензичко вјештачење.
- Запослени у Служби за специјалне истражне методе су прошли опсежну обуку код акредитованих организација и посједују потребно знање и искуство за обављање темељног вјештачења, а своја открића представљају у формату погодном за судске поступке.

- У свим случајевима у којима су заједно с рачунарима ради испитивања одузети и мобилни телефони, њих ће обрадити Служба за специјалне истражне методе. Захтјеви за овим испитивањима се подносе у складу с поступком додјеле задатка Служби за специјалне истражне методе.
- У случајевима када су одузети само мобилни телефони, полицијски службеник се за савјет и упутства мора обратити Служби за специјалне истражне методе.
- Сви захтјеви за дигиталним форензичким вештачењем се морају достављати преко Службе за специјалне истражне методе, која ће одредити приоритете.

Високотехнолошки криминал као кривично дјело у домаћем законодавству с посебним освртом на тзв. cyberbullying и grooming

1. Увод

У свјетлу глобалног тренда кибернетичког дружења и живота у кибернетичком простору неминовно је да се суочимо с виктимизацијом младих на друштвеним мрежама. Томе несумњиво доприноси недовољна компјутерска информациона писменост родитеља, али много више недовољна свијест младих о ризицима које пласирање личних информација и постављање фотографија са собом носи. Данашњи свакодневни живот нарочито младих постао је готово незамислив без употребе информационих технологија. Млади људи су од најранијих дана упућени на технологију. С њима их најприје упознају родитељи дајући им своје мобилне телефоне или таблет-рачунаре да се занимају док су они заузети послом или су у кафићу, у посјети код пријатеља. Дјеца се тако забављају, упознају свијет, играју игрице које нису увијек едукативне, уче комуницирати, а да не морају да изговоре ниједну ријеч. Временом дјеца сматрају постојање интернета просто питањем живота и без њега не би могли функционисати. При свему томе родитељи неминовно почну каскати с умјешношћу употребе најновије технологије, чији је развој незаустављив и они немају времена, интересовања и воље да све то испрате. То даље доводи до немогућности родитеља да већ у неким раним узрастима остваре адекватан надзор над активностима дјеце на интернету па и незнања да сами препознају опасности које вребају. Способност родитеља да контролишу дјецу на интернету зависи од више фактора, од којих су неки степен отворености и блискости с дјецом, образовање родитеља, посвећеност дјеци и др. С једне стране родитељи су свјесни да је интернет неисцрпан извор информација и забаве те да би самим искључивањем дјеце из свих тих активности могли угрозити социјализацију дјеце, али истовремено свјесни и да појачан надзор може довести до сукоба с дјецом. Код чињенице да не мањкају одрасли који интернет користе на различите злонамјерне начине, те да дјеца такођер брзо науче како да га злоупотријебе, данашње друштво се суочава с озбиљним проблемом - несигурношћу дјеце на интернету, нарочито на друштвеним мрежама.

Организација за европску сигурност и сарадњу систематизовала је ризике којима су изложена дјеца као корисници интернета. Сви ризици су подијељени на ризике усљед излагања непримјереним садржајима *(content risk)* и на ризике усљед несигурних контаката с другим корисницима *(contact risk)*.

Непримјерени садржаји се могу подијелити на оне чије је циркулисање законом забрањено, на садржај непримјерен узрасту дјеце и на садржаје које популаришу негативне обрасце понашања. Тако је у највећем броју држава илегално промовисање расизма и бестијалности и растурање материјала који садрже елементе дјечије порнографије (нелегални садржаји). Сцене насиља и порнографски садржаји спадају у материјале непримјерене узрасту, док би

давање савјета за самоповређивање и самоубиство или пропагирање поремећаја у исхрани попут анорексије могли окарактерисати као утјецај на усвајање негативних образаца понашања.

Несигурне контакте на интернету експерти OEBS-а дијеле на 1) контакте путем којих се стварају предувјети како би се касније остварио контакт, при којем би дијете могло бити виктимизовано (грађење односа у којима дијете стјече повјерење у особе с којима контактира – *grooming*, да би се потом остварила сексуална експлоатација дјетета), 2) контакте усљед којих су дјеца изложена агресивном понашању других корисника (вријеђање и подсмијех обично од других вршњака или *cyberbullying*) 3) контакте путем којих због непромишљености дијете доприноси настанку штетне посљедице (коцкање на интернету, учествовање у пиратерији које може увјетовати каснију одговорност и сл.).[43]

2. Кривични закони, појмовна одређења и заштита дјеце и малољетника

Према одредбама Кривичног закона Босне и Херцеговине – у даљем тексту: КЗ БиХ, дјететом се сматра особа која није навршила 14 година, док се под малољетником подразумијева особа која није навршила 18 година живота (чл. 1. ст. 13. и 14.). Идентичне одредбе садрже Кривични закон Федерације БиХ – у даљем тексту: КЗ ФБиХ и Кривични закон Дистрикта Брчко БиХ, док Кривични законик Републике Српске – у даљем тексту: КЗ РС у чл. 123. 7) под дјететом ако је жртва кривичног дјела, подразумијева особу која није навршила 18 година живота. Закони о заштити и поступању с дјецом и малољетницима у кривичном поступку који су на снази у ентитетима и Дистрикту Брчко БиХ дефинишу дијете као особу која није навршила 18 година живота (чл. 2. ст. 1. ЗЗПДМКП ФБиХ, чл. 2. ст. 1. ЗЗПДМКП РС и ЗЗПДМКП БД БиХ). У вези с наведеним ипак треба правити разлику између, у кривичноправном смислу „дјетета жртве", заправо дјетета на чију штету је почињено кривично дјело у којем случају се ради о особи (дјетету) која није навршила 18 година живота и „дјетета у сукобу са законом" заправо починитеља кривичног дјела, у кривичноправном смислу малољетника, којим се означава особа (дијете) од навршених 14 па до навршених 18 година живота.

У погледу значења израза „компјутерски систем" и компјутерски податак" кривични закони у Босни и Херцеговини не садрже одредбе о значењу наведених израза и они су одређени законима о кривичном поступку. Тако Закон о кривичном поступку Босне и Херцеговине – у даљем тексту: ЗКП БиХ у чл.20. у. као компјутерски систем дефинише сваку направу или групу међусобно спојених или повезаних направа, од којих једна или више њих на основу програма аутоматски обрађују податке, и в) као „компјутерски податак" дефинише свако исказивање чињеница, информација или концепата у облику прикладном за обраду у компјутерском систему, укључујући и програм који је у стању проузроковати да компјутерски систем изврши одређену функцију. Идентичне одредбе садрже и Закон о кривичном поступку Федерације БиХ – у даљем тексту: ЗКП ФБиХ у чл. 20. у) и в), затим Закон о кривичном поступку Републике Српске – у даљем тексту: ЗКП РС у чл. 20. р) и с) те Закон о кривичном поступку Дистрикта Брчко БиХ – у даљем тексту: ЗКП БД БиХ у чл. 20. у) и в). Треба напоменути да сва четири закона дефинишу и значење „телекомуникацијска адреса", што је појам у директној вези с процесуирањем компјутерског криминала. У том смислу „телекомуникацијска адреса" представља сваки телефонски број, линијски или

[43] OEBS

мобилни или е-маил или интернет адресу коју посједује или користи одређена особа [ЗКП БиХ чл. 20. с); ЗКП ФБиХ чл. 21. с); ЗКП РС чл. 20. п) и ЗКП БД БиХ чл. 20. с)].

Кривична дјела компјутерског криминала прописана су ентитетским кривичним законима и Кривичним законом БД БиХ. КЗ ФБиХ прописује кривична дјела компјутерског криминала у Глави XXXII под називом „Кривична дјела против система електронске обраде података". Ради се о слиједећим кривичним дјелима:

1. Оштећење рачунарских података и програма (чл. 393);
2. Рачунарско кривотворење (чл. 394);
3. Рачунарска превара (чл. 395);
4. Ометање рада система и мреже електронске обраде података (чл. 396);
5. Неовлаштени приступ заштићеном систему и мрежи електронске обраде података (чл. 397) и
6. Рачунарска саботажа (чл. 398).

КЗ РС кривична дјела компјутерског криминалитета прописује такође у Глави XXXII под називом „Кривична дјела против безбједности компјутерских података". То су:

1. Оштећење компјутерских података и програма (чл. 407);
2. Компјутерска саботажа (чл. 408);
3. Израда и уношење компјутерских вируса (чл. 409);
4. Компјутерска превара (чл. 410);
5. Неовлаштени приступ заштићеном компјутеру, компјутерској мрежи, телекомуникацијској мрежи и електронској обради података (чл. 411);
6. Спречавање и ограничавање приступа јавној компјутерској мрежи (чл. 412) и
7. Неовлаштено коришћење компјутера или компјутерске мреже (чл. 413);

КЗ БД БиХ као и претходна два закона кривична дјела компјутерског криминала такође прописује у посебној глави. Инкриминисана су у Глави XXXII као „Кривична дјела против система електроничке обраде података". Ради се о слиједећим кривичним дјелима:

1. Оштећење рачунарских података и програма (чл. 387);
2. Рачунарско кривотворење (чл. 388);
3. Рачунарска превара (чл. 389);
4. Ометање рада система и мреже електроничке обраде података (чл. 390);
5. Неовлаштени приступ заштићеном систему и мрежи електроничке обраде података (чл. 391) и
6. Рачунарска саботажа (чл. 392).

Каталози кривичних дјела компјутерског криминала из КЗ-а БД БиХ и КЗ-а ФБиХ практично су идентични како по називима, тако и по законским описима ових кривичних дјела за разлику од КЗ-а РС, који се од њих разликује како по броју прописаних кривичних дјела, тако дијелом и по њиховом законском опису, односно радњи и објекту извршења. Ипак, како детаљна анализа свих тих кривичних дјела није од примарног значаја за наше разматрање, као што је то заштита дјеце и малољетника, то се у њу нећемо нити упуштати.

Овдје треба такођер истакнути како наведена кривична дјела нису и једина кривична дјела компјутерског криминала или криминала у вези с њим, јер се у посебним дијеловима кривичних закона сусрећу и друга кривична дјела која имају обиљежја високотехнолошког криминала, с обзиром на то да се нпр. као средство извршења појављује компјутерски систем, мрежа или комуникација. Наводимо неке од тих примјера:

1. искориштавање компјутерске мреже или комуникације другим техничким средствима за извршење кривичних дјела сексуалног злостављања или искориштавања дјетета (чл. 178. КЗ-а РС);
2. неовлаштено коришћење личних података (чл. 157. ст. 2. КЗ-а РС);
3. повреда приватности дјетета (чл. 189. ст. 2. КЗ-а РС);
4. повреда тајности писама или других пошиљки (чл. 186. ст. 2. КЗ-а ФБиХ);
5. неовлаштено прислушкивање и звучно снимање (чл. 185. КЗ-а БД БиХ) и друга кривична дјела.

У наредном поглављу, а с обзиром и на природу самог водича, слиједи анализа кривичних дјела на штету дјеце и малољетника из одредби ентитетских и Кривичног закона БД БиХ с фокусом на сексуално искориштавање и злостављање. Нагласит ћемо да КЗ БиХ не познаје групу кривичних дјела против сполне слободе и морала, односно сполног интегритета те сексуалног искориштавања и злостављања дјеце. Исте међутим у потпуности или само дјелимично, а када је ријеч о сексуалном злостављању или искориштавању дјеце и малољетника прописују остали кривични закони који су на снази у Босни и Херцеговини.

3. Заштита дјеце од сексуалног злостављања и искориштавања у Босни и Херцеговини

3.1. Република Српска

Република Српска је једина од три законодавне разине у Босни и Херцеговини, на којима се осигурава кривичноправна заштита дјеце и малољетника, која је у оквире својих кривичноправних норми имплементирала и одредбе Конвенције Вијећа Европе о заштити дјеце од сексуалног искориштавања и сексуалне злоупотребе из 2007. (Ланзароте конвенција), а коју је Босна и Херцеговина, како смо то већ претходно установили, потврдила још 2012. године. То се посебно може уочити по чину имплементације потпуно нове групе кривичних дјела сексуалног искориштавања и злостављања дјеце у Глави XV Кривичног законика из 2017. године. Новим рјешењима заштита сполног интегритета дјеце и малољетника те посебно заштита дјеце од сексуалног злостављања и искориштавања остварена је кроз двије групе кривичних дјела: оних из Главе XIV „Кривична дјела против сполног интегритета“ и оних из Главе XV „Кривична дјела против сполног злостављања и искориштавања дјеце“. Управо је потоња група резултат настојања да се што адекватније проведу одредбе Ланзароте конвенције и тиме остваре циљеви спречавања и сузбијања сексуалног искориштавања и злоупотребе дјеце. Но, морамо нагласити и да законодавац у Републици Српској своје опредјељење за остваривањем максималне заштите дјеце од оваквог вида злоупотребе није исказао само увођењем нових инкриминација те унапређењем постојећих већ и имплементацијом других кривичноправних солуција које томе требају допринијети. Овдје ћемо укратко навести неке од њих:

- забрана ублажавања казне у случајевима обљубе над дјететом млађим од 15 година (чл. 54. ст. 3);
- мјера сигурности потпуне забране вршења позива, дјелатности или дужности, при чијем обављању се остварује непосредан контакт с дјецом починиоцу кривичног дјела учињеног на штету сполног интегритета дјетета (чл. 77. ст. 2.);
- осуда за кривично дјело почињено на штету сполног интегритета дјетета неће се брисати из казнене евиденције (чл. 89. ст. 5.);
- вођење посебног регистра у оквиру казнене евиденције о особама које су правомоћно осуђене за кривична дјела на штету сполног интегритета дјетета (чл. 92. ст. 2.);
- почетак тока застаре кривичног прогона за кривична дјела почињена на штету сполног интегритета дјетета тек од дана пунољетства жртве (чл. 96. ст. 3.) и др.

Додатну посебност рјешења у РС-у на подручју кривичноправне заштите дјеце и малољетника чини и постојање Закона о посебном регистру лица правоснажно осуђених за кривична дјела сексуалне злоупотребе и искоришћавања дјеце[44] чији је циљ заштита дјеце од сексуалне злоупотребе, злостављања и искоришћавања, те спречавање лица правоснажно осуђених за та кривична дјела да поново изврше исто или слично кривично дјело.

3.1.1. Кривично дјело искоришћавање дјеце за порнографију (чл. 175. КЗ-а РС)

Кривично дјело "Искоришћавање дјеце за порнографију" прописано је у чл. 175. КЗ-а РС и припада каталогу кривичних дјела из Главе XV "Кривична дјела сексуалног злостављања и искоришћавања". Ово дјело чини онај:

- *(1) ко наводи дијете на учествовање у снимању дјечије порнографије или ко организује или омогући снимање дјечије порнографије;*
- *(2) ко неовлаштено сними, произведе, нуди, чини доступним, дистрибуише, шири, увози, извози, прибавља за себе или за другога, продаје, даје, приказује или посједује дјечију порнографију или јој свјесно приступа путем рачунарске мреже и*
- *(3) ко употребом силе, пријетње, обмане, преваре, злоупотребом положаја или тешких прилика дјетета или односа зависности, присили или наведе дијете на снимање дјечије порнографије.*

За наведене облике кривичног дјела искоришћавања дјеце за порнографију из ст. 1. и 2. прописане су затворске казне у трајању од шест мјесеци до пет година, односно једна до осам година, а за квалификовани облик из ст. 3. казна затвора у трајању од двије до десет година.

У складу са ст. 4. предмети коришћени за извршење овог дјела се одузимају, а порнографски материјал који је настао извршењем дјела се уништава. Важна је одредба ст. 5., према којој се дијете неће казнити за производњу и посједовање порнографског материјала који приказује њега лично или њега и друго дијете ако су они сами тај материјал произвели и посједују га уз пристанак сваког од њих и искључиво за њихову личну употребу. Одредбом

[44] „Службени гласник РС", бр. 31/18

ст. 6. дата је и дефиниција дјечије порнографије као материјала који визуелно или на други начин приказује дијете или је реално приказано непостојеће дијете или особа која изгледа као дијете, у правом или симулираном (експлицитном) евидентном сексуалном понашању или који приказује сполне органе дјеце у сексуалне сврхе. Коначно, ст. 7. прописује да се материјали који имају умјетнички, медицински или научни значај не сматрају порнографијом у смислу овог члана.

3.1.2. Искоришћавање дјеце за порнографске представе (чл. 176. КЗ-а РС)

Кривично дјело "Искоришћавање дјеце за порнографске представе" прописано је у чл. 176. КЗ-а РС и такође припада каталогу кривичних дјела из Главе XV. Ради се о кривичном дјелу које је у оквирима ранијег кривичног законодавства у РС-у било дијелом двију инкриминација "Искоришћавања дјеце и малољетних особа за порнографију" из чл. 199. и "Производња, посједовање и приказивање дјечије порнографије" из чл. 200. КЗ-а РС[45], који више није на снази. Новим рјешењима постаје посебним кривичним дјелом уз инкриминисање и оних који под одређеним околностима гледају порнографску представу у којој учествује дијете.
Ово дјело чини онај

- *(1) ко наводи дијете на учествовање у порнографским представама.*

Прописана казна за ово кривично дјело је казна затвора у трајању од шест мјесеци до пет година. Квалификовани облик дјела прописан је у ст. 2. и њега чини онај:

- *(2) ко употребом силе, пријетње, обмане, преваре, злоупотребом положаја или тешких прилика дјетета или односа зависности, присили или наведе дијете да учествује у порнографској представи. Казнит ће се казном затвора од двије до десет година.*

За овај облик дјела прописана је казна затвора у трајању од двије до десет година. Коначно, у ст. 3. истог члана инкриминисано је и само гледање порнографске представе у којој учествује дијете.

- *(3) ко гледа порнографску представу уживо или путем комуникацијских средстава ако је знао или је требало и могло да зна да у њој учествује дијете.*

Прописана казна је као и за основни облик одјела. Коначно у ст. 4. посебно се прописује да ће се предмети коришћени за извршење дјела одузети, а порнографски материјал који је настао извршењем дјела уништити.

3.1.3. Упознавање дјеце с порнографијом (чл. 177. КЗ-а РС)

Кривично дјело "Упознавања дјеце с порнографијом" прописано је у чл. 177. КЗ-а РС и као и претходна дјела припада каталогу кривичних дјела из Главе XV. Ово дјело чини онај:

- *(1) ко дјетету млађем од 15 година прода, поклони, прикаже или јавним излагањем, посредством компјутерске мреже или других видова комуникације или на други начин учини доступним списе, слике, аудио-визуелни материјал или друге предмете порнографске садржине или му прикаже порнографску представу.*

[45] „Службени гласник РС" бр. 49/2003, 108/2004, 37/2006, 70/2006, 73/2010, 1/2012 и 67/2013

За ово кривично дјело прописана је казна затвора у трајању од шест мјесеци до три године. Као и у случају осталих кривичних дјела на штету дјеце у складу са ст. 2. предмети кориштени за извршење овог дјела се одузимају, а порнографски се материјал уништава.

У ст. 3. дефинише се порнографија под којом се подразумијева материјал који визуелно или на други начин приказује особу у правом или симулираном евидентном сексуалном понашању или који приказује сполне органе људи у сексуалне сврхе.

Коначно, одредбом ст. 4, а када је у питању ово кривично дјело из оквира порнографије, искључују се материјали који имају умјетнички, медицински или научни значај.

3.1.4. Искоришћавање компјутерске мреже или комуникације другим техничким средствима за извршење кривичних дјела сексуалног злостављања или искоришћавања дјетета (чл. 178. КЗ-а РС)

И кривично дјело "Искоришћавање компјутерске мреже или комуникације другим техничким средствима за извршење кривичних дјела сексуалног злостављања или искоришћавања дјетета" из чл. 178. КЗ-а РС припада каталогу кривичних дјела из Главе XV. Ово дјело није познавало раније кривично законодавство РС-а и у потпуности је резултат имплементације Ланзароте конвенције. Ово дјело чини онај:

- *(1) ко с дјететом старијим од 15 година, користећи компјутерску мрежу или комуникацију другим техничким средствима, договори састанак ради вршења обљубе или с њом изједначене сполне радње, или ради производње порнографског материјала, или ради других облика сексуалног искоришћавања и појави се на договореном мјесту ради састанка.*

Прописана казна за основни облик овог дјела је једна до пет година затвора. Квалификовани облик дјела прописан је у ст. 2.:

- *(2) ако је дјело из става 1. извршено према дјетету млађем од 15 година.*

За овај облик дјела прописана казна је од двије до осам година.

3.2. Федерација Босне и Херцеговине

У Федерацији БиХ заштита дјеце од сексуалног злостављања и искоришћавања још се заснива на одредбама које нису усклађене са захтјевима Ланзароте конвенције и које стога тешко да могу у савременим увјетима одговорити захтјевима сузбијања оваквог вида криминалног понашања.

3.2.1. Искоришћавање дјетета или малољетника ради порнографије (чл. 211. КЗ-а ФБиХ)

„Искоришћавање дјетета или малољетника ради порнографије" прописано је чл. 211. КЗ-а ФБиХ и дијелом је каталога кривичних дјела из Главе XIX „Кривична дјела против сполне слободе и морала". Ово кривично дјело чини онај:

- *(1) ко дијете или малољетника сними ради израде фотографија, аудио-визуелног материјала или других предмета порнографског садржаја, или посједује или увози или продаје или распачава или приказује такав материјал, или те особе наведе на учествовање у порнографској представи.*

Прописана казна јесте једна до пет година затвора. У ст. 2. прописује се обавеза одузимања предмета који су били намијењени или употријебљени за учињење овог кривичног дјела као и уништење оних предмета који су настали учињењем кривичног дјела.

3.2.2. Упознавање дјетета с порнографијом (чл. 212. КЗ-а ФБиХ)

Кривично дјело „Упознавање дјетета с порнографијом“ из чл. 212. КЗ-а ФБиХ такође припада каталогу кривичних дјела из Главе XIX истог Закона.
Ово кривично дјело чини онај:

- *(1) ко дјетету прода, прикаже или јавним излагањем или на други начин учини приступачним списе, слике, аудио-визуелне и друге предмете порнографског садржаја или му прикаже порнографску представу.*

Прописана казна јесте новчана или казна затвора до једне године. У ст. 2. прописује се одузимање предмета порнографског садржаја.

3.2.3. Неовлаштено оптичко снимање (чл. 189. ст. 3. КЗ-а ФБиХ)

Кривично дјело “Неовлаштено оптичко снимање” прописано је чл. 189. КЗ-а ФБиХ и припада каталогу кривичних дјела из Главе XVII “Кривична дјела против права и слобода човјека и грађанина”, а за потребе овог Водича је представљено из разлога што један од квалификованих облика овог дјела чини и околност да је почињено према дјетету или малољетнику. Ово кривично дјело чини онај:

- *(1) ко фотографски, филмски или на други начин сними другу особу без њезиног пристанка у њезиним просторијама или ко такав снимак директно пренесе трећем или ко му такав снимак покаже или му на који други начин омогући да се с њим директно упозна.*

Прописана казна за основни облик дјела јесте новчана казна или казна затвора до три године.

Квалификовани облици дјела постоје у случају да:

- *(2) ово кривично дјело почини службена особа у вршењу службе с прописаном казном затвора у трајању од шест мјесеци до пет година као и*
- *(3) ко дијете или малољетника сними ради израде фотографија, аудио-визуалног материјала или других предмета порнографског садржаја, или посједује или увози или продаје или распарчава или приказује такав материјал, с прописаном казном затвора у трајању од једне до пет година.*

Коначно, у ст. 4. прописано је одузимање предмета који су били намијењени или употријебљени за учињење овог кривичног дјела, односно уништење оних предмета који су почињењем овог дјела настали.

3.3. Брчко дистрикт Босне и Херцеговине

Рјешења која сусрећемо у Брчко дистрикту БиХ, а када је у питању заштита дјеце и малољетника од сексуалног злостављања и искоришћавања у потпуности одговарају рјешењима у Федерацији БиХ осим различите енумерације кривичних дјела. Тако је кривично дјело „Искоришћавања дјетета или малољетника ради порнографије" прописано у чл. 208, а дјело „Упознавање дјетета с порнографијом" у чл. 209. КЗ-а БДБиХ. Кривично дјело „Неовлаштено оптичко снимање" прописано је у чл. 186. КЗ-а БД БиХ. Као и у Федерацији БиХ ова су дјела каталогизирана у оквиру Главе ХИХ „Кривична дјела против сполне слободе и морала", односно Главе ХВИИ „Кривична дјела против права и слобода човјека и грађанина".

3.4. Сексуално, односно сполно узнемиравање

На крају да дамо и кратак осврт на кривична дјела сполног узнемиравања, која, иако нису првенствено усмјерена на заштиту дјеце и малољетника, у модерно вријеме заузимају значајно мјесто у оквирима супротстављања протуправном понашању које смјера повреди или угрожавању сполног интегритета појединца. Неријетко, управо је сполно узнемиравање прва иницијална форма недозвољеног понашања која касније прераста у најтеже облике кривичних дјела против сполног интегритета, односно сполне слободе, као што су силовање и друга слична кривична дјела.

Кривично дјело сполног насиља, узнемиравања и сексуалног узнемиравања у Босни и Херцеговини прописано је Законом о равноправности сполова у БиХ.[46] Према чл. 29. наведеног Закона ово кривично дјело чини онај:

- *ко на основу спола врши насиље, узнемиравање или сексуално узнемиравање којим се угрози мир, душевно здравље и тјелесни интегритет.*

Казна прописана за ово кривично дјело је казна затвора од шест мјесеци до пет година. Под насиљем на основу спола наведени закон подразумијева свако дјеловање којим се наноси или може бити нанесена физичка, психичка, сексуална или економска штета или патња, као и пријетња таквим дјеловањем које спутавају особу или групу особа да ужива у својим људским правима и слободама у јавној и приватној сфери живота. Такођер, насиље по основу спола укључује, али се не ограничава на: а) насиље које се дешава у породици или домаћинству; б) насиље које се дешава у широј заједници; ц) насиље које почине или толеришу органи власти и други овлаштени органи и појединци; д) насиље по основу спола у случају оружаних сукоба (чл. 6.). Чл. 5. Закона садржи дефиниције узнемиравања и сексуалног узнемиравања. Тако узнемиравање представља свако нежељено понашање по основу спола којим се жели повриједити достојанство особе или групе особа и створити застрашујуће, непријатељско, деградирајуће, понижавајуће или увредљиво окружење или којим се постиже такав учинак. Сексуално узнемиравање, с друге стране, јесте сваки нежељени облик вербалног, невербалног или физичког понашања сполне природе којим се жели повриједити достојанство особе или групе особа, или којим се постиже такав учинак, нарочито кад то понашање ствара застрашујуће, непријатељско, деградирајуће, понижавајуће или увредљиво окружење. Од кривичних закона у Босни и Херцеговини једино КЗ-а РС прописује кривично дјело сличне природе и то у чл. 170. под називом

[46] Пречишћени текст - "Службени гласник БиХ", бр. 32/10

„Сполно узнемиравање“. За разлику од оног прописаног Законом о равноправности сполова у БиХ, које се гони по службеној дужности, кривично дјело сполног узнемиравања из КЗ-а РС гони се по приједлогу оштећеног и за њега је предвиђена казна затвора у трајању до двије године.

На крају да кажемо и то да у Босни и Херцеговини још нема посебног закона који би установио регистар починилаца кривичних дјела на штету сполног интегритета дјеце и малољетника односно њиховог сексуалног злостављања и искоришћавања. У КЗ-у РС, истина, имплементиране су одредбе о вођењу посебног регистра у оквиру казнене евиденције за починиоце ове врсте кривичних дјела, но нема сумње да би доношење једног таквог закона за простор цијеле Босне и Херцеговине и унификацијом правних рјешења унаприједило сузбијање овог вида криминала. Сматра се да иако доношење једног таквог закона темељем којег би се прикупљали и чували подаци о починиоцима кривичних дјела сексуалног злостављања и искоришћавања дјеце не би ријешило проблем сексуалног злостављања дјеце, ипак би допринијело њиховој бољој заштити, прије свега сталним надзором над особама које су већ осуђене за ова кривична дјела.[47]

4. Grooming – поглавље прилагођено рјешењима у Босни и Херцеговини

Уобичајени начин извршења је да извршилац настоји најприје да дође до „пријатељског“ зближавања порукама које ће код дјетета учврстити увјерење да комуницира с особом која има разумијевања за дјететова размишљања, дијели интересовања за исте друштвене мреже и онлајн игре и сл. Посебан аспект те проблематике се везује управо за дјеловање у кибернетичком свијету, нарочито у виду неспособности дјеце да схвате значај просљеђивања различитих информација различитим путевима на интернету па тако се наводи гдје раде тата или мама, како се родитељи зову, колико година имају, какво им је радно вријеме, када су и колико одсутни од куће, што може бити од користи извршиоцу.

Потом се извршилац окреће ненаметљивом увођењу дјетета у разговоре о интимним стварима, постепеном излагању дјетету сексуално експлицитних материјала. Затим се неагресивно предлаже *screen-to-screen* ћаскање или комуницирање преко web-камере, што обично води даље у добровољно слање властитих компромитујућих фотографија дјетета. Коначно, извршилац договара мјесто и вријеме састанка. Извршиоци се при свему томе лажно представљају или употребљавају податке других малољетних особа као и њихове фотографије да би се лажно представили жртвама као вршњаци. Дешава се да се лажни идентитет употријеби више пута за вршење истих или различитих криминалних радњи.

Онлајн подвођење малољетника је веома фрустрирајуће за многе оптужене јер не захтијева завршни “акт” с малољетном особом, а наиме да је извршено неко од побројаних кривичних дјела. Типичан оптужени ће тврдити “Ја је нисам пипнуо, зашто сам оптужен?” Са становишта одбране окривљени је у суштини оптужен за једноставан чин комуникације на одређени начин с малољетном особом.

За тражење на интернету или онлајн подвођење малољетника начин контакта мора укључивати неку врсту комуникације електронским путем. Докле год је метод електронски и

[47] В. *Заштита дјеце од сексуалног злостављања и искоришћавања: Регистар починилаца кривичних дјела сексуалног злостављања дјеце, потребе и обавеза* (2016). World Vision International у Босни и Херцеговини, Бања Лука

разговор истовремено укључује захтјев за сусрет с дјететом како би се извршило неко од наведених дјела, онда оптужени може бити оптужен за *grooming*.

Када се сагледају искази оштећених особа, може се видјети да су претежно женског спола, а што се тиче посљедица, различито се изјашњавају. Неке жртве наводе да су имале ноћне море, да се плаше да упознају нове људе, да не смију више ноћу да се крећу саме, затворили су профиле и након доста времена још осјећају срамоту јер је нпр. цијела школа видјела голишаве слике или да и даље има осјећај стида пред оцем. Поједине жртве су рекле да је то непријатно искуство довело до раскола у породици, до међусобног окривљавања како између родитеља, тако и између родитеља и дјеце, што је за њих била још додатна фрустрација.

У ситуацији не баш богате домаће судске праксе указат ћемо на нека искуства држава које се одавно у великом броју и већ дуже вријеме суочавају с овим кривичним дјелом. Између осталог, поставило се и питање је ли оптужба неодржива уколико је оптужени имао комуникацију с припадником полиције који се само представљао као дијете? У неким случајевима окривљени су се бранили да су их полицајци агресивно циљали да их увјере да почине кривично дјело које они иначе нису имали предиспозицију да почине. Намјештаљка, клопка, подстрекивање, провоцирано кривично дјело је била теза одбрана. Многе државе у SAD су баш зато промијениле своје законе како би омогућиле осуду засновану на вјеровању окривљеног да разговора с малољетном особом. Још један одбрамбени угао је покушај да се докаже да оптужени није знао да је особа с друге стране малољетна. Већина држава има законе по којима држава није дужна да докаже да је оптужени знао колико је дијете било старо, већ само да је знао да је у питању малољетна особа. Оптужени се бране и позивањем да су му прекршена права на слободу говора, али таква одбрана није успјешна. Примјер сљедећег навода одбране је да је разговор био само онлајн фантазија или доказивање да окривљени никада није ни намјеравао да заиста сусретне малољетника. Имајући у виду га је извршење овог кривичног дјела по нашем законодавству неопходно да се извршилац појави на мјесту састанка, случајно затицање на истом мјесту би било тешко прихватљиво.

Посљедњих година уочена је појава *секстинга* (кованица од ријечи секс и текстинг) веома заступљена међу тинејџерима, која подразумијева размјену текстуалних порука експлицитног садржаја и фотографија на којима се виде наги дијелови тијела и/или сексуални чин. Поруке и фотографије се прије свега размјењују између вршњака, с тим што једанпут послата порука лако стиже до оних којима није била намијењена. Висок процент адолесцената практикује данас секстинг, а све више се сада говори о посљедицама које такво понашање може изазвати у тинејџерским годинама. Грешка младог човјека може довести до одбацивања или исмијавања од вршњака, али и посљедица коју секстинг може имати и на друштвени углед па чак и каснију могућност запослења. Излагање фотографија и личних података може резултовати негативним посљедицама и онда када није ријеч о фотографијама које приказују нагост. Фотографије се могу смјестити у негативан контекст, попраћене негативним коментарима, што може погубно утјецати на самопоуздање дјетета.

Овдје ће се приказати занимљив примјер из америчке државе Илиноис, гдје особа врши кривично дјело дјечије порнографије ако сними или фотографише особу за коју зна је млађа од 18 година и која је ангажована у било ком сексуалном акту или у пози која укључује непристојно приказивање наге особе или гениталија, стидне области, задњице или женских груди. Не постоји изузетак за сликање себе. Тражење или мамљење особе за коју треба знати да је млађа од 18 година да се појави на таквој слици или на видеозапису се санционише као дјечија порнографија, али и просљеђивање секстинг порука другима или ширење таквих слика другима. Дјело врши и особа која, знајући садржај или природу,

посједује фотографију или филм који приказује некога за кога треба знати да је малољетан. Посједовање се сматра вољним, кад особа "свјесно набави или добије" незаконити материјал "с довољно времена да оконча посједовање."

Сљедећи примјер ставља претходно наведена дјела у перспективу: 16-годишња дјевојка која снима сексуалну слику себе полуголе и пошаље је као телефонску поруку свом дечку извршила је најмање три кривична дјела: стварање, ширење и посједовање дјечије порнографије. Ако јој је њен дечко тражио да му пошаље такву поруку, он ће одговарати за најмање два кривична дјела: навођење и добровољно посједовање сексинг поруке. Тако једна не баш мудра младалачка несмотреност може резултовати у пет кривичних дјела и неколико тинејџера је спреман за уписивање у регистар "сексуалних пријеступника."[48]

5. Виртуелно злостављање (Cyberbullying)

Bullying - вршњачко насиље је нежељено, агресивно понашање међу дјецом школског узраста које укључује стварну или перципирану неравнотежу моћи. Cyberbullying је такво понашање које се јавља на интернету употребом пријетећег или злог језика у намјери узнемиравања или емоционалног повређивања једне особе или групе људи, слањем текстуалних порука, електронске поште у онлајн игрицама, собама за чатовање, на дискусионим групама или web-страницама и др.

Понашање се понавља или има потенцијал да се понови током времена. Дјеца која су малтретирана, али и она која малтретирају друге могу имати озбиљне трајне проблеме. Потреба да се други малтретира обично потјече из насилног понашања негдје другдје у животу дјеце која у школама или на другим мјестима понављају она понашања која су искусила, видјела или научила код куће.

Као један од почетних корака за извршење кривичног дјела је и крађа идентитета. Информације од значаја за извршиоце кривичних дјела који се баве крађом идентитета широм свијета обухватају имена и презимена, адресе, здравствене податке и све друго што касније могу злоупотријебити. За крађу идентитета врло често се употребљавају рачунарски вируси који обављају функције као што су снимања откуцаја карактера на тастатури *(Keylogger)*, снимање процеса на мониторима рачунара *(Screen Logger),* редирекције интернетског саобраћаја, убацивање "тројанаца" у систем, крађа личних и других података корисника и њему блиских особа. До личних података може се доћи и без коришћења рачунара крађом података из личне поште, крађом електронских уређаја - мобилних телефона, таблета или проналажењем заборављених или изгубљених предмета у којима се налазе лични подаци као што су новчаници, нотеси и телефонски именици. У оквиру цубербуллунга говори се и о крађи или погађању лозинке дјетета, па се затим та лозинка мијења или се блокира, закључава, тако да дијете више не може приступити свом налогу. Послије крађе обично слиједи злоупотреба идентитета, која подразумијева употребу личних података неке особе који су претходно прибављени без њеног знања и одобрења за извршење кривичних дјела под њеним идентитетом.

Када се говори о насиљу преко интернета, оно између осталог подразумијева:

- слање узнемирујуће поруке е-маилом или на чату,
- слање порука непримјереног садржаја,

[48] https://www.isba.org/ibj/2010/04/sextingitsnojokeitsacrime

- слање нежељене поште, спамова и вируса путем електронске поште или на било који други начин на интернетској мрежи,
- слање фотографија које вријеђају достојанство, интегритет, слободу и сигурност,
- крађу или промјену лозинке за е-маил или надимак на чату,
- објављивање приватних података или неистине на чату, блогу или интернетској страници,
- постављање интернетске анкете о жртви,
- потицање говора мржње и мржње уопће на интернету,
- потицање комуникације увреда и ниподаштавања,
- прослеђивање туђих фотографија и тражење коментара или било каквог садржаја о другом са захтјевом за коментарисање,
- повређивање приватности упадањем у туђи компјутер и читањем туђих садржаја комуникације на интернету,
- лажно представљање и употребу лажног идентитета,
- производњу и дистрибуцију дјечије порнографије[49].

Осим наведених, примјери онлајн насиља подразумијевају и слање пријетњи, провокативних увреда или расне или етничке увреде, сексуално погрдно обраћање, дијељење примљених е-маилова без дозволе оног који га је написао, застрашивање и пријетње или стварно насиље или други облици дискриминације усмјерени на особе које су (или за које извршилац сматра да су) припадници ЛГБТ популације, затрпавање е-маил инбоха насилним порукама, дијељење слика снимљених у непријатним ситуацијама, без дозволе особа на фотографији, увјеравање других да искључе неког из заједнице (*online* или *offline*), постављање или ширење лажних информација о особи с циљем да се повриједи та особа или њена репутација, слање у више наврата непријатних, злих порука, ругање, сплеткарење.

Овдје треба указати на то да је Протоколом поступања у установи у одговору на насиље, злостављање и занемаривање[50] наведено да се насиље и злостављање може јавити као физичко, психичко (емоционално) и социјално. Осим наведених облика, насиље и злостављање препознаје се и кроз: злоупотребу, сексуално насиље, експлоатацију дјетета и ученика, електронско насиље и др. Електронско насиље и злостављање је злоупотреба информационих технологија која може имати за посљедицу повреду друге личности и угрожавање достојанства и остварује се слањем порука електронском поштом, SMS-ом, MMS-ом, путем web-странице, чатовањем, укључивањем у форуме, социјалне мреже и сл.

Облици психичког насиља и злостављања су нарочито: омаловажавање, оговарање, вријеђање, ругање, називање погрдним именима, псовање, етикетирање, имитирање, "прозивање", уцјењивање, пријетње, неправедно кажњавање, забрана комуницирања, искључивање, манипулисање, застрашивање. Облици социјалног насиља и злостављања су нарочито: добацивање, подсмјехивање, искључивање из групе или заједничких активности, фаворизовање на основу различитости, ширење гласина, сплеткарење, ускраћивање пажње од групе (игнорисање), неукључивање, неприхватање, манипулисање, искориштавање, пријетње, изолација, малтретирање групе према појединцу или групи, организовање

[49] http://internetbezbednost.weebly.com/105310721089108011131077-10851072-108010851090107710881085107710901091.html
[50] "Службени гласник РС", бр. 30/2010

затворених група (кланова), што за посљедицу има повређивање других. Облици сексуалног насиља и злостављања су нарочито неумјесно са сексуалном поруком: ласцивни коментари, ширење прича, етикетирање, показивање порнографског материјала, показивање интимних дијелова тијела, свлачење. Облици насиља и злостављања злоупотребом информационих технологија и других комуникационих програма су нарочито: узнемиравајуће позивање, слање узнемиравајућих порука SMS-ом, MMS-ом, оглашавање, снимање и слање видеозаписа, злоупотреба блогова, форума и чатовања, снимање камером појединаца против њихове воље, снимање насилних сцена камером, дистрибуисање снимака и слика, дјечија порнографија. Све наведено, иако се тиче просвјете, а имајући у виду да се говори о вршњачком насиљу, може бити од користи како тужиоцима, тако и судијама у предметима по којима ће поступати ради правилне оцјене да ли се у конкретном случају може несумњиво (у)тврдити да се ради о противправном понашању.

Cyberbullyng се углавном посматра као ситуација када једно дијете одабере као циљ друго дијете, користећи интерактивну технологију. Вршњачко насиље може трајати много дуже него што траје школовање и прати жртве свуда гдје год користе своје мобилне телефоне или гдје се логују на интернет, може се догађати 24 сата дневно, седам дана у недјељи, у било које доба дана или ноћи, може доћи до дјетета чак и када је само. Поруке и слике могу се објавити анонимно и брзо се дистрибуисати широкој публици. Може бити веома тешко, а понекад и немогуће пратити извор док је брисање непримјерених или узнемирујућих порука, текстова и слика готово немогуће након објављивања или слања.

Постоје два начина cyberbullynga, а то су директни напади, тј. поруке које су послате дјетету директно или оне које су послате преко других, који им у томе требају помоћи, без обзира на то јесу ли они тога свјесни. То је cyberbullyng помоћу *proxyja*, који често обухвати и одрасле који су укључени у то и самим тим је због тога и опаснији за више особа.

Директни напади се извршавају путем текстуалне поруке, понекад и хиљаде текстуалних порука на мобилни телефон, када дјеца шаљу поруке мржње или пријетеће поруке другој дјеци, а да понекад нису да свјесни да су, иако нису изречене у стварном животу, такве поруке веома подобне да повреде и умију бити веома озбиљне. Ови напади могу бити и на блоговима или на web-страницама. Наиме, данас су дјеца толико технолошки описмењена да знају креирати интернетску страницу специфично дизајнирану како би се неко вријеђао. Даље, дјеца врло често фотографишу друге у свлачионицама или уколико су у могућности у купатилу, тоалетима и онда постављају те слике или их шаљу другима путем мобилних телефона. Директни напади чине дјеца која шаљу вирусе или *spyware* и који на тај начин просто шпијунирају своју жртву. "Тројанци" такође омогућују cyberbullyng и то на тај начин да контролишу с даљине рачунар жртве или користе своја умијећа како би се избрисао хард диск жртве.

Internet polling представља неку врсту анкете којој се постављају питања и позивају други да гласају ко је од понуђених вршњака најдебљи, најружнији итд. Такође, могу се поставити питања типа ко је згодан или згодна, а ко није, или *who's hot, who's not*, или ко је највећа "дроља" или „највећа даска" у одређеном разреду. Питања су углавном веома увредљива, а оно што је најстрашније јесте да су их креирала дјеца или тинејџери. Што се тиче *gaminga*, огроман број дјеце игра интерактивно игрице било на *sony playstationu*, *xbox liveu* или рачунару. Игра се често онлајн и пружа се могућност међусобне комуникације путем чатовања или *live internet* везе с било ким ко истовремено игра. Тада понекад дјеца вербално малтретирају другу дјецу, користе пријетње или неки ружан рјечник, а понекад чак иду и корак даље, искључујући их из игара или шире некакве лажне вести о њима.

Cyberbullyng помоћу прохуја је један од најозбиљнијих и најопаснијих врста, јер врло често укључује одрасле особе. То се најчешће чини тако што се малтретирање уствари спроводи преко некога ко обавља "прљав посао", врло често без своје воље и без знања да се то чини уопће. *Warning* или *notify words* су примјери оваквог cyberbullynga путем прохуја. Дјеца, наиме кликну на дугме за упозорење или за обавјештење на свом екрану, или чату или на е-маил страници и на тај начин упозоравају пружаоца интернета да је жртва учинила нешто што крши њихова правила. Пружаоци услуга су упознати с овом врстом злоупотребе, често провјеравају да би видјели да ли је упозорење заиста оправдано. Али све што извршилац треба учинити је да довољно разљути жртву толико да она сада заиста пошаље некакав ружан коментар или коментар пун мржње. Тачније, да узврати таквим коментаром што је довољно, па у таквој ситуацији, пошто је провајдер већ једанпут упозорен (лажно), поново се упозорава на исти начин тако се представља као да је жртва та која је све започела. У том случају пружалац интернетског сервиса је уствари један недужни саучесник у овом процесу виртуелног насиља. Понекад су ти нежељени саучесници и родитељи саме жртве. Уколико извршилац може учинити да изгледа као да жртва ради нешто погрешно, лоше и о томе обавијести жртвине родитеље, велика је вјероватноћа да ће родитељи казнити жртву.

Врло често ће се десити да извршиоци злонамјерно региструју жртву за "е-маилинг" или за инстант поруке на порнографским страницама. Тада се деси да жртва прими стотине е-маилова од таквог сајта. Осим овога, може бити и много озбиљније, а то је у ситуацијама када извршиоци постављају информације о жртви у собама за чатовање злостављача дјеце и чак рекламишући жртву за секс. Онда они просто само сједе и чекају да чланови те *хате* групе или групе за злостављаче дјеце нападају или контактирају жртву било онлајн, а понекад чак и offline. Замјеном личности, односно представљајући се као жртва, извршилац може начинити значајну штету. Они могу поставити провокативну поруку у соби за чатање неке *хате* групе и на тај начин позивају на напад према жртви, врло често остављају име, адресу, па и телефонски број жртве, што даље проузрокује да *хате* група има врло лак посао. Друго, извршиоци често шаљу поруку некоме представљајући се да су они уствари жртве, говорећи неке пријетеће ствари или говор мржње. Такође, они могу измијенити поруку која долази од жртве, тако да замијене улоге у тексту, представљајући да је жртва уствари рекла ружне ствари о неком другом.

Cyberbullyng је ситуација када су у цијелу причу укључени само малољетници и то с обје стране, било као извршилац било као жртва или макар треба бити иницирано од малољетника према другом малољетнику. Извршиоци увијек код вршњачког насиља покушавају укључити што више других у цијелу ову причу. Одрасли се могу укључити у ову причу најчешће када се управо на ове сајтове за злостављаче дјеце или за сексуалне "предаторе" заинтересују за те постове, нарочито уколико је постављен навод да је жртва заинтересована наводно за секс, што може да води у *grooming*. У стварности се врло често дешава и да у једном тренутку онај ко је жртва постане извршилац и обратно. Посљедице могу бити од оних које нису тако угрожавајуће, до убиства почињена или до самоубистава почињених након што је неко био укључен у cyberbullyng.

Кад је ријеч о мотивима извршиоца, врло често се ради о неком бијесу, освети или просто фрустрацији. Некада то чине ради своје "забаве" или зато што им је досадно, или имају превише времена и превише *гадгета*, односно превише технолошких "играчки" које су им доступне. Многи то чине просто ради стјецања пажње или просто реакције других. Дешава се и да се то учини случајно, или се пошаље порука погрешном примаоцу, или се не размишља пре него што се било шта од свега наведеног до сада учини. Они који су жељни неке надмоћи или моћи над другима то чине да би мучили друге или због свог ега.

Међутим, треба имати у виду да је могуће и погрешно разумијевање. Откуцана ријеч просто не може исказати какав тон би пратио изговорену ријеч и свакако се значајно разликује од информације коју бисмо добили када бисмо чули глас особе која се обраћа или видјели говор тијела. Треба, дакле, размишљати и о објективном критерију добијених информација приликом процјене или оцјене, а не да се оне базирају само на томе како су се те ријечи учиниле жртви, водећи свакако рачуна о узрасту, с обзиром да та оцјена може бити погрешна и понекад се тешко може избјећи да се ријечи протумаче изван контекста. Те ријечи, уколико нису праћене неким емотиконом или акронимом као *јк*, у смислу *just kidding* могу бити погрешно схваћене. Све то онда даље може да резултира у повријеђеним осјећањима, у љутњи и бијесу, у фрустрацији или у осјећају страха или просто осјећају да неко прије ти.

Преглед судске праксе

Рјешењем Вијећа за малољетнике према малољетној особи је изречена мјера упозорења судског укора и то због кривичног дјела угрожавања сигурности из члана 138 став 1. Наиме, малољетна особа је угрозила сигурност оштећене малољетне особе на тај начин што је са свог мобилног телефона на његов упутила поруку садржине "Исели се из нашег града, било би ти боље... црно ти се пише". Бранила се тако што је рекла да је била с другарицом у пицерији када јој је она испричала да је оштећени причао за њу да је трудна и да је курва. Затражила је његов број телефона и са свог му послала поруку с наведеном садржином. Оштећени је у свом исказу навео да се уплашио за своју личну сигурност, јер су ријечи "црно ти се пише" биле написане великим словима, а поруку је примио с непознатог броја. Суд је у току доказног поступка извршио увид у криминалистичко-техничку документацију, утврдио текст поруке, датум слања и број с којег је послата, а потом је извршен увид и у листинг одлазних порука с мобилног телефона малољетне. Суд је закључио да се у радњама малољетне стичу сви законски елементи кривичног дјела из члана 138. став 1. налазећи да порука с наведеном садржином представља озбиљну пријетњу с обзиром на то да је објективно подобна да код онога коме се пријети односно оштећеног изазове осјећај страха или несигурности, што је оштећени потврдио.

Други примјер за исто кривично дјело је пресуда којом је окривљени проглашен кривим што је угрозио сигурност оштећеног пријетњом да ће напасти на живот и тијело те особе на тај начин што је на мрежи Facebook са свог корисничког профила послао оштећеном пријетеће поруке између осталог и садржине "Мртав си, мајмуне, одробијат ћу те", а потом је на свом корисничком профилу поставио слику на којој се налазио оштећени са заокруженом главом на којој је био постављен текст "Последњи поздрав".

Примјер за кривично дјело из члана 138. став 2. је пресуда којом је окривљена проглашена кривом што је са свог кућног рачунара угрозила сигурност више особа двије оштећене, пријетњом да ће напасти на њихов живот и тијело тако што је на интернетској презентацији друштвене мреже Facebook с корисничког профила, који је креирала под лажним именом, на кориснички профил малољетне оштећене упутила пријетње: "Слушај мала, поручи мами да се смири да јој не би јебали маму, ..., реци јој да се смири да не би ми тебе малтретирали ... ово је посљедња опомена, доћи ћу и развалит ћу је од батина".

Пред Вишим судом у Београду донесена је пресуда којом је прихваћен споразум о признању кривичног дјела искоришћавања рачунарске мреже или комуникација другим техничким средствима за извршење кривичних дјела против сполне слободе према малољетној особи из члана 185 б. став 1. КЗ-а у вези с чланом 184. став 2. у вези са ставом КЗ-а у вези с чланом 30 КЗ-а и то које је окривљеном стављено на терет. Окривљени је

проглашен кривим што је у стању урачунљивости свјестан свог дјела да је забрањено, при чему је хтио његово извршење, у намјери да изврши кривично дјело посредовања у вршењу проституције из члана 184. став 2. у вези са ставом 1., користећи рачунарску мрежу с умишљајем покушао да договори састанак с малољетном оштећеном особом старом 13 година на тај начин што је са свог мобилног телефона електронским путем користећи свој профил на Facebooku ступио у контакт с оштећеном, којој је најприје послао захтјев за пријатељство да би након што га је оштећена прихватила и саопћила му да има 14 година, почео да јој шаље поруке сексуалне садржине као и поруке којима је наводи и потиче на проституцију : "Ћао мачкице, ајде да ти дам 500 еура мјесечно за повремено виђање у тајности", "Важи мачкице моја ..... ако будеш добра у кревету, онда и више ћеш да добијеш, јеси већ водила љубав с неким" и слично, након чега је тражио број телефона оштећене, а након чега је оштећена прекинула комуникацију с њим. Осуђен је на казну затвора у трајању од једне године, која ће се извршити у кућним увјетима уз електронски надзор и изречена је новчана казна у износу од 50.000,00 динара као и мјера сигурности одузимања предмета, рачунара, мобилних телефона. Према окривљеном је на основу члана 89а КЗ-а изречена мјера сигурности забране приближавања и комуникације с оштећеном и то на удаљености мањој од 200 метара, стану у којем оштећена живи и основној школи коју похађа малољетна оштећена, а затим је на основу члана 7. став 1. тачка 2. и 3. Закона о посебним мјерама за спречавање вршења кривичних дјела против сполне слободе према малољетницима (тзв. Маријин закон) према окривљеном изречена мјера забране посјећивања мјеста на којима се окупљају малољетне особе (вртићи, школе и слично) и обавезно посјећивање професионалних савјетовалишта и установа. Одређено је да ће се мјере спроводити послије издржане казне затвора, најдуже 20 година послије извршене казне затвора, с тим што ће суд по службеној дужности по истеку сваке четири године од почетка примјене ових мјера одлучити о потреби њиховог даљег спровођења.

Примјер за 185б КЗ-а је још један прихваћен споразум о признању кривичног дјела којим је окривљени проглашен кривим што је у намјери да изврши обљубу над дјететом користећи рачунарску мрежу с умишљајем покушао да договори састанак с оштећеним дјететом старим 11 година на тај начин што је са свог мобилног телефона електронским путем преко интернета на друштвеној мрежи Фацебоок, на којем се лажно представљао као 12-годишњи дјечак, ступио у контакт с оштећеним дјечаком, представљајући се као дјечак који га зна с фудбала да би након тога почео да му шаље поруке сексуалне садржине напримјер "Кад би те ухватио, оборио би те у кревет, онда би ти ноге раширио и онда знаш", "Знаш гдје би те јебао, ставио би ти моју киту и јако те ударао, дал да будем јако груб или мало према теби, оћеш да ти кажем како би те растурио, знаш шта волим да радим дјечацима после утакмице", да би му послао поруке у којима наводи да жели да дође на тренинг одређеног датума, упозна се с малољетним оштећеним те да ће доћи у свлачионицу након тренинга, након чега је оштећени прекинуо комуникацију с њим. Осуђен је на казну затвора у трајању од једне године и то у просторијама у којима станује, изречена је мјера сигурности одузимања мобилног телефона и SIM-картица, а примијењена је одредба члана 89а КЗ-а изречена мјера сигурности забрана приближавања и комуникације с оштећеним и то на удаљености од 200 метара, забрањен је приступ у простор око мјеста становања око школе коју малољетни похађа и 200 метара од школе фудбала те спортске сале, забрањено му је узнемиравање оштећеног односно даља комуникација с оштећеним и та мјера према изреци пресуде може трајати најдуже три године. Примијењена је и одредба члана 7. став 1. тачка 2. и 3. Закона о посебним мјерама за спречавање вршења кривичних дјела против сполне слободе према малољетницима и то забрана посјећивања мјеста на којима се окупљају малољетне обавезе и обавезно посјећивање професионалних савјетовалишта и установа.

Примјер је и пресуда којом је окривљени проглашен кривим због извршења кривичног дјела из члана 185. став 2. у вези са ставом 1. у вези с чланом 180. став 1. и због извршења кривичног дјела из члана 185. став 4. КЗ-а и то зато што је у намјери да изврши обљубу с дјететом, користећи рачунарску мрежу и комуникацију другим техничким средством – мобилним телефоном, с умишљајем договорио састанак с малољетном оштећеном особом старом 12 година и појавио се на договореном мјесту ради састанка, тако што је електронским путем, преко интернета, на друштвеној мрежи Facebook, користећи свој кориснички профил, ступио у контакт с оштећеном особом, упутио јој поруку: "Лијеп поздрав за тебе, хвала ти за додавање... врло си лијепа и посебна... волио бих да се више упознамо... ако си мало више знатижељна, имам неке јако лијепе приче за тебе, интригантне... посебне... врло си слатка... женствена и врло сексi", након чега је малољетна оштећена пријавила поруку својој мајци, која је промијенила лозинку наведеног профила, наставила комуницирати с окривљеним, представљајући се као дијете, да би након тога окривљени у порукама које су послате преко ове мреже почео да јој упућује поруке експлицитног садржаја, са сексуалном конотацијом попут: "Јако бих волио да те дирам и још нешто... па нормално да желим да уђем у тебе или да те јебем... како хоћеш... рецимо да својом руком стављам у тебе... и да те гледам и слушам како свршаваш... узимам само најбоље и најмлађе... много волим да јебем три цурице у круг... најмлађа 12... оне двије старије за годину... добију поклон, али ја одлучујем о томе, ако ти се буде посрећило, можда га и ти примиш.... јако желим да ти га трпам и у гузу, да ти свршавам у уста, по сисама... колике су ти...", све вријеме у увјерењу да комуницира с дјететом, након чега је договорио да се с дјететом састане у Београду, при чему се појавио на заказаном састанку како би се упознао с дјететом, у намјери да изврши кривично дјело обљуба с дјететом из члана 180. став 1. КЗ-а, након чега је лишен слободе, као и што је посједовао 606 слика порнографске садржине, насталих искориштавањем малољетних особа, а што је пронађено приликом претреса стана у којем станује. Према окривљеном је изречена мјера сигурности одузимања предмета – лаптопа, двије флеш меморије, један мобилни телефон и примијењена одредба члана 7. у вези с чланом 9. и 10. Закона о посебним мјерама за спречавање... и то забрана посјећивања мјеста на којима се окупљају малољетне особе, као што су школске зграде, школска дворишта, вртићи, игралишта, дјечије манифестације и сл., као и обавезно посјећивање професионалних савјетовалишта и установа према програму који ће му бити одређен од организационе јединице Управе за извршење кривичних санкција, надлежне за третман и алтернативне санкције. Наведене мјере ће се спроводити према окривљеном након издржане казне затвора.

Апелациони суд у Београду је одбио као неосновану жалбу браниоца окривљеног и потврдио наведену пресуду. У образложењу одлуке се наводи да постојање комуникације између два профила на друштвеној мрежи Facebook дјетета и окривљеног, телефонским путем преко SMS-порука и позива те садржине порука није спорио ни окривљени, а потврђена је писменим доказима у списима и то записником о претресању стана и других просторија, потврдом о привремено одузетим предметима, извјештајем о прикупљању података из мобилних телефона, вјештачењем CD-медија (преглед уређаја) као и извјештајем МУП Дирекције полиције УКП. Оптужени се бранио да није заинтересован за дјецу и дјевојчице млађег узраста као и за дјечију порнографију, али и да није комуницирао с дјететом, већ да је све вријеме знао да се дописује с мајком. Међутим, таква одбрана основана од првостепеног суда није прихваћена као вјеродостојна. Несумњиво је утврђено да је окривљени и раније током 2013., 2014. и 2016. године користећи рачунарску мрежу контактирао с малољетним дјевојчицама других корисничких профила, садржина тих порука такође је сексуалне конотације, што је првостепени суд несумњиво утврдио из вјештачења CD-медија. На лаптоп-рачунару који је од окривљеног одузет као и на двије USB флеш

меморије пронађено је и одузето укупно 606 фотографија с дјечијом порнографијом, а посједовање таквог материјала окривљени није спорио, а потврдили су га и писани докази у списима. Да је окривљени све вријеме комуникације током које је договорио састанак с малољетном оштећеном био увјерен да их шаље дјетету, да је то и хтио управо у намјери да изврши обљубу с дјететом, првостепени суд је несумњиво утврдио како из садржине послатих порука које се у већини односе на сексуалне односе с дјецом, тако и оцјеном осталих писаних доказа у списима, али и исказа мајке малољетне, свједока који је у свему сагласан с материјалним доказима. Даље је суд утврдио да је окривљени дошао на договорени састанак, да је мијењао мјесто гдје ће се наћи инсистирајући да то буде на аутобуској станици, да ће он стајати у бочној улици и бити у паркираном возилу с укљученим жмигавцима, да малољетна дође до кола, а у телефонском разговору је и поновио да јој је понио мобилни телефон који јој је претходно обећао.

Примјер за кривично дјело приказивање, прибављање и посједовање порнографског материјала и искориштавање малољетне особе за порнографију из члана 185. став 3. у вези са ставовима 1. и 2. и ставом 4. КЗ-а и кривично дјело искориштавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дјела против сполне слободе према малољетној особи из члана 185б. став 2. у вези са ставом 1. КЗ-а у вези с чланом 180. став 1. КЗ-а у вези с чланом 30. КЗ-а је и поступак у којем је окривљеном стављено на терет да је учинио доступним слике и аудио-визуелни материјал порнографске садржине дјетету старом осам година и у више наврата искористио дијете за производњу слика порнографске садржине на тај начин што је преко интернета путем друштвене мреже Facebook преко свог корисничког профила ступио у контакт с оштећеном особом и у више наврата слао слике свог сполног органа у ерекцији и приликом ејакулације и видеоснимак на којем се самозадовољава те од оштећене особе захтијевао да му шаље своје слике на којима је она нага и при том давао упутства на који начин и које дијелове да слика, што је она учинила и послала му укупно осам слика те је на електронски начин учинио доступним наведене слике порнографске садржине настале искориштавањем малољетне особе тако што је преко Facebooka послао три фотографије на којој је малољетна оштећена нага корисницима других профила. Осим тога, окривљеном је даље стављено на терет да је у периоду од недјељу дана у намјери да изврши обљубу с дјететом користећи рачунарску мрежу Facebook с умишљајем покушао договорити састанак с оштећеном на тај начин што је упутио више порука сљедеће садржине "А знаш да ми је велики, ја мислим да ти не би цио могао стати, хоћемо пробати једном то, мислим да видимо да ли би ти могао стати, па једино да ти дођеш код мене, јер би хтјела да једну ноћ спавамо заједно", али с умишљајем започето дјело није довршио јер је оштећена прекинула контакт с њим. Предложени су докази: записник о претресању стана и других просторија, потврда о привремено одузетим предметима, извјештаји службе за специјалне истражне методе о вјештачењу хард диска одузетог од окривљеног, дио комуникације издвојен у фотодокументацији, комуникација између окривљеног и корисника профила на које је слао фотографије. Предложено је да се изврши увид у садржај медија који је достављен уз извјештај вјештачења електронске опреме одузете од окривљеног и то слика као и видеоклипа који се налазе у означеном фолдеру као и садржаја CD-медија достављеног списима.

Сљедећи примјер је кривично дјело из члана 185. став 3. у вези са ставом 2. у стицају с кривичним дјелом принуде из члана 135. став 1. и осуђујућа пресуда којом је окривљени проглашен кривим да је искористио дијете старо 13 година за производњу слика и видеоклипова порнографске садржине. Озбиљном пријетњом да ће фотографије оштећене на којима се налази без одјеће и видеоснимак на којем је приказана оштећена без горњег дијела одјеће поставити на интернет принудио је оштећену да нешто учини на тај

начин што је користећи друштвену мрежу Facebook креирао више лажних профила, затим од малољетне захтијевао да се фотографише и свлачи пред web-камером која је инсталирана на њеном рачунару, да приказује своје голе груди, свој сполни орган – вагину, при чему је све то снимао и чувао на свом рачунару. Наведени материјал је користио да би пријетио оштећеном дјетету да ће фотографије објавити јавно и доставити њеним пријатељима и на тај начин је принудио да му и даље доставља своје наге фотографије и свлачи се пред web-камером те када је малољетна хтјела да прекине контакт, пријетње је остварио поставивши наведене слике на "зид" налога на Facebooku оштећене и потом их послао њеним пријатељима из основне школе. За наведена кривична дјела утврђене су му појединачне казне и то уз примјену ублажавања, најприје за члан 185. став 3. у вези са ставом 2. казна затвора у трајању од десет мјесеци, а за кривично дјело принуда из члана 135. став 1. казна затвора од три месеца те је осуђен на јединствену казну затвора у трајању од једне године, која се има извршити у просторијама у којима осуђени станује. Изречена је и мјера сигурности одузимања телефона, кућишта desktop-рачунара и SIM-картица.

Примјер за кривично дјело приказивање, прибављање и посједовање порнографског материјала и искоришћавање малољетне особе за порнографију из члана 185. став 2. у вези с чланом 33. КЗ-а је и примјер пресуде којом су окривљени проглашени кривим што су искористили малољетног оштећеног за производњу аудио-визуелног предмета порнографске садржине и порнографску представу тако што су га наговорили да има сексуални однос с кобилом, за које вријеме је један окривљени држао кобилу за узде спречавајући је да се удаљи с лица мјеста, а други окривљени држао реп како би омогућио малољетном оштећеном да има сполни однос с кобилом потичући га на то, а за то вријеме је трећи окривљени снимио сполни однос телефоном и снимак поставио на Youtubeu. За наведено кривично дјело изречене су им увјетне осуде.

Сљедећи примјер је примјер укинуте пресуде за кривично дјело из члана 185б КЗ-а којом је окривљени, студент, неосуђиван, проглашен кривим што је у намјери да изврши недозвољену сполну радњу над малољетником, користећи рачунарску мрежу и комуникацију, путем мобилног телефона договорио састанак с оштећеном малољетном особом и појавио се на договореном мјесту ради састанка, преко интернета, електронским путем, на друштвеној мрежи Facebook, користећи лажни профил, лажно се представљао као дјевојка која се бави манекенством, ступио у контакт с оштећеном особом која је имала 14 година, упутио јој поруку да је лијепа и згодна, питање "да ли би жељела да се бави фотомоделингом", да ће увијек имати шта пожели, шминку, гардеробу, упитао које је годиште, а оштећена је све ово пријавила свом оцу, који је с њом наставио комуницирати с окривљеним, да би након тога окривљени у порукама почео упућивати питања "какав доњи веш носи, да ли носи халтере и штикле, да ли пије и сл.", послао јој је поруку у којој је навео да уколико жели на лакши начин да постане фотомодел, може да оде код његовог шефа, да му "издрка" или "попуши", а ако то не жели да уради њему, може имати сексуални или орални однос с његовим сином, након чега је тражио број мобилног телефона, па пошто му га је она послала, оштећеној је послао поруку да ће број телефона прослиједити шефовом сину, који ће с њом комуницирати путем мобилног телефона, потом ју је контактирао, договорио се да се с њом састане у ресторану, појавио се на састанку, рекао јој да га сачека да уђе у мушки тоалет, да ће је позвати одатле и да га орално задовољи, да би након уласка у тоалет позвао телефоном оштећену и рекао јој: "Ајде, гдје си више, чекам те". Првостепеном пресудом је проглашен кривим и осуђен на казну затвора у трајању од шест мјесеци и новчану казну у износу од 50.000,00 динара, одузет му је мобилни телефон и кућиште за компјутер и изречена мјера у смислу члана 89а КЗ-а и примијењена одредба члана 7. став 1. тачка 2. и 3. Закона о посебним мјерама за спречавање. Окривљени се у овом поступку бранио шутњом. Није признао извршење кривичног дјела.

Наведена пресуда је укинута, с обзиром на то да је садржавала битне повреде одредби кривичног поступка јер је изрека пресуде неразумљива и проутријечна сама себи, а разлози нејасни и неразумљиви. Ово стога што првостепени суд није опредијелио кривично дјело за које је везао одредбу члана 185-б КЗ. Наиме, одредбом члана 185. КЗ-а прописано је да је извршилац овог кривичног дјела онај ко у намјери извршења кривичног дјела силовање из става 4. (дијете), обљуба над немоћном особом, обљуба с дјететом, обљуба злоупотребом положаја, недозвољене сполне радње, подвођење и омогућавање вршења сполног односа, посредовање у вршењу проституције, искоришћавање малољетне особе за производњу... и навођење малољетне особе на присуство сполним радњама, искористи рачунарску мрежу или комуникацију другим техничким средствима, договори с малољетником састанак и појави се на договореном мјесту ради састанка, што значи да се у конкретном случају ради о сложеном кривичном дјелу, а првостепени суд није одредио радње за које је везао одредбу члана 185-б став 1 КЗ-а. У изреци је наведено да је окривљени имао намјеру да изврши недозвољену сполну радњу над малољетником. Дакле, из изреке ожалбене пресуде произлази да се противправно поступање окривљеног састоји у намјери вршења недозвољене сполне радње над малољетником, што би упућивало на одредбу члана 182 став 1 КЗ-а, међутим, том одредбом прописано је да је извршилац кривичног дјела онај ко под условима из цитираних чланова изврши неку другу сполну радњу, што даље говори да је одредба упућује на увјете, а то су: да је потребно постојање принуде, односно силе или пријетње или да је оштећени немоћна особа или да је у односу подређености или зависности у односу на окривљеног, па како из чињеничног описа кривичног дјела за које је окривљени оглашен кривим не произлази постојање силе или пријетње, нити однос подређености или зависности, то је изрека пресуде неразумљива и протуријечна сама себи.

Опће мјере заштите и исказ дјетета у кривичном поступку

1. Увод

У посљедњих неколико деценија нарочита пажња на међународном плану посвећена је успостављању дјелотворне заштите дјеце жртава савремених облика криминалитета, посебно имајући у виду неопходност подузимања законодавних и других мјера за спречавање свих видова сексуалне експлоатације и сексуалног злостављања дјеце, као и потребу њихове заштите, уважавајући да најбољи интереси дјетета и право дјетета да се његово мишљење чује и узме у разматрање представљају један од основних принципа у остваривању, поштовању и заштити њихових права. Државе уговорнице, свјесне обима и карактера ових појава, посебно повећане међународне трговине дјецом, искоришћавања дјеце у проституцији и порнографији, односно све изражене злоупотребе рачунарских система и мрежа у циљу регрутовања дјеце у споменуте сврхе, поред осталог, реаговале су и успостављањем нових међународних норми и стандарда. У том смислу, поред јасног појмовног дефинисања шта све треба да садрже законски описи кривичних дјела на нивоу материјалног кривичног права, од изузетне важности су и јасно дефинисане одредбе које се односе на специфичности процесног положаја дјеце жртава сексуалне експлоатације и сексуалног злостављања.

2. Опће мјере заштите дјетета оштећеног/свједока у кривичном поступку

Закон о ратификацији Факултативног протокола уз Конвенцију о правима дјетета о продаји дјеце, дјечијој проституцији и дјечијој порнографији, између осталог, обавезује државе уговорнице да усвоје одговарајуће мјере за заштиту права дјетета[51] у свим фазама кривичног поступка (члан 8. *Протокола*), а нарочито:

- признавањем угрожености дјеце жртава и прилагођавањем поступака да би се уважиле њихове посебне потребе, укључујући њихове посебне потребе као свједока;
- обавјештавањем дјеце жртава о њиховим правима, њиховој улози и обиму, временском распореду и напредовању поступка и разматрању њихових случајева;
- допуштањем да се у поступку у ком су угрожени њихови лични интереси презентују и размотре гледишта, потребе и преокупације дјеце жртава, на начин који је у складу с правилима националног процесног права;

[51] Вучковић-Шаховић, Н. (2006) *Експлоатација дјеце с посебним освртом на Факултативни Протокол уз Конвенцију о правима дјетета о продаји дјеце, дјечијој проституцији и дјечијој порнографији*, Београд: Центар за права дјетета & Save the Children UK – канцеларија у Београду, стр. 36.

- осигурањем одговарајућих служби подршке дјеци жртвама током читавог правног процеса;
- заштитом, када је то одговарајуће, приватности и идентитета дјеце жртава и подузимањем мјера у складу с националним правом како би се избјегло неподесно ширење информација које би могле довести до идентификовања дјеце жртава;
- осигурањем, у одговарајућим случајевима, сигурности дјеце жртава, као и сигурности њихових породица и свједока који свједоче у њихово име, од застрашивања и одмазде;
- избјегавањем непотребног одгађања разматрања случајева и извршавања налога или уредби о давању обештећења дјеци жртвама.

Такође, у смислу *Протокола*: "Државе уговорнице ће осигурати да неизвјесност у погледу стварне старосне доби жртве не спријечи покретање кривичног поступка, укључујући истражне радње усмјерене на утврђивање старосне доби жртве. Да у поступању од система кривичног правосуђа, с дјецом жртвама незаконитих радњи описаних у овом протоколу најбољи интерес дјетета буде приотитет". Државе уговорнице подузет ће такође мјере како би осигурале одговарајућу обуку, посебно правну и психолошку, за особе које раде са жртвама незаконитих радњи забрањених према овом *Протоколу* и усвојити мјере како би заштитиле сигурност и интегритет особа и/или организација укључених у спречавање и/или заштиту и рехабилитацију жртава таквих незаконитих радњи.

Закон о потврђивању Конвенције Вијећа Европе о заштити дјеце од сексуалне експлоатације и сексуалног злостављања изузетно детаљно регулише опће мјере заштите дјетета жртве у кривичном поступку, али и сам начин разговора с њим. У том смислу државе уговорнице ове *конвенције* се обавезују на подузимање неопходних законодавних и других мјера за заштиту права жртава као и њихових посебних потреба у улози свједока у свим фазама кривичног поступка, а посебно:

а. упознавајући их, осим ако они не желе да приме такве информације, са службама које им стоје на располагању, њиховим правима, њиховој улози као и праћењу и поступку након што поднесу тужбу, о опћем току поступака, оптужбама као и исходу њиховог предмета;

б. старањем да барем у случајевима гдје евентуално постоји опасност за жртву или њену породицу они могу бити обавијештени, ако је неопходно, када је гоњена или осуђена особа привремено или коначно пуштена на слободу;

ц. омогућавањем да на начин који је у складу с правилима домаћих поступака буду саслушани, изведу доказе или изаберу средства путем којих ће представити и на разматрање ставити своје ставове, потребе и интересе, непосредно или преко посредника;

д. пружајући им одговарајуће услуге подршке тако да се њихова права и интереси могу благовремено предочити и узети у обзир;

е. заштитом њихове приватности, идентитета и слике о њима и, у складу с домаћим прописима, спречавањем ширења у јавности било каквих информација на основу којих би се могао утврдити њихов идентитет;

ф. старањем за њихову сигурност, као и њихове породице и свједока у њихово име, од застрашивања, освете и обнове виктимизације;

г. старањем да се контакт између жртава и учиниоца у суду или органу унутрашњих послова избјегне, осим ако надлежни органи не одреде другачије у најбољем интересу дјетета или кад је због истраге или поступака такав контакт неопходан.

Организација поступка, окружење по мјери дјетета и језик прилагођен дјетету

Методе рада које су конципиране тако да буду по мјери дјетета требају омогућити дјеци да се осјећају сигурно. Ако дјецу прати особа у коју они могу имати повјерења, осјећају се сигурније и лагодније током поступка.

У зградама у којима се налазе судови могу, кад год је то могуће, бити одређене посебне просторије за разговоре с дјецом и саслушање дјеце, тако што ће се увијек водити рачуна о најбољим интересима дјетета.

Правосуђе у кривичном поступку примјерено дјетету подразумијева и да дјеца заиста схвате природу и обим одлука које се доносе као и посљедице тих одлука.

Разговор с дјететом

Закон о потврђивању Конвенције Вијећа Европе о заштити дјеце од сексуалне експлоатације и сексуалног злостављања посебно установљава и обавезу да у ситуацијама када се ради о дјетету жртви сексуалног злостављања, односно сексуалне експлоатације, државе уговорнице подузму неопходне законодавне и друге мјере којима се осигурава:

- да се разговори с дјететом одрже без неоправданог одгађања по пријављивању чињеница надлежним органима;
- да се разговори с дјететом обаве, када је неопходно, у просторијама за то пројектованим или адаптираним;
- да разговоре с дјететом води стручњак за то оспособљен и по могућности иста особа;
- да број разговора буде што мањи и то само онолико колико је потребно за потребе кривичног поступка;
- односно да дијете прати његов правни представник или када је одговарајуће, одрасла особа по његовом избору, сем ако суд не донесе образложену одлуку о супротном у погледу те особе (члан 35).

Приликом разговора с малољетном особом (поготово млађе старосне доби) важно је...

1. ”Спустити се на ниво” малољетне особе (сјести поред ње, али не сувише близу да не угрозите њен простор)
2. Започети разговор тако да пробудите интересовање малољетне особе (почните разговор једноставним питањима, обратите пажњу на невербалну комуникацију – водите рачуна и о свом невербалном изражавању...)
3. Објаснити малољетној особи зашто сте ту и шта намјеравате урадити:

- *Поставит ћу ти много питања...*
- *Ја ћу понављати оно што си ми рекао-ла, ако погријешим, реци ми да сам погрешно разумио-ла;*
- *Уколико ти треба пауза, реци ми и прекинут ћемо разговор на неколико минута;*
- *Када завршим с питањима, ако имаш нека питања за мене, ја ћу покушати одговорити на њих...*

Такође, важно је имати на уму да дјеца предшколског узраста имају капацитет памћења као и одрасли, али они не обраћају увијек пажњу на детаље које одрасли сматрају релевантним - проблеми везани за сугестибилност: малољетне особе (поготово млађег узраста) мање су сугестибилне у погледу чињеница, него у погледу интрепретације тих чињеница.

Малољетне особе не лажу више од одраслих (већ с пет година дјеца разумију потребу да говоре истину, док дјеца школског узраста већ разумију саму потребу утврђивања чињеница).

Дјеца већ у узрасту од двије до три године могу једноставним језиком да опишу опажени догађај.

С пет година дјеца су у стању да користе сложеније реченице.

С десет година дјеца су у стању да опишу вријеме, процијене трајање, одреде сукцесију или број догађаја.

Млађа дјеца боље комуницирају невербално.

С млађом дјецом треба употребљавати једноставни језик и избјегавати употребу замјеница.

3. Поштовање принципа најбољег интереса дјетета и права на партиципацију у кривичним поступцима

Најбољи интерес дјетета представља један од основних принципа у остваривању, поштовању и заштити права дјетета. Обавеза државе, свих релевантних институција, па и суда јесте да у свим поступцима који се тичу дјетета воде рачуна о његовим најбољим интересима. Уједно најбољи интерес дјетета представља правни стандард који се цијени према околностима сваког појединачног случаја. То значи да се приликом доношења сваке одлуке морају сагледати околности сваког појединачног случаја и одлука донијети у најбољем интересу дјетета о чијим се правима одлучује.

Обавеза поступања у складу с најбољим интересом дјетета садржана је у члану 3. став 1. *Конвенције о правима дјетета*[52], у којем је прописана обавеза свих јавних или приватних институција социјалног старања, судова, административних органа или законодавних тијела да у свим активностима које се тичу дјетета воде рачуна о његовим најбољим интересима.[53]

[52] *Конвенција о правима дјетета*, "Службени лист СФРЈ - Међународни уговори", бр. 15/90.
[53] Вучковић Шаховић, Н., Доек, Ј., Зерматтен, Ј. (2012) *The Rights of the Child in International Law, Berne: Stampfli Publications Ltd.*, стр. 303-309.

У тачкама 8. и 9. *Закона о потврђивању Факултативног протокола уз Конвенцију о правима дјетета о продаји дјеце, дјечијој проституцији и дјечијој порнографији се* посебно указује на то да је држава дужна осигурати заштиту најбољег интереса дјетета жртве у свим фазама кривичног поступка уз првенствено признавање принципа правичности и непристраности.

Обавеза поштовања принципа најбољег интереса дјетета садржана је и у другим међународним документима, посебно од Босне и Херцегове ратификованој *Конвенцији Вијећа Европе о заштити дјеце од сексуалног искоришћавања и сексуалног злостављања* и *Смјерницама* Комитета *министара Вијећа* Европе о *правосуђу по мјери дјетета*, а у којима је јасно указано на обавезу поступања у складу с најбољим интересом дјетета у кривичним поступцима, на обавезу заштите малољетног оштећеног (дјетета свједока/жртве) у кривичном поступку, као и успостављања система правосуђа по мјери дјетета.

Најважнији аспект утврђивања најбољег интереса дјетета јесте да се дјетету омогући да утврди свој најбољи интерес. У том смислу најбољи интерес дјетета је уско везан с правом дјетета на партиципацију тј. с правом дјетета да изрази мишљење о питањима која га се тичу и да то мишљење буде узето у обзир приликом доношења одлука.

Приликом процјене најбољих интереса дјеце која су у укључена у кривични поступак као жртве или свједоци, важно је узети у обзир:

а) њихове ставове и мишљења;

б) сва друга права дјетета, као што је право на достојанство, слободу и равноправно поступање требају у сваком тренутку да се поштују;

ц) сви надлежни органи власти требају усвојити свеобухватан приступ како би на одговарајући начин узели у обзир све интересе о којима се ту ради, укључујући психолошко и физичко благостање и правне, социјалне и економске интересе дјетета.

Право дјетета на партиципацију је један од основних принципа права дјетета. Члан 12. *Конвенције о правима дјетета* садржи обавезу државе да осигура дјетету које је способно да формира мишљење право на слободу изражавања мишљења о свим питањима која се тичу дјетета и да посебно пружи могућност дјетету да буде саслушано у свим судским и административним поступцима који га се тичу, било непосредно или преко заступника или одговарајућег органа, на начин који је у складу с националним правилима процесног законодавства. Партиципација дјетета је у складу са схватањем дјетета као субјекта права које активно партиципира у остваривању својих права. Ово право је уско везано с правом дјетета на информисање и правом дјетета на слободу изражавања, а што подразумијева обавезу поступајућих органа да прије изражавања мишљења дјетета осигурају да дијете буде информисано о свим чињеницама које су од значаја за доношење одлуке и то на језику који је прилагођен дјетету, као и да му омогуће да своје мишљење изрази слободно.

Право је сваког дјетета да буде обавијештено о својим правима, да му се укаже на одговарајуће путеве који су му осигурани ради приступа правосуђу и да буде консултовано и саслушано у поступцима у којима учествује или који утјечу на њега. Дјецу треба сматрати пуним носиоцима права и тако треба поступати према њима.

3.1. Кривичноправни систем и уважавање принципа најбољег интереса дјетета и права на партиципацију у кривичним поступцима у Босни и Херцеговини

Сматра се како је појава злоупотребе и занемаривања дјеце егзистирала током читаве хисторије људског рода, али до признавања и уважавања ове појаве долази тек шездесетих година XX стољећа, након што је амерички педијатар Хенру Кемпе први употријебио емоционално набијен термин „синдром претученог дјетета'' описујући и документујући драстичне случајеве физичког злостављања дјеце с фаталним исходом.[54] Заштита дјеце и малољетника у домену савременог кривичног права представља један од његових највећих изазова. Иако кривично право није једино правно подручје у оквиру којег се пружа заштита дјеци и малољетницима као категорији особа од посебног интереса за једно друштво, управо ће мањкава, али исто тако и напредна рјешења на подручју ове гране у највећој мјери одражавати степен укупне заинтересованости друштва за здраво и слободно одрастање оних који ће чинити то друштво у догледној будућности. Интерес дјетета, односно најбољи интерес дјетета установљен је Конвенцијом о правима дјетета УН из 1989. године[55] иако је заштита дјеце и прије тога била предметом међународних докумената као што су Декларација о правима дјетета Лиге народа из 1924. године[56], Декларација о правима дјетета Опће скупштине УН-а из 1959 године[57] и други. Чл. 3. ст. 1. Конвенције УН установио је обавезу према којој у свим акцијама које у вези с дјецом подузимају јавне или приватне установе социјалне скрби, судови, државна управа или законодавна тијела, првенствено се има водити рачуна о интересима дјетета. Као елементи релевантни за највећи број ситуација у којима се дијете или група дјеце може наћи, а са стајалишта процјене и утврђивања стандарда најбољег интереса дјетета сматрају се:

1. *Мишљење дјетета: без обзира на то ко и у којој ситуацији одлучује о питању које се тиче дјетета, став дјетета о том питању је основни елемент, а у исто вријеме и средство за процјену и утврђивање његовог најбољег интереса. У складу с његовим узрастом и зрелошћу, дјетету се мора увијек дати могућност да утјече на одређење свог најбољег интереса.*
2. *Идентитет дјетета: свако дијете је другачије од другог па се при процјени најбољег интереса дјетета мора узети у обзир његов идентитет, односно карактеристике које су укључене у њега, као што су спол, сполна оријентација, национално поријекло, религија, културни идентитет.*
3. *Очување породичне средине и одржавање односа дјетета с родитељима и члановима породице: дијете се интервенцијом надлежних органа и тијела, односно изрицањем мјера може одвојити од породице само ако се на други начин не може заштитити. Онда када се одвоји од једног или оба родитеља, односно од других чланова породице, мора му се осигурати одржавање редовних и квалитетних личних односа и непосредних контаката с њима.*
4. *Старање, заштита и сигурност дјетета: дјетету се у свим ситуацијама и доношењем одлуке о свим питањима која га се тичу треба осигурати добробит, односно задовољење основних примарних, материјалних, образовних и емотивних потреба те потребе за љубављу и сигурношћу.*

[54] Салкић, С. (2013). *Кривична дјела насиља анд дјецом: Стање и проблеми*, Сарајево, стр. 1.
[55] „Службени лист РБиХ", број: 25/93 – Међународни уговори
[56] Женевска декларација о правима дјетета из 1924. (*Geneva Declaration of the Rights of the Child*), Лига нација O.J. Спец. Супп. 21, 43 (1924)
[57] Одлука Генералне скупштине из 1386. (XIV) од 20. новембра 1959.

5. *Стање рањивости дјетета (дијете с потешкоћама у развоју, припадник националне мањине, жртва насиља, мигрант, избјеглица итд.): најбољи интерес дјетета се не може процјењивати на исти начин за ову и осталу дјецу, као ни за сву дјецу из истог стања рањивости.*
6. *Право дјетета на здравље и његово здравствено стање: дјетету се мора пружити безувјетна и адекватна здравствена заштита, која укључује превентивну и медицинску његу, без обзира на његов статус осигурања.*
7. *Право дјетета на образовање: образовање је основно људско право сваког дјетета које је садржано у бројним међународним документима и законима у Босни и Херцеговини. Ово право је повезано с остваривањем других права, чиме се утječе на квалитет живота сваког појединца.*[58]

У Босни и Херцеговини данас, што посебно долази до изражаја у Федерацији БиХ, као и Дистрикту Брчко БиХ, кривичноправна заштита дјеце и малољетника, премда постоји, ипак како смо то имали прилике констатовати у дијелу Водича који се односи на кривичноправна рјешења у вези с инкриминисањем сексуалног злостављања и искоришћавања дјеце, у потпуности не одражава ни захтјеве преузете потврђивањем међународних докумената, ни стварне потребе босанскохерцеговачког друштва за адекватним уређењем овог правног подручја. Једини изузетак чине законодавна рјешења у Републици Српској, која у значајном капацитету слиједе обавезе преузете потврђивањем Ланзароте али и Истанбулске конвенције.

Поред дијела инкриминација усмјерених на заштиту дјеце и малољетника када је у питању високотехнолошки криминал, кривичноправна заштита обухвата и друга кривична дјела из кривичних закона чији је циљ такође заштитити дјецу и малољетнике, било кроз засебне инкриминације нпр. Обљуба с дјететом млађим од 15 година или кроз прописивање квалификованих облика других кривичних дјела уколико су почињени на штету дјеце или малољетника, нпр. силовање.

Осим одредби материјалног кривичног права, заштита дјеце односно малољетника осигурава се и одредбама процесног кривичног права. Тако закони о кривичном поступку који су на снази у Босни и Херцеговини прописују посебне одредбе у околностима када се у неком процесном статусу појављује дијете, односно малољетник. Наводимо неке од њих из ЗКП ФБиХ уз напомену како сличне одредбе прописују и други закони о кривичном поступку који су на снази у Босни и Херцеговини:

- *Здравствени радници, наставници, васпитачи, родитељи, старатељи, усвојитељи и друге особе које су овлаштене или дужне да пружају заштиту и помоћ малољетним особама, да врше надзор, одгајање и васпитавање малољетника, а који сазнају или оцијене да постоји сумња да је малољетна особа жртва сексуалног, физичког или неког другог злостављања, дужни су о тој сумњи одмах обавијестити овлаштену службену особу или тужиоца (чл. 228. ст. 2.).*
- *Позивање као свједока малољетне особе која није навршила 16 година живота врши се преко родитеља, односно законског заступника, осим ако то није могуће због потребе да се хитно поступа или других околности (чл. 95. ст. 2.).*
- *Малољетна особа која с обзиром на узраст и душевну развијеност није способна схватити значај права да не мора свједочити не може се саслушати као свједок у кривичном поступку (чл. 96. ст. 1. д).*

[58] *Смјернице за процјену и утврђивање најбољег интереса дјетета: Водич за професионалце*, (2018). Босна и Херцеговина, Министарство за људска права и избјеглице, Сарајево

- *Приликом саслушања малољетне особе, нарочито ако је она оштећена кривичним дјелом, поступит ће се обазриво да саслушање не би штетно утјецало на психичко стање малољетника. Саслушање малољетне особе извршит ће се уз помоћ педагога или друге стручне особе (чл. 100. ст. 4.)*
- *Заштита интереса малољетника је један од разлога за искључење јавности с главне расправе (чл. 250.).*

Осим кривичних закона и закона о кривичном поступку у ентитетима и Брчко дистрикту БиХ на снази су и закони о заштити и поступању с дјецом и малољетницима у кривичном поступку. Иако наведени закони у највећем обиму прописују одредбе материјалног, процесног и извршног кривичног права у околностима када се у улози починиоца кривичног дјела појављује малољетна особа, један, истина, мали дио норми усмјерен је и на заштиту дјеце и малољетника на чију је штету кривично дјело и почињено. Уз напомену како у одредбама наведених закона постоје становита одступања између Федерације БиХ, Републике Српске и Дистрикта Брчко БиХ представит ћемо неке од одредби прописане Законом о заштити и поступању с дјецом и малољетницима у кривичном поступку Републике Српске, који је и први законски пропис такве природе који је ступио на снагу и почео се примјењивати у Босни и Херцеговини.

- *Судија за малољетнике или судија који има посебна знања суди и пунољетним починиоцима за кривична дјела прописана Кривичним законом када се у кривичном поступку као оштећени појављује дијете и малољетна особа, као што су кривична дјела: а) убиство, б) тешко убиство; ц) убиство дјетета при порођају, д) навођење на самоубиство и помагање у самоубиству, е) тешка тјелесна озљеда, ф) отмица… (чл. 184. ст. 1.).*
- *Истрагу води тужилац који је стекао посебна знања из области права дјетета и кривичноправне заштите малољетних особа (чл. 185. ст. 2.).*
- *У истражним радњама поступају специјализована овлаштена службене особе које су стекле посебна знања из области права дјетета и кривичноправне заштите малољетних особа (чл. 185. ст. 3.).*
- *Код поступања у кривичним предметима против починилаца кривичних дјела на штету дјеце, при спровођењу процесних радњи посебно обазриво се односи према дјетету на чију штету је учињено кривично дјело, имајући у виду његов узраст, особине његове личности, образовање и прилике у којима живи, како би се избјегле могуће штетне посљедице на његов будући живот, васпитање и развој. Саслушање дјетета се обавља уз помоћ стручног савјетника или друге стручне особе (чл. 186. ст. 1.).*
- *Стручно лице је стручни радник органа старатељства - психолог, педагог, социјални педагог - дефектолог, специјални педагог - дефектолог, социјални радник који посједује цертификат о стручној оспособљености за обављање послова из области преступништва младих и кривичноправне заштите дјеце, искуство на пословима заштите и бриге о дјеци и професионалне вјештине у комуникацији са дјецом, а уз чију помоћ се обавља саслушање дјетета као свједока оштећеног кривичним дјелом из члана 184 (чл. 186а ст. 1.).*
- *Ако се као свједок саслушава дијетем оштећено кривичним дјелом из члана 184. Закона (тешка кривична дјела), саслушање се може спровести највише два пута (чл. 186. ст. 2.).*
- *Ако се као свједок саслушава дијете или малољетник који је озбиљно физички или психички трауматизован околностима под којима је извршено кривично дјело или пати од озбиљних психичких поремећаја који га чине посебно осјетљивим, забрањено је вршити његово суочење с осумњиченим, односно оптуженим (чл. 187).*

- *Ако препознавање осумњиченог, односно оптуженог врши малољетник оштећен кривичним дјелом или је очевидац учињеног кривичног дјела, такво препознавање у свим фазама поступка врши се на начин који у потпуности онемогућава да осумњичени, односно оптужени, види малољетну особу (чл. 188.) и др.*

Даље, заштита дјеце и малољетника осигурана је и законима о заштити свједока под пријетњом и угрожених свједока на свим разинама у Босни и Херцеговини. Тако Закон о заштити свједока под пријетњом и угрожених свједока Федерације БиХ[59] у чл. 3. ст. 3. под угроженим свједоком поред свједока који је озбиљно физички или психички трауматизован околностима под којима је извршено кривично дјело или који пати од озбиљних психичких поремећаја који га чине изузетно осјетљивим, третира и дијете односно малољетника са свим процесним учинцима којима такав статус резултира.

Коначно, посебан вид заштите дјеце и малољетника осигуран је и неким подзаконским прописима у околностима када се они појаве као жртве трговине људима. То су Правила о заштити жртава и свједока жртава трговине људима држављана Босне и Херцеговине[60] те Правилник о заштити странаца жртава трговине људима.[61] Наводимо неколико одредби потоњег документа:

- *дијете које није држављанин Босне и Херцеговине ужива иста права на бригу и заштиту као и дјеца која су држављани Босне и Херцеговине (чл. 20. ст. 2.);*
- *уколико се доб странца не може утврдити са сигурношћу, а постоје разлози за вјеровање да се ради о дјетету, он се третира као дијете све до потврђивања његове старосне доби. Према тој особи се подузимају све посебне прописане мјере у циљу заштите најбољег интереса дјетета, те се обавјештава мјесно надлежни општински орган управе за послове социјалне заштите у циљу осигурања привременог старатеља (чл. 10. ст. 5);*
- *дијете које има одобрен привремени боравак као жртва трговине поред осталих права као што су: право на адекватан и сигуран смјештај, приступ хитној медицинској заштити, право на психолошку помоћ… има и приступ образовању (чл. 15. ст. 2.);*
- *током провођења поступка смјештаја дјетета у склониште надлежна организациона јединица Службе обавјештава орган управе надлежан за послове социјалне заштите, у мјесту гдје се склониште налази о потреби именовања старатеља који је у обавези заступати интересе дјетета у поступку до налажења трајног рјешења (чл. 20. ст. 3.);*
- *дијете жртва трговине које није држављанин Босне и Херцеговине има право на повратак у државу поријекла или уобичајеног боравка или у државу која га прихвата (чл. 22. ст. 1.);*
- *дијете жртва трговине неће бити враћено у државу поријекла или уобичајеног боравка или у државу која га прихвата ако постоји оправдана сумња, а након процјене ризика и сигурности, да постоје разлози да повратак дјетета угрожава његову сигурност или сигурност чланова његове породице (чл. 22. ст. 4.) и др.*

На крају, да кажемо још и то да унаточ томе што на плану сузбијања ове врсте криминала у Босни и Херцеговини постоји мноштво запрека, као што је то случај и с другим облицима криминала, законодавац, али и тијела, односно субјекти који проводе прописе, морају бити опредијељени за бољитак дјеце и младих као категорије од посебног интереса за друштво у цјелини. Ово посебно на пољу њихове кривичноправне заштите. Само на тај начин може се гарантовати и здрава будућност Босне и Херцеговине.

[59] „Службене новине ФБиХ“, бр. 36/03.
[60] „Службени гласник БиХ“, бр. 66/07
[61] „Службени гласник БиХ“, бр. 90/08

Препоручена литература

1. Бајрамовић, М. (2013) Правна анализа усклађености националног законодавства с Конвенцијом о заштити дјеце од сексуалног искоришћавања и сексуалне злоупотребе (Ланзароте конвенција). Бања Лука и Тузла: Организација "Здраво да сте" и Удружење "Земља дјеце" Тузла
2. Бајрамовић, М. (2014). Заштита дјеце од сексуалног насиља и искоришћавања. Бања Лука: "Здраво да сте" Бања Лука.
3. Будимлић, М. и Пухарић, П. (2009) *Компјутерски криминалитет: криминолошки, кривичноправни, криминалистички и сигурносни аспекти, Факултет за криминалистику, криминологију и сигурносне студије*, Сарајево
4. Марковић, И. (2012) Усклађивање националног законодавства са међународним стандардима у области кривичноправне заштите полног интегритета дјеце, објављен у зборнику Релевантна питања примене међународног кривичног права у националном праву, Тара, јун 2012. године, у издању Удружења за међународно кривично право, стр. 245-25;
5. Марковић, И. (2012) Кривичноправна заштита полног интегритета дјеце и малољетних лица у кривичном законодавству Републике Српске, Зборник радова ИХ традиционалног међународног научног скупа „Правнички дани Проф. др Славко Царић", на тему Савремене тенденције развоја правних система држава у реогиону, Нови Сад, 2012. издавач Правни факултет за привреду и правосуђе, Универзитет Привредна академија, стр. 450-462.;
6. Марковић, И. (2010) Полно насиље над дјететом, Правни живот, часопис за правну теорију и праксу, тематски број Право и простор, број 10/2010. година LIX, том II, Београд, с. 167-177 .
7. Марковић, И. (2018) Сексуално злостављање и искоришћавање дјеце (новине у кривичном законику Републике Српске) , Годишњак Правног факултета, с. 27-45, Годишњак часопис за правну теорију и праксу, број 40, Бања Лука
8. Муратбеговић , Е. Кобајица, С. и Вујовић, С. (2016). Анализа у области борбе против сексуалног насиља и других облика злостављања дјеце на интернету у Босни и Херцеговини, Save the Children, Сарајево
9. Муратбеговић, Е. Кобајица, С. и Вујовић, С. (2016). *Насиље над дјецом путем информационо-комуникаијских технологија у Босни и Херцеговини*, CPRC, Save the Children, Сарајево
10. Салкић, С. *Кривична дјела насиља анд дјецом: Стање и проблем*, Сарајево
11. *Смјернице за процјену и утврђивање најбољег интереса дјетета: Водич за професионалце*, (2018). Босна и Херцеговина, Министарство за људска права и избјеглице, Сарајево
12. *Заштита дјеце од сексуалног злостављања и искоришћавања: Регистар починилаца кривичних дјела сексуалног злостављања дјеце, потребе и обавеза* (2016). World Vision International у Босни и Херцеговини, Бања Лука
13. Банић, М., Стевановић, И. (2015) *Како до правосуђа по мери детета: заштита деце жртава у кривичним поступцима и стање у пракси у Републици Србији*, Београд: Центар за права детета.

14. Милосављевић-Ђукић, И. Танкосић, Б., Петковић, Ј., Марковић, М. (2017) "Јединице за подршку деци жртавама и сведоцима у кривичном поступку Домаће право и пракса", *Темида*, бр. 1, стр. 45-64.
15. *Посебни протокол о поступању правосудних органа у заштити малољетних лица од злостављања и занемаривања,* 2009, Београд: Министарство правде Републике Србије.
16. *Посебним протоколом о поступању полицијских службеника у заштити малољетних лица од злостављања и занемаривања,* 2012, Београд: Министарство унутрашњих послова Републике Србије, доступно на сјту: www.mup.gov.rs
17. Стевановић, И.(а) (2014) „Кривичноправни систем и заштита малољетних лица (национални нормативни аспект)", у: Вучковић Шаховић, Н. и др. *Заштита деце жртава и сведока кривичних дела*, Београд: International Management Group, стр. 30-42.
18. Стевановић, И.(б) (2014) *Моје право да будем заштићен*, Београд: Институт за криминолошка и социолошка истраживања.
19. Вучковић-Шаховић, Н. (2006) *Експлоатација деце с посебним освртом на Факултативни Протокол уз Конвенцију о правима детета о продаји деце, дечијој проституцији и дечијој порнографији*, Београд: Центар за права детета & Save the Children UK – канцеларија у Београду.
20. Вучковић Шаховић, Н., Доек, Ј., Зерматтен, Ј. (2012) "The CRC Committee's General Comment No. 10", in: *The Rights of the Child in International Law, Berne: Stampfli Publications Ltd.*
21. Шкулић, М. (2002) Кривичнопроцесне могућности заштите жртава кривичних дела повезаних са трговином људским бићима, *Темида,* бр. 1.
22. Шкулић, М. (2014) "Заштита деце/малољетних лица као оштећених и сведока у кривичном поступку", у: Вучковић, Шаховић, Н. и др. *Заштита деце жртава и сведока кривичних дела*, Београд: International Management Group - IMG, стр. 43-70.
23. Шкулић, М. (2016) "Положај жртве/оштећеног у кривичноправном систему Србије уопште и у односу на Директиву EU 2012-29", *Казнена реакција у Србији ВИ део*, (ур. Ђ. Игњатовић), *едиција Цримен*, Београд: Правни факултет Универзитета у Београду

Препоручени интернетски ресурси

www.osintframework.com

Оквир OSINT је фокусиран на онлајн прикупљање информација од бесплатних алата и ресурса на интернетској мрежи. Намјера је да се помогне истражиоцима да пронађу бесплатне OSINT ресурсе ради идентификовања извршилаца и жртви високотехнолошког криминала. Неки од сајтова могу захтијевати регистрацију или нуде више података за новчану надокнаду, али је већина алата за онлајн истраге у кибернетичком простору бесплатна.

http://pametnoibezbedno.gov.rs/pametno/category/bezbednost_dece_na_internetu/?lng=lat

Стратегија информационе безбедност за даље јачање дигиталне заштите

http://www.netpatrola.rs/sr/naslovna.1.1.html

Нет патрола је онлајн механизам за подношење пријава Центра за сигурни интернет који је основан у сврху пријема и обраде пријава о нелегалним или штетним садржајима на интернету.

www.GetSafeOnline.org

- Internet Safety Advice (савјети о сигурности на интернету)
- Crime Prevention Advice (савјети о спречавању криминала)

www.ThinkUKnow.co.uk

- Child Protection Online Advice (савјети о заштити дјеце онлајн)
- Public Portal to report suspected child abuse online (јавни портал за пријаву сумње на злостављање дјетета онлајн)
- Crime Prevention Advice (Children & Parents) (савјети о спречавању криминала; дјеца и родитељи)

www.InternetWatchFoundation.org.uk

- Public Hotline for reporting child abuse images, video"c or Text observed online (for anywhere in the world). (јавна телефонска линија за пријаву слика, видеа или текстова злостављање дјетета онлајн – за било гдје у свијету)

www.ActionFraud.org.uk

- Public Hotline for reporting fraud (јавна телефонска линија за пријаву преваре)
- Support and advice about fraud (подршка за савјете о превари)
- Crime Prevention Advice (савјети за спречавање криминала)

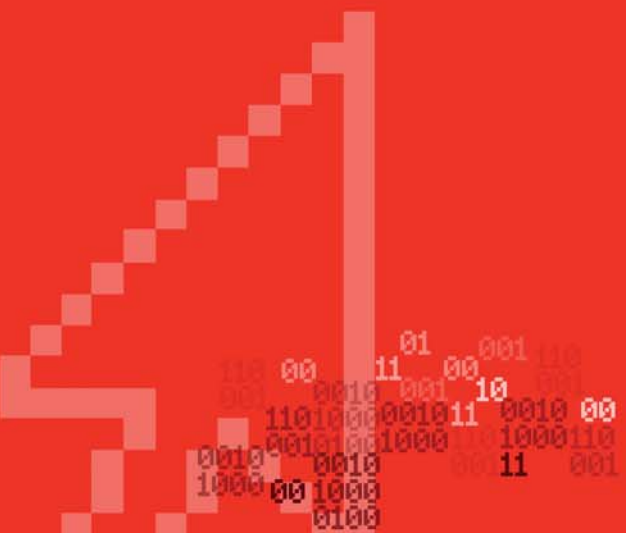
www.APWG.org

- Anti-Phishing Working Group (радна група за спречавање лажног представљања)
- Public Hotline for reporting phishing emails and websites (јавна телефонска линија за пријаву е-маилова и web-страница лажног представљања)
- Crime Prevention Advice (савјети о спречавању криминала)

www.ic3.gov

IC3 је сајт за онлајн пријаве интернетског криминала који за посљедицу преваре има материјалну штету. У захтјеву је потребно да пружите сљедеће информације приликом подношења пријаве:

- име оштећеног, адресу, телефон и е-маил,
- информације о финансијским трансакцијама (нпр. информације о налогу, датум трансакције и износ, и др.),
- име субјекта којем је дозначен новац, адресу, телефон, е-маил, web, и IP-адресу,
- детаље о томе како сте били жртва преваре,
- е-маил заглавља (и),
- све друге релевантне информације које сматрате важним.



Save the Children za sjeverozapadni Balkan
Ljubljanska 16, Sarajevo, Bosna i Hercegovina

Tel +387 (0) 33 290 671, Fax +387 (0) 33 290 675 |
info.nwbalkans@savethechildren.org

https://nwb.savethechildren.net

savethechildrennwb

savethechildrennwb

scnwb

SavethechildrenNWB

Zajedno možemo učiniti više. Šta misliš o našem radu?
reci-nam@savethechildren.org