Republika e Kosovës
Republika Kosova-Republic of Kosovo
Qeveria–Vlada-Government
Zyra e Kryeministrit - Ured Premijera - Office of the Prime Minister
Zyra për Qeverisje të Mirë/Kancelarija za Dobro Upravljanje/Office on Good Governance

PLANI STRATEGJIK PËR MBROJTJEN E FËMIJËVE NGA RREZIQET NË INTERNET

2015-2019

Prishtinë, Shkurt 2015

Zyra e Kryeministrit
Zyra për Qeverisje të Mirë

Plani Strategjik për Mbrojtjen e Fëmijëve nga Rreziqet në Internet 2015-2019

Ky plan u hartua në kuadër të projektit të financuar nga BE-ja “Mbrojtja e fëmijëve nga rreziqet në internet - PROCON” që menaxhohet nga Zyra e Bashkimit Evropian në Kosovë. Projekti zbatohet nga Qendra për Arsim e Kosovës (KEC) në bashkëpunim me Këshillin Rinor Kosovar (KYC) dhe International Children Safety Service (ICSS) dhe në partneritet me Ministrinë e Arsimit, Shkencës dhe Teknologjisë (MAShT) dhe Zyrën për Qeverisje të Mirë (ZKM/ZQM). Përmbajtja e këtij dokumenti është përgjegjësi e organizatave zbatuese dhe në asnjë rrethanë nuk i atribuohet donatorit.

TABLE OF CONTENTS

LISTA E SHKURTESAVE

ARKEP	Autoriteti Rregullativ Komunikimeve Elektronike dhe Postare
BE	Bashkimi Evropian
CERT	Qendrës Kompjuterike dhe Reagime Emergjente
COP	Child Online Protection
FIT	Qendra për studime të avancuara
ICSS	International Children's Safety Service
ITU	Unioni Ndërkombëtar i Telekomunikacionit
KEC	Qendra për Arsim e Kosovës
KYC	Këshillin Rinor Kosovar
MAShT	Ministria e Arsimit, e Shkencës dhe e Teknologjisë
MPMS	Ministria e Punës dhe e Mirëqenies Sociale
PROCON	Protecting Children Online (Mbrojtja e Fëmijëve nga rreziqet në internet)
STIKK	Shoqata e Teknologjisë së Informacionit dhe Komunikimeve të Kosovës
TIK	Teknologjia e Informacionit dhe Komunikimit
ZKM	Zyra e Kryeministrit
ZQM	Zyra për Qeverisje të Mirë

PARATHËNIE

Fëmijët dhe të rinjtë kalojnë shumë kohë në internet - kjo mund të jetë një mënyrë e mirë që ata të shoqërohen, të studiojnë dhe të argëtohen. Ata fillojnë të përdorin internetin në një moshë mjaft të re dhe aftësitë e tyre për teknologji janë mbresëlënëse.

Përdorimi i internetit mund të ndihmojë fëmijët të përmirësojnë rezultatet e tyre në shkollë, të zhvillojnë aftësitë kompjuterike, të përmirësojnë aftësitë e tyre të komunikimit dhe vetëbesimit si dhe të gjejnë hobi dhe gjëra të reja me interes për ta.

Fatkeqësisht, të njëjtat përparësi të teknologjisë së kompjuterëve dhe telekomunikimit që ju mundësojnë fëmijëve tanë të arrijnë burime të reja të njohurive dhe përvojave kulturore, i lënë ata gjithashtu të pambrojtur ndaj abuzimeve dhe lëndimeve, siç janë: qasje në përmbajtje të papërshtatshme, cyberbullying, apo rreziqet nga keqpërdorimi i të dhënave personale. Mbrojtja dhe promovimi i të drejtave të fëmijëve janë prioritete për Bashkimin Evropian dhe institucionet e saj, dhe trajtimi i rreziqeve me të cilat përballen fëmijët në internet po bëhet gjithnjë e më shumë politikë prioritare për shumicën e qeverive të vendeve të Bashkimit Evropian dhe vendeve partnere të saj në mbarë botën.

Qeveritë nuk janë të vetme në angazhimet e tyre për të mbrojtur fëmijët nga rreziqet në internet. Prindërit, kujdestarët, edukatorët, bizneset dhe shoqëria civile gjithashtu mund të ndihmojnë fëmijët për të përfituar nga interneti. Ata gjithashtu kanë përgjegjësi të mbrojnë fëmijët nga rreziqeve në internet dhe të gjithë këta kanë treguar përkushtimin e tyre në kontributin e dhënë për hartimin e këtij plani strategjik.

Ky plan strategjik për mbrojtjen e fëmijëve nga rreziqet në internet vlerëson kornizën aktuale legjislative në Kosovë, burimet njerëzore në dispozicion, koordinimin e palëve te interesit dhe të ngritjes së vetëdijes së përgjithshme. Plani ofron qëllimin, objektivat dhe rekomandimet konkrete për mbrojtjen e fëmijëve nga rreziqet në internet, duke përfshirë planin e veprimit dhe buxhetin e strategjisë.

Përkundër progresit të shënuar të institucioneve të Kosovës në fushën e mbrojtjes së fëmijëve, mbetet ende shumë për t'u bërë në përmirësimin e legjislacionit, politikave dhe strukturave për të mbuluar rreziqet e ndryshme me të cilat përballen fëmijët. Zyra e Bashkimit Evropian në Kosovë beson se institucionet relevante të Kosovës do të ndërmarrin gjitha veprimet afatshkurta dhe afatgjata në mënyrë që të zbatohen këto rekomandime në interes të fëmijëve.

Zyra e BE-së në Kosovë është e përkushtuar qe të vazhdojë mbështetjen e institucioneve të Kosovës në parandalimin dhe mbrojtjen e fëmijëve nga të gjitha format e dhunës. Investimi në fëmijë dhe të rinj nënkupton investim në të ardhmen, veçanërisht në një shoqëri si kjo që ka Kosova, ku fëmijët dhe të rinjtë përbëjnë me shume se 60 për qind të popullsisë.

Samuel Žbogar
Shefi i Zyrës së Bashkimit Evropian/Përfaqësuesi Special i BE-se
Prishtinë, Shkurt 2015

1. HYRJE

PROCON – Mbrojtja e Fëmijëve nga rreziqet në internet është projekt që ka për qëllim të sigurojë mbrojtje më të mirë për fëmijët nga rreziqet në internet, përmes vetëdijesimit, fuqizimit dhe aktiviteteve të bashkërenditura të Qeverisë, Shoqërisë Civile dhe Industrisë për marrjen e masave mbrojtëse. Projekti zbatohet nga Qendra për Arsim e Kosovës (KEC), në bashkëpunim me Këshillin Rinor Kosovar (KYC) dhe International Children's Safety Service (ICSS) nga Hungaria, ndërsa financohet nga Bashkimi Evropian.

Projekti dyvjeçar i filluar në dhjetorin e vitit 2013 ka dy komponentë:

1. Mbrojtja e fëmijëve nga rreziqet në internet – Në kuadër të këtij komponenti është krijuar Grupi i Palëve me Interes që koordinohet nga MAShT, e në punën e të cilit marrin pjesë institucione relevante qeveritare, organizata të bizneseve, ofertues të shërbimeve të Internetit dhe organizata të shoqërisë civile. Përveç ndërtimit të kapacitetit të këtij grupi politikëbërës, kjo komponent mbështetë edhe zhvillimin e këtij plani strategjik.
2. Vetëdijesimi dhe fuqizimi - Projekti mbështet krijimin dhe mirëmbajtjen e një webfaqeje për internet të sigurte, sipas modelit të vendeve të shumta të botës. Po ashtu, mbështet zhvillimin e materialeve informative për fëmijë, mësimdhënës dhe prindër, të cilat përdoren si bazë për organizimin e sesioneve informative në 100 shkolla të Kosovës. Projekti organizon edhe aktivitete vetëdijesimi në nivel të shkollave dhe nivel kombëtar.

Procesi i planifikimit Strategjik ka filluar në shtatorin e vitit 2014 dhe ndahet në 5 faza:

Faza e parë : Ngritja e Ekipit të Planifikimit Strategjik

Grupi i Palëve me Interes ka themeluar Ekipin e Planifikimit Strategjik, i cili përbëhet nga rreth 30 anëtarë. Ekipi përfaqëson gamë të gjerë të palëve të interesit duke përfshirë autoritetet shtetërore, ekspertë, profesionistë, shoqërinë civile dhe partnerë zhvillimorë. Detyra kryesore e ekipit është që të sigurojë të dhëna për procesin e planifikimit strategjik dhe komentojnë draft dokumentin, ndërsa Grupi i Palëve me Interes do të vazhdojë të drejtojë procesin.

Faza e dytë: Analiza e situatës dhe përcaktimi i qëllimeve

Një seminar treditor me pjesëmarrjen e anëtarëve të Grupit të Planifikimit Strategjik është mbajtur prej 20-23 Nëntor 2014. Në punëtori është bërë analiza SWOT, bazuar në të dhënat dhe informatat në dispozicion. Pastaj janë diskutuar strategjitë për t'i shfrytëzuar sukseset, tejkaluar dobësitë, përfituar nga mundësitë dhe për t'u mbrojtur nga rreziqet. Më vonë, fokusi është zhvendosur në përcaktimin e objektivave të Strategjisë, dhe përcaktimin e aktiviteteve që çojnë në arritjen e tyre.

Faza e tretë: Drafti i parë i Planit Strategjik

Pas punëtorisë planifikuese është hartuar drafti i parë i Planit Strategjik. Tri pjesët kryesore të këtij dokumenti janë 1) Hyrje; 2) Analizë e situatës bazuar në shqyrtimet ekzistuese dhe analizës SWOT; 3) Objektivat dhe aktivitetet me një përshkrim të detajuar të këtyre të fundit, duke ofruar zgjidhje të përshtatshme për kontekstin e Kosovës dhe në bazë të dokumenteve ekzistuese strategjike, kontributeve nga punëtoria dhe praktikave më të mira nga vendet e tjera.

Faza e katërt: Diskutimi i draftit të parë të Planit Strategjik

Draft dokumenti është diskutuar në kuadër të Ekipit Planifikues përmes një punëtorie njëditore. Objektivi i punëtorisë ishte të mbledh informacione kthyese fillestare nga të gjithë palët relevantë për të marrë vendim përkatës mbi drejtimet strategjike.

Faza e pestë: Versioni final i Planit Strategjik

Pas konsultimeve, është hartuar versioni final i Planit Strategjik, i cili është plotësuar me përmbledhje ekzekutive, plan të veprimit dhe kalkulime buxhetore. Ky version do t'i dorëzohet Zyrës për Qeverisje të Mirë për procedim të mëtutjeshëm.

2. ANALIZA E GJENDJES

2.1. HYRJE

Përkundër varfërisë me të cilën përballet Kosova, penetrimi në Internet arrin shkallën prej 76.626% (STIKK, 2013) që është e krahasueshme me disa vende anëtare të Bashkimit Evropian, si Bullgaria dhe Greqia. Si në vendet tjera të botës, ashtu edhe në Kosovë, Interneti më së shumti shfrytëzohet nga fëmijët dhe të rinjtë që i jep një dimension të veçantë këtij fenomeni, pasi Kosova ka popullatën më të re në Evropë, kështu që numri i fëmijëve të moshës deri në 18 vjeç është proporcionalisht më i madh se në çdo vend tjetër.

Nuk ka dyshim se interneti ofron shumë mundësi dhe përfitime për fëmijët, në kuptim të ndikimit që ka në arsimimin e tyre dhe përfshirjen në shoqëri. Nga ana tjetër, interneti mund edhe t'i vë fëmijët në rrezik për shkak të qasjes që kanë në përmbajtje që nuk i përgjigjen moshës së fëmijëve, mundësive që të jenë viktima të dhunës verbale ose ngacmimit seksual, ose joshjes nga komunitete të caktuara online që nxisin anoreksi, dhunë, ekstremizëm dhe shkaktim të dëmit ndaj vetvetes. Po ashtu, Interneti mund t'i inkurajojë fëmijët të publikojnë të dhëna personale, fotografi dhe video regjistrime, që mund t'i vënë në rrezik nga keqpërdoruesit e llojeve të ndryshme.

Hapi i parë në këtë planifikim strategjik ka qenë analiza e dokumenteve që ofrojnë informacion për gjendjen ekzistuese në fushën e mbrojtjes së fëmijëve nga rreziqet "online". Me gjithë se dokumentet e tilla për Kosovën janë të pakta, ka studime që analizojnë gjendjen në kontekste të tjera, të ngjashme me atë kosovar. Pastaj, është realizuar një punëtori ku është bërë analiza SWOT e gjendjes në fushën e mbrojtjes së fëmijëve nga rreziqet online, e ku kanë marrë pjesë anëtarët e Grupit të Palëve me interes themeluar nga MAShT.

Fillimisht, në këtë punëtori janë identifikuar një numër i konsiderueshëm i sukseseve, dobësive, mundësive dhe rreziqeve nga fusha e mbrojtjes së fëmijëve "online", të cilat pastaj janë klasifikuar në pesë grupe:

1. Legjislacioni dhe politikat
2. Kapacitetet vendore
3. Arsimi
4. Bashkëpunimi dhe koordinimi
5. Vetëdijesimi

Në vijim, për secilën nga këto fusha është dhënë një përmbledhje e shkurtër e gjendjes.

2.2. LEGJISLACIONI DHE POLITIKAT

Në Kosovë ka legjislacion specifik për mbrojtjen e fëmijëve nga rreziqet në Internet, siç është Ligji për Krime Kibernetike, por, kryesisht mungon legjislacioni sekondar që operacionalizon veprimet.

Sfidat kryesore:

- Mbrojtja e mangët që ofron legjislacioni aktual nga rreziqet "online"
- Masat për mbrojtjen e fëmijëve nga përmbajtje joadekuate ose të rrezikshme për ta
- Raportimi i rasteve të abuzimit "online"
- Zbatimi i legjislacionit në fuqi

Ndërkaq, Politika Sektoriale për komunikime elektronike – Agjenda digjitale 2013-2020 (2013) i referohet në veçanti nevojës për mbrojtjen e fëmijëve nga përmbajtjet ilegale në Internet, si dhe parasheh krijimin e një linje për raportim dhe qendrave për vetëdijesimin nga rreziqet e Internetit, megjithëse nuk e përcakton as numrin as formën e veprimit të tyre. Më 15 shkurt 2013, në Dubrovnik të Kroacisë është mbajtur takimi i ministrave dhe zyrtarëve të lartë të ministrive të brendshme dhe të sigurisë, të ministrive të drejtësisë dhe shërbimeve të prokurorisë të vendeve dhe rajoneve pjesëmarrëse në Projektin CyberCrime@IPA, ku janë propozuar një varg prioritetesh strategjike për luftimin e krimit kompjuterik, e ku parashihen masa për mbrojtjen e fëmijëve kundër shfrytëzimit seksual dhe abuzimit seksual në Internet.

Për momentin, në Kosovë ekziston problemi i mos definimit të qartë të veprave që bëhen kundër fëmijëve me përdorimin e Internetit, si dhe problemi i zbatimit të legjislacionit ekzistues në dobi të mbrojtjes së fëmijëve nga rreziqet që sjell interneti. Kështu, legjislacioni në Kosovë nuk parasheh asnjë lloj obligimi për ofertuesit e shërbimeve të internetit, ose për ata që u bëjnë të mundur fëmijëve qasjen në internet, që të parandalojnë qasjen në përmbajtje që nuk i përgjigjet moshës së fëmijëve, qoftë ajo ilegale ose dëmshme për ta. Nga ana tjetër, dyshohet se rastet e abuzimit përmes Internetit nuk raportohen në masën e duhur, aq më pak, pasi nuk ekziston ndonjë sistem i raportimit on-line, ose ndonjë linjë ku qytetarët mund të drejtohen në rast të abuzimit të fëmijëve. Edhe ato politika që ekzistojnë dhe janë të aprovuara nuk fuqizohen, kështu që mbetet një zbrazëti ligjore, e cila mund të shfrytëzohet nga keqpërdoruesit që t'i shkaktojnë dëme fëmijëve.

Megjithatë, një mundësi e mirë për ta plotësuar legjislacioni në fushën e mbrojtjes së fëmijëve nga rreziqet në internet është trendi i përafrimit të legjislacionit kosovar me atë të BE, si pjesë e procesit të stabilizim-asocimit. Ndryshimet në legjislacion duhet shfrytëzuar për t'i bërë plotësimet e domosdoshme me norma që paraqesin mbrojtje të drejtpërdrejtë të fëmijëve nga abuzimet "on-line". Procesi i stabilizim-asocimit dhe monitorimi i vazhdueshëm që i bëhet Kosovës në fushën e sundimit të ligjit është, po ashtu, mundësi e mirë për të këmbëngulur në zbatimin e plotë të legjislacionit ekzistues, pasi as ai nuk është i zhveshur nga të gjitha mekanizmat që mbrojnë fëmijët nga abuzimi "on-line".

2.3. KAPACITETET VENDORE

Përkundër informacionit të shtuar për mundësitë e abuzimit të fëmijëve “online”, si dhe për mundësitë e luftimit të kësaj dukurie, këto njohuri nuk zbatohen sa duhet nga politikëbërësit. Besohet se kjo ndodhë për shkak të faktit se në botën e internetit, fëmijët ende nuk njihen si një grup i veçantë që ka nevojë për vëmendje të veçantë. Kështu, ndodhë që për rreziqet që i kërcënojnë fëmijët nga interneti të fajësohet vet mediumi, ndërkohë që, nga mos informimi ose mosbindja, dështohet në marrjen e masave mbrojtëse.

Sfidat kryesore:

- Kapacitetet njerëzore për adresimin e çështjeve të sigurisë në internet
- Kapacitetet infrastrukturore për mbrojtje nga rreziqet
- Dhuna verbale përmes Internetit
- Kontrolli i rrjeteve te ofertuesit

ARKEP është në proces të krijimit të Qendrës Kompjuterike për Reagime Emergjente/CERT në nivel nacional, e cila do të ketë rol edhe në shtimin e sigurisë në Internet, e në veçanti në ndërtimin e kapaciteteve për të ofruar internet të sigurt. Po ashtu, ekzistojnë nisma të organizatave të shoqërisë civile për shtimin e sigurisë “online”, të cilat, deri tani kanë rezultuar me krijimin e grupeve të punës që do ta adresojnë këtë çështje si dhe të materialeve informative për fëmijë, mësimdhënës dhe prindër. Këto nisma kanë ndikuar të vihen në lëvizje edhe institucionet shtetërore, kështu që, me përkrahjen e projektit “PROCON” është krijuar grupi i palëve të interesit ku, përveç agjencive qeveritare, janë të përfaqësuara edhe bizneset e fushës së TIK-ut, ofertuesit e shërbimeve të internetit dhe organizatat e shoqërisë civile. Policia e Kosovës ka sektor të veçantë për krimin kompjuterik, i cili merret edhe me rastet eventuale të abuzimit të fëmijëve dhe rasteve te tjera përmes rrjetit global.

Megjithëkëtë, nuk mund të thuhet se zyrtarët policorë janë të trajnuar për t’i menaxhuar situatat kur fëmijët janë viktima të aktiviteteve të sofistikuara përmes internetit. Po ashtu, është e pranishme dukuria e mos raportimit të rasteve të abuzimit përmes internetit. Në mungesë të kontrollit të rrjetit global, fëmijët i janë të ekspozuar të gjitha llojeve të rreziqeve, duke filluar nga qasja në përmbajtje joadekuate me moshën e deri te format e ndryshme të ngacmimit apo edhe dhunës verbale. Ç’është e vërtetë, zhvillimi i shpejtë i teknologjisë dhe përhapja e përdorimit të saj ka bërë që të mos zhvillohen sa duhet mekanizmat për mbrojtje nga keqpërdorimet. Deri tani nuk ka ndodhur që ndonjë autoritet, ose ofertues i shërbimeve të internetit ta bllokojë ndonjë faqe abuzuese në internet për përdoruesit nga Kosova në bazë të një procedure të strukturuar, por ka pasur raste individuale kur kompanitë ose autoritete përgjegjëse kanë vepruar në këtë drejtim. Gjithashtu, programet e kontrollit prindëror nuk janë shumë të përhapura. Po ashtu, internet kafetë e shumta funksionojnë si biznese të cilave ju mungon kontrolli i shfrytëzuesve dhe i përmbajtjes që ju ofrohet atyre, kështu që ka raste kur përmes kompjuterëve në këto lokale fëmijët rrezikohen nga Interneti.

Në vendet evropiane tanimë ekziston përvoja relevante për të ju kundërvënë dhunës përmes internetit, ndërkaq në Kosovë ka individë dhe organizata që, me entuziazëm, merren me këtë fushë. Prandaj, edhe nuk duhet reshtur së kërkuari strategji të reja për të ofruar një internet më të sigurte, e që shtrihen nga aktivitetet masive të vetëdijesimit, deri te përfshirja aktive e ofertuesve të internetit në mbrojtjen e klientëve të tyre të vegjël nga rreziqet që sjell ai.

Mungesa e kontrollit të rrjetit në nivelin e ofertuesit paraqet një rrezik të përhershëm për sigurinë e fëmijëve që e shfrytëzojnë rrjetin global. Tanimë ka raste kur fëmijët dhe të rinjtë janë joshur nga bashkëbisedues virtualë për t'u shantazhuar më pastaj ose edhe me qëllim trafikimi. Për këtë arsye, ofertuesit duhet të kenë mekanizma për gjurmimin e keqbërësve për aq sa një gjë të tillë e lejon teknologjia në dispozicion. Një rrezik tjetër që mund të shfaqet me kohën, si rezultat i zgjerimit të përdorimit të teknologjisë, është shtimi i dhunës verbale përmes internetit. Rrjetet sociale, telefonat celularë, rrjetet 3G, ofrojnë kushte për abuzime të tilla në çdo vend dhe në çdo kohë.

2.4. ARSIMI

Rezultatet e hulumtimeve të deritanishme flasin për shtimin e dukurisë së dhunës "online", pikërisht në kontekstin arsimor. Anketa me 1,150 nxënës të moshës 9-16 vjeç e zhvilluar nga FIT (Qendra për Studime të Avancuara) në shtatë komunat më të mëdha të Kosovës tregon se vetëm 35% të nxënësve ndihen shumë të sigurt gjatë përdorimit të Internetit. Pastaj, 41% të anketuarve pranojnë se kanë shikuar përmbajtje pornografike, ndërkaq 28% e tyre kanë përjetuar dhunën verbale përmes Internetit. Të gjitha këto të dhëna flasin në favor të nevojës që të shfrytëzohet konteksti arsimor, pra shkolla, ku fëmija e kalon një pjesë të mirë të ditës, për të ndërtuar kapacitetin e fëmijëve që t'i kundërvihen rrezikut që vjen nga Interneti.

Sfidat kryesore:

- Kapacitetet e personelit arsimor për t'i udhëzuar fëmijët të mbrohen nga rreziqet
- Kapaciteti i komunitetit shkollor për mbrojtje
- Infrastruktura teknologjike në institucionet arsimore
- Vetedijesimi dhe fuqizimi i nxënësve për t'u mbrojtur nga rreziqet

Organizatat ndërkombëtare si ITU, rrjeti Evropian për Internet të Sigurt, madje edhe OJQ-të vendore si FIT, kanë nxjerrë materiale për vetëdijesimin e fëmijëve, prindërve dhe të mësimdhënësve, madje janë kujdesur që këto materiale t'ia përshtatin grup-moshave të ndryshme. Këto materiale tanimë janë shpërndarë në disa shkolla, duke përmirësuar aftësinë e fëmijëve për vetëmbrojtje nga rreziqet e Internetit. MASHT, OSCE dhe Policia e Kosovës kanë punuar së bashku në kuadër të projektit "Programi për vetëdijesimin në bashkësi", ku janë trajnuar policë dhe mësimdhënës, si dhe janë zhvilluar disa mësime model të cilat edhe janë realizuar në kuadër të procesit mësimor. Po ashtu disa shkolla kanë filluar të përpilojnë rregulla për shfrytëzimin e Internetit dhe pajisjeve të TIK-ut me qëllim të vetëm që të edukohen fëmijët për përdorimin e drejtë të tyre. Në përgjithësi, autoritetet arsimore janë treguar të hapura ndaj nismave për vetëdijesimin e nxënësve për rreziqet nga Interneti dhe kanë lejuar që në shkollat publike të

zhvillohen aktivitete të kësaj natyre. Disa shkolla kanë shkuar edhe më larg, duke pasur sukses që aktivitetin e tyre vetëdijësues ta shtrijnë edhe në komunitetin të cilit i shërbejnë.

Me gjithë vullnetin e mirë, akoma nuk mund të thuhet se shkollat janë të përgatitura për t'i aftësuar fëmijët që të mbrohen nga rreziqet e ndryshme që sjell rrjeti global. Në radhë të parë, kjo ndodhë për shkak të mospërgatitjes së mësimdhënësve që të ballafaqohen me probleme të tilla, por, në masë të madhe bëhet fjalë edhe për mungesën e nismave në nivel shkolle, si dhe për mangësitë në teknologjinë me të cilën disponon shkolla. Po ashtu, teknologjia e informacionit dhe interneti nuk përdoren shumë për realizimin e përmbajtjeve mësimore dhe kjo bën që fëmijët, kryesisht ta shfrytëzojnë internetin për qëllime socializmi ose për lojë, duke mos e kuptuar sa duhet fuqinë dhe dobinë e vërtetë që ai sjell.

Mungesa e kontrollit prindëror në shfrytëzimin e internetit është një faktor tjetër që ka ndikim mjaft të madh tek fëmijët, duke marrë parasysh se interneti më pak shfrytëzohet në shkollë, e më shumë në shtëpi, kur fëmija duhet të jetë nën mbikëqyrjen e prindit.

Një mundësi e mirë për të punuar në kontekstin shkollor është Korniza e Re e Kurrikulit, e cila shkollës i jep një shkallë të gjerë të autonomisë në përzgjedhjen e përmbajtjeve që do të zhvillohen me nxënës. Kjo Kornizë ofron mundësi që interneti të shfrytëzohet si burim i materialeve mësimore, duke shpalosur para fëmijëve një aspekt të ri të dobisë së rrjetit global. Implementimi i Kornizës së Kurrikulit përkrahet nga Projekti i Binjakëzimit i financuar nga BE "Mbështetje për Zbatimin e Planit Strategjik të Sektorit të Arsimit në Kosovë 2011-2016" i cili inkurajon shfrytëzimin e teknologjisë për arritjen e këtij qëllimi. Mbështetja tjetër do të vjen nga "Projekti TIK në fushën e arsimit – faza 2" i financuar nga BE, i cili promovon përdorimin e mësimit elektronik në klasë. Po ashtu, pajisja e shkollave me teknologji adekuate dhe qasje në internet në të ardhmen, hap mundësi që fëmijët të njihen me rreziqet, duke shfrytëzuar materiale adekuate të transmetuara nga njerëz të kualifikuar. Shkolla mund të jetë pika përmes së cilës bëhet vetëdijesimi për rreziqet, jo vetëm i fëmijëve, por edhe mësimdhënësve dhe prindërve që duhet t'i mbështesin ata.

Prirja e të rinjve për t'i përvetësuar shumë më shpejtë teknologjitë e reja paraqet një rrezik të vazhdueshëm që mësimdhënësit dhe prindërit të ngecin në përpjekje për t'i ndihmuar fëmijët në shmangien e rreziqeve, duke mos qenë në gjendje ta identifikojnë problemin atëherë kur shfaqet dhe duke mos qenë në gjendje për të reaguar në mënyrë adekuate. Një rrezik tjetër është mospërshtatja e një numri të konsiderueshëm të mësimdhënësve me trendet. Duke harruar se teksti mësimor nuk është më burimi i vetëm i informacionit për nxënësit dhe duke anashkaluar internetin, ata i bëjnë një shërbim të keq fëmijëve, nga se krijojnë tek ata përshtypjen se arsimimi është i ndarë nga konteksti në të cilin ata jetojnë, e ky është konteksti kur pothuajse secili fëmijë e shfrytëzon internetit, në mënyrë të drejtë ose të gabuar, duke krijuar dobi ose dëm për vetveten.

2.5. BASHKËPUNIMI DHE KOORDINIMI

Meqë interneti është një medium global, një rol i veçantë për rregullimin e çështjeve në këtë fushë i takon organizmave ndërkombëtarë. Kështu, në vitin 1999, Bashkimi Evropian ka iniciuar Programin e Internetit të Sigurt (Safer Internet Program), i cili ka rezultuar me krijimin e qendrave për internet të sigurt në të gjitha vendet anëtare, si dhe me nisma për një internet të sigurte anekënd botës. Në vitin 2008, Unioni Ndërkombëtar i Telekomunikacionit (ITU) ka iniciuar nismën për mbrojtjen e fëmijëve "online" (Child Online Protection – COP), duke ndërtuar ura bashkëpunimi në mes të agjencive të ndryshme qeveritare dhe ndërqeveritare, përfshirë ato që janë të autorizuara për zbatimin e ligjit.

Sfidat kryesore:

- Krijimi i një fonti të përbashkët për mbrojtjen e fëmijëve nga rreziqet në internet
- Shkëmbimi i informatave dhe materialeve në mes të palëve të ndryshme
- Implementimi i strategjive dhe planeve për minimizimin e rrezikut në internet

Aktiviteti i palëve me interes duhet të jetë i përbashkët dhe i bashkërenditur, sepse ato mbulojnë aspekte të ndryshme të sigurisë në internet. Kështu, shkolla nuk mund të bëj asgjë pa familjen dhe ofertuesit e shërbimeve të internetit, ndërkaq agjencitë shtetërore nuk mund ta zbatojnë asnjë normë ligjore për mbrojtjen e fëmijëve nga rreziqet pa i vetëdijesuar fëmijët dhe qytetarët për këto rreziqe.

Qeveria e Kosovës ka bërë disa përpjekje për ta përmirësuar gjendjen në fushën e TIK-ut, si duke furnizuar institucionet shtetërore, edukative-arsimore dhe shkencore me pajisje adekuate, ashtu edhe duke nxitur përdorimin e teknologjisë në kryerjen e punëve të përditshme dhe ofrimin e shërbimeve për qytetarë. Në këtë aspekt, janë bërë përpjekje edhe për ta përmirësuar sigurinë e shfrytëzimit të teknologjisë, duke bashkëpunuar me të gjitha palët me interes në luftimin e dukurive negative siç janë pornografia e fëmijëve, dhuna përmes Internetit, e të ngjashme. Për shembull, Agjencia Shtetërore për Mbrojtjen e të Dhënave Personale në Strategjinë e vet për periudhën 2014-2017 shpreh përkushtimin që të punojë për "të arsimuar e trajnuar gjeneratat e reja lidhur me shfrytëzimin e sigurt të përdorimit të internetit dhe teknologjisë informative", si dhe për të "bashkëpunuar me institucionet edukativo-arsimore dhe shoqërinë civile, ombduspersonin etj., në mbrojtjen dhe sensibilizimin e qytetarëve rreth të drejtave të tyre lidhur me mbrojtjen e të dhënave personale" (Agjencia Shtetërore për Mbrojtjen e të Dhënave Personale, 2013). Megjithatë, nevojitet një përkushtim shumë më i madh që teknologjia informative të depërtojë në institucione edukative arsimore, duke bërë furnizimin e tyre me pajisje të duhura, si dhe duke financuar mirëmbajtjen e tyre.

Përkundër faktit se një numër i institucioneve shtetërore dhe i organizatave të shoqërisë civile kanë proklamuar qëllimin për të ofruar një internet më të sigurt, bashkëpunimi në mes të

këtyre palëve nuk është në nivelin e duhur. Ende ka raste kur këto palë zhvillojnë strategji dhe veprimtari të izoluara për të adresuar problemin e sigurisë në internet pa i kushtuar rëndësi të duhur faktit se siguria në internet është ndërmarrje shumë komplekse që mund të bëhet vetëm në bashkëpunim të ndërsjellë. Akoma nuk ekziston një databazë e rasteve të cenimit të sigurisë në internet që do të mundësonte analiza më të thella të shkaqeve të këtyre dukurive dhe zgjidhjeve që çojnë drejt përmirësimit. Edhe ofertuesit e internetit deri tani nuk kanë marrë ndonjë nismë për ngritjen e sigurisë së shfrytëzimit, qoftë duke aplikuar filtra ose duke zhvilluar aktivitete vetëdijesimi për konsumatorët. Përderisa nuk ekzistojnë faqe kreative që joshin fëmijët për të zhvilluar aktivitete kuptim plota dhe në pajtim me moshën e tyre, ekziston rreziku që ata të orientohen drejt faqeve me përmbajtje të papërshtatshme për ta, madje edhe të rrezikshme.

Mundësitë e bashkëpunimit në mes të palëve relevantë në fushën e mbrojtjes së fëmijëve nga rreziqet e internetit, hapin perspektiva për adresimin e problemeve që nuk janë adresuar në mënyrë adekuate deri tani. Kështu, shfrytëzimi i materialeve që janë krijuar deri tani dhe koordinimi i veprimeve për zhvillimin e mekanizmave të ri mbrojtës ofrojnë mundësi të reja për gjetjen e zgjidhjeve kreative që i bëjnë fëmijët më të sigurt në internet.

Mos implementimi i strategjive që adresojnë çështjen e sigurisë në internet, e në veçanti, mos implementimi i kësaj strategjie, paraqesin një rrezik për eskalimin eventual të problemeve të sigurisë në internet në incidente serioze që mund t'i dëmtojnë fëmijët. Gjëra të tilla mund të ndodhin nëse do të mungon gatishmëria për bashkëpunim në mes të palëve me interes që janë të obliguara të merren me adresimin e çështjeve të sigurisë në internet.

2.6. VETËDIJESIMI

Ka pak të dhëna për mënyrën se si prindërit dhe mësimdhënësit i përgjigjen sfidës së mbrojtjes së fëmijëve në mjedisin "online", por dihet se ata nuk kanë informacion të mjaftueshëm për mundësitë e keqpërdorimit të fëmijëve përmes teknologjive të reja. Hulumtimet tregojnë se fëmijët dhe të rinjtë, të shumtën, nuk i shohin prindërit si adresën e parë që i drejtohen në rast të ndonjë abuzimi që mund ta përjetojnë përmes internetit, nga se të shumtën mendojnë se prindërit nuk e kuptojnë botën në të cilën ndodhë abuzimi. Megjithatë, hulumtimet tregojnë se shumë fëmijë do të kishin dashur që prindërit të jenë më shumë të përfshirë (UNICEF, 2012).

Sfidat kryesore:

- Dallimi në shkathtësi teknologjike në mes të të rriturve dhe të rinjve
- Shkalla e lartë e shfrytëzimit të internetit nga fëmijët pa ndonjë kufizim
- Balanci në mes të shfrytëzimit normal dhe vënies së vetes në situata të rrezikshme

Edhe në Kosovë, janë bërë disa studime për internetin dhe industrinë e Teknologjisë së Informacionit që kanë vënë në pah nevojën për të punuar për një siguri më të madhe në internet, e në veçanti, për mbrojtjen e fëmijëve. Kosova është bërë pjesë e nismës Safer Internet Day dhe në shkurt të vitit 2015 do të organizohet një konferencë për promovimin e

sigurisë në rrjetin global. Në këtë drejtim, vlen të përmendet hulumtimi që e ka bërë organizata joqeveritare FIT, në bashkëpunim me "Save the Children", e ku për herë të parë jepen disa të dhëna për shkallën dhe modalitetet e përdorimit të internetit tek fëmijët. Hulumtimi tregon se rreth 93% e fëmijëve në shkollat e qyteteve të mëdha të Kosovës të moshës 9-16 vjeç janë përdorues të internetit, por kjo vlen vetëm për 76% të prindërve të tyre.

Në Kosovë kanë filluar të zhvillohen disa aktivitete vetëdijesimi për mbrojtjen e fëmijëve nga rreziqet "online" të mbështetura nga organizata të shoqërisë civile, por edhe disa institucione shtetërore. Po ashtu, janë prodhuar disa materiale promovuese në gjuhën shqipe që paraqesin bazë të mirë për zhvillimin e aktiviteteve të vetëdijesimit. Si rezultat i këtyre aktiviteteve dhe ndërgjegjësimit të përgjithshëm të shoqërisë, është ngritur vetëdija për rrezikun që interneti mund të paraqet për fëmijët, gjithnjë duke pasur kujdes që dobia e internetit të mos anashkalohet në emër të rreziqeve që ai sjell. Është e nevojshme që këto materiale të vihen në dispozicion edhe në gjuhën serbe dhe turke, në mënyrë që të mund të shfrytëzohen nga pjesëtarët e të gjitha komuniteteve etnike.

Me gjithë progresin, në Kosovë ka mjaft vështirësi për të ofruar një mjedis të sigurte për fëmijët në internet, në radhë të parë për faktin se prindërit dhe mësimdhënësit ngecin pas fëmijëve në kuptim të njohjes së rreziqeve të pranishme dhe strategjive për luftimin e tyre. Me shtimin e telefonave të tipit "smart" fëmijët fitojnë gjithnjë e më shumë mundësi që t'i qasen internetit jashtë kontrollit të të rriturve. Gjithashtu, nuk janë të njohura sa duhet burimet ekzistuese që ofrojnë materiale promovuese dhe vetëdijesuese për mbrojtje nga rreziqet që sjell interneti. Një portal i tillë është www.internetisigurte.org.

Kohëve të fundit, mediat e shkruara dhe elektronike kanë interesim për të trajtuar temën e internetit të sigurte, kështu që përfshirja e tyre shihet si një mundësi e mirë për të organizuar një fushatë të mirëfilltë vetëdijesimi. Po ashtu, ekziston disponimi që të inkuadrohen edhe operatorët e internetit dhe televizionit kabllovik, të cilët mund t'i përcjellin mesazhet përmes kanaleve të tyre. Softuerët për "parental access control" janë në dispozicion dhe janë pa pagesë, kështu që mund të shfrytëzohen nga prindërit për të ushtruar një lloj kontrolli ndaj fëmijëve të tyre, kuptohet me kusht që njerëzit të vetëdijesohen për përdorimin e tyre.

Ekzagjerimi i rreziqeve nga interneti mund të jetë krejtësisht kundër produktiv për shfrytëzuesit e vegjël, nga se i privon ata nga mundësia që t'i shfrytëzojnë burimet e rrjetit global në emër të mbrojtjes nga rreziku i supozuar. Megjithatë, vet interneti, realisht, paraqet rrezik të vazhdueshëm për fëmijët, nëse ata nuk janë të përgatitur për t'u vetëmbrojtur nga kanosjet ose për të kërkuar ndihmën e të rriturve në këtë drejtim. Po ashtu, disa pajisje teknologjike të integruara në mjetet për komunikim si web kamerat mund të paraqesin rrezik për shfrytëzuesin që komunikon me njerëz të panjohur. Një rrezik i vazhdueshëm është dështimi për të bërë dallimin në mes të realitetit të vërtetë dhe atij virtual, që mund të shkaktojë konfuzion tek fëmijët që rezulton me veprime të rrezikshme për ta.

3. QËLLIMI DHE OBJEKTIVAT STRATEGJIKE

Qëllimi kryesor i këtij plani strategjik është që të krijohet një mjedis më i sigurt për fëmijët në Internet, ku ata mbrohen nga format e ndryshme të abuzimit. Kjo nënkupton:

- Vetëdijesimin dhe fuqizimin e fëmijëve që ata të jenë më rezistentë ndaj rreziqeve që ju kanosen nga shfrytëzimi i internetit;
- Ndëshkimin e abuzuesve me fëmijë në internet;
- Reduktimin e qasjes së fëmijëve në materiale të dëmshme për ta;
- Ofrimi i ndihmës fëmijëve që janë në rrezik nga abuzimi përmes internetit.

Komisioni Evropian (2012) ka adaptuar Strategjinë Evropiane për Internet më të mirë për fëmijët, e cila fton për krijimin e një mjedisi më të sigurt dhe të dobishëm për fëmijët, duke kombinuar masa të karakterit legjislativ, si dhe ato vetë-rregulluese dhe financiare.

Edhe ky plan strategjik nxjerr në pah masa të karakterit legjislativ, të kombinuara me ngritjen e kapaciteteve dhe vetëdijes publike për të adresuar mbrojtjen e fëmijëve në Internet. Rëndësi e veçantë i kushtohet koordinimit më të mirë në mes të palëve relevante të interesit, si dhe fuqizimit të fëmijëve përmes shkollës.

Gjatë procesit të planifikimit janë përcaktuar pesë objektiva të Planit Strategjik:

1. Kornizë ligjore që garanton siguri të plotë gjatë qasjes së fëmijëve në internet.
2. Kapacitetet e ngritura të palëve të interesit, që mbështesin dhe garantojnë sigurinë e fëmijëve në internet.
3. Sistem arsimor me kapacitete të mjaftueshme njerëzore dhe teknologjike për të mbrojtur fëmijët nga rreziqet në internet
4. Koordinimi dhe bashkëpunimi mes autoriteteve publike dhe palëve tjera të interesit që angazhohen për sigurinë e fëmijëve në internet
5. Vetëdije e ngritur e publikut për rol aktiv në mbrojtje të fëmijëve nga rreziqet në internet.

OBJEKTIVI 1: KORNIZË LIGJORE QË GARANTON SIGURI TË PLOTË GJATË QASJES SË FËMIJËVE NË INTERNET

Konventa për të Drejtat e Fëmijës kërkon nga të gjitha shtetet që në zhvillimin e legjislacionit, sigurimin e zbatimit të tij, si dhe në ofrimin e mbrojtjes sociale dhe masave mbrojtëse, interesat e fëmijës të jenë gjithnjë në qendër. Prandaj, korniza ligjore duhet të ofrojë bazë për mbrojtjen e fëmijëve nga abuzimi, por edhe për ndjekjen e vet abuzuesve. Nga ana tjetër, të drejtat e garantuara në Konventë duhet të aplikohen për të gjithë fëmijët, pa diskriminim, prandaj korniza ligjore duhet ta ketë parasysh shumësinë e mënyrave se si fëmijët e shfrytëzojnë internetin dhe të abuzimeve që mund të ndodhin. Po ashtu, korniza ligjore duhet të nxisë krijimin e mundësive për të përfituar nga shfrytëzimi i internetit, duke siguruar njëkohësisht që fëmijët të mos dëmtohen duke iu ekspozuar përmbajtjeve të papërshtatshme ose rreziqeve që vijnë nga mjedisi “online”.

Meqë korniza ligjore në Kosovë është krijuar në kohën e shfrytëzimit masiv të kompjuterit dhe rrjeteve kompjuterike, ajo edhe përmban norma që adresojnë çështje nga komunikimet elektronike, me gjithë se jo gjithnjë me përqendrim te mbrojtja e fëmijëve dhe të drejtave të tyre.

Masat

Masa 1.1. Analiza e legjislacionit ekzistues

Përshkrimi: Legjislacioni ekzistues ofron shkallë minimale të mbrojtjes së fëmijëve nga rreziqet që sjell interneti, por kjo mbrojtje, kryesisht, ka të bëj me sanksionimin e abuzimeve, e jo me parandalimin në mënyre specifike. Për këtë arsye, do të bëhet një analizë e detajuar e legjislacionit ekzistues, me qëllim të identifikimit të zbrazëtive që krijojnë hapësirë për abuzime. Në veçanti do të analizohen Ligji për mbrojtjen e të dhënave personale, Ligji për komunikimet elektronike, Kodi Penal i Kosovës, Ligji për krimet kibernetike, drafti i Ligjit për mbrojtjen e fëmijëve, si dhe aktet nënligjore përkatëse. Krahas kësaj do të analizohet edhe legjislacioni evropian për sigurinë në internet si dhe dokumentet strategjike të Komisionit Evropian që shërbejnë si bazë për hartimin e legjislacionit në vendet anëtarë. Pritet që e gjithë kjo analizë të rezultojë me një raport që do të përmbajë rekomandime të qarta dhe të zbatueshme për ndryshime legjislative që avancojnë mbrojtjen e fëmijëve gjatë shfrytëzimit të internetit në Kosovë.

Procesi do të udhëhiqet nga Zyra për Qeverisje të Mirë në Zyrën e Kryeministrit dhe do të nënkuptojë konsultim me bazë të gjerë të të gjitha palëve me interes, në veçanti të agjencive qeveritare që merren me mbrojtje të fëmijëve, por edhe organizatave joqeveritare dhe komunitetit të biznesit.

Masa 1.2. Plotësimi/ndryshimi i ligjeve ekzistuese

Përshkrimi: Varësisht nga analiza e legjislacionit ekzistues dhe rekomandimet që do të dalin nga kjo analizë, do të bëhen ndryshime dhe plotësime të legjislacionit, në mënyrë që të sigurohet një shkallë më e lartë e mbrojtjes së fëmijëve nga rreziqet në internet. Legjislacioni i ri do të hartohet në bashkëpunim me të gjitha palët e interesit, e në veçanti organizatat joqeveritare që merren me mbrojtjen e të drejtave të fëmijës, si dhe me industrinë e TIK-ut. Gjatë procesit do të konsultohet legjislacioni evropian dhe i vendeve anëtare të BE, në mënyrë që zgjidhjet e propozuara të jenë në përputhje me praktikat më të mira dhe të ofrojnë mbrojtje sa më të mirë të fëmijëve.

Aprovimi i ligjeve të reja do të bëhet duke ndjekur procedurat e përcaktuara me Kushtetutë dhe me Rregulloren e Punës të Kuvendit të Kosovës.

Masa 1.3. Hartimi i legjislacionit sekondar

Përshkrimi: Qëllimi i legjislacionit sekondar është zbatimi efektiv i ligjeve të aprovuara nga organi ligjvënës. Këto ligje duhet të specifikojnë në mënyrë të qartë se cilat akte nënligjore duhet të pasojnë dhe kush i sjell ato. Prandaj, në këtë fazë, është vështirë të paragjykohet se çfarë legjislacioni sekondar do të duhet të aprovohet.

Megjithatë, ndihet nevoja për udhëzime të qarta që kërkojnë nga ofruesit e shërbimeve të internetit të aplikojnë filtra për përmbajtje të papranueshme siç janë faqet që nxisin pedofilinë ose format e tjera të dhunës ndaj fëmijëve. Po ashtu, pritet që ofruesit e shërbimeve të kontribuojnë në vetëdijesimin e fëmijëve dhe publikut të gjerë për rreziqet që sjell interneti. Akte të tjera nënligjore mund të rregullojnë format e kontrollit që ushtrohen nga agjenci shtetërore ndaj ofruesve të shërbimeve të internetit, përfshirë edhe internet caffe-të, por edhe paraqitjen në media të fëmijëve për të minimizuar mundësitë për viktimizimin eventual të tyre.

OBJEKTIVI 2: KAPACITETET E NGRITURA TË PALËVE TË INTERESIT, QË MBËSHTESIN DHE GARANTOJNË SIGURINË E FËMIJËVE NË INTERNET

Qeveria, përfshirë agjencitë shtetërore si ARKEP, policia, gjyqësori dhe pushteti lokal patjetër duhet të sigurojnë mekanizma efektivë për mbrojtjen e fëmijëve në internet. Mirëpo, ka edhe palë të tjera që duhet të kontribuojnë në këtë proces siç janë: institucionet arsimore, organizatat e shoqërisë civile, bizneset, e kështu me radhë. Kapaciteti i këtyre palëve për të adresuar çështjet e sigurisë së fëmijëve në internet, në fakt, kushtëzon, shkallën e kësaj sigurie dhe cilësinë e mbrojtjes që u ofrohet atyre.

Masat

Masa 2.1. Identifikimi dhe analiza e palëve kyçe

Përshkrimi: MAShT tanimë ka formuar grupin e palëve të interesit që përfshin ARKEP-in, si rregullator i komunikimeve elektronike, STIKK-un si asociacionin e bizneseve nga fusha e teknologjisë së informacionit dhe komunikimit, PTK-në, IPKO-n dhe "Kujtesën" si tre ofertuesit më të mëdhenj të shërbimeve të Internetit, si dhe dy organizata joqeveritare me interes për të punuar në këtë fushë – KEC dhe KYC. Megjithatë, numri i palëve kyçe që mund dhe duhet të përfshihen në procesin e krijimit të internetit më të sigurt është shumë më i madh. Pjesë e këtij procesi duhet të jenë edhe agjenci të tjera shtetërore që kanë mision krijimin e një mjedisi më të sigurt për qytetarë dhe zbatimin e Ligjit, siç janë: Ministria e Punës dhe e Mirëqenies Sociale, Zyra për Qeverisje të Mirë, Policia e Kosovës, Gjyqësori, Agjencia për Mbrojtjen e të Dhënave Personale,etj., pastaj përfaqësuesit e tjerë të sektorit privat që janë të përfshirë në fushën e TIK-ut dhe komunikimeve elektronike, institucione arsimore, si dhe organizata të shoqërisë civile që kanë interes për të ndihmuar krijimin e një mjedisi të sigurt "online" për të gjithë.

Zyra për Qeverisje të Mirë e Kryeministrit (ZQM) do të bëj identifikimin e palëve kyçe që mbështesin dhe garantojnë sigurinë e fëmijëve në internet, me qëllim të bashkimit të forcave dhe arritjes së rezultati sa më efektiv. Disa prej këtyre palëve kyçe, siç janë institucionet arsimore dhe organizatat e shoqërisë civile, kanë nevojë për ndërtim kapaciteti me qëllim që pastaj të mund ta ofrojnë ndihmën e vet.

Masa 2.2. Mbledhja e të dhënave për sigurinë në Internet

Përshkrimi: Për të siguruar një mbrojtje sa më të mirë të fëmijëve në internet duhet të njihen më thellë format e cenimit të sigurisë së tyre, si dhe shkalla e cenimit të sigurisë. Për këtë qëllim, do të mbështeten hulumtime që çojnë në përshkrimin e shkaqeve dhe rrethanave të cenimit të sigurisë dhe ofrojnë rekomandime për

përmirësimin e sigurisë. Po ashtu, do të mblidhen të dhëna statistikore që do të shërbejnë si tregues për matjen e progresit dhe për hartimin e politikave dhe ndërhyrjeve të reja në këtë fushë.

Masa 2.3. Zhvillimi i burimeve njerëzore

Përshkrimi: Duke marrë parasysh faktin se pjesëmarrës në ofrimin e një mjedisi të sigurt për fëmijët në internet janë palë të ndryshëm, edhe nevojat e tyre për ndërtim të kapaciteteve njerëzore janë të ndryshme. Për shembull, zyrtarët policorë duhet të njihen më mirë me format e abuzimit përmes internetit për të qenë në gjendje t'i identifikojnë rastet që kërkojnë procedim ligjor, ndërkaq zyrtarët e ARKEP duhet t'i njohin përvojat e vendeve të tjera për të përcaktuar se ç' masa duhet të kërkojnë nga ofruesit e shërbimeve që fëmijët të jenë të sigurt në Internet. Ndërkaq, organizatat e shoqërisë civile duhet të përgatiten për fushata ndërgjegjësimi, si dhe për të punuar në rehabilitimin e viktimave eventuale të abuzimit përmes internetit.

Për këtë arsye, nuk është e mundur të krijohet një program i përgjithshëm i ndërtimit të kapaciteteve që do t'i shërbente të gjithë palëve me interes në përmbushjen e misionit të përbashkët. Megjithatë, ZQM, me ndihmën e partnerëve, mund të hartojë një program vetëdijesimi që do të ofronte informacion themelor për problemin në fjalë dhe, pak-a-shumë, do të mund të zbatohej tek të gjitha palët me interes. Pastaj, secili prej tyre duhet t'i zhvillojë programet specifike për ndërtim të kapacitetit që i përgjigjen natyrës së punës dhe funksionit të tyre. Po ashtu, zbatimi i programeve, qofshin ato në formë trajnimi, apo në forma të tjera, i takon vet palëve me interes, që nuk përjashton bashkëpunimin në mes tyre.

Masa 2.4. Zhvillimi i kapaciteteve infrastrukturore

Përshkrimi: Infrastruktura për ofrimin e sigurisë "online" ka të bëj me pajisjet harduerike dhe softuerin e nevojshëm për kryerjen e kësaj detyre. Gjithsesi, institucionet e Kosovës, në përputhje me autorizimet e veta, duhet të përcaktojnë se cili lloj i harduerit dhe softuerit duhet të përdoret për të krijuar internet më të sigurt për fëmijët dhe kush duhet ta instalojë atë. Kërkesa të veçanta mund të bëhen ndaj ofertuesve të shërbimeve të internetit, nga të cilët kërkohet të kenë infrastrukturë që mundëson shqyrtimin e rasteve potenciale të abuzimit me fëmijë përmes internetit, por edhe ndikon në mënyrë preventive.

Një ide është që softuerët e tipit "parental lock" të shpërndahen falas, bashkë me udhëzimet për përdorim, ndërsa ato të tipit "open source" edhe mund të përkthehen në gjuhët zyrtare të Kosovës.

OBJEKTIVI 3: SISTEM ARSIMOR ME KAPACITETE TË MJAFTUESHME NJERËZORE DHE TEKNOLOGJIKE PËR TË MBROJTUR FËMIJËT NGA RREZIQET NË INTERNET

Në kohën e sotme fëmijët fillojnë ta përdorin internetin në moshë shumë më të vogël se më herët, ndërkohë që vazhdimisht paraqiten shërbime të reja që mund të ndikojnë në sigurinë e fëmijëve. Sot nuk mjafton vetëm të mbrohen fëmijët në mjedisin "online", por kërkohet që ata të pajisjen me shkathtësi digjitale që bëjnë të mundur vetëmbrojtjen e tyre dhe marrjen e përgjegjësive në mjedisin "online". Është me rëndësi që fëmijët të jenë në gjendje të bëjnë zgjedhjen e vet në internet dhe, nëse hasin në rrezik, ta dinë se si të reagojnë dhe ku të kërkojnë ndihmë. Arritja e këtij qëllimi kërkon, jo vetëm të punohet me fëmijë, por edhe me prindër dhe profesionistë që punojnë me fëmijë, që ata të jenë në gjendje t'u ofrojnë fëmijëve mbështetjen më të mirë të mundshme.

Prandaj, brenda sistemit arsimor duhet të punohet me fëmijë, punonjës arsimi dhe prindër, duke i marrë parasysh nevojat specifike të secilit nga këto tri grupe të synuara.

Masat

Masa 3.1. Zhvillimi i programeve trajnuese dhe materialeve pedagogjike dhe vetëdijesuese për ndërtim kapaciteti

Përshkrimi: Tanimë ekzistojnë programe dhe materiale për mbrojtjen e fëmijëve nga rreziqet e internetit që janë hartuar nga organizata ndërkombëtare dhe projekte të realizuara në vend dhe në botë, por ato vazhdimisht duhet të adaptohen dhe t'i përshtaten të arriturave teknologjike dhe sfidave që vijnë bashkë me to. Kështu, FIT ka zhvilluar program fuqizimi për nxënës dhe mësimdhënës, i cili është përshtatur nga projekti PROCON për të shtuar sigurinë e përdorimit të internetit.

Me rastin e hartimit të programeve dhe materialeve duhet pasur parasysh nevojat specifike të nxënësve, mësimdhënësve dhe prindërve, rolin e tyre në krijimin e një mjedisi të sigurt për fëmijë, si dhe kohën që kanë në dispozicion. Kështu, fëmijët duhet të mësojnë se si ta shfrytëzojnë internetin në mënyrë të sigurt, si ta kuptojnë natyrën e rreziqeve "online" dhe t'i shmangin ato. Nga ana tjetër mësimdhënësit dhe prindërit duhet të aftësohen t'i vlerësojnë në mënyrë reale rreziqet, pa i dekurajuar fëmijët që t'i shfrytëzojnë të mirat që ofron interneti.

Materialet që zhvillohen duhet të jenë të përshtatshme për auditorin të cilit i dedikohen dhe sipas mundësisë, të shoqërohen me sesione informative ose sesione trajnimi që mbahen nëpër shkolla.

Masa 3.2. Ndërtimi i kapaciteteve të nxënësve, mësimdhënësve dhe prindërve

Përshkrimi: Fëmijët, si shfrytëzuesit e drejtpërdrejtë të internetit, duhet të aftësohen për t'u "vetëmbrojtur" nga rreziqet që u kanosen. Për këtë qëllim ata duhet të kuptojnë: 1) Cilat janë të drejtat e tyre në internet për informacion, privatësi, mbrojtje dhe pjesëmarrje; 2) Si të përdoret interneti në mënyrë të sigurt e me përgjegjshmëri, duke respektuar të drejtat dhe privatësinë e të tjerëve; 3) Cila është natyra e rreziqeve "online" dhe si t'i shmangen atyre; 4) Ku të drejtohen nëse ndihen të kërcënuar ose të frikësuar.

Përmbajtjet për nxënës mund të zhvillohen, përmes sesioneve të veçanta informative, por edhe si pjesë e programit mësimor të rregullt. Korniza e Re e Kurrikulës ia lë shkollës zhvillimin e përmbajtjes mësimore dhe secila shkollë mund ta trajtojë çështjen e sigurisë në internet, në kuadër të saj. Natyrisht, për të qenë e mundur një qasje tillë, paraprakisht duhet të përgatiten mësimdhënësit, të cilët do t'ua përcjellin nxënësve këto njohuri.

Në përgjithësi, mësimdhënësit dhe prindërit kanë nevojë për informacion për: 1) aktivitetet që bëjnë nxënësit dhe të rinjtë në internet; 2) përfitimet dhe rreziqet që sjell interneti; 3) mënyrat se si të krijohet siguri për nxënësit dhe të rinjtë; 4) mekanizmat për filtrimin dhe bllokimin e sajteve të dëmshme; 5) burimet e ndryshme për mësimdhënës dhe prindër. Ata duhet t'i kuptojnë format e ndryshme të sjelljes së dëmshme ose të rrezikshme të nxënësit, të jenë në gjendje t'i dallojnë simptomat dhe të bisedojnë me të rinjtë për sjelljen dhe raportet e tyre në internet.

Aftësimi i mësimdhënësve mund të bëhet përmes programeve të trajnimit që zhvillohen nga ofertues të ndryshëm, të akredituar nga MAShT, ndërkaq sesione informative për prindër mund të mbahen nga vet mësimdhënësit ose edhe organizata të shoqërisë civile.

Për të siguruar qëndrueshmërinë e kësaj ndërhyrjeje është e domosdoshme që përmbajtjet e tilla të gjejnë vend në programet e Fakultetit të Edukimit, në veçanti në atë pjesë që ka të bëj me edukimin e mësimdhënësve të ardhshëm për shfrytëzimin e teknologjisë në punën e tyre dhe kujdesin që duhet të tregojnë ndaj fëmijëve kur ata bëhen ose mund të bëhen viktima të abuzimeve online.

Masa 3.3. Vetëdijesimi i komunitetit shkollor

Përshkrimi: Një formë tjetër e vetëdijesimit të nxënësve, prindërve dhe mësimdhënësve për rreziqet që lidhen me shfrytëzimin e internetit nga fëmijët është organizimi i aktiviteteve vetëdijesuese në nivel të shkollës, e që mund të organizohen në formë të aktiviteteve kurrikulare dhe jashtë-kurrikulare.
Në këto aktivitete mund të marrin pjesë edhe organizatat e shoqërisë civile, si dhe pjesëtarët e komunitetit të shkollës, në mënyrë që ato të jenë sa më efektive.

Masa 3.4. Pajisja e institucioneve arsimore me infrastrukturë teknologjike

Përshkrimi: Me gjithë se ky plan strategjik ka të bëj me mbrojtjen e fëmijëve nga rreziqet që sjell interneti, pajisja e institucioneve arsimore me infrastrukturë teknologjike konsiderohet si hap me rëndësi drejt edukimit të fëmijëve që të mbrohen nga këto rreziqe. Shkollat e Kosovës duhet të jenë të pajisura me numër optimal kompjuterësh që janë të lidhur në internet dhe poashtu, duhet të mundësohet qasja në internet, për qëllime mësimore, edhe me pajisjet që i sjellin fëmijët.

Gjithsesi, qasja në internet duhet të shfrytëzohet për qëllime mësimore, prandaj edhe në shkolla duhet kufizuar qasjen në websajte që nuk janë në funksion të mësimit, e sidomos në websajte që mund ta zhvendosin vëmendjen e fëmijëve nga procesi mësimor.

OBJEKTIVI 4: KOORDINIMI DHE BASHKËPUNIMI MES AUTORITETEVE PUBLIKE DHE PALËVE TJERA TË INTERESIT QË ANGAZHOHEN PËR SIGURINË E FËMIJËVE NË INTERNET

Përvoja e deritanishme ka treguar që problemet e sigurisë në internet mund të zgjidhen vetëm përmes një qasjeje shumëdimensionale. Pjesëmarrja e të gjitha palëve relevante me interes është me rëndësi për të ofruar mbrojtje dhe përkrahje më të mirë të mundshme për fëmijët. Kështu krijohen kushte për qasje sistemore ndaj problemit të mbrojtjes së fëmijëve "online", si në kuptim të parandalimit, ashtu edhe të reagimit, përderisa interneti u vihet në dispozicion të gjithëve, pa diskriminim. Fëmijët dhe të rinjtë e kanë prioritet se si ta shfrytëzojnë internetin, e jo si të jenë të sigurt gjatë këtij procesi, prandaj është barrë e sektorit publik dhe atij privat të kujdeset që të krijohet një mjedis i sigurt edhe për këta shfrytëzues.

Bashkëpunimi dhe koordinimi i veprimeve në mes të palëve me interes bën të mundur që secili prej tyre të kontribuojë maksimalisht në krijimin e këtij mjedisi të sigurt, prandaj është me rëndësi të krijohen dhe forcohen mekanizma që mundësojnë koordinimin dhe bashkëpunimin.

Masat

Masa 4.1. Themelimi i trupit koordinues

Përshkrimi: Grupi i Palëve me Interes që koordinohet nga MAShT është trup i themeluar me mbështetjen e projektit PROCON dhe funksionon me mbështetjen e këtij projekti. Pas përfundimit të projektit, në fund të vitit 2015, duhet të themelohet një trup koordinues ku përfshihen të gjitha palët me interes dhe të koordinohet nga Zyra për Qeverisje të Mirë.

Detyrë themelore e këtij trupi do të jetë të bashkërendisë veprimet e autoriteteve publike, bizneseve, organizatave të shoqërisë civile dhe faktorëve të tjerë në ofrimin e një mjedisi më të sigurt për fëmijët në internet.

Ky trup koordinues do të shfrytëzojë kapacitetet administrative të ZQM për nevojat e sekretarisë së tij, duke mos shkaktuar implikime financiare për vet koordinimin.

Masa 4.2. Krijimi i sistemit te avancuar për shkëmbimin e informatave dhe materialeve

Përshkrimi: Trupi koordinues që do të themelohet nga ZQM, përveç qëllimit kryesor të bashkërendimit të veprimeve të gjithë palëvee, do ta ketë për qëllim edhe krijimin e një sistemi për shkëmbim të informatave dhe materialeve. Ky sistem (p.sh. takimet e rregullta, mailing lista, hapësire e përbashkët virtuale, buletini periodik etj.) do të mundësojë që të gjithë palët të japin dhe të marrin informacionet nga fusha e mbrojtjes së fëmijëve nga rreziqet në internet. Sistemi mund të ndërtohet dhe mirëmbahet nga Agjencia për Shoqëri

Informative që funksionon në kuadër të Ministrisë së Administratës Publike.

Po ashtu, krijimi i një sistemi të tillë do të ndihmonte të gjitha institucionet qeveritare dhe joqeveritare për qasje të përbashkët dhe koordinim të mirëfilltë. Do të pamundësonte dyfishimin e panevojshëm të veprimeve nga palë të ndryshme dhe do të ngritë nivelin e përgjegjshmërisë dhe llogaridhënies.

Masa 4.3. Funksionalizimi i njësisë për veprim të shpejtë

Përshkrimi: Do të funksionalizohet Ekipi për Reagim ndaj Emergjencave Kompjuterike – CERT (Computer Emergency Response Team) në nivel nacional që do të jetë përgjegjës për hetimin e incidenteve të sigurisë së rrjeteve dhe shërbimeve të komunikimeve elektronike. CERT do të funksionojë në kuadër te ARKEP.

Me qellim të luftimit të përmbajtjeve joligjore në internet, institucionet përgjegjëse krijojnë një sistem të thirrjeve telefonike (116) për edukimin e shoqërisë (posaçërisht të fëmijëve). Sistemi i thirrjeve telefonike do të funksionojë në kuadër të MPB dhe MZHE. Rol të rëndësishëm me rastin e reagimit duhet të ketë edhe MPMS, pasi sektorët e kësaj ministrie janë përgjegjës për mirëqenien e fëmijëve.

Institucionet përgjegjëse duhet të gjejnë mënyra për themelimin e një linje për këshillim (blueline) për të gjithë, me theks të veçantë tek fëmijët. Varësisht nga kapacitetet, ky shërbim mund të ofrohet nga bartës të tjerë joinstitucionalë.

OBJEKTIVI 5: VETËDIJE E NGRITUR E PUBLIKUT PËR ROL AKTIV NË MBROJTJE TË FËMIJËVE NGA RREZIQET E INTERNETIT

Qendra për Internet të Sigurt do të jetë bartëse e aktiviteteve të vetëdijesimit për mbrojtjen e fëmijëve nga rreziqet e internetit, por aktivitete të vetëdijesimit do të zhvillohen edhe nga palët e tjera me interes si institucionet qeveritare, bizneset dhe organizatat e shoqërisë civile. Qëllimi kryesor i aktiviteteve të tilla është që njerëzit të mendojnë për sigurinë e vet dhe të fëmijëve gjatë shfrytëzimit të internetit, duke shmangur kështu rreziqet e mundshme. Poashtu, përmes vetëdijesimit qytetarët njoftohen edhe me mundësitë dhe mekanizmat për paraqitjen dhe trajtimin e rasteve të abuzimit të sigurisë në internet.

Masat

Masa 5.1. Krijimi i platformës nacionale vetëdijësuese për rreziqet në internet

Përshkrimi: Në përputhje me praktikat vendeve të tjera evropiane, edhe Kosova do të krijojë një Qendër të Internetit të Sigurt (Safe Internet Center) e cila do të marr përgjegjësinë për të promovuar sigurinë në shfrytëzimin e internetit. Qendra e tillë do të menaxhohet nga një institucion që do të emërtohet në ndërkohë dhe do ta ketë për detyrë të ngrisë vetëdijen qytetare për sigurinë e internetit.

Përmes kësaj qendre do të shpërndahen materiale promovuese dhe vetëdijesuese, si dhe do të organizohen ngjarje që promovojnë përdorimin e internetit të sigurt.

Qendra për Internet të Sigurt do të jetë kontakti nacional me rrjetin ndërkombëtar të qendrave të tilla që funksionojnë shumë shtete të botës.

Masa 5.2. Organizimi i aktiviteteve për Ditën e Internetit të Sigurt

Përshkrimi: Dita e Internetit të Sigurt organizohet në muajin shkurt në mbi 100 vende të botës, duke filluar nga viti 2004. Prej vitit 2015, Dita e Internetit të Sigurt (SID) organizohet edhe në Kosovë nga Komiteti i Kosovës për shënimin e SID, i cili është i anëtarësuar në rrjetin evropian të SID. Në këtë ditë do të organizohen aktivitete që promovojnë përdorimin e internetit të sigurt, përfshirë edhe debate publike dhe konferenca. Njëkohësisht, mund të organizohen edhe promovime në shkolla, komunitete, ku do të shpërndahen materiale promovuese, ndërsa të njëjta mund të shpërndahen edhe përmes pikave të shitjes të ofertuesve të shërbimeve të Internetit. Për të gjitha këto ngjarje do të sigurohet mbulimi medial adekuat.

Dita e Internetit të Sigurt do të organizohet nga Qendra për Internet të Sigurt, në bashkëpunim me të gjitha institucionet tjera që ndikojnë në sigurinë e internetit, në veçanti institucionet shtetërore, bizneset, institucionet arsimore dhe organizatat e shoqërisë civile.

Masa 5.3. Seanca informative me bazë në komunitet

Përshkrimi: Qendra për Internet të Sigurt, në bashkëpunim me bizneset, institucionet arsimore dhe organizatat e shoqërisë civile, do të organizojë edhe aktivitete vetëdijesimi me bazë në komunitet.

Këto aktivitete mund të mbahen në shkolla, qendra publike të internetit, qendra komunitare dhe, përmes tyre, mund të njihen fëmijët, të rinjtë dhe pjesëtarët e komunitetit me rreziqet që kërcënohen nga shfrytëzimi i internetit. Po ashtu, gjatë këtyre aktiviteteve mund të shpërndahen edhe materiale promovuese.

Masa 5.4. Përfshirja e mediumeve në shpërndarjen e mesazheve dhe materialeve vetëdijesuese

Përshkrimi: Qendra për Internet të Sigurt dhe të gjitha palët me interes që punojnë për ofrimin e internetit të sigurt do të punojnë me mediet e shkruara dhe elektronike që mesazhet e tyre të përcillen tek qytetarët. Përveç zhvillimit të emisioneve edukative, debatuese për sigurinë në internet, përmes medieve do të shpërndahen informata për përdorimin e filtrave dhe softuerëve kontrolluese për internet. Po ashtu, do të emetohen spote promovuese që ndikojnë në ndërgjegjësimin e qytetarëve, si dhe do të publikohen banerë që çojnë në web faqen e Qendrës për Internet të Sigurt.

4. PLANI I VEPRIMIT DHE BUXHETI

Plani i veprimit dhe buxheti janë zhvilluar për gjithë periudhën e implementimit të Strategjisë. Që të dyja, plani i veprimit dhe buxheti, kanë karakter orientues dhe duhet të shërbejnë si bazë për plane dhe buxhete vjetore që hartohen nga agjenci përgjegjëse qeveritare duke ndjekur ciklin e zakonshëm të planifikimit. Kostoja totale financiare për përudhen 5-vjeçare është €345,100 dhe, kryesisht, do të mbulohet nga Buxheti i Konsoliduar i Kosovës. Nga ana tjetër, është e mundur që financimi nga burime të tjera të përdoret për t'i mbuluar shpenzimet e implementimit ose të zbatimit të aktiviteteve komplementare.

Agjencia përgjegjëse qeveritare e ngarkuar me implementimin e Planit Strategjik është Zyra e Kryeministrit për Qeverisje të Mirë. Sidoqoftë, në implementimin e Planit Strategjik do të përfshihet edhe një numër i agjencive të tjera si MASHT, ARKEP, Policia, si dhe autoritetet lokale.

Tabela 1 paraqet buxhetin e vlerësuar për implementimin e Planit Strategjik sipas objektivave strategjikë dhe viteve. Duhet vërejtur se buxheti për vitin 2015 është shumë më i ulët sesa buxheti për vitet pasuese, për shkak të faktit se procesi i planifikimit strategjik u zhvillua pasi kishte përfunduar procesi i planifikimit të buxhetit të Qeverisë.

Tabela 1. Buxheti për implementimin e Planit Strategjik

Fusha	Buxheti					
	2015	**2016**	**2017**	**2018**	**2019**	**Gjithsej**
Kornizë ligjore që garanton siguri të plotë gjatë qasjes së fëmijëve në internet	€ 4,500	€ 15,200	€ 18,000	€ 6,000	€ 0	€ 43,700
Kapacitetet e ngritura të palëve të interesit, që mbështesin dhe garantojnë sigurinë e fëmijëve në internet	€ 5,000	€ 11,850	€ 2,600	€ 600	€ 600	€ 20,650
Sistem arsimor me kapacitete të mjaftueshme njerëzore dhe teknologjike për të mbrojtur fëmijët nga rreziqet në internet	€ 0	€ 16,250	€ 24,000	€ 24,000	€ 24,000	€ 88,250
Koordinimi dhe bashkëpunimi mes autoriteteve publike dhe palëve tjera të interesit që angazhohen për sigurinë e fëmijëve në internet	€ 5,500	€ 10,800	€ 14,400	€ 14,400	€ 14,400	€ 59,500
Vetëdije e ngritur e publikut për rol aktiv në mbrojtje të fëmijëve nga rreziqet ne internet	€ 0	€ 44,800	€ 29,400	€ 29,400	€ 29,400	€ 133,000
	€ 15,000	**€ 98,900**	**€ 88,400**	**€ 74,400**	**€ 68,400**	**€ 345,100**

Plani i detajuar i zbatimit dhe kalkulimet buxhetore sipas objektivave strategjikë dhe masave strategjike janë dhënë në tabelat vijuese.

Objektivi 1: Kornizë ligjore që garanton siguri të plotë gjatë qasjes së fëmijëve në internet

Masa 1.1	**Analiza e legjislacionit ekzistues**									
Kodi	Aktiviteti	Periudha e zbatimit	Bartësi	Përshkrimi i shpenzimeve	B U XH E T I (EUR)					
					2015	2016	2017	2018	2019	Gjithsej
1.1.1	Themelohet grupi i ekspertëve për analizën e legjislacionit	shtator 2015	ZQM	30 ditë pune x 150 EUR = 4,500 EUR	4,500					4,500
1.1.2	Bëhet analiza e legjislacionit ekzistues dhe legjislacionit evropian	tetor-dhjetor 2015	Grupi i ekspertëve							-
1.1.3	Prezantohet raporti i analizës	janar 2016	ZQM	Shpenzimet e prezantimit		200				200
				Subtotali 1.1	4,500	200	-	-	-	4,700
Masa 1.2	**Plotësimi/ndryshimi i ligjeve ekzistuese**									
Kodi	Aktiviteti	Periudha e zbatimit	Bartësi	Përshkrimi i shpenzimeve	B U XH E T I (EUR)					
					2015	2016	2017	2018	2019	Gjithsej
1.2.1	Hartohet plani i veprimit për plotësimin dhe ndryshimin e legjislacionit për mbrojtjen e fëmijëve online	shkurt-mars 2016	Zyra ligjore e KM ZQM							-
1.2.2	Përgatiten draft-ligjet e reja dhe/ose ndryshimet e ligjeve ekzistuese	prill 2016-qershor 2017	Zyra ligjore e KM	Grupi i ekspertëve për një ligj: 50 ditë pune x 150 EUR = 7,500 EUR Kosto për 4 ligje: 30,000 EUR		15,000	15,000			30,000
1.2.3	Procedohen ligjet për aprovim në Kuvendin e Kosovës	2017	Qeveria							-

			Subtotali 1.2		-	15,000	15,000	-	-	30,000
Masa 1.3	**Hartimi i legjislacionit sekondar**									
Kodi	Aktiviteti	Periudha e zbatimit	Bartësi	Përshkrimi i shpenzimeve	B U XH E T I (EUR)					
					2015	2016	2017	2018	2019	Gjithsej
1.3.1	Hartohet plani për nxjerrjen e akteve nënligjore përkatëse bazuar në legjislacionin e aprovuar	korrik-shtator 2017	Zyra ligjore e KM në koordinim me ministritë përkatëse							-
1.3.2	Hartohen aktet nënligjore në bazë të planit të hartuar	tetor 2017 - qershor 2018	Ministritë përkatëse	Shpenzimet për hartimin e një akti nënligjor (ekspertiza) - 1,500 EUR 6 akte nënligjore x 1,500 EUR = 9,000 EUR			3,000	6,000		9,000
			Subtotali 1.3		-	-	3,000	6,000	-	9,000
				Gjithsej Objektivi 1:	**4,500**	**15,200**	**18,000**	**6,000**	**-**	**43,700**

Objektivi 2: Kapacitetet e ngritura të palëve të interesit, që mbështesin dhe garantojnë sigurinë e fëmijëve në internet

Masa 2.1	**Identifikimi dhe analiza e palëve kyçe**									
Kodi	Aktiviteti	Periudha e zbatimit	Bartësi	Përshkrimi i shpenzimeve	B U XH E T I (EUR)					
					2015	2016	2017	2018	2019	Gjithsej
2.1.1	Hartohet lista e palëve me interes për sigurinë e fëmijëve në internet	prill-maj 2015	ZQM							-
2.1.2	Zhvillohen takime dhe mbahen kontakte me palët me interes	Duke filluar nga qershori i vitit 2015	ZQM							-
2.1.3	Përfshihen palët me interes në aktivitetet që synojnë sigurinë e fëmijëve në internet	Duke filluar nga qershori i vitit 2015	ZQM							-
			Subtotali 2.1		-	-	-	-	-	-
Masa 2.2	**Mbledhja e të dhënave për sigurinë në internet**									
Kodi	Aktiviteti	Periudha e zbatimit	Bartësi	Përshkrimi i shpenzimeve	B U XH E T I (EUR)					
					2015	2016	2017	2018	2019	Gjithsej
2.2.1	Mbështeten hulumtime që çojnë drejt përmirësimit të sigurisë në internet	qershor 2015 - qershor 2017	ZQM	3 hulumtime x 2,000 EUR	2,000	2,000	2,000			6,000
2.2.2	Përcaktohen llojet e statistikave që duhet të mblidhen për të avancuar sigurinë në internet	shtator-dhjetor 2015	ZQM	Ekspertizë vendore: 20 ditë pune x 150 EUR	3,000					3,000
2.2.3	Bëhet mbledhja e të dhënave statistikore për sigurinë në internet	Duke filluar nga janari i vitit 2016	ZQM							-
			Subtotali 2.2		5,000	2,000	2,000	-	-	9,000

Masa 2.3	Zhvillimi i burimeve njerëzore									
Kodi	Aktiviteti	Periudha e zbatimit	Bartësi	Përshkrimi i shpenzimeve	B U XH E T I (EUR)					
					2015	2016	2017	2018	2019	Gjithsej
2.3.1	Hartohet një program informimi për sigurinë në internet që do të ju shërbente palëve me interes	janar-mars 2016	ZQM	Ekspertizë vendore: 50 ditë pune x 150 EUR		750				750
2.3.2	Mbahen sesione informimi për palët me interes	Duke filluar nga prill i vitit 2016	ZQM	Kosto për një sesion: Prezantimi: 150 EUR Shpenzime të tjera:150 EUR Dy sesione brenda vitit		600	600	600	600	2,400
			Subtotali 2.3		-	1,350	600	600	600	3,150
Masa 2.4	**Zhvillimi i kapaciteteve infrastrukturore**									
Kodi	Aktiviteti	Periudha e zbatimit	Bartësi	Përshkrimi i shpenzimeve	B U XH E T I (EUR)					
					2015	2016	2017	2018	2019	Gjithsej
2.4.1	Nxirret rregullorja për pajisjet e duhura të ofertuesve të internetit për të garantuar sigurinë në Internet	qershor - dhjetor 2016	ARKEP	Ekspertize vendore: 30 ditë pune x 150 EUR = 4,500 EUR Shpenzimet e konsultimit: 1,500 EUR		6,000				6,000
2.4.2	Kontekstualizohet softueri i tipit "parental lock" dhe hartohen udhëzime për përdorimin e tij	qershor-dhjetor 2016	ZQM	Ekspertizë vendore (mbikëqyrja edhe hartimi udhëzimit): 10 ditë pune x 150 EUR = 1,500 EU Shpenzimet e përkthimit: 1,000 EUR		2,500				2,500
2.4.3	Shpërndahet softuer i tipit "parental lock"	Nga janari i vitit 2017	ISP							
			Subtotali 2.4		-	8,500	-	-	-	8,500

Gjithsej Objektivi 2:	**5,000**	**11,850**	**2,600**	**600**	**600**	**20,650**				

Objektivi 3: Sistem arsimor me kapacitete të mjaftueshme njerëzore dhe teknologjike për të mbrojtur fëmijët nga rreziqet në internet

Masa 3.1	**Zhvillimi i programeve trajnuese dhe materialeve pedagogjike dhe vetëdijesuese për ndërtim kapaciteti**									
Kodi	Aktiviteti	Periudha e zbatimit	Bartësi	Përshkrimi i shpenzimeve	B U XH E T I (EUR)					
					2015	2016	2017	2018	2019	Gjithsej
3.1.1	Aktualizohen materialet ekzistuese për vetëdijesim nga rreziqet në internet dhe zhvillohen materiale të tjera	janar-prill 2016	MASHT	Ekspertizë vendore: 30 ditë pune x 150 EUR = 4,500 EUR Shpenzimet e shtypjes: 2,000 EUR		6,500				6,500
3.1.2	Zhvillohen programe të vetëdijesimit për mësimdhënës, prindër dhe nxënës	janar-prill 2016	MASHT	Ekspertizë vendore: 5 ditë pune x 150 EUR = 750 EUR		750				750
			Subtotali 3.1		-	7,250	-	-	-	7,250
Masa 3.2	**Ndërtimi i kapaciteteve të nxënësve, mësimdhënësve dhe prindërve**									
Kodi	Aktiviteti	Periudha e zbatimit	Bartësi	Përshkrimi i shpenzimeve	B U XH E T I (EUR)					
					2015	2016	2017	2018	2019	Gjithsej
3.2.1	Hartohet plani i sesioneve informative në shkolla	Në qershor, duke filluar nga viti 2016	MASHT							-
3.2.2	Ndërtohet kapaciteti i prezantuesve	maj-qershor 2016	MASHT	Seminar 2-ditor për 30 persona		1,000				1,000
3.2.3	Organizohen sesione informative në shkolla	Gjatë vitit shkollor, duke filluar nga shtatori i vitit 2016	MASHT & DKA	Kostoja e prezantimit 2-orësh: 40 EUR 1000 shkolla x 2 prezantime x 40 EUR = 80,000 EUR		8,000	24,000	24,000	24,000	80,000
			Subtotali 3.2		-	9,000	24,000	24,000	24,000	81,000

Masa 3.3	Vetëdijesimi i komunitetit shkollor									
Kodi	Aktiviteti	Periudha e zbatimit	Bartësi	Përshkrimi i shpenzimeve	B U XH E T I (EUR)					
					2015	2016	2017	2018	2019	Gjithsej
3.3.1	Organizohen aktivitete vetëdijesimi në nivel shkolle	Detyrë e vazhdueshme	MASHT & DKA	Mbështetja e aktiviteteve shkollore nga DKA: deri në 100 EUR për shkollë						-
			Subtotali 3.3		-	-	-	-	-	-
Masa 3.4	**Pajisja e institucioneve arsimore me infrastrukturë teknologjike**									
Kodi	Aktiviteti	Periudha e zbatimit	Bartësi	Përshkrimi i shpenzimeve	B U XH E T I (EUR)					
					2015	2016	2017	2018	2019	Gjithsej
3.4.1	Instalohet interneti dhe teknologjia bashkëkohore e rrjetit në të gjitha shkollat	2015-2020	MASHT	Kalkulimi i shpenzimeve për 1000 shkolla: rreth 7.5 mil. EUR						-
3.4.2	Pajisen shkollat me kompjuterë dhe aksesorë, si dhe sigurohet mirëmbajtja e tyre	2015-2020	MASHT	Kalkulimi i shpenzimeve për 32,000 kompjuterë krahas 8,000 kompjuterëve ekzistues: rreth 18.6 mil. EUR						-
			Subtotali 3.4		-	-	-	-	-	-
				Gjithsej Objektivi 3:	**-**	**16,250**	**24,000**	**24,000**	**24,000**	**88,250**

Objektivi 4: **Koordinimi dhe bashkëpunimi mes autoriteteve publike dhe palëve tjera të interesit që angazhohen për sigurinë e fëmijëve në internet**

Masa 4.1	**Themelimi i trupit koordinues**									
Kodi	Aktiviteti	Periudha e zbatimit	Bartësi	Përshkrimi i shpenzimeve	B U XH E T I (EUR)					
					2015	2016	2017	2018	2019	Gjithsej
4.1.1	Hartohen termat e referencës të trupit koordinues	shtator 2015	ZQM							-
4.1.2	Zhvillohen konsultime me palët me interes rreth anëtarësisë në trupin koordinues	tetor-nëntor 2015	ZQM							-
4.1.3	Emërohen anëtarët e trupit koordinues	dhjetor 2015	ZQM							-
			Subtotali 4.1		-	-	-	-	-	-
Masa 4.2	**Krijimi i sistemit te avancuar për shkëmbimin e informatave dhe materialeve**									
Kodi	Aktiviteti	Periudha e zbatimit	Bartësi	Përshkrimi i shpenzimeve	B U XH E T I (EUR)					
					2015	2016	2017	2018	2019	Gjithsej
4.2.1	Diskutohet themelimi i sistemit për shkëmbimin e informatave	janar-shkurt 2016	Agjencia për Shoqëri të Informacionit							-
4.2.2	Nxirret buletini informativ 6-mujor për sigurinë në Internet	Çdo gjashtë muaj duke filluar nga qershori i vitit 2016	Agjencia për Shoqëri të Informacionit							-
			Subtotali 4.2		-	-	-	-	-	-
Masa 4.3	**Funksionalizimi i njësisë për veprim të shpejtë**									
Kodi	Aktiviteti	Periudha e zbatimit	Bartësi	Përshkrimi i shpenzimeve	B U XH E T I (EUR)					
					2015	2016	2017	2018	2019	Gjithsej

4.3.1	Hartohen termat e referencës për Ekipin për Reagim ndaj Emergjencave Kompjuterike – CERT	tetor-dhjetor 2015	ARKEP	Konsulentë vendore: 10 ditë x 150 EUR = 1500 EUR	1,500					1,500
4.3.2	Angazhohen punonjësit e CERT	janar-mars 2016	ARKEP	Pagat vjetore të punonjësve të CERT 2 punonjës x 12 muaj x 600 EUR = 14,400 EUR		10,800	14,400	14,400	14,400	54,000
4.3.3	Trajnohen punonjësit e CERT	prill-dhjetor 2015	ARKEP	Fondi për ndërtim kapaciteti	4,000					4,000
4.3.4	Themelohet linja emergjente telefonike	janar-mars 2016	MPB							-
			Subtotali 4.3		5,500	10,800	14,400	14,400	14,400	59,500
				Gjithsej Objektivi 4:	**5,500**	**10,800**	**14,400**	**14,400**	**14,400**	**59,500**

Objektivi 5: Vetëdije e ngritur e publikut për rol aktiv në mbrojtje të fëmijëve nga rreziqet ne internet

Masa 5.1	**Krijimi i platformës nacionale vetëdijësuese për rreziqet në Internet**									
Kodi	Aktiviteti	Periudha e zbatimit	Bartësi	Përshkrimi i shpenzimeve	B U XH E T I (EUR)					
					2015	2016	2017	2018	2019	Gjithsej
5.1.1	Hartohet plani i detajuar për krijimin e Qendrës për Internet të Sigurt (SIC)	shtator-dhjetor 2015	ZQM							-
5.1.2	Sigurohen pajisjet për SIC	janar-mars 2016	ZQM	Vlera e pajisjeve: 8,000 EUR		8,000				8,000
5.1.3	Angazhohen punonjësit e SIC	janar-mars 2016	ZQM	Pagat vjetore të punonjësve të SIC 2 punonjës x 12 muaj x 600 EUR = 14,400 EUR		10,800	14,400	14,400	14,400	54,000
5.1.4.	Zhvillohen aktivitetet e rregullta të SIC	Duke filluar nga prilli i vitit 2016	SIC	Buxheti vjetor për aktivitete: 8000 EUR		6,000	8,000	8,000	8,000	30,000
			Subtotali 5.1		-	24,800	22,400	22,400	22,400	92,000
Masa 5.2	**Organizimi i aktiviteteve për Ditën e Internetit të Sigurt**									
Kodi	Aktiviteti	Periudha e zbatimit	Bartësi	Përshkrimi i shpenzimeve	B U XH E T I (EUR)					
					2015	2016	2017	2018	2019	Gjithsej
5.2.1	Hartohet programi për SID	tetor-dhjetor i çdo viti	SIC							-
5.2.2	Organizohet SID në përputhje me programin e hartuar	Në shkurt të çdo viti	SIC	Buxheti vjetor për SID: 3000 EUR		3,000	3,000	3,000	3,000	12,000
			Subtotali 5.2		-	3,000	3,000	3,000	3,000	12,000
Masa 5.3	**Seanca informative me bazë në komunitet**									
Kodi	Aktiviteti	Periudha e zbatimit	Bartësi	Përshkrimi i shpenzimeve	B U XH E T I (EUR)					
					2015	2016	2017	2018	2019	Gjithsej

5.3.1	Zhvillohen plane për seanca informative në komunitet	qershor-korrik, duke filluar nga viti 2016	SIC							-
5.3.2	Realizohen seancat informative në komunitet	shtator-maj, duke filluar nga viti 2016	SIC	Fondi për seanca informative: 4000 EUR		1,000	4,000	4,000	4,000	13,000
			Subtotali 5.3		-	1,000	4,000	4,000	4,000	13,000
Masa 5.4	**Përfshirja e mediumeve në shpërndarjen e mesazheve dhe materialeve vetëdijesuese**									
Kodi	Aktiviteti	Periudha e zbatimit	Bartësi	Përshkrimi i shpenzimeve	B U XH E T I (EUR)					
					2015	2016	2017	2018	2019	Gjithsej
5.4.1	Përgatiten spote promovuese dhe shpallje promovuese për medie	maj-korrik 2016	SIC	Spotet promovuese: 3000 EUR Shpalljet promovuese: 1000 EUR		4,000				4,000
5.4.2	Publikohen në medie spotet promovuese dhe shpalljet promovuese	shtator-dhjetor 2016	SIC	Publikimi i spoteve: 10000 EUR Publikimi i shpalljeve: 2000 EUR		12,000				12,000
			Subtotali 5.4		-	16,000	-	-	-	16,000
				Gjithsej Objektivi 5:	**-**	**44,800**	**29,400**	**29,400**	**29,400**	**133,000**

REFERENCAT

Agjencia Shtetërore për Mbrojtjen e të Dhënave Personale (2013), Strategjia e mbrojtjes së të dhënave personale në Republikën e Kosovës. Prishtinë.

European Commission (2012), EC Communication COM(2012) 196.

FIT (2014), Siguria e fëmijëve në Internet. Prishtina: Save the Children.

Ministry of Economic Development (2013), Electronic Communication Sector Policy – Digital Agenda for Kosova 2013-2020. Prishtina.

STIKK (2013). Internet penetration and Usage in Kosovo. Prishtina: Kosovo Association for Information and Communication Technology.

UNICEF (2012), Child Safety Online – Technical Report.

PJESËMARRËSIT NË PROCESIN E PLANIFIKIMIT

1. Agnesa Qerimi, Këshillin Rinor Kosovar
2. Alban Kastrati , IPKO
3. Arben Shala, ekspert i planifikimit strategjik
4. Argjend Osmani, Ministria e Arsimit, e Shkencës dhe e Teknologjisë
5. Besim Kajtazi, Zyra Ligjore, Zyra e Kryeministrit
6. Dukagjin Pupovci, Qendra për Arsim e Kosovës
7. Egzon Gashi, Këshillin Rinor Kosovar
8. Fadil Abdyli, Policia e Kosovës
9. Feride Dashi, UNICEF
10. Genta Gagica, Save the Children
11. Gladiola Strugaj, Koalicioni i Organizatave për Mbrojtjen e Fëmijëve
12. Gresa Statovci, Qendra për Studime të Avancuar a-FIT
13. Habibe Buzuku – Pllana, Ministria e Arsimit, e Shkencës dhe e Teknologjisë
14. Habit Hajredini, Zyra për Qeverisje të Mirë, Zyra e Kryeministrit
15. Kushtrim Bajrami, Qendra për Arsim e Kosovës
16. Liridon Hoti, Autoriteti Rregullativ Komunikimeve Elektronike dhe Postare
17. Lorik Mullaademi, Shoqata e Teknologjisë së Informacionit dhe Komunikimeve të Kosovës
18. Luan Sahitaj, Ministria e Arsimit, e Shkencës dhe e Teknologjisë
19. Mentor Cakolli, Policia e Kosovës
20. Mimoza Hasani, Ministria e Arsimit, e Shkencës dhe e Teknologjisë
21. Petrit Tahiri, Qendra për Arsim e Kosovës
22. Rrezarta Ajeti, Autoriteti Rregullativ Komunikimeve Elektronike dhe Postare
23. Sadete Demaj, Zyra për Qeverisje të Mirë, Zyra e Kryeministrit
24. Shqipe Gashi, Ministria e Arsimit, e Shkencës dhe e Teknologjisë
25. Teuta Sopjani-Mekuli, Ministria e Arsimit, e Shkencës dhe e Teknologjisë
26. Teuta Zymeri, Qendra për Studime të Avancuar a-FIT