



**Republika e Kosovës**  
**Republika Kosova - Republic of Kosovo**  
*Qeveria - Vlada - Government*

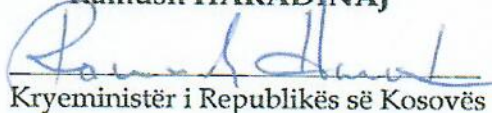
---

Nr. 19/64  
Datë: 11.09.2018

Në mbështetje të nenit 92 paragrafi 4. dhe të nenit 93 paragrafi (4) të Kushtetutës së Republikës së Kosovës, duke u bazuar në nenin 4 të Rregullores nr. 02/2011 për Fushat e Përgjegjesisë Administrative të Zyrës së Kryeministrit dhe Ministrive, e ndryshuar dhe e plotësuar me Rregulloren nr. 14/2017, me Rregulloren nr. 15/2017, me Rregulloren nr. 16/2017 dhe me Rregulloren nr. 07/2018, si dhe në nenin 19 të Rregullores së Punës së Qeverisë së Republikës së Kosovës nr. 09/2011, Qeveria e Republikës së Kosovës, në mbledhjen e mbajtur më 11 shtator 2018, nxjerr këtë:

**V E N D I M**

1. Aprovohet Koncept Dokumenti për Parandalimin dhe Luftimin e Krimit Kibernetik.
2. Obligohet Ministria e Punëve të Brendshme dhe institucionet tjera kompetente për zbatimin e këtij vendimi, në pajtim me Rregulloren e Punës së Qeverisë.
3. Vendimi hyn në fuqi ditën e nënshkrimit.

**Ramush HARADINAJ**  
  
Kryeministër i Republikës së Kosovës

**Iu dërgohet:**

- Zëvendëskryeministrave
- të gjitha ministrive (ministrave)
- Sekretarit të Përgjithshëm të ZKM-ës
- Arkivit të Qeverisë



**Republika e Kosovës**  
**Republika Kosova-Republic of Kosovo**  
**Qeveria –Vlada-Government**  
**Ministria e Punëve të Brendshme / Ministarstvo Unutrašnjih Poslova /**  
**Ministry Of Internal Affairs**

**KONCEPT DOKUMENT PËR PARANDALIMIN DHE LUFTIMIN E KRIMIT  
KIBERNETIK**

**Maj 2018**

## **Kapitulli 1: Hyrje**

Rregullimi i fushës së parandalimit dhe luftimit të krimit kibernetik ndërlidhet me Programin e Qeverisë 2015-2018, më saktësisht me Prioritetin Strategjik të Qeverisë Nr. 2. Qeverisja e mirë dhe fuqizimi i sundimit të ligjit. Kjo fushë ndërlidhet edhe me Programin Kombëtarë për Zbatimin e Marrëveshjes së Stabilizim-Asocimit, më saktësisht Kapitullin 24: Drejtësia, Liria dhe Siguria, në të cilin janë paraparë politika dhe masa në luftimin e krimit kibernetik. Së fundmi, Plani Vjetor i Punës së Qeverisë përkatësisht Ministrisë së Punëve të Brendshme ka paraparë aktivitete përkatëse në fushën e parandalimit dhe luftimit të krimit kibernetikë.

Koncept dokumenti për parandalimin dhe luftimin e krimit kibernetikë kontribuon në forcimin e mekanizmave për parandalimin dhe luftimin e krimit kibernetikë e paraparë në strategjinë shtetërore për sigurinë kibernetike dhe planit të veprimit 2016 - 2019 e aprovuar nga Qeveria e Republikës së Kosovës në Janar 2016.

Zhvillimi i kornizës ligjore për parandalimin dhe luftimin e krimit kibernetike është paraparë në Planin e Veprimit për Zbatimin e Strategjisë Shtetërore për Siguri Kibernetike 2016-2019, më saktësisht parasheh objektivi 2.4 "Infrastruktura ligjore". Pika 2.4.1 e planit të veprimit parasheh rishikimin e Ligjit për Parandalimin dhe Luftimin e Krimit Kibernetikë.

Zhvillimi i këtij koncept dokumenti është pjesë e Listës së koncept dokumenteve për vitin 2017 të Qeverisë së Republikës së Kosovës.

## **Kapitulli 2: Përshkrimi dhe përkufizimi i çështjes /problemit kryesorë**

### *Shpjegim*

Kuvendi i Republikës së Kosovës më 10 Qershor 2010 ka aprovuar Ligjin Nr. 03/L-166 për Parandalimin dhe Luftimin e Krimit Kibernetikë.

Ky ligj ka për qëllim parandalimin dhe luftimin e krimit kibernetikë me masa konkrete, parandalimin, zbulimin dhe sanksionimin e shkeljeve përmes sistemeve

kompjuterike, duke ofruar respektimin e të drejtave të njeriut dhe mbrojtjen e të dhënave personale.

Duke marrë parasysh zhvillimet dhe avancimet teknologjike nga viti 2010 e deri më tani, krijimin dhe ndryshimet e legjislacionit përkatës në BE që ka të bëjë më luftimin dhe parandalimin e krimit kibernetikë dhe nevoja për të qenë në harmoni më legjislacionin e BE-se, nevojat nga mekanizmat e sigurisë në vendin tonë, ky koncept dokument ofron shpjegime rreth nevojës për plotësim ndryshimin e ligjit për parandalimin dhe luftimin e krimit kibernetikë.

Problemi kryesor i ligjit aktual është se nuk ka gjetur zbatim. Orientimi më i madh ka qenë kah Kodi Penal i cili i parasheh disa vepra penale që bien në fushën e krimeve kibernetike.

Që nga themelimi i Sektorit për Hetimin e Krimit Kibernetikë (Shtator 2011), numri i rasteve që bien në fushën e krimeve kibernetike në vazhdimësi është rritur dukshëm. Siç u cek edhe në përgjigjen e parë, këto raste janë trajtuar sipas Kodit penal.

Nga veprat e krimeve kibernetike ka pasur shkaktim i dëmeve materiale, humbje e të dhënave zyrtare, humbje dhe keqpërdorim i të dhënave personale, humbje e të dhënave të kompanive të ndryshme, raste tjera që kanë prekur integritetin personal të individëve.

Në kuadër të Policisë së Kosovës ekziston Sektori për Hetimin e Krimit Kibernetikë i cili si i tillë merret më luftimin e krimit kibernetikë. Kurse, sa i përket parandalimit, ky term është mjaft i gjerë dhe përfshin një numër të madh mekanizmash dhe veprimesh. P.sh. Policia e Kosovës ligjëron nëpër shkolla për rreziqet që vijnë nga interneti. Strategjia Shtetërore për Siguri Kibernetike përfshin një mori aktiviteteve që ndikojnë në parandalimin e sulmeve dhe krimeve kibernetike. Në strategji bëjnë pjesë institucionet kryesore të vendit. Vlerësojmë se këta mekanizma, edhe pse me përvojë të re në këtë fushë, kanë qenë efikas dhe kanë ecur në hap me trendin botëror të luftimit dhe parandalimit të krimeve kibernetike.

Bazuar në strategji është themeluar CERTI nacional në kuadër ARKEP i emërtuar KOS-CERT mirëpo përgjegjësit e CERT nacional nuk janë të definuara në ligjin për komunikime elektronike, andaj e ka bërë të vështir realizimin e aktiviteteve që ndërliidhen më parandalimin e krimeve kibernetike.

Problemi tjetër ka qenë mos krijimi i pikës së kontaktit i përcaktuar më ligjin aktual mirëpo nuk është definuar institucioni përgjegjës për themelimin e kësaj pike, qëllimi i së cilës është shkëmbimi i informatave në kohë reale. Për luftimin e krimit kibernetikë, i cili kryhet përmes internetit, është mëse e domosdoshme që të ketë një pikë kontakti sepse mundëson bashkëpunimin ndërkombëtar dhe trajtimin e informatave në mënyrë të përshpejtuar, por njëkohësisht shërben edhe për bashkëpunim publiko-privat që është njëra ndër pesë objektivat kryesore të strategjisë shtetërore për siguri kibernetike.

Ligji për parandalimin dhe luftimin e krimit kibernetikë, është i bazuar në Konventën e Budapestit (ETS No.185), e nënshkruar më 23 Nëntor 2001 dhe ka hyrë në fuqi më 1 Korrik 2004. Deri më sot kjo Konventë është ratifikuar nga 57 shtete dhe e kanë nënshkruar 4 shtete. Nëse i referohemi legjislacionit të vendeve të rajonit, ato e kanë ratifikuar Konventën e Budapestit (ETS No.185) dhe e kanë inkorporuar në Kodin Penal, vërehet se asnjë shtet i rajonit nuk ka Ligj Special për Luftimin e Krimit Kibernetikë. Gjithashtu, në kuadër të Konventës janë nxjerrë:

- Protokoll Shtesë të Konventës për Krimin Kibernetikë që trajton penalizimin e veprimeve raciste dhe ksenofobike të kryera përmes sistemeve kompjuterike (i ratifikuar nga 29 shtete dhe i nënshkruar nga 13 shtete), dhe
- “Shënimet Udhëzuese” nga Komiteti i Konventës së Krimeve Kibernetike, udhëzime këto që përshkruajnë në mënyrë më të qartë forma kryesore të krimit kibernetikë, janë nxjerrë në vitin 2012.

Sa i përket Protokollit Shtesë, në kuadër të pyetjeve për input për raportin e progresit, ka pasur pyetje: a është çështje në vendin tuaj Urrejtja dhe Diskriminimi në internet? Çfarë masash janë marrë për implementimin e Protokollit Shtesë të

Konventës për Krimin Kibernetikë që trajton penalizimin e veprimeve raciste dhe ksenofobike të kryera përmes sistemeve kompjuterike i Këshillit të Evropës të cilin e kanë ratifikuar të gjitha vendet?

- Përgjigja e jonë ka qenë: Urrejtja dhe diskriminimi në internet nuk është e rregulluar as me Kod Penal e as me Ligjin për Parandalimin dhe Luftimin e Krimit Kibernetikë. Në fakt, në mënyrë të përgjithësuar nxitja e urrejtjes është e rregulluar me nenin 147 (Kodi Penal) por nuk është e rregulluar “përmes internetit”. Vlerësojmë se duhet të përfshihet si vepër penale.

Për arsye të evoluimit të lloj-llojshmërisë së krimeve kibernetike, në BE me datën 12 Gusht 2013 (tri vite pasi që ligji i sipër përmendur ka hyrë në fuqi ligji) është aprovuar Direktiva:

“DIREKTIVA E BE-së 2013/40 E PARLAMENTIT DHE KËSHILLIT EVROPIAN PËR MBROJTJEN E SISTEMËVE TË INFORMACIONIT” (“DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JH<sup>1</sup>).

#### *Çka përmban kjo Direktivë e re?*

Komisioni Evropian ka vendosur se një instrument i ri ligjor është i nevojshëm për të trajtuar kërcënimet e reja që nuk janë marrë parasysh në vitet paraprake.

Kërcënime e reja përfshijnë:

- Sulmet në shkallë të gjerë kundër sistemeve të informacionit,
- Rritjen e përdorimit kriminal të te ashtuquajturve "botnets", që paraqesin rrjetet e kompjuterëve të infektuar që mund të kontrollohen nga distanca në shkallë shumë të gjerë, dhe të shërbejnë për sulme të koordinuara.

---

<sup>1</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF>

Asnjëra nga këto kërcënime të sipër përmendura nuk janë të përfshira në Ligjin nr. 03/L-166 në Kosovë.

Direktiva në fjalë përmban koncepte të reja të cilat nuk janë të parapara në ligjin nr. 03/L-166 e të cilat janë:

- Qasje të paligjshme (illegal access),
- Ndërhyrje të paligjshme në Sisteme (illegal system interference) dhe
- Ndërhyrje të paligjshme në të dhëna (illegal data Interference).

Po ashtu në këtë direktiv paraqiten konceptet e reja të sulmeve kibernetike si për shembull "botnet", pastaj marrja pa të drejtë e fjalëkalimeve (password-ëve) të kompjuterit, etj., që më këtë direktiv konsiderohen si vepra penale.

Direktiva gjithashtu rritë nivelin e dënimeve penale për një afat maksimal me burgim prej së paku dy vjet (në Kosovë në ligjin aktual 03/L-166 është 6 muaj), ose së paku pesë vjet për veprat penale të kryera në kuadër të një organizate kriminale (në Kosove minimumi është 1 vit, pra diferenca është 4 vite).

Direktiva po ashtu penalizon nxitjen, ndihmën, mbështetjen dhe përpjekjen e veprave kriminale dhe shton rrethana të reja rënduese si:

- Një dënim maksimal prej të paktën tre vjet, kur një numër i konsiderueshëm i sistemeve të informacionit janë prekur nëpërmjet botnet-eve (që nuk janë parapara në ligjin nr. 03/L-166), dhe
- Një dënim maksimal prej të paktën pesë vjet, kur vepra shkakton dëme serioze materiale ose kur vepra penale është kryer kundër një sistemi të informacionit të infrastrukturës kritike.

Përveç kësaj, direktiva synon të përmirësojë drejtësinë penale evropiane (European Criminal Justice) dhe bashkëpunimin policor përmes:

- Forcimit të strukturës ekzistuese të pikave të kontaktit 24/7. Shtetet anëtare të BE-së tani janë të obliguara që të reagojnë brenda tetë orësh ndaj kërkesave urgjente
- Kërkon prej shteteve që të mbledhin të dhëna themelore (statistika) për krimet kibernetike më qëllim që të analizohen trendët.

Tabela më pikat që janë të parapara në direktiv dhe mënyra se si janë të paraqitura në ligjin nr.. 03/L-166.

DIREKTIVA 2013/40/EU	LIGJI 03/L-166
"Botnets"	Nuk përmendet
Infrastruktura Kritike	Nuk përmendet
Dënim penal për një afat maksimal me burgim prej së paku dy vite.	Dënim me burgim prej së paku gjashtë muaj
Dënim penal për një afat maksimal me burgim prej së paku pesë vite.	Dënim me burgim prej së paku një vit. Kur kryhet brenda kuadrit të një organizate kriminale.
24/7 Pika kontakti - reagimi brenda 8 orëve	Nuk përmendet
Monitorimi dhe Statistika	Nuk përmendet



## **Politika aktuale**

Politika aktuale lidhur për sigurinë kibernetike përfshinë disa ligje kryesore, akte nënligjore dhe strategji por nuk janë këto te vetmet.

*Ligjet dhe aktet nënligjore* - të cilat ndërlidhen me projektligjin për sigurinë kibernetike, përfshinë, por nuk kufizohen vetëm në ligjet dhe aktet nënligjore të mëposhtme:

- **Strategjia shtetërore për siguri kibernetike 2016 – 2019.**
- **Ligji nr. 03/L-050 për Themelimin e Këshillit të Sigurisë së Kosovës**

Këshilli i Sigurisë së Kosovës ka rol këshillues në të gjitha çështjet që lidhen me sigurinë e Kosovës dhe kontributin e tij për stabilitetin rajonal;

- **Ligji nr.03/L -166 për Parandalimin dhe Luftimin e Krimit Kibernetikë**

Ky ligj ka për qëllim parandalimin dhe luftimin e krimit kibernetikë me masa konkrete, parandalimin, zbulimin dhe sanksionimin e shkeljeve përmes sistemeve kompjuterike, duke ofruar respektimin e të drejtave të njeriut dhe mbrojtjen e të dhënave personale;

- **Ligji nr. 04/L-145 për Organet Qeveritare të Shoqërisë së Informacionit**

Qëllimi i këtij ligji është përcaktimi i organeve përgjegjëse për zhvillimin e shërbimeve të shoqërisë së informacionit në institucionet e Republikës së Kosovës, si dhe kompetencat, përgjegjësitë, organizimi dhe funksionimi i tyre;

- **Ligji nr. 04/L-094 për Shërbimet e Shoqërisë Informatike –**

1. Ky ligj përcakton dokumentacionin në formë elektronike juridikisht të barabartë me dokumentacionin tradicional të paraqitur në format të letrës, për të lehtësuar

shërbimet elektronike që përfshijnë, por që nuk kufizohen në shitblerje që bëjnë konsumatorët nëpërmjet Internetit (eTregtia), shërbimet elektronike bankare dhe ato financiare (ePagesa), ofrimin e shërbimeve qeveritare (eQeverisja), blerjen në formë elektronike nga ndërmarrjet (eProkurimi) dhe aplikimin e nënshkrimit elektronik.

2. Qëllimi i këtij ligji është krijimi i mundësive dhe rrethanave të favorshme për zhvillimin e tregtisë elektronike, përdorimin e transaksioneve elektronike dhe përdorimin e nënshkrimit elektronik si nga Qeveria, bizneset por edhe qytetarët. Gjithashtu, ky ligj ka për qëllim edhe zvogëlimin e problemeve potenciale të keqpërdorimeve gjatë transaksioneve elektronike si dhe adresimin e sigurisë së sistemeve informatike;

• **Ligji nr. 04/L-109 për Komunikimet Elektronike**

Qëllimi i këtij ligji është rregullimi i aktiviteteve të komunikimeve elektronike bazuar në parimin e neutralitetit teknologjik dhe kornizën rregullatore të BE-së për komunikimet elektronike, duke promovuar konkurrencën dhe infrastrukturën efikase në komunikimet elektronike, si dhe garantimin e shërbimeve të duhura e të përshtatshme në territorin e Republikës së Kosovës;

• **Ligji nr.05/L-030 për Përgjimin e Komunikimeve Elektronike**

1. Ky ligj rregullon procedurat dhe kushtet mbi përgjimin e komunikimeve elektronike që realizohen për nevoja të procedurës penale nga institucionet shtetërore të themeluara me ligj, dhe procedurat dhe kushtet e përgjimit për nevojat e sigurisë së Republikës së Kosovës dhe qytetarëve të saj të themeluara me ligj.

2. Ky ligj përcakton rregullat, detyrimet dhe procedurat për Operatorët e Rrjeteve dhe Ofruesit e Shërbimeve në lidhje me përpunimin e të dhënave të caktuara nga ana e tyre. 3. Ky ligj përcakton detyrimet dhe autorizimet e institucioneve shtetërore të themeluara me ligj për të garantuar respektimin e të drejtave dhe lirive të njeriut

në procesin e përgjimit të ligjshëm, si dhe kontrollin në zbatimin e procedurave të përgjimit.;

- **Ligji nr.03/L - 172 për Mbrojtjen e të Dhënave Personale**

Ky Ligj përcakton të drejtat, përgjegjësitë, parimet dhe masat lidhur me mbrojtjen e të dhënave personale dhe themelon institucionin që është përgjegjës për mbikëqyrjen e legjitimitetit të përpunimit të të dhënave. ;

- **Ligji nr. 04/L-076 për Policinë -**

Ky ligj rregullon autorizimet dhe detyrat e Policisë së Republikës së Kosovës, organizimin e saj dhe çështje të tjera lidhur me aktivitetet dhe veprimet e Policisë së Republikës së Kosovës;

- **Ligji nr. 03/L-142 për Rendin dhe Qetësinë Publike**

Qëllim i këtij ligji është rregullimi i sjelljes personale në mënyrë që të ruhet rendi dhe qetësia publike;

- **Ligji nr. 03/L063 për Agjencinë e Kosovës për Inteligjencë**

Me këtë ligj themelohet Agjencia e Kosovës për Inteligjencë;

- **Ligji nr. 04/L-065 për të Drejtën e Autorit dhe të Drejtat e Përafërta**

1. Të drejtat e autorit që, në bazë të pronës intelektuale, u takojnë autorëve përkitazi me veprat e tyre në lëmin e letërsisë, shkencës dhe artit, në vijim e drejta e autorit; 2. të drejtat që, në bazë të pronës intelektuale, janë të përafërta me të drejtat e autorit;

- **Ligji nr. 04/L-213 për Ndhimën Juridike Ndërkombëtare në Çështje Penale**

Ky ligj rregullon kushtet dhe procedurat për bashkëpunim juridik ndërkombëtar në çështje penale mes Republikës së Kosovës dhe shteteve të tjera, në qoftë se nuk është përcaktuar ndryshe me marrëveshje ndërkombëtare.;

• **Ligji nr. 04/L-052 për Marrëveshjet Ndërkombëtare**

Ky ligj përcakton procedurën e lidhjes, nënshkrimit, ratifikimit, rezervave dhe deklaratave, ndryshimit dhe plotësimit, tërheqjes nga marrëveshja, si dhe zbatimin e marrëveshjeve ndërkombëtare të Republikës së Kosovës;

• **Ligji nr. 04/L-093 për Bankat, Institucionet Mikrofinanciare dhe Institucionet Financiare Jobankare**

Qëllimi i këtij ligji është nxitja dhe mbarëvajtja e një sistemi të qëndrueshëm financiar nëpërmjet promovimit të menaxhimit të shëndoshë dhe të matur të bankave, institucioneve mikrofinanciare dhe institucioneve tjera financiare jobankare dhe sigurimit të një niveli të përshtatshëm mbrojtës të interesave të depozitorëve;

• **Ligji nr. 04/L-064 për Agjencinë e Kosovës për Forenzikë**

Ky ligj rregullon themelimin, misionin, organizimin, funksionet, detyrat, përgjegjësitë dhe financimin e Agjencisë së Kosovës për Forenzikë;

• **Ligji nr. 04/L-198 për Tregtinë e Mallrave Strategjike**

1. Ky ligj rregullon eksportin, importin, transitin, trans-ngarkimin, ri-eksportin dhe ri-transferimin e mallrave strategjike, ofrimin e shërbimeve të ndërlidhura, si dhe kontrollin, mbikëqyrjen, të drejtat dhe detyrimet e palëve që marrin pjesë në aktivitetet e biznesit nga kjo fushë.

2. Qëllimi i këtij ligji është ta avancojë sigurinë shtetërore dhe interesat e politikës së jashtme të Republikës së Kosovës, drejt përmbushjes së detyrimeve dhe marrëveshjeve ndërkombëtare në lidhje me mospërhapjen e armëve të shkatërrimit në masë dhe mallrave tjera strategjike të shfrytëzuara për qëllime ushtarake dhe t'i kontribuojë përpjekjeve ndërkombëtare dhe rajonale për rregullimin e tregtisë me mallrat strategjike.;

• **Ligji nr. 04/L -004 për Shërbimet Private të Sigurisë**

1. Ky ligj rregullon të gjitha aktivitetet në fushën e sigurisë private.
2. Dispozitat e këtij ligji nuk zbatohen në aktivitetet që rregullohen me Ligjin për policinë, dhe aktivitetet e tjera të sigurisë që u janë caktuar institucioneve shtetërore ose qeveritare.
3. Kushtet e punës për punëtorët e sigurimit rregullohen me ligjet e aplikueshme për punë. ;

• **Kodi nr. 03/L-109 Doganor dhe i Akcizës i Kosovës**

Ky Kod bën rregullimin e elementeve bazë të sistemit për mbrojtjen doganore të ekonomisë së Republikës së Kosovës dhe të drejtat e obligimet e të gjithë pjesëmarrësve, në zbatimin e legjislacionit doganor. ;

• **Ligji nr.03/L-178 për Klasifikimin e Informacioneve dhe Verifikimin e Sigurisë**

Qëllimi i këtij ligji është themelimi i një sistemi unik për klasifikimin dhe ruajtjen e informacioneve që kanë të bëjnë me interesat e sigurisë së Kosovës si dhe për verifikimin e sigurisë së personave që kanë qasje në këto informacione;

• **Kodi nr. 04/L-082 Penal i Republikës së Kosovës**

Bazat dhe kufijtë e sanksioneve penale

1. Veprat penale dhe sanksionet penale parashihen vetëm për ato sjellje me të cilat cenohen apo dëmtohen në atë masë liritë dhe të drejtat e njeriut si dhe të drejtat tjera dhe vlerat shoqërore të garantuara dhe të mbrojtura me Kushtetutën e Republikës së Kosovës dhe me të drejtën ndërkombëtare, mbrojtja e të cilave nuk do të mund të realizohet pa dhunën penalo juridike.

2. Parashikimi i veprave penale si dhe llojet e masave dhe lartësia e sanksioneve penale për kryesit e veprave penale bazohen në domosdoshmërinë e sanksionit penalo juridik dhe proporcionalitetit të shkallës dhe natyrës së rrezikshmërisë për liritë dhe të drejtat e njeriut dhe të vlerave shoqërore;

#### • **Kodi nr. 04/L-123 i Procedurës Penale**

Fushëveprimi i këtij Kodi

1. Me këtë Kod përcaktohen rregullat e procedurës penale të cilat janë të detyrueshme për punën e gjykatave, prokurorisë së shtetit si dhe të pjesëmarrësve të tjerë në procedurën penale të paraparë me këtë Kod.

2. Me këtë Kod caktohen rregullat që garantojnë se asnjë person i pafajshëm nuk do të dënohet, ndërsa dënimi ose sanksioni tjetër penal mund t'i shqiptohet vetëm personit i cili ka kryer veprë penale sipas kushteve të parapara me Kodin Penal dhe me ligjet tjera të Kosovës në bazë të të cilave janë paraparë veprat penale sipas procedurës së zbatuar në mënyrë të drejtë dhe të ligjshme para gjykatës kompetente.

3. Para marrjes së aktgjykimit të formës së prerë, liritë dhe të drejtat tjera të te pandehurit mund të kufizohen vetëm sipas kushteve të përcaktuara në këtë Kod.

#### • **Ligji nr.03/L-122 për Shërbim të Jashtëm të Republikës së Kosovës**

Qëllim i këtij ligji është rregullimi i veprimtarisë së shërbimit të jashtëm, i organizimit,

bashkërendimit dhe funksionimit të organeve që e përbëjnë shërbimin e jashtëm, dhe rregullimi i statusit të personelit të misionit diplomatik. ;

- **Kodi nr.03/L-193 i Drejtësisë për të Mitur**

Ky Kod rregullon procedurën e shqiptimit dhe ekzekutimit të masave dhe dënimeve ndaj të miturve, procedurën gjyqësore si dhe procedurën e ndërmjetësimit për të mitur;

**Aktet nënligjore:**

- **Rregullore nr.18/2011 për shpërndarjen dhe transferimin e informacionit të klasifikuar**

Kjo rregullore ka për qëllim krijimin e një sistemi unik për shpërndarjen dhe transferimin e informacioneve të klasifikuara për të gjitha institucionet publike të Republikës së Kosovës si dhe ndaj personave të cilët kanë leje përkatëse të sigurisë.

- **Rregullore (MAP) nr. 02/2015 për standarde për softuer dhe harduer.**

Qëllimi i kësaj rregullore është përcaktimi i standardeve të përdorimit të softuerit dhe harduer nga zyrtarët e institucioneve të Republikës së Kosovës.

- **Udhëzim administrativ (MAP) nr. 02/2015 për llogaritë elektronike zyrtare**

Ky udhëzim administrativ përcakton procedurat e krijimit, administrimit, shfrytëzimit dhe mbylljes së llogarisë elektronike zyrtare për të gjithë shfrytëzuesit dhe administratorët e llogarisë elektronike të sistemit shtetëror të Teknologjisë Informative (në vijim: TI) në të gjitha institucionet e Republikës së Kosovës (në vijim: IRK).Rregullore mbi standardet teknike dhe organizative për sigurinë dhe integritetin e rrjetave dhe/ose shërbimeve të komunikimeve elektronike nr. 29, nr. prot. 046/b/16.

- **UA 01/2011 për menaxhimin dhe përdorimin e internetit në IRK.**

- UA për menaxhimin e sigurisë informative 02/2010
- UA 01/2010 për sigurinë dhe qasjen në baza të të dhënave
- UA për uebfaqe
- UA 02/2012 për portalin qeveritar
- Rregullorja 02/2016 për koordinimin ndërmjet ASHI dhe strukturave organizative ose zyrtarëve të ti dhe komunikimit nëpër institucione.

Institucionet kryesore qeveritare për miratimin dhe zbatimin e këtyre ligjeve dhe strategjive janë:

#### **Kuvendi i Republikës së Kosovës**

- përcakton kahjet themelore të organizimit dhe zbatimit të mbrojtjes nga fatkeqësitë natyrore dhe fatkeqësitë tjera;
- me propozimin e Qeverisë, merr vendime lidhur me furnizimin me resurse dhe çështje tjera të rimëkëmbjes nga fatkeqësitë e mëdha natyrore.

#### **Qeveria e Republikës së Kosovës**

- drejton dhe koordinon organizimin, përgatitjen dhe zbatimin e mbrojtjes nga kërcënimet kibernetike, fatkeqësitë natyrore dhe fatkeqësitë tjera në vend;
- miraton strategjinë shtetërore për sigurinë kibernetike dhe planin e veprimit
- miraton planet kombëtare të reagimit emergjent;
- Emëron koordinatorin nacional për sigurinë kibernetike
- menaxhon mbrojtjen dhe rimëkëmbjen nga fatkeqësitë e mëdha natyrore dhe fatkeqësitë tjera;



## **Ministria e Punëve të Brendshme**

- Emëron këshillin shtetëror për siguri kibernetike
- Udhëheq, koordinon, organizon dhe ndihmon në zbatimin e strategjisë për siguri kibernetike dhe planit të veprimit;
- MPB është përgjegjëse për hartimin dhe monitorimin e politikave dhe legjislacionit në fushën e sigurisë së përgjithshme dhe sigurisë kibernetike.
- Përmes njësisë CERT trajton dhe zgjidh rastet e incidenteve të sigurisë kibernetike brenda MPB-së.

## **Agjencia e Shoqërisë së Informacionit**

- Propozon dhe koordinon të gjitha politikat që ndërlidhen me teknologjinë e informacionit dhe të komunikimit në institucionet e Republikës së Kosovës.
- Harton dhe siguron zbatimin e strategjisë së qeverisjes elektronike dhe të planit të veprimit përkatës, për aprovim në Qeveri.
- Udhëheq dhe mbikëqyr zbatimin e projekteve që ndërlidhen me teknologjinë e informacionit në institucionet e Republikës së Kosovës.
- Agjencia përkrah zhvillimin e teknologjisë së informacionit, nxit investimet në fushën e shoqërisë së informacionit, zhvillimin e sistemeve të aftësimin në teknologjinë e informacionit dhe bën koordinimin, udhëheqjen dhe mbikëqyrjen e proceseve dhe të mekanizmave të qeverisjes elektronike në fushat e mëposhtme:
  - infrastrukturën e TIK-ut për institucionet e Republikës së Kosovës dhe rritjen e shkallës së përdorimit të TI-së;
  - zgjerimin e shërbimeve të internetit dhe të përmbajtjeve të internetit në institucionet e Republikës së Kosovës;
  - akumulimin, administrimin, përhapjen dhe ruajtjen e të dhënave, duke krijuar Qendrën shtetërore të të dhënave elektronike;

- sigurinë dhe mbrojtjen e infrastrukturës komunikuese elektronike dhe të të dhënave;
- sipas nevojës, ndihmon institucionet relevante në luftimin e krimit elektronik (cyber crime);
- përkujdeset për menaxhimin dhe ruajtjen e pronës intelektuale dhe të drejtat në lidhje me bazat e të dhënave dhe softuerët, që janë pronë e shtetit;
- siguron mbrojtjen e të dhënave personale në formë elektronike, në pajtim me legjislacionin në fuqi;
- Përmes njësisë CERT qeveritar trajton dhe zgjidh rastet e incidenteve të sigurisë kibernetike brenda qeveris.

#### **Policia e Kosovës**

- Zbaton urdhrat dhe udhëzimet e lëshuara në mënyrë të ligjshme nga prokurori publik ose gjyqtari kompetent lidhur me krimet kibernetike;
- Bashkëpunon dhe i raporton Zyrës së Prokurorit Publik kompetent për informatat lidhur me akuzat për aktivitete të dyshimta kriminale që kanë të bëjnë me krimet kibernetike, për të cilat policia është njoftuar në pajtim me ligjin e aplikueshëm;
- Ndërton kapacitete të duhura kadrovike, teknike dhe teknologjike për të luftuar dhe për t'u ballafaquar me sfidat që dalin në luftën ndaj sulmeve kibernetike;
- Përmes sektorit për krime kibernetike heton veprat penale që lidhen me krimet kibernetike, duke filluar nga gjetja e provave materiale të vlefshme, si dëshmi deri në kompletimin e rastit dhe dërgimin në gjykatë;
- Përmes njësisë CERT trajton dhe zgjidh rastet e incidenteve të sigurisë kibernetike brenda Policisë së Kosovës.

### **Agjencia e Kosovës për Forenzikë**

- Agjencia e Kosovës për Forenzikë është një agjenci e pavarur në kuadër të MPB-së, dhe në mënyrë të veçantë merret me ekzaminimet specifike dhe mjeteve të krimeve kibernetike.
- Përmes ekspertizave forenzike zbulon veprat penale që kanë të bëjnë me krimet kibernetike.
- Forenzika e Teknologjisë Informative, është aplikimi i ekzaminimit, hetimit dhe analizimit të pajisjeve elektronike duke përdorur teknika të ndryshme me qëllim të mbledhjes së dëshmive dhe prezantimit të tyre në gjykate si dëshmi të vlefshme.
- Agjencia e Kosovës për Forenzikë, gjegjësisht Divizionit për ekzaminim të kompjuterëve është Divizioni i cili merret me ekzaminimin e pajisjeve elektronike për të cilat dyshohet se janë përdorur për kryerjen e veprës penale apo nëse në këto pajisje janë të deponuara (mbahen, ruhen, fshihen, etj.) dëshmi të ndonjë veprës penale.

### **Këshilli Gjyqësor i Kosovës**

Siguron që gjykatat në Kosovë të jenë të pavarura, profesionale dhe të paanshme, me qëllim që sistemi gjyqësorë të jetë sa më efikas në luftë kundër krimit kibernetikë.

### **Këshilli Prokurorial i Kosovës**

Siguron që sistemi prokurorial në Kosovë të jetë i pavarur, i paanshëm dhe profesional në ushtrimin e ndjekjes, hetimit dhe zbulimit të veprave penale të krimit kibernetikë dhe të përfaqësojë në gjykata aktet akuzuese në emër të shtetit.

### **Prokuroritë dhe Gjykatat**

Janë institucionet përgjegjëse për ndjekjen penale të kryesve, ndëshkimin adekuat të tyre, për konfiskimin e pasurisë dhe asetëve të fituara me anë të aktiviteteve kriminale.

### **Sekretariati i Këshillit të Sigurisë së Kosovës**

Sekretariati, si pjesë përbërëse e Këshillit të Sigurisë së Kosovës bën përgatitjen e raporteve periodike dhe analizave për Qeverinë e Republikës së Kosovës dhe Këshillin e Sigurisë së Kosovës që kanë të bëjnë me çështjet politike të sigurisë, si dhe ofron ndihmë në hartimin e politikave të sigurisë në Kosovë, përfshirë edhe ndërtimin e kapaciteteve, instrumentet e politikave dhe hulumtimit, ofrimin e mbështetjes administrative dhe funksionale Këshillit të Sigurisë së Kosovës.

### **Agjencia e Kosovës për Inteligjencë**

AKI bën identifikimin e kërcënimeve që rrezikojnë sigurinë e Kosovës. Kërcënim ndaj sigurisë së Kosovës konsiderohet kërcënimi ndaj integritetit territorial, integritetit të institucioneve, rendit kushtetues, stabilitetit dhe zhvillimit ekonomik, si dhe kërcënimet ndaj sigurisë globale në dëm të Kosovës.

### **Ministria për Forcën e Sigurisë së Kosovës**

MFSK zhvillon dhe fuqizon mbrojtjen kibernetike për sistemet e komunikimit dhe informacionit të MFSK-së/FSK-së, të cilat sisteme përdoren për kryerjen e detyrave në përmbushje të misionit kushtetues. FSK mund të angazhohet në mbështetjen e autoriteteve civile në mbrojtjen e të dhënave dhe infrastrukturës kritike në rast të ndonjë krize në vend.

### **Autoriteti Rregullativ i Komunikimeve Elektronike dhe Postare**

Miraton legjislacionin sekondar lidhur me implementimin e ligjit për komunikimet elektronike, ligjit për shërbimet postare dhe strategjitë/politikat e miratuara nga Qeveria.

- Monitoron dhe rregullon dispozitat e komunikimeve elektronike publike të rrjetave dhe shërbimeve.
- Miraton Planin Kombëtar të numeracionit, Planin për përdorimin e Radio-Frekuencave (kanaleve) dhe planet e zhvillimit të radio komunikimit.

- Zbaton detyrat që lidhen me kompatibilitetin elektromagnetik, përdorimin e pajisjeve dhe mjeteve, radio-monitorimin dhe eliminimin e Interferencave (ndërhyrjeve) të Radios.
- Në bazë të autorizimeve të marra, lidhë marrëveshjet bilaterale dhe multilaterale në fushën e komunikimeve elektronike.
- Kryen funksionet e CERT më qëllim të ballafaqimit me rreziqet për sistemet publike të komunikimeve elektronike. Përmes njësisë CERT trajton dhe zgjidh rastet e incidenteve të sigurisë kibernetike në nivel shtetëror.

### *Kapitulli 3: Synimet dhe Objektivat*

#### **Synimi**

Synimi i këtij koncept dokumenti është për të analizuar, caktuar dhe për të forcuar rregullat për parandalimin dhe luftimin e krimit kibernetikë në Republikën e Kosovës kundër çdo kërcënimi apo sulmi që mund të ndodh

Objektivat. Objektivi kryesor është përafrimi i legjislacionit vendor me legjislacionin e BE-se ne fushën e parandalimit dhe luftimin e krimit kibernetikë. Aktivitetet në realizimin e këtij objektivi janë:

- Paraqitja e koncepteve të reja të kërcënimeve të sulmeve kibernetike që janë identifikuar pas miratimit të ligjit në vitin 2010.
- Ngritja e dënimeve në raste të nxitjes, ndihmës, mbështetjes dhe përpjekjeve për kryerje të këtyre veprave kriminale.
- Planifikimi për ngritjen e një qendre të thirrjeve 24/7 që mundëson përgjigje në raste të sulmeve kibernetike.
- Harmonizim më legjislacion evropian në fushën e sigurisë kibernetike.

## ***Kapitulli 4: Opsionet***

### *Opsioni 1: Status Quo*

Zbatimi i Ligjit aktual për parandalimin dhe luftimin e krimit kibernetikë. Zbatimi i kornizës ligjore e cila është e bazuar në Konventën e Budapestit, e nënshkruar më 23 Nëntor 2001 është i papërshtatshëm për shkak se teknologjia informacionit ka evoluar shumë brenda këtyre 7 viteve dhe shumica e veprave të reja penale nuk kanë qenë të parapara në atë kohë kur është hartuar.

*Opsioni 2: Plotësim ndryshimi i ligjit për parandalimin dhe luftimin e krimit kibernetikë apo draftimi i ligjit për siguri kibernetike. Në vijim po paraqesim nevojat për ndryshime nga ligje aktuale.*

#### **- Keqpërdorimi i kartelave bankare dhe të kreditit**

E rregulluar me Kodin Penal (neni 293 dhe 307) dhe LPLKK (neni 13). Ka zbrazëtira në rregullimin adekuat të veprës penale.

Propozim: Reformulim i nenit 13 - Prodhimi, posedimi dhe mbajtja e paautorizuar e kartelave të kreditit. Përmes këtij neni të rregullohet posedimi pa autorizim në mënyrë elektronike apo fizike i të dhënave të kartelave bankare dhe të kreditit.

Sanksioni të përcaktohet varësisht nga sasia dhe mënyra se si janë marrë në posedim të dhënat.

#### **- Hyrja në sistemet kompjuterike**

E rregulluar me Kodin Penal (neni 339) dhe LPLKK (neni 10, 11, 12, 13, 14). Ka zbrazëtira në rregullimin adekuat të veprës penale, respektivisht e rregulluar me shumë nene.

Propozim: kjo formë e veprës penale mund të rregullohet me dy apo tri nene me nga disa paragrafë.

- **Vjedhja e të dhënave personale**

Nuk është e rregulluar as me Kod Penal e as me LPLKK. Vlerësojmë se duhet të përfshihet si vepër penale.

*Vjedhja e identitetit është përdorimi i qëllimshëm i identitetit të dikujt tjetër, zakonisht si një metodë për të fituar një avantazh financiar ose të marrë kredi dhe përfitime të tjera në emër të personit tjetër, dhe ndoshta në dëm ose humbje e personit tjetër. Personi identiteti i të cilit ka qenë i supozuar mund të vuaj pasoja të dëmshme, nëse ata janë përgjegjës për veprimet e kryerësit. Vjedhja e identitetit ndodh kur dikush përdor të dhënat personale të personit tjetër, si emrin, numrin personal të identifikimit, ose numrin e kartës së kreditit, pa lejen e tyre, për të kryer mashtrim apo krime të tjera.*

Ky është një definicion i cili mund të haset më së shpeshti dhe nëse i referohemi praktikës sonë mund të themi se i përshtatet rasteve të cilat i trajtojmë.

Propozim: si formë e veprës penale të rregullohet me nen të ri.

- **Urrejtja dhe diskriminimi në internet**

Nuk është e rregulluar as me Kod Penal e as me LPLKK. Në fakt, në mënyrë të përgjithësuar nxitja e urrejtjes është e rregulluar me nenin 147 (Kodi Penal) por nuk është e rregulluar “përmes internetit”. Vlerësojmë se duhet të përfshihet si vepër penale.

Propozim: rregullimi i këtij neni të bëhet sipas Protokollit Shtesë të Konventës së Krimeve Kibernetike, ky protokoll në mënyrë specifike e trajton këtë çështje, ose të plotësohet neni 147 i kodit penal.

- **Neni 3 paragrafi 3.10.** - përkufizimi I “ **Materialet pornografike me të mitur** - çdo material që paraqet një të mitur apo një person të rritur i paraqitur si i mitur me një sjellje eksplicite seksuale apo imazhe të cilat, edhe pse nuk paraqesin person real, simulon, në mënyrë të besueshme një të mitur me sjellje eksplicite seksuale”.

**Propozimi:** Largimi i paragrafit 1.10 tek LPLKK.

- **Neni 3 paragrafi 1.11.** - Ligji jep përkufizimin “**Interceptimi** “ - marrjen, nxënien pa të drejtë të të dhënave nga persona të paautorizuar.



**Propozimi:**

Interceptimi nuk është e njohur si shprehje ne Kodin Penal te Kosovës.  
Interceptimi nuk është fjale shqipe.

Paragrafi 1.11 i nenit 3 të largohet

Paragraf i ri: Kodi/programi keqbërës - term që përdoret për të përshkruar ndonjë kodë në sistemin kompjuterik që ka për qëllim të shkaktoj efekte të padëshiruara, shkelje të sigurisë ose dëmtim të një sistemi.

o *Neni 5 - Parandalimi, siguria dhe fushatat informative*

1. Në mënyrë që të sigurohen sistemet kompjuterike dhe mbrojtja e të dhënave personale, autoritetet dhe institucionet publike me kompetenca në këtë fushë, ofruesit e shërbimeve, organizatat joqeveritare dhe përfaqësuesit e shoqërisë civile kryejnë aktivitete dhe programe për parandalimin e krimit kibernetikë.

2. Autoritetet dhe institucionet publike me kompetencë në këtë fushë në bashkëpunim me ofruesit e shërbimeve dhe organizatat joqeveritare si dhe përfaqësuesit e tjerë të shoqërisë civile zhvillojnë politikat, praktikat, masat, procedurat dhe standardet minimale për sigurinë e sistemeve kompjuterike.

3. Autoritetet dhe institucionet publike me kompetenca në këtë fushë në bashkëpunim me ofruesit e shërbimeve, organizatat joqeveritare dhe përfaqësuesit e tjerë të shoqërisë civile organizojnë fushata informative mbi krimin kibernetikë dhe rreziqet për shfrytëzuesit e sistemeve të kompjuterit.

**Propozim:** Të diskutohet ndryshimi apo largimi i këtij neni.

o *Neni 6 - Mbajtja, plotësimi dhe shfrytëzimi i bazës së të dhënave*

1. Ministria e Drejtësisë në bashkëpunim me Ministrinë e Punëve të Brendshme mbajnë dhe plotësojnë në mënyrë të vazhdueshme bazën e të dhënave mbi krimin kibernetikë.

2. Ministria e Transportit dhe Postë-Telekomunikacionit, Shërbimi i Inteligjencës së Kosovës dhe institucionet tjera relevante mundë të jenë

shfrytëzues të bazës së të dhënave në përputhje me rregullat dhe procedurat e mbajtësit të bazës së të dhënave.

3. Instituti Kombëtar i Kriminalistikës kryen studime periodike në mënyrë që të identifikoj shkaktarët dhe kushtet që përcaktojnë dhe favorizojnë krimin kibernetikë

**Propozim:**

Ndryshimi i paragrafit 1, "Policia e Kosovës mbanë të dhënat për krimet kibernetike të cilat mund të shfrytëzohen nga institucionet e tjera relevante."

Paragrafi 2 dhe 3 të largohen nga ky nen.

o *Neni 7 - Trajnimet dhe programet speciale*

Ministria e Drejtësisë, Ministria e Punëve të Brendshme, Ministria e Transportit dhe Postë-Telekomunikacionit, Ministria e Shërbimeve Publike dhe Shërbimi i Inteligjencës së Kosovës zhvillojnë programe speciale trajnuese për personelin me qëllim të parandalimit dhe luftimit të krimit kibernetikë në përputhje me kompetencat që ushtrojnë.

**Arsyetim**

*Nuk ekzistojnë këto programe speciale, Ministria e Shërbimeve Publike nuk ekziston.*

**Propozim:**

Neni 7 të largohet dhe në fund të këtij ligji të propozohet që më akte nënligjore institucionet relevante të zhvillojnë programe speciale trajnuese për personelin me qëllim të parandalimit dhe luftimit të krimit kibernetikë në përputhje me kompetencat që ushtrojnë.

o *Neni 8 - Obligimet e pronarëve dhe administratorëve*

1. Për një kategori sistemesh kompjuterike, në të cilat qasja është e kufizuar ose plotësisht e ndaluar, pronarët, administratorët e këtij sistemi, detyrohen ta rregullojnë që në mënyrë të qartë dhe automatike të paralajmërohet përdoruesi: me informacion, si dhe në çfarë kushtesh mund ta përdorë, ose se është i ndaluar përdorimi i këtij sistemi kompjuterik dhe për pasojat ligjore për qasje të paautorizuar.

2. Mosrespektimi i detyrimit të përcaktuar në paragrafin 1 të këtij neni, është kundërvajtje dhe kryesi i saj dënohet prej pesëqind (500) deri pesëmijë (5000) Euro.

**Propozim:**

Ndryshimi i paragrafit 1 të nenit 8, "Për të gjitha sistemet kompjuterike, në të cilat qasja është e kufizuar ose plotësisht e ndaluar, pronarët, administratorët e këtij sistemi, detyrohen ta rregullojnë që në mënyrë të qartë dhe automatike të paralajmërohet përdoruesi: me informacion, si dhe në çfarë kushtesh mund ta përdorë, ose se është i ndaluar përdorimi i këtij sistemi kompjuterik dhe për pasojat ligjore për qasje të paautorizuar."

*Neni 9 – Veprat penale kundër konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave të sistemeve kompjuterike*

1. Qasja në mënyrë të paligjshme në sistemet kompjuterike është vepër penale dhe kryesi i saj dënohet me burgim prej gjashtë (6) muaj deri tre (3) vite.

2. Kur vepra penale nga paragrafi 1 i këtij neni kryhet me qëllim të marrjes së të dhënave kompjuterike kryesi i saj dënohet me burgim prej gjashtë (6) muaj deri në katër (4) vite.

3. Kur vepra penale nga paragrafët 1 dhe 2 të këtij neni kryhet duke i shkelur masat e sigurisë së sistemeve kompjuterike, kryesi i saj dënohet me burgim prej tri (3) vite deri në pesë (5) vite.

**Propozim:**

Të largohet neni 9 i cili zëvendësohet me paragrafë tek neni 10.

○ *Neni 10 - Interceptimi pa autorizim*

1. Interceptimi pa autorizim i transmetimeve jopublike të të dhënave kompjuterike, nga, për, në, ose brenda një sistemi kompjuterik, është vepër penale dhe kryesi i saj dënohet me burgim prej gjashtë (6) muaj deri tre (3) vjet. Nëse kryhet nga pjesëtari i organizatës kriminale, kryesi i saj dënohet me burgim prej një (1) deri pesë (5) vite.

2. Interceptimi pa autorizim i emetimeve elektromagnetike nga sistemet kompjuterike, që mbajnë të dhëna jopublike kompjuterike, është vepër penale dhe kryesi i saj dënohet me burgim prej një (1) deri pesë (5) vite.

**Propozim:**

Zëvendësimi i nenit 10 më nene të reja (referohemi kodit penal të Shqipërisë neni 192/B, 293/A, 293/B, 293/C).

*Neni i ri - Hyrja e paautorizuar kompjuterike*

Hyrja e paautorizuar apo në tejkalim të autorizimit për të hyrë në një sistem kompjuterik a në një pjesë të tij, nëpërmjet cenimit të masave të sigurimit, dënohet me gjobë ose me burgim deri në tre vjet.

Kur kjo vepër kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga tre deri në dhjetë vjet."

*Neni i ri - Përgjimi i paligjshëm i të dhënave kompjuterike*

Përgjimi i paligjshëm me mjete teknike i transmetimeve jopublike, i të dhënave kompjuterike nga/ose brenda një sistemi kompjuterik, përfshirë emetimet elektromagnetike nga një sistem kompjuterik, që mbart të dhëna të tilla kompjuterike, dënohet me burgim nga tre deri në shtatë vjet.

Kur kjo vepër kryhet nga/ose brenda sistemeve kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga shtatë deri në pesëmbëdhjetë vjet.

*Neni i ri - Ndërhyrja në të dhënat kompjuterike*

Dëmtimi, shtrembërimi, ndryshimi, fshirja apo suprimimi i paautorizuar i të dhënave kompjuterike dënohen me burgim nga gjashtë muaj deri në tre vjet. Kur kjo veprë kryhet në të dhënat kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo të dhënë tjetër kompjuterike, me rëndësi publike, dënohet me burgim nga tre deri në dhjetë vjet.

#### *Neni i ri - Ndërhyrja në sistemet kompjuterike*

Krijimi i pengesave serioze dhe të paautorizuara për të cenuar funksionimin e një sistemi kompjuterik, nëpërmjet futjes, dëmtimit, shtrembërimit, ndryshimit, fshirjes apo suprimimit të të dhënave, dënohet me burgim nga tre deri në shtatë vjet.

Kur kjo veprë kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga pesë deri në pesëmbëdhjetë vjet.

#### *Neni 11 - Transferi i pa autorizuar*

1. Ndryshimi, shlyerja, asgjësimi i të dhënave kompjuterike ose kufizimi i tyre pa autorizim është veprë penale dhe kryesi i saj dënohet me burgim prej një (1) deri tre (3) vite.

2. Transferi i paautorizuar i të dhënave nga sistemet kompjuterike është veprë penale dhe kryesi i saj dënohet me burgim prej tre (3) deri pesë (5) vite.

3. Transferi i paautorizuar i të dhënave nga baza e tyre me sisteme kompjuterike është veprë penale dhe kryesi i saj dënohet me burgim prej tre (3) deri pesë (5) vite.

**Propozim:**

Largimi i paragrafit 1. Ndryshimi i paragrafit 2 , dënimi zbutet prej 6 muaj deri në 3 vjet ose më gjohë.

Paragraf i ri, “Nëse transferimi i paautorizuar i të dhënave nga baza e të dhënave e klasifikuar sipas ligjit për klasifikimin e informacioneve dhe ka shkaktuar pasoja për sigurinë nacionale kryesi dënohet më burgim 3 – 5 vjet”.

o *Neni 12 – Pengimi i funksionimit të sistemeve kompjuterike*

Pengesat serioze për funksionimin e sistemeve kompjuterike, duke futur informata, duke bartur, ndryshuar, shlyer ose duke i shkatërruar të dhënat kompjuterike ose duke e kufizuar qasjen pa autorizim në të dhënat e tilla, është veprë penale dhe kryesi i saj dënohet me burgim prej tre (3) muaj deri tre (3) vjet. Nëse kryhet nga pjesëtari i organizatës kriminale, kryesi i saj dënohet me burgim prej një (1) deri pesë (5) vite.

**Propozim:**

Paragraf i ri: “Kur vepra penale e paraparë në paragrafin 1, të këtij neni kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga tri deri në pesë vjet.”

o *Neni 14 - Veprat penale lidhur me kompjuterë*

1. Futja e informatave, ndryshimi ose shlyerja pa autorizim e të dhënave kompjuterike ose kufizimi pa autorizim i qasjes në të dhëna të tilla, që rezulton në të dhëna jo-autentike, me qëllim të shfrytëzimit të tyre për përvetësim të një të drejte, është veprë penale dhe kryesi i saj dënohet me burgim gjashtë (6) muaj deri tri (3) vite. Nëse kryhet nga pjesëtari i organizatës kriminale, dënohet me burgim prej një (1) deri pesë (5) vite.

2. Për tentativë të kryerjes së veprës penale, sipas këtij neni, kryesi dënohet me burgim prej tre (3) muaj deri një (1) vit.

**Propozim:**

**Neni 14** riformulohet:

*Falsifikimi kompjuterik*

Futja, ndryshimi, fshirja apo heqja e të dhënave kompjuterike, pa të drejtë, për krijimin e të dhënave të rreme, me qëllim paraqitjen dhe përdorimin e tyre si autentike, pavarësisht nëse të dhënat e krijuara janë drejtpërdrejt të lexueshme apo të kuptueshme, dënohen me burgim nga gjashtë muaj deri në gjashtë vjet.

Kur kjo vepër kryhet nga personi, që ka për detyrë ruajtjen dhe administrimin e të dhënave kompjuterike, në bashkëpunim, më shumë se një herë ose ka sjellë pasoja të rënda për interesin publik, dënohet me burgim tre deri në dhjetë vjet."

○ **Neni 15 -**

**Propozim:**

Ndryshimi i titullit nga prona tek pronësisë.

○ **Neni 16** - Pornografia me fëmijë përmes sistemeve kompjuterike në paragrafin 1 thuhet

1. Personi, që kryen vepër penale sipas nën-paragrafëve 1.1 deri 1.5 të këtij paragrafi, dënohet me burgim prej gjashtë (6) muaj deri tri (3) vite. Nëse cilësohet se është kryer në rrethana rënduese, kryesi dënohet prej një (1) deri dhjetë (10) vite.

1.1. prodhimin e pornografisë me fëmijë, me qëllim të shpërndarjes së tij nëpërmjet një sistemi kompjuterik;

1.2. ofrimin apo vënien në dispozicion të pornografisë me fëmijë nëpërmjet një sistemi kompjuterik;

1.3. shpërndarjen apo transmetimin e pornografisë me fëmijë nëpërmjet një sistemi kompjuterik;

1.4. prokurimin e pornografisë me fëmijë nëpërmjet një sistemi kompjuterik për vete apo për të tjerët;

1.5. zotërimin e pornografisë me fëmijë nëpërmjet një sistemi kompjuterik apo në medime memoruese të të dhënave kompjuterike.

2. Kryesi i tentativës së veprës penale, nga paragrafi 1 i këtij neni, dënohet me burgim prej gjashtë (6) muaj deri tri (3) vite.

**Propozim:**

Duhet harmonizim më kodin penal. Duhet të rriten dënimet prej 3 deri në 5 për personin që kryen veprën penale dhe nëse ekzistojnë rrethana rënduese, prej 5 deri në 10 vite.

*Neni 17, 18 dhe 19* – Të ri-shikohen dhe formulohen duke u bazuar edhe në ligjet e tjera në fuqi.

- *Neni 20* Bashkëpunimi ndërkombëtarë dhe *Neni 21* Hetimet, parashohin mundësinë e bashkëpunimit ndërkombëtar.

**Propozim:**

Këto nene duhet të harmonizohen me ligjin për bashkëpunim ndërkombëtarë në çështjet penale. I cili ligj në hollësi përmban dispozita të bashkëpunimit ndërkombëtar, përfshirë edhe hetimin. Meqë procedura e bashkëpunimit ndërkombëtar është e rregulluar me Ligjin për bashkëpunim ndërkombëtar në çështjet penale nuk ka nevojë fare të kemi dispozita në ligjin për parandalim dhe luftim të krimit kibernetikë.

- ***Neni 22 - Pika e kontaktit***

1. Në mënyrë që të sigurohet një bashkëpunim i përhershëm ndërkombëtar në fushën e krimit kibernetikë, Qeveria e vë në dispozicion një pikë të përhershme kontakti.

2. Kjo pikë e përhershme kontakti ka kompetencat si vijon:

2.1. ofron ndihmë të specializuar dhe informata mbi legjislacionin në fushën e krimit kibernetikë si dhe informon pikat e kontaktit të shteteve tjera;

2.2. urdhëron ruajtjen e shpejtë të të dhënave si dhe konfiskimin e pajisjeve që përmbajnë të dhëna kompjuterike ose të dhëna që kanë të bëjnë me të dhënat mbi trafikun e të dhënave të kërkues nga autoriteti kompetent i huaj;



2.3. ekzekuton ose ndihmon ekzekutimin, sipas dispozitave ligjore, në rastet e luftimit të krimit kibernetikë, duke bashkëpunuar me të gjitha autoritetet kompetente kosovare.

3. Qeveria në afat prej gjashtë (6) muajve nga hyrja në fuqi e këtij ligji me një akt nënligjor përcakton krijimin e pikës së kontaktit të paraparë në paragrafin 1 të këtij neni.

**Propozim:**

Kjo pikë kontakti nuk është funksionale, është shumë e nevojshme që të rregullohet me dokument krijimi i kësaj pike të kontaktit përfshirë detyrat dhe përgjegjësitë, të caktohet autoriteti përgjegjës që do të menaxhoj me të.

Bazuar në përvojën e deritanishme dhe praktikave të vendeve tjera, një pikë kontakti për parandalimin dhe luftimin e krimit kibernetikë është e domosdoshme, në raste të krimeve kibernetike duhet të vepruhet shpejt pasi që të dhënat që gjenerohen nga trafiku i internetit janë të paqëndrueshme. Kjo pikë kontakti gjithashtu ndikon drejtpërdrejt edhe në ndërtimin e besimit me vendet partnere.

Pika e kontaktit duhet të caktohet brenda Policisë së Kosovës. Policia e Kosovës më akte nënligjore duhet të rregulloj funksionimin e kësaj pike dhe kohën e nevojshme për reagim.

**Propozim vendosja e nenit të ri:**

***Neni i ri*** – Programet kompjuterike keqbërëse

1. Kushdo që shkruan/ofron, vë në dispozicion, shpërndan ose transmeton kodin keqbërës nëpërmjet sistemit elektronik ose pajisjeve elektronike më qëllim që të shkaktoj dëm ose përfitim material, në ndonjë sistem elektronik ose që rezulton më komprometim, shkatërrim, ndryshim, vjedhje ose humbje të të dhënave kryen veprë penale sanksionohet më burgim prej 1 deri në 3 vite.
2. Kur vepra penale e paraparë në paragrafin 1, të këtij neni kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik,

të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga tri deri në pesë vjet.

**Neni i ri** - Ekipi Kombëtar për Reagim ndaj Emergjencave Kompjuterike (KOSCERT)

1. Kryen funksionet e qendrës kompjuterike për reagime emergjente me qëllim të ballafaqimit me rreziqet për sistemet publike/jopublike të komunikimeve elektronike.

2. KOSCERT paraqet autoritet kombëtar të sigurisë në internet që mundëson sigurinë e informacionit elektronik nëpërmjet parandalimit, zbulimit dhe reagimit për qeverinë, biznesin dhe shoqërinë. KOSCERT do të mundësoj bashkëpunimin më CERT-at ndërkombëtar në fushën e parandalimit dhe përgjigjes ndaj incidenteve kompjuterike.

## Kapitulli 5: Përmbledhje e Opsioneve

Karakteristikat kryesore	Opsioni 1	Opsioni 2
Karakteristikat kryesore të opsionit.	<b>Zbatimi i kornizës ligjore aktuale të paefektshme që merret në mënyrë të pamjaftueshme me parandalimin dhe luftimin e krimit kibernetikë</b>	Draftimi i ligjit për siguri kibernetike
Segment i popullsisë / sektori / rajoni i synuar.	Republika e Kosovës	Republika e Kosovës
Karakteristikat e zbatimit – kush është përgjegjës – portofol i qeverisë (kush), sektori privat, qytetarët.	ARKEP, Ministria e Zhvillimit Ekonomik	MPB/ Departamenti për Administrim të Sistemeve dhe Komunikimeve dhe ministritë tjera relevante

Administrimi ose zbatimi i programit ose shërbimit	ARKEP, Ministria e Zhvillimit Ekonomik	Departamenti për Administrim të Sistemeve dhe Komunikimeve
Ligjet, aktet nënligjore, ndryshimet në ligjet ekzistuese, zbatimi dhe dënimet.	Baza ligjore mbetet e njëjtë	Të hartohet ligji për siguri kibernetikë
Stimujt ose stimujt jo ekonomik – subvencione apo taksa.	Jo	Jo
Fushata të edukimit dhe komunikimit.	Jo	jo
Udhëzimet dhe kodet.	Nuk ka	
Afatet kohore – kur opsioni bëhet efektiv.	Në fuqi.	Pas shpalljes së ligjit.

## Kapitulli 6: Analiza e Opsioneve

### *Përfitimet*

#### Opsioni 1: *Status quo*

Nuk ka përfitime me zbatimin e këtij opsioni.

#### Opsioni 2: *Hartimi i Ligjit për siguri kibernetike*

- Paraqitja e koncepteve të reja të kërcënimeve të sulmeve kibernetike që janë identifikuar pas miratimit të ligjit në vitin 2010.
- Ngritja e dënimeve në raste të nxitjes, ndihmës, mbështetjes dhe përpjekjeve për kryerje të këtyre veprave kriminale.

- Planifikimi për ngritjen e një qendre të thirrjeve 24/7 që mundëson përgjigje në raste të sulmeve kibernetike.

*Pasojat negative*

Opsioni 1: *Status quo*

- Parandalimi dhe luftimi i krimit kibernetikë nuk harmonizohet me Direktivën 2013/40/BE të Parlamentit Evropian Dhe e Këshillit e datës 12 Gusht 2013
- Mekanizëm joefektiv dhe i pasigurt për parandalimin dhe luftimin e krimit kibernetikë;
- Nuk ka përgjegjësi të qarta të përcaktuara dhe caktuara.

Opsioni 2: *Hartimi i Ligjit për Plotësim ndryshimin e ligjit për parandalimin dhe luftimin e krimit kibernetikë*

Nuk ka pasoja negative me zbatimin e këtij opsioni.

*Efektet e shpërndarjes*

Siç është shpjeguar më herët, sulmet në shkallë të gjerë kundër sistemeve të informacionit, rritjen e përdorimit kriminal të te ashtuquajturve “botnets”, që paraqesin rrjetet e kompjuterëve të infektuar që mund të kontrollohen nga distanca në shkallë shumë të gjerë, dhe të shërbejnë për sulme të koordinuara. Asnjëra nga këto kërcënime të sipër përmendura nuk janë të përfshira në Ligjin nr. 03/L-166 në Kosovë.

*Kostot*

Përmbledhje e Vlerësimit të Ndikimit Financiar				
	Viti aktual - (do	Viti 2	Viti 3	Viti 4

	të thotë viti kur është bërë regjistrimi, varësisht nga viti i shpalljes së ligjit ).			
<b>Opsioni 1</b>				
Diferenca neto në alokimin e shpenzimeve.	n/a	n/a	n/a	n/a
Diferenca neto në gjenerimin e të hyrave.	n/a	n/a	n/a	n/a
Financimi i pritur nga donatorët.	n/a	n/a	n/a	n/a
<b>Opsioni 2</b>				
Ngritja e kapaciteteve në fushën e sigurisë kibernetike	500,000	500,000	500,000	

## Kapitulli 7: Konsultimi

Puna është konsultuar në mënyrë aktive me OSBE, Komisionin Evropian, këshilltarët e ICITAP-it, si dhe disa ekspertë ndërkombëtar. Drafti është hartuar bashkërisht me partnerët ndërkombëtarë.

Përveç kësaj, përfaqësuesit e Departamentit për Administrim të Sistemeve dhe Komunikimeve, Policisë së Kosovës (Departamenti i Teknologjisë Informative dhe Komunikimit, Sektori i Krimeve Kibernetike), Agjencisë së Kosovës për Forenzikë (Departamenti për Teknologji Informative - Forenzike), CERT nacional, Agjencia e Shoqërisë Informative dhe përfaqësues tjerë nga sektorët relevant të Ministrisë së Punëve të Brendshme kanë qenë anëtarë të grupit punues dhe inputet e tyre janë të përfshira në këtë koncept.

Për më tepër, procesi konsultimeve paraprake dhe me pub likun të do të bëhet në bazë të Rregullores nr. 09/2011 e Punës së Qeverisë, që do të thotë se para se të

vazhdon koncepti dokumenti në Qeverinë e Republikës së Kosovës për miratim të gjitha institucionet relevante dhe grupet e tjera të interesit do të konsultohen.

## **Kapitulli 8: Krahasimi i opsioneve**

### *Opsioni 1: Status quo*

Opsioni 1 për momentin nuk është i zbatuar plotësisht pasi që disa vepra penale të kryera përmes sistemeve kompjuterike nuk janë të përfshira në Ligjin aktual. Aktualisht ligji në fuqi nuk përputhet me politikat e BE-së në këtë fushë

*Opsioni 2: Hartimi i Ligjit për Plotësim ndryshimin e ligjit për parandalimin dhe luftimin e krimit kibernetikë.*

Opsioni 2 do të krijojë një mjedis të sigurt dhe do të zvogëlojë kërcënimin ndaj fushës kibernetike, duke parandaluar, sanksionuar dhe ndëshkuar veprat e ndryshme penale që kryhen në këtë fushë.

## **Kapitulli 9: Rekomandimi**

Grupi i punës i rekomandon Qeverisë së Republikës së Kosovës që të miratojë Opsionin 2 dhe të hartojë një ligj të veçantë për Plotësim ndryshimin e ligjit për parandalimin dhe luftimin e krimit kibernetikë. Përveç kësaj, grupi i punës rekomandon gjithashtu:

- Paraqitjen e koncepteve të reja të kërcënimeve të sulmeve kibernetike që janë identifikuar pas miratimit të ligjit në vitin 2010.
- Ngritja e dënimeve në raste të nxitjes, ndihmës, mbështetjes dhe përpjekjeve për kryerje të këtyre veprave kriminale.
- Planifikimi për ngritjen e një qendre të thirrjeve 24/7 që mundëson përgjigje në raste të sulmeve kibernetike.

- Përcaktimin e përgjegjësive për ekipin reagues ndaj emergjencave kompjuterike (KOSCERT) për parandalim, zbulim dhe reagim ndaj incidenteve kibernetike, në harmoni më praktikatat e vendeve evropiane.

### **Kapitulli 10: Komunikimi**

Pas miratimit të këtij Koncept Dokumenti, Ministria e Punëve të Brendshme do të bëjë një komunikim publik dhe do të njoftojë për miratimin e koncept dokumentit dhe procedurave të tjera që do të pasojnë.